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

Wilson Goudalo

# Vers une ingénierie avancée de la Sécurité des Systèmes d'Information d'entreprise : une approche conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques

## THÈSE DE DOCTORAT

Pour obtention du grade de Docteur

**UNIVERSITÉ DE VALENCIENNES ET DU HAINAUT-CAMBRESIS**

Mention : **Informatique**

Spécialité : **Informatique, Génie Informatique**

**Présentée et soutenue par**

**Wilson GOUDALO**

**Le 18/07/2017, à Valenciennes**

**École doctorale :**

Sciences Pour l'Ingénieur (SPI)

**Equipe de recherche, Laboratoire :**

Département Automatique et Département Informatique, Laboratoire d'Automatique, de Mécanique et d'Informatique, industrielles et Humaines (**LAMIH**)

# JURY

## Président du jury

- Ahmed Seffah, Professeur, Lappeenranta University of Technology, Lappeenranta, Finlande

## Rapporteurs

- Camille Sabroux-Rosenthal, Professeur, Université de Paris Dauphine, Paris, France
- Nada Mata, Professeur, Université de Technologie de Troyes, Troyes, France

## Examinateur

- Jean-René Ruault, Docteur, UVHC, Valenciennes, France

## Directeurs de thèse

- Kolski, Christophe, Professeur, UVHC, Valenciennes, France.
- Vanderhaegen, Frédéric, Professeur, UVHC, Valenciennes.

***"We must develop a comprehensive and globally shared view of how technology is affecting our lives and reshaping our economic, social, cultural, and human environments. There has never been a time of greater promise, or greater peril."***

***Klaus Schwab, Founder and Executive Chairman, World Economic Forum***
***[Schwab, 2016]***

***En français : « Nous devons développer une lecture claire et globalement partagée de la façon dont la technologie affecte nos vies et comment elle reconditionne notre environnement économique, social, culturel et humain. Il n'y a jamais eu une période de plus grandes promesses ou de plus grandes menaces. »***

***Monsieur Klaus Schwab est Ingénieur et Economiste, Fondateur et PDG du célèbre forum économique mondial (World Economic Forum) qui se tient annuellement à Davos en Suisse.***

***Le dépassement de la nature humaine grâce à la technologie n'est pas un mythe. Nous nous devons d'être vigilants et d'y apporter une solution efficace. La méthodologie ICSUR pour les systèmes sociotechniques en est notre humble contribution.***

# Remerciements

*Cette thèse n'aurait pu aboutir sans l'aide et le soutien de nombreuses personnes*

*Je tiens d'abord à exprimer ma reconnaissance à mes directeurs :*

*Les Professeurs Christophe Kolski et Frédéric Vanderhaegen pour leur aide, leurs judicieux conseils et leurs remarques pertinentes. Cette thèse est menée à terme grâce à leur dévouement, l'intérêt constant porté à mes travaux de recherche et les motivations qu'ils savent bien me transmettre.*

*Les Professeurs Alexander Rudolfovich Liss et Vladimir Ivanovich Vorobyev, Le Docteur Sergey Vladimirovich Afanasyev, Les Professeurs Charles-François Ducateau, Dominique Seret, Ahmed Seffah et Le Docteur Jean-René Ruault ont su m'inspirer et m'aider aux moments opportuns, je les remercie sincèrement.*

*Je tiens vivement à remercier les membres de jury :*

*Les Professeurs Camille Sabroux-Rosenthal et Nada Mata pour m'avoir fait l'honneur d'accepter d'être les rapporteurs de ce mémoire.*

*Le Professeur Ahmed Seffah et Le Docteur Jean-René Ruault pour m'avoir fait l'honneur d'accepter d'être les examinateurs de ce mémoire.*

*Merci pour votre disponibilité, pour la lecture de ce mémoire et aussi d'avoir accepté de juger cette thèse.*

*Ce travail a pu voir le jour grâce au soutien du LAMIH, où j'ai pleinement bénéficié d'un environnement humain stimulant.*

*Je ne peux terminer ces lignes sans remercier profondément ma famille, Willae et William, mes frères et sœurs, mes amis et mes collègues pour leur soutien et leur patience.*

*Merci à tous !*

*A*

*GOUDALO JOspy*

# Table des matières

i

**Table des matières** ..... i

**Liste des figures et tableaux** ..... i

**Introduction générale** ..... 1

**Chapitre 1 : Problématique de la sécurité dans les entreprises et organisations** ..... 7

**1.1. Introduction** ..... 7

**1.2. Le contexte actuel de la sécurité** ..... 7

**1.3. Les attaques et menaces de sécurité** ..... 10

**1.4. Synthèse et conclusion du chapitre** ..... 12

**Chapitre 2 : Etat de l'art – Inspiration et encrage** ..... 15

**2.1. Introduction** ..... 15

**2.2. Les percés dans l'ingénierie logicielle et l'ingénierie des systèmes d'information** 15

2.2.1 La percée de l'ingénierie logicielle ..... 16

2.2.1.1 Introduction ..... 16

2.2.1.2 Paradigmes cartésien et systémique pour l'analyse et la conception ..... 17

2.2.1.3 Les approches de base en ingénierie logicielle ..... 19

2.2.1.4 Modélisation et méta-modélisation ..... 23

2.2.1.5 Processus de développement logiciel ..... 26

2.2.2 Méthodes agiles dans l'ingénierie logicielle et systèmes d'information ..... 30

2.2.3 Ingénierie d'élaboration de méthodes ..... 34

**2.3. Cadres de la sécurité des systèmes d'information** ..... 36

2.3.1 Cadres internationaux de la sécurité des systèmes d'information ..... 36

2.3.2 EBIOS le cadre de référence en France ..... 37

2.3.2.1 Présentation du cadre EBIOS ..... 37

2.3.2.2 La démarche inhérente au cadre EBIOS ..... 38

2.3.3 Synthèse sur les principaux cadres existants et leurs manquements ..... 40

**Chapitre 3 : Fondations préalables à notre méthodologie d'ingénierie avancée** ..... 45

**3.1. Fondements et Métriques de la sécurité des systèmes d'information** ..... 45

3.1.1 Les principes fondamentaux de la sécurité – les trois critères invariants de la sécurité ..... 45
3.1.2 Le critère de confidentialité ..... 47
3.1.2.1 Définition et concept général ..... 47
3.1.2.2 Le Modèle de confidentialité dit à matrice d'accès (modèle HRU) ..... 49
3.1.2.3 Le modèle de Bell et La Padula ..... 50
3.1.2.4 Le modèle de contrôle de flux d'information ..... 52
3.1.3 Métriques et Indicateurs de suivi de la sécurité ..... 53
**3.2. Fondements et Métriques de la Résilience des systèmes d'information ..... 57**
3.2.1 Fondements et concepts de la résilience ..... 57
3.2.2 Fonctions de résilience ..... 58
3.2.3 Métriques de la résilience ..... 59
**3.3. Fondements et Métriques de l'Utilisabilité dans les systèmes d'information ..... 60**
3.3.1 Fondements de l'Utilisabilité ..... 60
3.3.2 Des catégories de l'utilisabilité ..... 61
3.3.3 Métriques de l'utilisabilité ..... 62
**3.4. Analyse critique sous l'angle d'approches conjointes ..... 63**
**3.5. Systèmes sociotechniques ..... 65**
**3.6. Synthèse et conclusion du chapitre ..... 65**
**Chapitre 4 : Contribution à une méthodologie d'Ingénierie Conjointe de la Sécurité, de l'Utilisabilité et de la Résilience (ICSUR) ..... 69**
**4.1. Introduction ..... 69**
**4.2. Le positionnement du SST (Système Sociotechnique) dans la nouvelle industrie des services numériques, sous le regard de la sécurité et de l'expérience utilisateur ..... 71**
4.2.1 Concepts de systèmes et approches sociotechniques ..... 71
4.2.2 Représentation de système sociotechnique et ses composantes ..... 72
4.2.3 L'expérience utilisateur dans les systèmes sociotechniques appréhendée sous l'angle de la sécurité ..... 74
**4.3. Analyse conjointe et modèle conceptuel avancé du SST ..... 76**
4.3.1 Eléments d'Analyse conjointe de la sécurité, de la résilience et de l'utilisabilité ..... 76
4.3.2 Modèle conceptuel résultant de l'analyse conjointe ..... 84
4.3.3 Concepts et Sémantiques ..... 85
4.3.3.1 Assets – les actifs ..... 85
4.3.3.2 Incident risks – risques d'incident ..... 87

4.3.3.3 Solutions ..... 87
4.3.4 Système de métriques homogènes ..... 88
**4.4. La méthodologie ICSUR pour les SST ..... 89**
4.4.1 Synoptique de la méthodologie d'ingénierie avancée ..... 90
4.4.2 Etape #1 – Identifier le périmètre du système sociotechnique concerné ..... 91
4.4.3 Etape #2 – Effectuer l'analyse de risques cross-domaines du système sociotechnique ..... 92
4.4.4 Etape #3 – Définir les solutions adéquates ..... 93
**4.5. Synthèse et conclusion du chapitre ..... 95**
**Chapitre 5 : Etude de cas d'illustration de la méthodologie ICSUR ..... 97**
**5.1. Introduction ..... 97**
**5.2. Etape #1 – Identifier le périmètre du système sociotechnique concerné ..... 98**
5.2.1 Les processus d'entreprise ..... 98
5.2.2 Les actifs et leur cotation ..... 100
**5.3. Etape #2 – Effectuer l'analyse de risques cross-domaines du système sociotechnique ..... 102**
**5.4. Etape #3 - Définir les solutions adéquates ..... 106**
**5.5. Synthèse et conclusion du chapitre ..... 113**
**Chapitre 6 : Discussions et Eléments d'appréciation ..... 115**
**6.1. Discussions sur la proposition ..... 115**
**6.2. Eléments d'appréciation de la proposition ..... 115**
**6.3. Relations des acteurs pour l'ingénierie avancée de la sécurité ..... 117**
6.3.1 Les principaux acteurs ..... 117
6.3.2 Les rôles ..... 118
6.3.3 Les interactions entre les acteurs ..... 119
**Conclusion générale ..... 121**
**Bibliographie ..... 123**

# Liste des figures et tableaux

Figure 2.1 : Facteurs de complexité des SI [Giraudin, 2007] ..... 17
Figure 2.2 : Démarche SADT / Paradigme cartésien [Lissandre, 1990] ..... 18
Figure 2.3 : Paradigme systémique / Théorie des systèmes de Boulding [Boulding, 1956] ..... 19
Figure 2.4 : Schéma illustrant le SPEM [OMG, 2008] ..... 26
Figure 2.5 : Processus d'ingénierie des systèmes en flocons [Hassine, 2005] ..... 30
Figure 2.6 : Comparaison entre les méthodes classiques et les méthodes agiles [ACCESS-DEV, 2017] ..... 32
Figure 2.7 : Schéma d'illustration de la méthode Scrum ..... 33
Figure 2.8 : Schéma illustré de la démarche du cadre EBIOS inspiré de [EBIOS, 2016] ..... 40
Figure 2.9 : Vision classique de la sécurité des systèmes d'information ..... 41
Figure 3.1 : Cotation des actifs de l'entreprise – critères de sécurité ..... 46
Figure 3.2 : Méta-modèle de la qualité de sécurité (inspiré de [Goudalo & Seret, 2009]) ..... 54
Figure 3.3 : Cycle d'ingénierie des méthodes [Rolland, 2005] ..... 66
Figure 4.1 : Représentation de système sociotechnique [Goudalo & Kolski, 2016] ..... 73
Figure 4.2 : Modèle conceptuel de l'ingénierie conjointe, inspiré de [Goudalo et al., 2017b] ..... 84
Figure 4.3 : Légende accompagnant le modèle conceptuel de l'ingénierie conjointe ..... 85
Figure 4.4 : Modèle conceptuel des actifs ..... 86
Figure 4.5 : Méthodologie d'ingénierie conjointe de la sécurité de l'utilisabilité et de la résilience, inspiré de [Goudalo et al., 2017c] ..... 90
Figure 5.1 : Modélisation des processus métier (avec mise en évidence des tâches ayant des problèmes potentiels) ..... 100

Tableau 4.1 : Impacts de sécurité et solutions correspondantes ..... 78
Tableau 4.2 : Impacts d'utilisabilité et solutions correspondantes ..... 80
Tableau 4.3 : Techniques et moyens de garantie de la résilience ..... 82
Tableau 5.1 : Trois processus métier (*business processes*) de FI MEDLAB ..... 99
Tableau 5.2 : Trois actifs sélectionnés et leurs métriques ..... 102
Tableau 5.3 : Trois activités détaillées ..... 103
Tableau 5.4 : Risques d'incident et leurs métriques ..... 106
Tableau 5.5 : Solution de design pattern pour le problème T1 ..... 107
Tableau 5.6 : Solution de design pattern pour le problème T2.1 ..... 108
Tableau 5.7 : Solution de design pattern pour le problème T2.2 ..... 108
Tableau 5.8 : Solution de design pattern pour le problème T2.3 ..... 109
Tableau 5.9 : Solution de design pattern pour le problème T2.4 ..... 109
Tableau 5.10 : Solution de design pattern pour le problème T3 ..... 110
Tableau 5.11 : Caractéristiques des solutions et leurs métriques ..... 112

# Introduction générale

Les systèmes d'information, et plus précisément les services qu'ils fournissent, ont complètement envahi nos vies et y jouent un rôle de plus en plus prépondérant. Ceci est vrai aussi bien pour les particuliers, que pour les organisations et pour les entreprises [Larson, 2008]. Les systèmes d'information sont composés d'applications métier, de composantes applicatives et techniques, d'autres ressources informatiques et non informatiques. A cela, sont ajoutées des infrastructures de sécurité et des lignes directrices en matière de sécurité, selon une politique de sécurité (si elle est en place). La vision globale de la sécurité est souvent parsemée de ruptures et le contrôle harmonisé n'est pas facile à tous les niveaux.

Au même moment, les entreprises et organisations doivent assurer leur bon fonctionnement dans une réalité concurrentielle assez difficile, auxquelles se rajoutent des contraintes règlementaires et légales accrues. Dans ces conditions délicates, la pratique de gestion de risques de sécurité évolue et prend de plus en plus d'ampleur dans les entreprises et organisations. Ceci est vrai notamment avec les exigences règlementaires, comme Sarbanes-Oxley [Sarbanes-Oxley Act, 2002] sur l'intégrité des données et processus relatifs à l'information financière et comptable (pour toutes les entreprises cotées aux Etats Unis). De même, dans l'industrie bancaire (en Europe), les accords Bâle[1] dès le numéro 2 [Chapelle et al., 2004] définissent le ratio de fonds propres en fonction de la maturité des activités de gestion de risques, y compris ceux relatifs aux Systèmes d'Information (risques opérationnels). Il ne serait pas judicieux de croire protéger efficacement l'ensemble du système contre tous les risques et attaques possibles, une approche soutenue de la sécurité des systèmes d'information s'avère nécessaire.

De même, les problèmes de sécurité et de respect de la vie privée ou *privacy* sont essentiels dans de nombreux services [SBIC, 2008], [IBM, 2014], [KPMG, 2014] et [Umhoefer et 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. Dans le domaine des systèmes informatiques, les initiatives ont été principalement

[1] *Exigence de fonds propres au regard de l'exposition aux risques, y compris les risques opérationnels.*

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. Pour améliorer la stratégie de sécurité en profondeur, Goudalo et Seret [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.

Aujourd'hui, nous sommes confrontés à un besoin urgent de nouvelles approches axées sur les aspects humains, y compris l'utilisabilité pour assurer la sécurité des systèmes. En effet les systèmes sont utilisés par les humains, bien que ces systèmes soient de plus en plus automatisés. Ferrary [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 Garfinkel [Cranor & Garfinkel, 2005] indique les tendances de la recherche en matière de sécurité et d'utilisabilité. Le livre de Clarke et Furnell [Clarke & Furnel, 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. Le risque zéro n'existe pas, quels que soient les efforts effectués, des problèmes surviennent. La prise en compte de la résilience[2] dans les travaux de sécurité devient nécessaire à l'ère de l'économie numérique. On constate à ce sujet que les récents travaux sur les systèmes cybernétiques et physiques (CPS – Cyber Physical Systems) intègrent la sécurité et la résilience ; une synthèse de ces travaux est présentée dans [Khaitan et McCalley, 2015]. Compte tenu des enjeux actuels, il en découle un besoin d'initiative conjointe pour traiter la sécurité, l'utilisabilité et la résilience dans les systèmes d'information des entreprises et organisation, à l'ère de l'économie numérique. Cette dernière est caractérisée par une utilisation prépondérante de services numériques dans toutes les activités socio-économiques et dans tous les secteurs, aussi bien de divertissement, d'importance stratégique et d'importance vitale.

[2] *Capacité à prévenir un incident et plus encore à restaurer un état stable après un accident ou une faute intentionnelle [Laprie, 2008]*

Dans ce mémoire de thèse, nous nous sommes inspirés des trois motivations suivantes pour élaborer notre proposition, prenant la forme d'une méthodologie d'ingénierie.

1- Les motivations et les développements de l'ingénierie des logiciels et des systèmes d'information constituent des opportunités d'inspiration, afin d'élaborer des approches d'ingénierie de la sécurité. L'émergence perpétuelle de nouveaux domaines de recherche dans les systèmes d'information étaye l'intérêt des méthodes d'ingénierie. Le CAME (Computer-Aided Method Engineering - Ingénierie de méthodes assistée par ordinateur) est une discipline ancienne qui reste pertinente, tant pour les chercheurs et pour les professionnels. Une analyse des travaux du domaine de CAME est résumée dans [Niknafs et Ramsin, 2008]. La discipline de l'ingénierie des méthodes est concernée par la définition de nouvelles méthodes d'ingénierie des systèmes d'information [Bonjean, 2013]. Il s'agit d'une discipline portant sur la conceptualisation, la conception, la construction, la réingénierie et l'adaptation des méthodes, des techniques et des outils pour le développement des systèmes d'information. L'ingénierie des méthodes situationnelles traite le développement de nouvelles méthodes adaptées à un contexte particulier à partir de méthodes existantes [Rolland, 2005].

2- De nombreuses réalisations de l'ingénierie des systèmes sont appliquées à la sécurité de l'information, avec succès. Ces réalisations concernent les concepts, les paradigmes, les techniques et les outils. L'ingénierie de sécurité doit inclure la compréhension de l'environnement opérationnel des entreprises et des organisations ; elle opère spécifiquement sur les objectifs de sécurité des entreprises et des organisations. L'ingénierie de sécurité traite les vulnérabilités, les menaces et les risques contre les actifs des organisations et des entreprises. Les actifs comprennent non seulement ce que l'organisation possède, mais aussi ce dont elle a droit, et qui présente de la valeur pour elle et pour ses opérations. [Jacobs, 2011] présente un résumé des approches d'ingénierie de la sécurité. Le développement des politiques de sécurité et le management de la sécurité utilisent le formalisme des processus de système d'information, et plus précisément les formalismes de processus métier (business processus, processus d'entreprise) [Goudalo et Seret, 2009], [Salloway et Trott, 2002], [Weske, 2012]. De nouvelles normes internationales sont de plus en plus développées dans cette tendance [ISO/IEC 27032, 2012].

3- L'étude de Ponemon Institute [Ponemon Institute LLC, 2016] met en évidence les causes de la violation de données sur l'année 2015. Dans cette étude, les attaques malveillantes ou criminelles sont d'environ 46%, les problèmes de système (défaillances relatives aux technologies de l'information et/ou processus métier) sont autour de 29% et les facteurs

humains (comme les négligences des employés et des contractuels) sont d'environ 25%. Dans des études similaires, les coûts totaux d'événements cybernétiques (cyber sécurité) sont estimés à environ 8,5 milliards de dollars par année [Romanosky, 2016]. Le rapport annuel de Symantec sur les menaces de sécurité sur Internet corrobore les mêmes tendances [Symantec, 2017]. Les ransomwares y sont classées l'une des menaces les plus significatives en matière de cybersécurité en 2016 [Les Echos, 2017]. Quoi que fassent les entreprises et les organisations pour la sécurité de l'information, des incidents se produisent et perturbent la fourniture de services. Une nouvelle ingénierie de la sécurité du système d'information d'entreprise devient cruciale.

Nous proposons une approche des systèmes sociotechniques, par le biais de design patterns basés sur l'expérience utilisateur, en nous situant dans une visée conjointe de la sécurité, de l'utilisabilité et de la résilience. Nous proposons également un système métrique homogène qui opère sur les aspects et les sous-aspects de la sécurité, de l'utilisabilité et de la résilience, de façon conjointe (Figure 4.2, page 84). Les approches sociotechniques peuvent aider à la conception des structures organisationnelles et des processus métier, ainsi qu'à la conception des systèmes techniques. Les approches de système sociotechnique [Singh, 2013] visent à modéliser de manière conjointe, les capacités humaines, sociales et technologiques, dans l'utilisation et le traitement des services à valeur ajoutée. Nous suggérons de présenter les solutions dans le formalisme de patrons de conception qui sont utilisés notamment dans les contextes qui recourent à la capitalisation de l'expérience et à l'apprentissage soutenu [Alexander et al., 1977 ; Gamma et al., 1995 ; Hassine, 2005].

Ce mémoire de thèse est organisé de la façon suivante :

- Dans le premier chapitre, nous présentons la problématique de la sécurité dans les entreprises et organisations ; ce qui met en évidence de façon plus détaillée les insuffisances et les verrous scientifiques et industriels jusqu'à présent. De plus les méthodes d'analyse de risques s'améliorent et s'étoffent au fil des années, mais la sophistication des stratégies d'attaques et le contexte changeant de l'industrie des services numériques continuent de créer des pertes importantes dans tous les secteurs d'activité. Ce premier chapitre présente à la fois la problématique et le contexte actuel, en démontrant la nécessité d'innover.
- Dans le deuxième chapitre, nous rappelons les diverses percées de l'ingénierie logicielle et de l'ingénierie des systèmes d'information dont nous nous inspirons, de même que les

concepts fondamentaux issus des cadres de sécurité qui constituent les points d'ancrage sur lesquels nous nous basons pour élaborer notre proposition. Dans ce chapitre, nous présentons également les points essentiels de l'ingénierie des méthodes et de l'ingénierie des méthodes situationnelles que nous avons suivies, afin d'élaborer une approche innovante qui a pour objectif de contribuer à lever les verrous scientifiques qui deviennent cruciaux pour la science et l'industrie.

- Dans le troisième chapitre, nous rappelons les notions fondamentales sur lesquelles nous nous basons pour élaborer notre proposition. Ce chapitre présente les fondements et métriques de la sécurité, de la résilience et de l'utilisabilité qui sont les trois concepts sur lesquels nous opérons de façon conjointe. A la fin de ce chapitre, nous effectuons la synthèse de l'état de l'art sur les approches conjointes.
- Dans le quatrième chapitre, nous développons notre proposition. Nous présentons d'abord le concept des systèmes sociotechniques comme une méthodologie d'ingénierie qui répond aux manquements auxquels nous faisons face, puis nous expliquons comment la résilience, l'utilisabilité et la sécurité peuvent être résolus en utilisant une approche systémique sociotechnique. Ensuite, nous présentons le modèle conceptuel avancé inhérent à notre approche d'analyse conjointe de la sécurité, de l'utilisabilité et de la résilience. Et enfin, nous suggérons des actes de l'ingénierie avancée de la sécurité, conjointement avec l'utilisabilité et la résilience. Les solutions élucidées sont présentées à l'aide de design patterns (patrons de conception) visant l'amélioration de l'expérience utilisateur ; et dans ce but un système métrique homogène cross-domaine vise à conférer à notre méthodologie d'ingénierie la capacité de traiter ensemble les critères quantitatifs et qualitatifs de la sécurité, de l'utilisabilité et de la résilience.
- Le cinquième chapitre illustre l'application de notre proposition sur une étude de cas. Nous avons retenu l'exemple d'un laboratoire d'analyses médicales. Aucun secteur d'activité n'est épargné et le secteur médical devient une cible de choix pour les attaquants.
- Le sixième chapitre présente une discussion et des éléments d'appréciation de notre proposition de méthodologie d'ingénierie.
- Le mémoire de thèse se termine par une conclusion et des perspectives pour des recherches futures.

# Chapitre 1 : Problématique de la sécurité dans les entreprises et organisations

## 1.1. Introduction

Ce chapitre a pour but de présenter les réalités auxquelles sont confrontées les entreprises et les organisations en termes de sécurité des systèmes d'information, malgré les efforts importants de recherches scientifiques dans les universités et les industries. L'état de l'art exige l'exploration de nouveaux horizons, de nouvelles approches innovantes, telles des approches systémiques et cross-domaines. Dans ce chapitre, nous évoquons les verrous scientifiques et industriels que nous suggérons de lever. En fin de chapitre, nous mettons en évidence la cible de choix qui s'oriente sur le secteur médical, même si aucun secteur d'activité n'est épargné.

## 1.2. Le contexte actuel de la sécurité

Plus précisément, en France, le nombre de cyberattaques a progressé à hauteur de 51% en 2015 par rapport à 2014, et les budgets de Sécurité des entreprises françaises ont augmenté en moyenne de 29%, soit autant que les pertes financières estimées imputables à ces incidents (un peu plus de 28%). Plus globalement au niveau mondial, le nombre de cyberattaques recensées a progressé de 38% en 2015 ; les budgets Sécurité des entreprises ont augmenté de 24%. Ces renseignements sont issus de l'étude « The Global State of Information Security® Survey 2016 » réalisée par le cabinet d'audit et de conseil PwC [PwC Etude Sécurité, 2016]. En collaboration avec les magazines CIO et CSO, il s'agit d'une étude sur la façon dont plus de 10.000 dirigeants dans 127 pays gèrent et améliorent la cybersécurité dans leurs organisations. Les chercheurs de RAND Corporation estiment les coûts totaux d'événements cybernétiques à environ 8,5 milliards de dollars par année [Romanosky, 2016].

### La sonnette d'alarme dans ce contexte nouveau

Le rapport de l'étude réalisée par le cabinet d'audit et de conseil PwC [PwC Etude Sécurité, 2016] a été introduit par une sonnette d'alarme fulgurante et très conforme à la réalité du terrain (*« The numbers have become numbing. Year after year, cyberattacks continue to escalate in frequency, severity and impact. Prevention and detection methods have proved largely ineffective against increasingly adept assaults, and many organizations don't know what to do, or don't have the resources to combat highly skilled and aggressive cybercriminals. »*). Les cas d'attaques informatiques sont devenus considérables et annihilants ; année après année, les cyberattaques 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.

Ce contexte actuel de la sécurité constitue le principal enjeu que nous adressons dans nos travaux ; cela représente le principal verrou scientifique que nous aimerions contribuer à lever, afin de pallier ce manquement scientifique qui s'aggrave d'année en année. Nous nous proposons de sortir des sentiers battus et d'explorer de nouveaux horizons qui ont fait leurs preuves dans leurs domaines respectifs et qui sont propices à ce nouveau contexte de l'industrie de services numériques. Les modèles d'exploitation et les business modèles des entreprises et des organisations subissent, à présent, des mutations profondes, dont l'impulsion provient de deux facteurs : d'une part des évolutions technologiques de plus en plus rapides, et d'autre part des attitudes de consommation changeantes et très volatiles. Les incidents de sécurité résultent de ces deux facteurs et sont aggravés par la criminalité, de plus en plus équipée, organisée et professionnalisée que constituent les attaques informatiques de nos jours.

### L'impact des technologies relatives au cloud computing dans ce contexte

Partout dans le monde, les scientifiques et les dirigeants des entreprises et organisations sont préoccupés et repensent aux pratiques de cybersécurité. Ils se recentrent sur les possibilités de technologies innovantes qui, d'une part, réduiront les risques et, d'autre part, amélioreront la

performance des entreprises et organisations. Nous ne pouvons plus continuer à entretenir une réflexion dichotomique, de choix entre la sécurité et le business.

La technologie du *cloud computing* est un exemple fédérateur qui fait tirer avantages et pour le business et pour la sécurité. Quand elle est bien menée, la technologie du *cloud computing*, d'une part apporte l'amélioration de la gestion d'entreprise avec tous les acteurs impliqués, et d'autre part elle participe à la réduction des risques. Les particuliers, les gouvernements, les entreprises et organisations de toute taille pourront tirer meilleur parti des technologies basées sur le cloud computing, comme des outils de cybersécurité, big data, nouveaux algorithmes d'analytique (*analytics*), d'authentification avancée. De nouvelles facilités pour les particuliers et opportunités de business trouvent leur essence dans les technologies du cloud computing telles que l'Internet des objets, la musique en ligne de n'importe quel endroit, les systèmes de paiement par mobile, les plates-formes de recherche participative pour la santé, les solutions d'e-citoyens ou e-gouvernement, etc. Ces technologies et leurs applications sont aussi de nouveaux terrains sensibles pour les attaques informatiques. Les grandes entreprises et organisations utilisent des approches collaboratives entre partenaires et fournisseurs et qui sont basées sur les technologies du cloud computing pour renforcer les résultats de la cybersécurité.

### Le facteur humain dans ce contexte

Il nous semble important de mettre en évidence dans le contexte actuel de la sécurité, un autre élément essentiel, c'est le facteur humain : les utilisateurs finaux, les contributeurs à la conception, à la mise œuvre et à l'exploitation des technologies, les collaborateurs et les experts. Ces derniers sont également désignés par les initiés, « *insiders* » en anglais. De nombreux cas de sécurité sont liés à leurs activités.

Le facteur humain pourrait constituer à la fois un très bon atout pour améliorer la sécurité ou bien un aspect important de sources d'incidents ou de pertes, en fonction de la manière dont il est pris en considération dans toutes les phases du cycle de vie des systèmes d'information, des services et des produits numériques.

Après avoir présenté le contexte actuel de la sécurité, nous positionnons dans la section suivante la typologie des attaques et menaces de sécurité.

## 1.3. Les attaques et menaces de sécurité

Le dernier rapport de l'enquête annuelle du Global Research and Analysis de Kaspersky Lab (GReAT) sur les risques informatiques au niveau mondial, contenant des informations stratégiques obtenues auprès de professionnels de l'informatique du monde entier, présente un nouvel éclairage sur les risques de sécurité et les préoccupations de 5564 entreprises interrogées, dans 38 pays [Kaspersky Lab, 2015]. Ce rapport précise que le coût moyen d'une violation de données pour les PME et les grandes entreprises s'élève à 38 000 $ et 551 000 $ respectivement, et 60 % des entreprises victimes d'une atteinte à la sécurité souffrent de dysfonctionnements importants qui entrainent des temps d'arrêt de service, causant des pertes d'opportunités commerciales. De même 56 % des événements de perte de données ont entraîné aussi une atteinte à l'image et à la réputation de l'entreprise en question.

Ce rapport met en lumière les chiffres suivants sur les professionnels interrogés :

- 50 % des professionnels de l'informatique interrogés ont cité la sécurité parmi leurs trois préoccupations principales ;
- 52 % pensent que leur organisation a besoin d'améliorer ses plans de réaction aux incidents pour les violations de données et autres événements de sécurité informatique ;
- 46 % des personnes interrogées doutent du fait que les cadres dirigeants (en dehors du service informatique) comprennent bien les risques de sécurité informatique auxquels leur entreprise est exposée.

Sur les entreprises elles-mêmes, les chiffres que ce rapport indique sont les suivants :

- 15 % des grandes entreprises interrogées ont connu des attaques ciblées au cours de l'année précédente, et plus de la moitié d'entre elles (53 %) ont signalé une perte de données sensibles suite à ces attaques ;
- 32 % des entreprises estiment avoir fait l'objet d'une attaque ciblée, dans le passé ou au moment de cette enquête ;
- 46 % estiment que le nombre d'attaques à l'encontre de sociétés comme la leur est en hausse ;
- 47 % souhaitent que les banques améliorent la sécurité des transactions en ligne ;
- 73 % ont subi un incident de sécurité interne en 2015 ;
- plus de 90 % ont subi une forme de menace externe au cours de l'année passée.

Nous rappelons que la gravité de ces menaces varie de mineure à extrême, pour une entreprise en activité. Il s'agit d'une statistique très troublante et qui présente la réalité du terrain.

### Le cas des dénis de services

Les attaques par déni de service distribué (DDoS - Distributed Denial of Service) existent depuis longtemps déjà, elles sont actuellement plus dangereuses qu'elles ne l'ont été au cours des dernières années [ANSSI, 2017]. Le coût du lancement d'une attaque DDoS a également diminué, ce qui a contribué à l'accroissement rapide du volume des attaques. Les attaques d'aujourd'hui sont par ailleurs plus complexes, rendant la défense beaucoup plus difficile. Parmi les entreprises interrogées, 50 % ont connu un certain degré de perturbation dû à une attaque DDoS au cours de l'année passée.

Très souvent, une attaque DDoS est combinée à une atteinte à la sécurité, pour un impact accru. L'année dernière, 45 % des attaques DDoS ont été combinées avec des programmes malveillants, 32 % avec une intrusion sur les réseaux ou un piratage, et 26 % avec une fuite de données.

Il nous semble important ici de mettre en évidence cet extrait de rapport : « le nombre d'attaques ciblées croît toujours, mais, plus inquiétant, les méthodes et les compétences des personnes qui les développent s'améliorent chaque année. Les attaques ciblées deviennent de plus en plus difficiles à détecter et il est parfois presque impossible de s'en débarrasser. » [Kaspersky Lab, 2015].

Les attaques ciblées sont très sophistiquées et combinent plusieurs scénarii. Elles sont le plus souvent perpétrées par des professionnels hautement qualifiés localisés à différents endroits géographiques et juridiques ; ils utilisent des ordinateurs zombies[3] répartis dans tous les pays, tous les endroits ayant accès à Internet. Quand une entreprise est vraiment ciblée, il y a de fortes chances qu'elle finisse par en être victime.

Comment savoir qu'on est ciblé et que devra-t-on faire pour être moins exposé, pour atténuer les risques et pour rebondir vite après incident, sans grands préjudices ? Telle est la question permanente que se pose tout responsable de la sécurité de l'information à l'ère de l'économie

[3] *Un ordinateur dont une personne malveillante prend le contrôle à distance.*

numérique. Cette thèse, en elle, toute seule, ne saurait y apporter une réponse biunivoque. Nous nous donnons pour objectif de définir un premier canevas de méthodologie d'ingénierie avancée contribuant à répondre de façon efficace à cette question d'actualité.

Dans la section suivante, nous concluons ce chapitre introductif, afin de présenter l'état de l'art et notre contribution par la suite.

## 1.4. Synthèse et conclusion du chapitre

Le numérique fait des progrès remarquables ; aussi très rapides sont leurs adoptions par la société, les individus, les entreprises, les organisations et les Etats. Des problèmes de sécurité cruciaux se révèlent de plus en plus, entrainant des pertes élevées chaque année. Et ce, malgré des budgets du marché de la sécurité à la hausse continuellement et les travaux continus de la communauté des scientifiques de l'industrie et des universités.

Ce paradoxe constitue un véritable manquement, tel un verrou scientifique que nous souhaitons contribuer à lever.

### Focus sur le secteur de soins et de la santé

Aucun secteur n'est épargné aujourd'hui par les incidents de sécurité. Une enquête menée récemment par l'institut SANS (*www.sans.org*) montre que l'industrie de santé n'est pas épargnée par cette problématique de la sécurité de l'information dans les entreprises et organisations [Filkins & Northcutt, 2016]. La prise en otage du système informatique d'un hôpital en Californie l'an dernier en constitue un exemple [Les Echos, 2016]. Le nombre de surfaces d'attaque continue d'augmenter à mesure que l'utilisation des appareils médicaux mobiles et des « Apps » (applications mobiles) relatives à la santé croit, et aussi que les dossiers électroniques de santé deviennent de plus en plus intégrés dans les milieux cliniques (hôpitaux, prestataires de services de santés, laboratoires d'analyse médicales). L'enquête de l'institut SANS montre que de nombreuses attaques sont internes et proviennent des initiés avec accès, que ce soit par simple négligence, par intention malveillante ou tout simplement par curiosité. L'enquête précise une amélioration du management des risques et une augmentation du budget alloué à la sécurité.

En décembre 2015, Munro a publié un article édifiant sur les violations de données de santé [Munro D., 2015]. Selon OCR aux US (Office of Civil Rights - Office des Droits Civils, comme la CNIL en France), il a été possible de dénombrer 253 violations qui ont touché 500 personnes ou plus avec une perte combinée de plus de 112 millions d'enregistrements. De ces pertes, 38% sont dues à des divulgations et accès non autorisés (Unauthorized Access/Disclosure), 21% sont dues à des attaques de sécurité informatiques réussies. Le même article révèle le commentaire suivant : « le groupe Health Insights de l'IDC prévoit que 1 sur 3 bénéficiaires de soins de santé sera victime d'une violation de données de soins de santé en 2016 ». Ces statistiques devraient être un appel de vigilance pour l'ensemble de l'industrie. En effet, les prédictions indiquent que les données de cartes de crédit vont diminuer de la valeur et d'attractivité sur le « marché souterrain », grâce à la sécurisation renforcée réussie par les institutions concernées. Malheureusement, les « personnes qui fréquentent du marché souterrain » vont exploiter les données de l'industrie des soins de santé pour voler les dossiers des patients et des informations personnelles d'identification pour commettre des fraudes relatives aux soins de santé. Ils vont écouter également sur les appareils médicaux non sécurisés qui créent un Internet "bavard" des objets [ANSSI, 2017b], [Adgeg, 2015].

Cette section ayant démontré que tout le monde, sans exception, peut être victime de cyber-attaques, le paragraphe suivant positionne notre contribution dans ce contexte d'économie numérique, à forts risques et fortes promesses.

### Positionnement de notre contribution

Pour apporter notre contribution à ce verrou scientifique d'ampleur, nous suggérons d'explorer d'autres horizons avec de nouveaux paradigmes dans la sécurité, conjointement avec l'utilisabilité et la résilience, au sein d'une ingénierie avancée à travers plusieurs domaines inter-corrélés, telle une innovation dans l'évolution (une « spirale vertueuse »). Nous désignons également cette démarche par une ingénierie cross-domaines ou ingénierie conjointe sur plusieurs axes : sécurité, utilisabilité et résilience. Pour ce faire, notre objectif est de chercher à tirer le meilleur parti d'expériences et avancées en ingénierie logicielle et système d'information, puis de les capitaliser au sein d'une approche proactive et systémique, telle une méthodologie d'ingénierie *ad hoc* (à partir de fragments de méthodes éprouvées et de meilleures pratiques dans différentes disciplines, dans le cadre d'une ingénierie de méthode).

Dans le chapitre suivant, dans un premier temps, nous présenterons les fondations de l'ingénierie logicielle et des systèmes d'information, et leurs percées, dont nous nous inspirerons par la suite. Puis dans un second temps, nous présentons les fondations de la sécurité, de l'utilisabilité et de la résilience, dont nous ferons un travail cross-domaine.

# Chapitre 2 : Etat de l'art – Inspiration et encrage

## 2.1. Introduction

Le numérique est essentiellement basé sur l'ingénierie logicielle, l'ingénierie des systèmes d'information, il en est de même pour ses vecteurs d'attaque de sécurité (les dispositifs utilisés pour perpétrer des attaques de sécurité). On pourrait également préciser le Web, la télécommunication, la microélectronique, les mathématiques et autres. A cela, s'ajoutent la théorie des organisations et l'économie. L'article de Vitali-Rosati [Vitali-Rosati, 2014] présente une définition pédagogique du numérique qui montre comment l'informatique et ses applications envahissent tous les secteurs de la vie socioéconomique.

Ce chapitre dresse un état de l'art des paradigmes et concepts auxquels nous avons recours dans le cadre de cette thèse, notamment les avancées dans l'ingénierie logicielle et l'ingénierie des systèmes d'information des entreprises et organisations. Il présente également les cadres de la sécurité des systèmes d'information, avec un focus spécialement sur EBIOS (le principal cadre en France). Ces éléments seront utiles dans le chapitre 4 pour présenter notre contribution.

## 2.2. Les percés dans l'ingénierie logicielle et l'ingénierie des systèmes d'information

Nous présentons dans cette partie les fondations de l'ingénierie logicielle, notamment ses évolutions, sa percée et les démarches d'ingénierie qui en découlent, notamment les aspects qui serviront à élaborer notre méthode d'ingénierie avancée de la sécurité (conjointement avec l'utilisabilité et la résilience) des systèmes d'information d'entreprise.

### 2.2.1 La percée de l'ingénierie logicielle

#### 2.2.1.1 Introduction

Les techniques et outils informatiques ont évolué d'une manière rapide depuis le milieu du vingtième siècle. Elles ont révolutionné les moyens mis à la disposition des entreprises et organisations (langages de programmation et environnements de développement de haut niveau, bases de données, progiciels intégrés, couple Internet-Web, infrastructures matérielles de plus en plus performantes, …) mais toutes les procédures d'informatisation n'ont pas toujours été menées dans le respect des bonnes règles d'ingénierie. Cette situation a évolué grâce à la performance des outils, des mécanismes et des nouvelles démarches, et surtout grâce à l'adhésion progressive des différents acteurs de l'entreprise à ces apports. Ces démarches sont basées sur des langages de spécification et des outils semi-formels ou formels combinés à des outils graphiques appropriés à la conceptualisation des systèmes, qui tout en étant directement « exécutables » les rendent compréhensibles par des non informaticiens. Nous héritons des travaux de James Martin [Martin, 1982, 1985], qui nous engageaient ainsi vers une informatique sans programmeurs pour concevoir des systèmes d'information intégrant des facilités de gestion mais aussi d'aide à la décision.

Avec les progrès impressionnants de l'informatique, notamment les interfaces et les réseaux sans fils, et le nouveau positionnement des systèmes d'information dans la dynamique et la concurrence accrue des entreprises et organisations, les démarches d'ingénierie informatique sont constamment mises à l'épreuve. Les exigences des nombreux et différents acteurs sont variées et très évolutives. Les entreprises et organisations sont dans une dynamique de fusion et d'acquisition. Elles cherchent en permanence à gagner des parts de marché. Les systèmes d'information deviennent complexes pour répondre à la problématique de « *Time To Market*[4] ». Les nouvelles démarches d'informatisation essaient de s'adapter à cette agilité et considèrent les systèmes d'information dans leur globalité face à cette complexité et à cette dynamique. Il s'agit des cadres d'architecture de systèmes d'information que nous présentons plus loin.

Les travaux du Professeur Giraudin [Giraudin, 2007], présentent la complexité des systèmes d'information d'entreprise à partir de trois facteurs, Figure 2.1 : Evolutivité (dynamisme

[4] *Aspect concurrentiel caractérisé par la course d'être premier sur le marché.*

constant), Autonomie (par opposition à Interactivité : échanges avec l'extérieur, partenaires et clients), Hétérogénéité (sous-systèmes et infrastructures de différentes technologies, équipes de travail et applications de différents métiers).

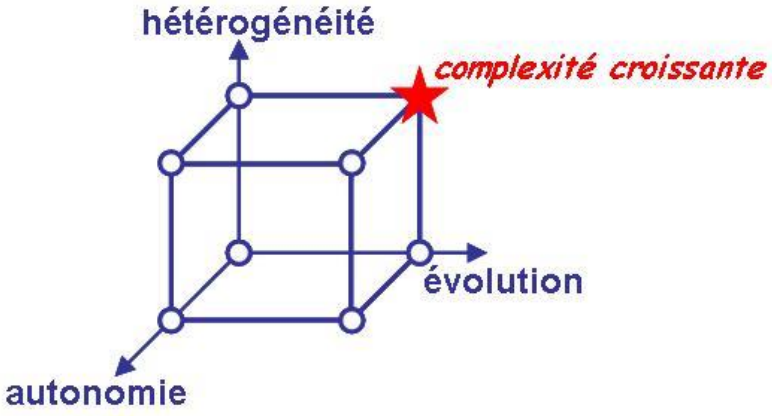


**Figure 2.1** : Facteurs de complexité des SI [Giraudin, 2007]

#### 2.2.1.2 Paradigmes cartésien et systémique pour l'analyse et la conception

Il est possible de regrouper les méthodes d'analyse et conception selon leur angle d'approche. Parmi les paradigmes, les plus connus sont le paradigme cartésien et le paradigme systémique.

### Paradigme cartésien

Le paradigme cartésien est effectué selon une démarche descendante de haut en bas, communément appelée "Top-down", qui part du général, va vers le particulier et met en œuvre le principe de Descartes. Cette démarche conduit l'analyste à décomposer la boîte initiale en autant de boîtes qu'il le faut pour parvenir à des boîtes dont le contenu soit intelligible. Considérant la boîte initiale comme étant la fonction de gestion dans l'entreprise ou organisation, la fonction de gestion est éclatée en un arbre de processus [Martin, 1986]. Les méthodes cartésiennes sont apparues dans les années 60. Elles sont basées sur la décomposition hiérarchique des processus et des flux d'information. Elles mettent l'accent sur la modélisation des processus. Cette décomposition met en évidence les interrelations entre processus au moyen de flux de données, de messages et de signaux de différentes sortes. Les méthodes cartésiennes sont applicables à des systèmes de taille moyenne, ayant peu d'interactions homme-machine et lorsque les fonctionnalités du système sont relativement claires. Un exemple représentatif de ces méthodes est la démarche SADT (Structured Analysis and Design Technique) [Lissandre,

1990] et [Ross et Scholman, 1977]. Outre la modélisation de données par datagramme, le concept manipulé par SADT est *l'actigramme* qui met l'accent sur la description des actions et leurs connexions au moyen de données. SADT fournit une règle de conduite de raffinement qui permet de décomposer chaque actigramme en trois à six actigrammes du niveau suivant, jusqu'à l'obtention du niveau de détail souhaité. Un actigramme est caractérisé par cinq éléments : 1) l'Action proprement dite, 2) les données en Entrée qui sont exécutées par l'action, 3) les données en Sortie qui sont produites par l'action, 4) les données de Contrôle qui influencent l'action et 5) les mécanismes représentant les ressources et outils qui aident à l'exécution de l'action. La Figure 2.2 représente une illustration schématique de la démarche de décomposition des activités dans SADT.

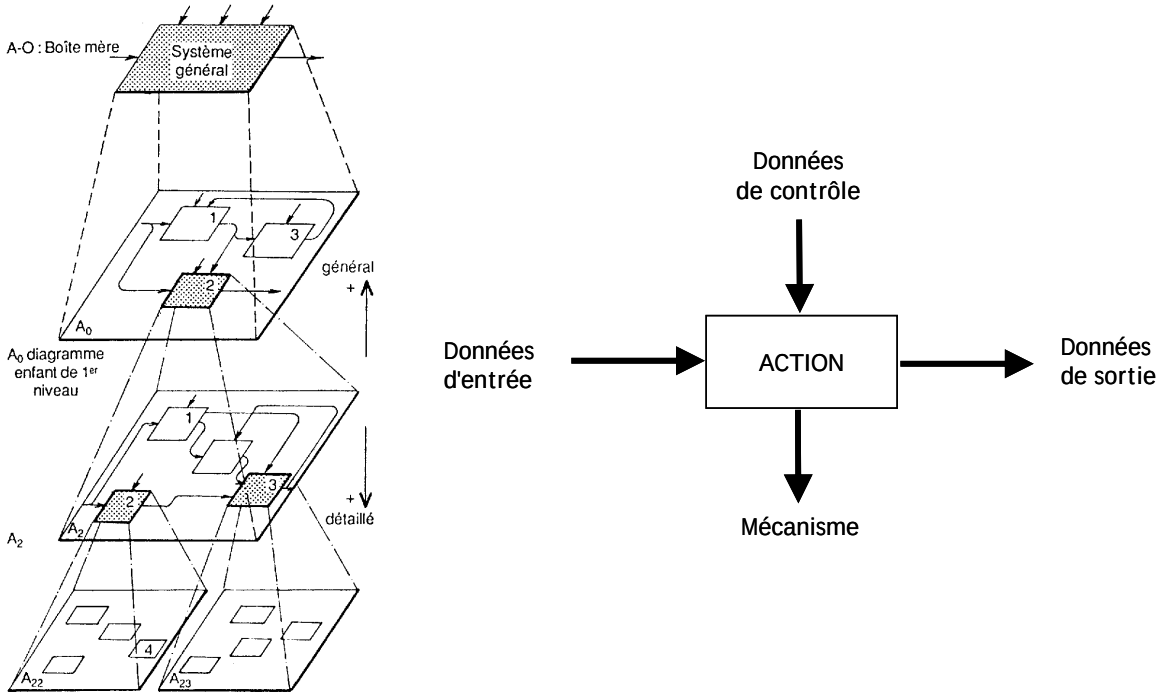


**Figure 2.2 :** Démarche SADT / Paradigme cartésien [Lissandre, 1990]

## Paradigme systémique

Comme son nom l'indique, le paradigme systémique provient de la théorie des systèmes, suivant laquelle il faut concevoir l'objet « Système général ». Nous présentons, ci-dessous, un schéma de référence qui illustre le système global dans lequel le système d'information est en relation avec le système opérationnel de l'organisation et avec son système de pilotage. Ce schéma est inspiré de la théorie de Boulding [Boulding, 1956], introduite en France par J. L.

Lemoigne [Lemoigne, 1977] et rendue populaire avec l'avènement de Merise [Nanci et al., 1992] et [Nanci et Espinasse, 2001].

Suivant le paradigme systémique, le système d'information est perçu comme un artéfact qui fournit une représentation des faits présents et passés dans la vie de l'entreprise ou l'organisation. Il s'agit des faits survenus dans son système opérant. C'est une mémoire collective des acteurs de l'entreprise ou organisation. A l'aide des informations stockées dans les bases, il permet aux acteurs de l'entreprise de retrouver les informations exactes sur l'embauche des employés, des commandes reçues, des livraisons effectuées, etc. Le système d'information est un *modèle*, i.e. une image abstraite de la réalité organisationnelle qui apporte aux acteurs et décideurs la connaissance dont ils ont besoin pour agir et décider. Il mémorise sous forme de données, l'image des faits pertinents et amplifie ainsi les capacités individuelles de mémorisation des acteurs de l'entreprise ou organisation.

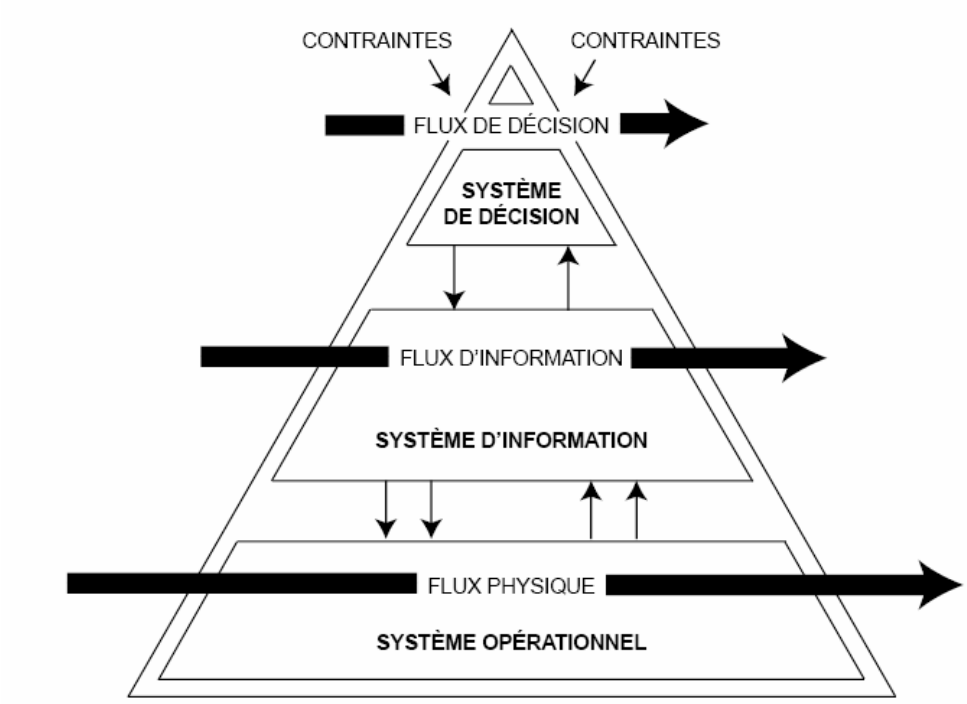


**Figure 2.3** : Paradigme systémique / Théorie des systèmes de Boulding [Boulding, 1956]

#### 2.2.1.3 Les approches de base en ingénierie logicielle

Dans cette section, nous présentons les approches de base, servant à la représentation, l'analyse et la conception en génie logiciel. Ces approches de l'ingénierie logicielle ont évolué au fil des efforts, elles ont progressé en efficacité et en maturité. Les approches plus avancées en

modélisation et en méta-modélisation s'en sont inspirées. Nous aussi, nous nous en inspirerons dans le modèle conceptuel de notre méthodologie d'ingénierie (qui sera proposée dans le chapitre 4 de Contribution).

### Approche conceptuelle

L'*approche conceptuelle*. Dans le contexte de paradigme cartésien, le processus de conception du SI est assimilé à un processus de modélisation qui, naturellement, s'est centré sur la modélisation des données. Une donnée est une valeur qui décrit, d'une certaine façon, un phénomène de la réalité et à partir de laquelle on obtient de l'information. L'information est l'incrément de connaissance que l'on infère d'une donnée. L'inférence est basée sur une interprétation des données et de leurs relations. Un modèle de données est un outil intellectuel qui permet une telle interprétation.

Les premiers modèles de données fournirent des règles d'interprétation qui étaient dépendantes de la méthode de stockage et d'accès aux données sur leurs supports physiques. Après de longs efforts sur une quinzaine d'années, de 1975 à 1990 environ de toute la communauté scientifique de chercheurs et d'experts du domaine, les modèles de données commencèrent à faciliter l'interprétation de leur sémantique ce qui avait permis la spécification du résultat de la modélisation à un niveau d'abstraction dans les termes de ce qui est appelé *Schéma conceptuel*.

### Modèle Entité-Association

Le *modèle Entité-Association* fournit des techniques de représentation sous forme de diagrammes de schéma conceptuel et est très utilisé pour la construction des schémas conceptuels. Il a été introduit par Peter Chen [Chen, 1976] qui avait suggéré de voir toute réalité comme composée d'entités ayant entre elles des associations. Le modèle entité-association est un modèle sémantique qui visualise les données et les liens qui existent entre elles. Une entité est une "chose" identifiée dans le SI, une personne, une facture ou une entreprise partenaire, par exemple. Une association est une combinaison d'entités dans laquelle chacune joue un rôle spécifique, la relation employeur-employé, par exemple. Le modèle entité-association est simple tout en présentant une très grande capacité d'expression. Il est largement reconnu dans la communauté des chercheurs et dans le milieu professionnel.

### Modèles binaires

Les *modèles binaires* adoptent la même vision du monde réel, mais restreignent les associations à des valeurs binaires entre entités. Le travail NIAM (Nijssen Information Analysis Methodology) de Nijssen et Halpin [Nijssen et Halpin, 1989] constitue une véritable concrétisation de ce modèle. Suivant cette méthode, le fait qu'une personne ait un nom ou qu'une personne habite dans une ville donnée, se représente de la même manière par un lien binaire. Les entités *personne* et *ville* sont des NOLOT (NOn Lexical Object Type). La méthode NIAM est de type linguistique et représente les faits (e.g. Paul habite à Paris) au moyen d'objets lexicaux (e.g. Paul et Paris) par une structure qui attache les objets lexicaux types (e.g. nom-personne et nom-ville) aux objets non lexicaux types correspondants (e.g. personne et ville). NIAM représente dans un même schéma *les classes de phénomènes réels* qui ont de l'intérêt pour le modélisateur (les NOLOT) et montre comment ce dernier a décidé de les décrire par des données (les LOT).

### Modèles sémantiques

Les *modèles sémantiques* introduits dans [Smith et Smith, 1977] apportent explicitement la notion d'*objets* (e.g. les entités types et les associations types). Gardarin et Valduriez [Gardarin et Valduriez, 1990] définissent l'*objet* comme "une collection d'éléments de données structurées et identifiée par une référence unique", et la *classe* comme "un groupe d'objets ayant les mêmes propriétés, caractérisés par une collection d'opérations qui s'appliquent aux objets de la classe en cachant la structure". Les objets sont associés par agrégation et généralisation afin de définir des objets plus complexes, qui à leur tour, participent à d'autres agrégations et généralisations. La collection des données est vue comme une hiérarchie d'objets. Le principe d'**abstraction** joue un rôle primordial dans cette structuration d'objets de ce modèle. Les principales formes d'abstraction sont la classification, l'agrégation, la composition-décomposition et la généralisation-spécialisation.

### Classification

La *classification* dissocie le niveau des instances de celui des classes. Elle range dans un même groupe désigné par un nom, des individus, des objets, des faits ou des phénomènes qui ont des caractéristiques communes. Une *classe d'objets* regroupe un ensemble d'instances de la même nature. Tous les modèles de données utilisent le principe de classification. Les modèles

sémantiques utilisent le terme d'objet pour désigner une classe et celui d'instance d'objet pour parler d'un élément de la même classe. Au début des années 80, la *notion de méta-classe* a été introduite par l'extension de la classification appliquée aux classes elles-mêmes. On distingue ainsi deux niveaux de classification : le niveau des concepts communs utilisables et les classes originales que l'ingénieur spécifiera comme éléments importants de modélisation d'un SI. Par exemple, en UML, classe, association, état, acteur, activité, etc., sont des concepts utilisables pour toute modélisation de SI, alors que ETUDIANT, DISCIPLINE et ENSEIGNANT sont des classes, ADMIS et OUVERTE sont des états, INSCRIPTION et ADMISSION sont des activités dans le SI d'un centre de formation.

### Agrégation

L'*agrégation* est une abstraction grâce à laquelle la relation entre objets (les *composants*) est vue comme un unique objet. En UML, le terme d'association est utilisé principalement au niveau structurel dans le modèle des classes et des objets pour décrire des ensembles de liens binaires, ternaires ou plus généralement n-aires entre objets. Le terme de relation quant à lui sert à distinguer les différents types de liaisons : une association (relation structurelle entre différents objets), une agrégation (type particulier d'association qui représente une relation structurelle entre un tout et ses parties), une généralisation-spécialisation (relation d'organisation hiérarchique des classes selon le principe « est-un, est-une-sorte-de » de représentation de connaissances), etc. Une association définie entre deux classes possède un nom qui l'identifie et sa définition est complétée par les noms des rôles de chaque classe et les cardinalités pour préciser des caractéristiques d'unicité ou de multiplicité, de partialité ou de totalité des liaisons possibles. Ces caractéristiques jouent un rôle analogue aux propriétés d'injection ou de surjection dans la définition des fonctions en mathématique. L'agrégation s'applique aussi bien au niveau des classes qu'au niveau des instances. L'utilisation répétitive de l'agrégation conduit à la hiérarchie des objets. L'agrégation est utilisée aussi bien dans une approche descendante pour structurer un objet complexe en le décomposant (top-down, en retrouvant ici le paradigme cartésien) que dans une approche ascendante pour regrouper des composants dans un même objet agrégat. L'approche ascendante est de type synthétique, alors que l'approche descendante est de type analytique et permet de concevoir un objet complexe. Dans la conception d'un SI réel, les deux approches sont souvent combinées.

### Composition-décomposition

La *composition-décomposition* est une forme d'abstraction qui permet de désigner une relation d'inclusion : un système inclut des sous-systèmes, un paquetage contient des paquetages, un cas d'utilisation comprend un autre cas d'utilisation. C'est une relation "*HAS-A*" qui ne doit pas être confondue avec une relation d'utilisation ou d'importation à caractère plus momentané. La composition complète la notion d'agrégation pour introduire une forte « possession » des parties par (le tout) par deux contraintes : une contrainte d'exclusivité pour préciser qu'une partie ne peut appartenir qu'à un tout et une contrainte de dépendance entre cycles de vie avec les parties qui peuvent être créées après le tout, mais qui "meurent" avec lui. Agrégations et compositions se distinguent dans un diagramme UML par deux représentations graphiques différentes : un losange blanc pour l'agrégation et un losange noir pour la composition. La composition-décomposition est une technique simple et générale, elle est aussi utilisée dans le paradigme cartésien.

### Généralisation

La *généralisation* est une forme d'abstraction qui désigne par un objet complexe mais unique (appelé *générique*), un ensemble d'objets appelés *spécialisés*. La généralisation exprime un lien "*IS-A*" entre un objet spécialisé et un objet générique, il s'agit d'un mécanisme de modélisation puissant qui classe des objets distincts dans d'autres objets plus généraux. La généralisation a favorisé des concepts intéressants qui sont utilisés jusqu'à présent : la simplification du schéma conceptuel en utilisant le principe d'héritage ; le raisonnement à différents niveaux d'abstractions, générique et spécialisé ; la description précise et fine de la réalité, organisation réelle.

#### 2.2.1.4 Modélisation et méta-modélisation

Le modèle M est considéré comme un objet théorico-formel construit analogue à une classe X de phénomènes (la réalité empirique). Cette analogie simule X et, ce faisant, étudie et répond à des questions Qx qui se posent à propos de X. Les modèles observent et conceptualisent la réalité et, aussi en reconstruisent certains aspects.

La modélisation est donc une simulation de la réalité. Elle alimente l'analyse conceptuelle qui consiste à abstraire des propriétés génériques, des régularités et des invariances de la diversité

profuse des phénomènes pour les organiser cognitivement, les catégoriser, les structurer par « inférences ». L'analyse conceptuelle subsume la diversité sous l'unité du concept. Elle se positionne comme complémentaire à la modélisation qui part du théorique et du conceptuel pour redescendre vers la diversité des phénomènes, mais une diversité construite et non plus donnée. Il s'agit de la synthèse "computationnelle", qui exige des algorithmes et théories génératifs pour élever la portée explicative des modèles à engendrer un grand nombre d'objets et de structures formels.

Ceci amène à retenir la modélisation comme un préalable indispensable à la conception des systèmes complexes et elle constitue une des conditions nécessaires de leur maîtrise. Pour réussir la modélisation, deux questions essentielles se posent : comment définir ce qu'il est convenable de modéliser ? Comment choisir les facettes adéquates sur lesquelles agir dans le système ?

Les modèles courants s'appuient sur des concepts naturels de base (classe, objet, propriété, association, acteur, événement, processus, état, composant, système, etc.) et sur un choix de notations graphiques. Ces dernières sont, d'une part, nécessaires à la communication, à l'aide à la compréhension, et d'autre part, elles sont utilisables pour des transformations progressives du SI « idéal » vers un système « réel ».

« Pour un opérateur O, un objet M est un modèle d'un objet A dans la mesure où O peut utiliser M pour répondre aux questions qui l'intéressent au sujet de A » [Minsky, 1968].

UML est un langage unifié de modélisation (Unified Modeling Language), standard mondial [OMG, UML, 2016], [Wirfs-Brock et Johnson, 1990] et [Korson et al., 1992]. Il est issu de la fusion de méthodes et langages de modélisation orientés objet comme OMT, Booch et OOSE. L'approche orientée objet répond à la flexibilité et à l'évolutivité des applications informatiques. Elle est constituée de méthodes et de langages de modélisation, de langages de programmation et d'outils de développement. Après avoir servi les applications techniques et les développements en temps réel, les approches objets ont pénétré le monde de la gestion et sont considérées dans les entreprises comme une évolution normale pour améliorer la productivité.

Des spécialistes du monde de la recherche et du monde des entreprises ont travaillé sur une étude comparative formelle des méthodologies d'analyse et de conception orientées objet [Hong et al., 1993]. De cette étude, il ressort que le maelstrom des méthodes ne constitue pas seulement une répétition. On y note aussi bien des similitudes, des complémentarités, des divergences ou des contrariétés, aussi bien sur des concepts simples que sur des principes majeurs (le changement par l'objet de sa classe d'appartenance). Chaque méthodologie est composée de descriptions informelles et présente ses propres définitions de ses concepts, techniques et notations. La fusion ayant abouti à l'UML constitue une opportunité pour l'approche orientée objet en général et une richesse pour la communauté à travailler au sein d'un organisme international de normalisation (OMG - Object Management Group), sur des paradigmes importants provenant de différentes origines.

La modélisation UML est semi-formelle et permet de visualiser, spécifier, construire et documenter les artéfacts d'un SI réel. Elle dispose d'une syntaxe concrète qui est son ensemble de diagrammes de notation et d'une syntaxe abstraite : le méta-modèle UML ou le model MOF (*Meta Object Facility)* de l'OMG, enrichi par les contraintes OCL (*Object Constraint Language*) de l'OMG.

Les méta-modèles sont des modèles pour construire (instancier, représenter) des modèles. Par exemple en UML, on distingue le méta-modèle des objets, exprimés dans le modèle, du modèle des classes et des objets d'un SI réel. Le modèle des objets du SI est conforme au méta-modèle UML qui, lui-même, est conforme au méta-modèle MOF. La méta-modélisation avec UML élabore la spécialisation d'UML pour un domaine concret (création de nouveaux modèles par instanciation), assure la communication et le partage de modèle avec un public cible (représentation unifiée de modèles), et met en œuvre un guide dans l'ingénierie des modèles (description formelle de modèles).

La Figure 2.4 illustre la méta-modélisation UML pour décrire le processus de développement en cascade simplifié. Ce dernier est modélisé en SPEM - *Software Process Engineering MetaModel* [OMG, 2008], lui-même modélisé en MOF. Il utilise des modèles de produits comme par exemple le modèle entité-association lors de l'activité d'analyse, le modèle relationnel lors de l'activité de conception, etc. Ces modèles de produits seront aussi (méta) modélisés en MOF. Dans ce cas, la complexité est liée aux multiples entrelacements (verticaux,

horizontaux) entre modèles : entre modèles de produits (entre modèle entité-association et modèle relationnel, ou entre modèle de classes et modèle d'état-transition par exemple), et entre modèles de processus et modèles de produits (entre le processus d'analyse et le modèle entité-association utilisé lors de ce processus d'analyse par exemple).

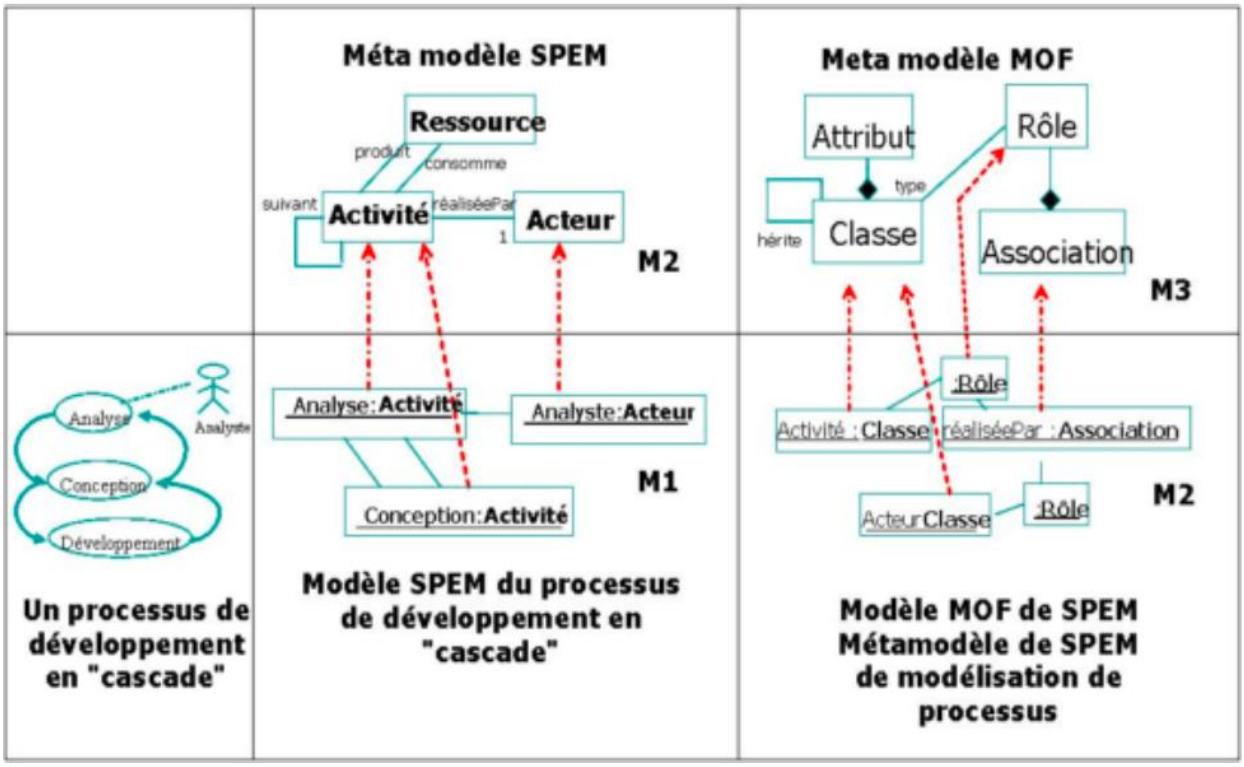


**Figure 2.4** : Schéma illustrant le SPEM [OMG, 2008]

### 2.2.1.5 Processus de développement logiciel

Le choix ou la définition d'une démarche pour guider les activités de modélisation et de réalisation dépend beaucoup des entreprises, de leur organisation, du type d'activités, etc. Les processus de développement ou cycles de vie du génie logiciel sont constitués de phases et correspondent aux premières contributions significatives pour organiser la modélisation des SI. Ils mettent en évidence les phases nécessaires, leur ordonnancement, les produits obtenus. Ils sont essentiels pour la gestion des projets informatiques. En une trentaine d'années, ces modèles de processus d'ingénierie se sont raffinés. Ils s'appuient sur des métaphores telles que cascade, fontaine, spirale, V, Y et bien d'autres. Nous les rappelons, ci-dessous, de façon succincte.

*Le cycle de la cascade* utilise des phases séquentielles [Royce, 1970], [BOEHM, 1981]. Son usage est délicat en cas d'erreur ; il faut refaire la phase en cours ou la phase précédente, voire une phase plus en amont. Cette démarche simple est critiquée d'une part pour son impact sur le coût d'une erreur décelée trop tardivement dans le cycle de développement, et d'autre part pour le délai trop long entre l'expression des besoins et la mise en exploitation du système opérationnel.

*Le cycle en V* améliore le cycle de la cascade et met l'accent sur les aspects vérification et validation. Les jeux de tests sont préparés dès les phases de spécifications ce qui améliore la production de logiciels corrects et valides. Le cycle en W (double V, deux fois V) est une première tentative pour s'intéresser au système en deux parties, toutes deux développées selon un V. Le premier V représente la partie centrale du système, alors que le deuxième V (et/ou d'autres V) correspond aux parties annexes.

*Le cycle en spirale* généralise le principe d'incrément et évite un temps trop long entre les premières spécifications de besoins et la livraison de tout le système [Boehm, 1976], [Boehm, 1988]. Il introduit la notion de prototype. Ce cycle de vie correspond à une adaptation du principe de la roue de Deming [Deming, 1982] utilisée en qualité.

*Le cycle en fontaine* met en exergue la notion de composant et favorise un processus de développement orienté réutilisation [Henderson-Sellers et Edwards, 1990]. Le modèle d'un système est modularisé : tout module est archivé et sert à nouveau pour modéliser d'autres systèmes.

*Le cycle en Y* traite les aspects techniques (branche droite) et les aspects fonctionnels (branche gauche) en parallèle pour traiter, à la jointure des deux branches, les phases de conception puis de réalisation (branche centrale) ; c'est le cas par exemple du processus 2TUP - *Two Track Unified Process* [Rocques et Vallée, 2001]. Une variante de ce cycle peut être proposée avec une branche centrale amont pour piloter et coordonner les deux premières branches, il s'agit du cycle en Ψ.

*La courbe du soleil* est une extension de Merise [Nanci et al., 1992]. La démarche Merise est basée sur des niveaux d'abstraction (conceptuel, organisationnel, logique, physique) et une dichotomie données-traitements. La courbe du soleil met en évidence les difficultés pour commencer une modélisation. Elle préconise de démarrer par une phase de compréhension ou rétro conception du système existant (partie montante de la courbe) pour ensuite appliquer une phase de type cascade (partie descendante de la courbe) pour réaliser le nouveau système à l'image du soleil qui se lève progressivement pour atteindre son apogée dans la journée (le schéma conceptuel) et ensuite décliner. Ce cheminement du processus est bien adapté dans le cas de la réingénierie d'un SI.

L'OMG a défini le modèle standard de définition de processus de développement SPEM (*Software Process Engineering MetaModel*) [OMG, 2008], [OMG, UML, 2016]. Le concept de composant induit des processus de développement combinant deux sous-processus : processus « par » réutilisation et processus « pour » réutilisation. En d'autres termes la notion de composant réutilisable combinée à l'approche MDA [OMG, 2005] place les processus de développement dans une perspective « patrimoniale » où il s'agit de construire un patrimoine, thésauriser sur ce patrimoine, utiliser et réutiliser ce patrimoine, faire évoluer ce patrimoine. Le niveau d'abstraction et de réutilisation peut être augmenté avec le concept de patron. Ce concept est proposé pour capitaliser des expériences en conception orientée objet tant d'un point de vue produit [Gamma et al., 1995], que d'un point de vue processus [Ambler, 1998]. Les patrons de type processus constituent une solution efficace pour formaliser une démarche [Gzara, 2000] et [Hassine, 2005]. Ainsi, le concept de Patron (encore désigné par Patron de Conception, Modèle de conception ou Design Pattern) est adopté dans les approches d'ingénierie du génie logiciel.

L'approche incrémentale et itérative est reprise dans le concept de processus unifié (UP - Unified Processus, RUP – Rational Unified Processus, etc.) construit sur UML [Booch et al., 1998]. La définition d'incréments de réalisation est un bon garde-fou pour limiter les risques de dérive. Chaque incrément fournit aux utilisateurs un résultat tangible de manière analogue à un tour de la roue de Deming ou à un pas de la spirale de Boehm. Les itérations caractérisent des degrés d'abstraction de plus en plus précis, des modèles de plus en plus détaillés qui à la fin correspondent à des modèles d'exécution ou à des applications déployées.

Philippe Kruchten [Kruchten, 1995] propose l'architecture logicielle des « 4+1 » vues qui part du principe de plans complémentaires pour ordonner l'usage des différents modèles UML dans

le cadre d'une approche centrée cas d'utilisation. Dans cette approche, la vue centrale (cas d'utilisation) pilote les quatre autres vues connexes (logique, processus, réalisation, physique). La vue logique décrit la conception du modèle d'objet, elle est très utilisée, notamment en conception orientée objet. La vue physique présente la cartographie du logiciel sur les infrastructures matérielles et reflète son aspect distribué.

Suite à plusieurs décennies de contributions scientifiques et d'améliorations soutenues par les professionnels en entreprises et les chercheurs, l'ingénierie des logiciels a énormément évolué pour continuer à soutenir les systèmes d'information des organisations entreprises, dans leurs complexités et leurs exigences accrues. De nos jours, les approches dirigées par le métier s'imposent par opposition aux approches dirigées par les techniques. Ainsi un objet métier peut être vu comme un modèle qui correspond à une abstraction d'un concept relatif à un métier. Un objet métier peut représenter différents types de connaissances : entités, processus, propriétés, etc. Il s'agit de maintenir ces abstractions dans un cycle de développement de l'expression des besoins à la réalisation des logiciels et à leur évolution. Il s'agit de la tendance de l'ingénierie dirigée par les modèles.

Ibtissem Hassine [Hassine, 2005] propose le cycle de vie en flocon qui est une amélioration du cycle de vie en Y, utilisant les paradigmes de l'ingénierie dirigée par les modèles. Le cycle de vie en flocons est composé d'un ensemble de cycles de développement en Y. Chaque cycle de développement en Y est centré sur un processus métier. Chaque processus métier est raffiné et peut être décomposé en sous-processus métier qui chacun à son tour sera développé selon un cycle en Y dont l'ensemble constitue un nouveau flocon.

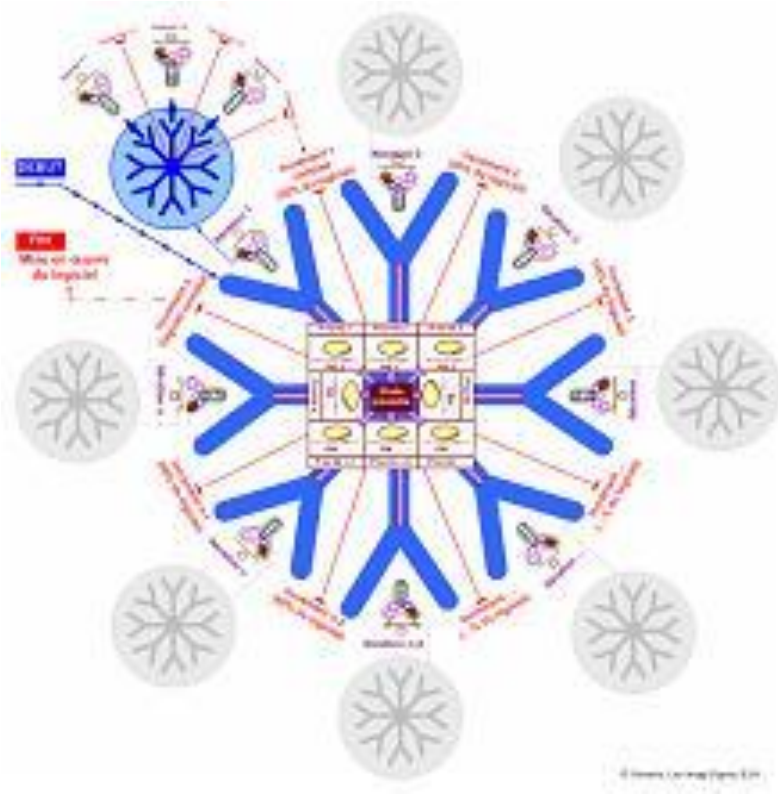

**Figure 2.5** : Processus d'ingénierie des systèmes en flocons [Hassine, 2005]

Cette section est inspirée des travaux du Professeur Giraudin [Giraudin, 2007] qui nous ont fait revisiter les recherches et les avancées de l'ingénierie logicielle et de l'ingénierie des systèmes d'information au fil des décennies. Notons que d'autres contributions scientifiques, en particulier des modèles enrichis sous l'angle de l'interaction homme-machine, existent également ; plusieurs de ces modèles sont présentés dans la thèse de Hela Ltifi [Ltifi, 2011] et dans [Kolski et al., 2001]. Dans le chapitre 4, l'ingénierie avancée de la sécurité que nous proposons s'en inspire également.

### 2.2.2 Méthodes agiles dans l'ingénierie logicielle et systèmes d'information

Les percées dans l'ingénierie logicielle et dans l'ingénierie des systèmes d'information ont conduit à des méthodes moins chronophages, afin de répondre aux exigences de souplesse et de rapidité, tout en garantissant l'efficacité. En effet, il n'est pas possible de tout connaître et de tout anticiper, quelle que soit l'expérience projet détenue. Le découpage d'un projet en itérations

est plus objectif plutôt que de vouloir tout prévoir et tout planifier, en sachant que des impondérables surviendront en cours de route. Les méthodes agiles utilisent un principe de développement itératif qui consiste à découper le projet en plusieurs étapes qu'on appelle « itérations ». Ces itérations sont en quelque sorte des mini-projets définis ensemble entre l'équipe projet et le client, en détaillant les différentes fonctionnalités qui seront développées en fonction de leur pertinence et de leur priorité.

Les méthodes agiles présentent des concepts communs élaborés au sein du Manifeste Agile [Agile, 2017]. Nous suggérons de rappeler ici (tels qu'indiqués dans le Manifeste Agile) les douze principes qui définissent le socle du Manifeste Agile, la plus haute priorité étant de satisfaire le client en livrant rapidement et régulièrement des fonctionnalités à grande valeur ajoutée : «

1- Accueillez positivement les changements de besoins, même tard dans le projet. Les processus Agiles exploitent le changement pour donner un avantage compétitif au client.
2- Livrez fréquemment un logiciel opérationnel avec des cycles de quelques semaines à quelques mois et une préférence pour les plus courts.
3- Les utilisateurs ou leurs représentants et les développeurs doivent travailler ensemble quotidiennement tout au long du projet.
4- Réalisez les projets avec des personnes motivées.
5- Fournissez-leur l'environnement et le soutien dont ils ont besoin et faites-leur confiance pour atteindre les objectifs fixés.
6- La méthode la plus simple et la plus efficace pour transmettre de l'information à l'équipe de développement et à l'intérieur de celle-ci est le dialogue en face à face.
7- Un logiciel opérationnel est la principale mesure d'avancement.
8- Les processus Agiles encouragent un rythme de développement soutenable. Ensemble, les commanditaires, les développeurs et les utilisateurs devraient être capables de maintenir indéfiniment un rythme constant.
9- Une attention continue à l'excellence technique et à une bonne conception renforce l'Agilité.
10- La simplicité – c'est-à-dire l'art de minimiser la quantité de travail inutile – est essentielle.
11- Les meilleures architectures, spécifications et conceptions émergent d'équipes auto organisées.
12- À intervalles réguliers, l'équipe réfléchit aux moyens de devenir plus efficace, puis règle et modifie son comportement en conséquence. »

Nous rappelons, ci-dessous, une comparaison succincte entre les méthodes classiques et les méthodes agiles.

| Thème | Approche traditionnelle | Approche agile |
|---|---|---|
| Cycle de vie | En cascade ou en V, sans rétroaction possible, phases séquentielles. | Itératif et incrémental. |
| Planification | Prédictive, caractérisée par des plans plus ou moins détaillés sur la base d'un périmètre et d'exigences définies et stables au début du projet. | Adaptative avec plusieurs niveaux de planification (macro- et microplanification) avec ajustements si nécessaires au fil de l'eau en fonction des changements survenus. |
| Documentation | Produite en quantité importante comme support de communication, de validation et de contractualisation. | Réduite au strict nécessaire au profit d'incréments fonctionnels opérationnels pour obtenir le feedback du client. |
| Équipe | Une équipe avec des ressources spécialisées, dirigées par un chef de projet. | Une équipe responsabilisée où l'initiative et la communication sont privilégiées, soutenue par le chef de projet. |
| Qualité | Contrôle qualité à la fin du cycle de développement. Le client découvre le produit fini. | Un contrôle qualité précoce et permanent, au niveau du produit et du processus. Le client visualise les résultats tôt et fréquemment. |
| Changement | Résistance voire opposition au changement. Processus lourds de gestion des changements acceptés. | Accueil favorable au changement inéluctable, intégré dans le processus. |
| Suivi de l'avancement | Mesure de la conformité aux plans initiaux. Analyse des écarts. | Un seul indicateur d'avancement : le nombre de fonctionnalités implémentées et le travail restant à faire. |
| Gestion des risques | Processus distinct, rigoureux, de gestion des risques. | Gestion des risques intégrée dans le processus global, avec responsabilisation de chacun dans l'identification et la résolution des risques. Pilotage par les risques. |
| Mesure du succès | Respect des engagements initiaux en termes de coûts, de budget et de niveau de qualité. | Satisfaction client par la livraison de valeur ajoutée. |

**Figure 2.6 : Comparaison entre les méthodes classiques et les méthodes agiles [ACCESS-DEV, 2017]**

La méthode Scrum est l'une des méthodes agiles les plus répandues en France (voir illustration sur la Figure 2.7). Elle a été créée par Ken Schwaber et Jeff Sutherland (signataires du Manifeste) en 1993 [Scrum, 2017]. Le Scrum ou « mêlée » est un terme emprunté au rugby qui désigne la solidarité et la force qui lient les membres de l'équipe au succès de l'itération. Le cycle de vie de Scrum est rythmé par des itérations de trois à quatre semaines qu'on appelle « *Sprints* ». Avant chaque sprint, on effectue une réunion de planification appelée le « *Sprint planning meeting* » qui consiste à sélectionner les exigences prioritaires pour le client dans le « *Backlog* du *produit* » qui seront développées, testées et livrées au client. Les exigences sélectionnées à chaque sprint sont appelées « *backlog du sprint* », c'est un sous-ensemble du

backlog produit. Des mêlées sont organisées quotidiennement (mêlée) durant le sprint afin de contrôler l'avancement pour s'assurer que les objectifs sont tenus. A la fin du sprint, une démonstration des derniers développements est faite au client qui donnera lieu à un bilan qualitatif sur le fonctionnement de l'équipe.

Les principales valeurs mises en avant par la méthode Scrum sont indiquées, ci-dessous.

- Visibilité : Avoir une vision réelle sur le résultat
- Inspection : Vérifier l'écart par rapport à l'objectif initial
- Adaptation : S'adapter en fonction des écarts constatés afin de les ajuster. Scrum est favorable à des petits ajustements fréquents

Le Figure 2.7 présente une illustration de la méthode Scrum.

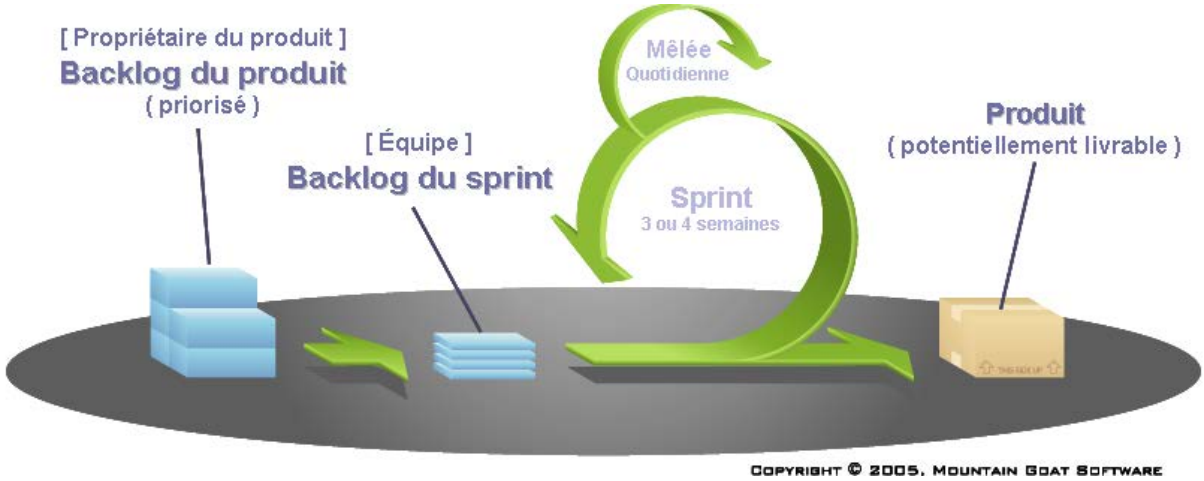


**Figure 2.7** : Schéma d'illustration de la méthode Scrum

Nous recensons également d'autres méthodes agiles, dont les plus populaires en usage aujourd'hui sont : l'eXtrême Programming (XP), Feature Driven Development (FDD), Lean Software Development, Agile Unified Process (Agile UP ou AUP), Crystal et Dynamic Systems Development Method (DSDM).

Dans le chapitre 4, l'ingénierie avancée de la sécurité que nous proposons s'en inspire également. A l'ère de l'économie numérique, il ne pourrait être judicieux de mener la démarche de sécurité de façon chronophage.

### 2.2.3 Ingénierie d'élaboration de méthodes

L'émergence perpétuelle de nouveaux domaines d'application de SI étaye l'intérêt pour l'ingénierie des méthodes qui est une discipline ancienne (CAME – Computer Aided Methods Engineering), mais qui demeure d'actualité, tant sur le plan de la recherche que sur celui de la pratique professionnelle. Une synthèse des travaux de comparaison des différentes ingénieries des méthodes est présentée dans l'article de Ralyté Jolita [Ralyté, 2001].

La discipline d'ingénierie des méthodes se préoccupe de la définition de nouvelles méthodes d'ingénierie des systèmes d'information. C'est une discipline de conceptualisation, de construction et d'adaptation de méthodes, de techniques et d'outils pour le développement des systèmes d'information. L'ingénierie des méthodes traite également l'élaboration de nouvelles méthodes à partir de méthodes déjà existantes.

Plus généralement, il ne peut être imposé l'utilisation de méthodes existantes comme point de départ de l'ingénierie des méthodes. En tout état de cause, une méthode d'ingénierie des systèmes d'information est une collection de procédures, de techniques, de descriptions de produit et d'outils pour le support effectif, efficace et consistant du processus d'ingénierie des systèmes d'information.

Dans la littérature, nous notons plusieurs propositions de définition de la notion de méthodes. La plupart d'entre elles convergent vers l'idée qu'une méthode est basée sur des modèles et consiste en plusieurs étapes qu'on exécute dans un ordre bien donné. L'un des pères fondateurs d'UML, Grady Booch [Booch, 1991], a donné la définition suivante du concept de méthode : « Une méthode d'ingénierie des systèmes est un processus rigoureux permettant de générer un ensemble de modèles qui décrit divers aspects d'un logiciel en cours de construction en utilisant une certaine notation bien définie ».

Nous sommes bien conscients qu'avec la croissance de la complexité des domaines applicatifs, la construction de nouvelles méthodes devient un enjeu crucial. Les méthodes ne sont pas universelles et, pendant leur élaboration, elles ne peuvent prévoir toutes les situations possibles. La question essentielle qui se pose dans l'ingénierie des méthodes se résume à la flexibilité et l'adaptabilité de la méthode pour s'accorder à la situation. Faudrait-il une méthode trop générique dépourvue de canevas ou bien, une méthode trop rigide qui ne peut s'appliquer qu'à un seul problème ? A cette question, nous proposons une méthode d'ingénierie pragmatique qui couvre entièrement le spectre du périmètre défini et surtout, qui s'accorde aisément à la

situation et, qui prend en compte les connaissances heuristiques accumulées au fur et à mesure de son application. Cette réponse nous rappelle l'ingénierie des méthodes situationnelles, dont la discipline vise à construire de nouvelles méthodes d'ingénierie des systèmes d'information en réutilisant et assemblant différents fragments de méthodes qui ont déjà fait leurs preuves.

Les travaux de Rolland et Prakash [Rolland et Prakash, 1996] et de Brinkkemper avec ses collègues [Brinkkemper et al., 1998] introduisent la notion de fragments de méthode et proposent des approches d'assemblage de ces fragments de méthodes. Les fragments peuvent se chevaucher en partie ou bien, ils peuvent être disjoints et complémentaires. Une méthode y est vue comme une collection de fragments réutilisables. Ainsi nous pouvons construire une nouvelle méthode en empruntant de différentes méthodes existantes les fragments qui sont les plus appropriés pour la situation que nous souhaitons traiter. Les méthodes résultantes sont elles-mêmes modulaires et peuvent être modifiées et étendues facilement. Les travaux [Ralité, 2001], [Ralité et al., 2008] et [Bonjean, 2013] traitent en détail l'ingénierie des méthodes situationnelles et la construction de méthodes par assemblage de composants.

A l'instar des Ateliers de Génie Logiciel (AGL ou CASE en anglais – Computer Aided Software Engineering), les Ateliers d'Ingénierie de Méthodes (AIM ou CAME en anglais – Computer Aided Method Engineering) sont apparus pour supporter les méthodes d'ingénierie de systèmes. L'ingénierie des méthodes y est considérée comme un processus discipliné pour construire, évaluer ou modifier une méthode par le moyen de spécifications des composants de méthode et des relations entre eux.

Grâce aux efforts des scientifiques, l'ingénierie logicielle et l'ingénierie des systèmes d'information ont connu de nombreux progrès afin d'atteindre aujourd'hui une maturité industrielle. Dans cette section 2.2 nous avons présenté les percées et les grandes tendances qui caractérisent l'ingénierie logicielle et l'ingénierie des systèmes d'information. Nous nous en inspirerons pour élaborer notre méthodologie d'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience.

Dans la prochaine section 2.3, nous présenterons l'état de l'art de la sécurité des systèmes d'information.

## 2.3. Cadres de la sécurité des systèmes d'information

Les cadres d'analyse de risques de sécurité définissent les modèles, les approches, méthodes et référentiels qui servent à conduire et réaliser les travaux de sécurité. Avec leurs différents niveaux de maturité dans les entreprises et organisations, les cadres de sécurité y apportent différents bénéfices. Entre autres, nous énumérons une meilleure capacité à identifier et prioriser les risques de sécurité, une meilleure capacité à détecter et atténuer rapidement les incidents de sécurité, à mieux sécuriser les données sensibles, mieux comprendre les écarts de sécurité afin de les traiter, et améliorer les communications et collaborations (internes et externes).

Des cadres de sécurité standards, les professionnels de l'industrie et de la recherche apportent des aménagements, des adaptations et/ou des extensions par assemblage de fragments plus opportuns qui sont extraits de différentes sources.

### 2.3.1 Cadres internationaux de la sécurité des systèmes d'information

Dans le monde entier, on utilise essentiellement les deux cadres de sécurité : NIST [NIST, 2016] et la famille de normes ISO 27 Milles [ISO/IEC 2700x, 2010].

La famille des normes ISO 27 Milles [ISO/IEC 2700x, 2010] est entièrement dédiée à la sécurité de l'information, y compris la dimension organisationnelle (entreprises publiques ou privées). Elle constitue aujourd'hui le principal cadre adopté dans le monde entier, même si chaque région stratégique (géopolitique et/ou géoéconomique) dispose encore de ses propres cadres d'influence. Les normes présentent comment établir, mettre en œuvre, maintenir et améliorer continuellement la sécurité de l'information et les systèmes de gestion de la sécurité de l'information. Les normes 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. Toutes les parties concernées (utilisateurs, opérateurs et propriétaires de systèmes sociotechniques) devraient avoir l'assurance que les risques de sécurité sont gérés de façon appropriée. D'autres normes internationales traitent également de la sécurité, ainsi que les risques de sécurité des systèmes d'information. La norme internationale ISO 15408 (Critères communs, CC) se concentre sur trois publics qui sont les producteurs, les évaluateurs et les utilisateurs. Nous rajoutons les normes internationales ISO 13335 et ISO 21827. Nous

identifions également des cadres locaux Cramm (en Angleterre), Mehari et Ebios (en France), Octave (USA et Canada).

Dans la section suivante, nous étayons le cadre Ebios. Il s'agit du cadre d'influence majeure en France, il est porté par l'agence ANSSI (Agence National de la Sécurité des Systèmes d'Information) [ANSSI, 2017c]. Cette agence est sous la responsabilité du Secrétariat général de la défense et de la sécurité nationale [SGDSN, 2017], un service du Premier ministre travaillant en liaison étroite avec la Présidence de la République.

### 2.3.2 EBIOS le cadre de référence en France

En France, nous utilisons davantage le cadre de sécurité des systèmes d'information EBIOS [EBIOS, 2016], et moins souvent Mehari [CLUSIF, 2016]. Dans cette section, nous présentons le cadre EBIOS et sa démarche. Nous y reviendrons avec une analyse approfondie dans le chapitre 5 « discussions et éléments de benchmark ».

#### 2.3.2.1 Présentation du cadre EBIOS

Le cadre EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est la référence en France, en tant que méthode de gestion des risques. C'est la méthode de gestion des risques de sécurité des systèmes d'information de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information - www.ssi.gouv.fr).

Il a été créé en 1995 par la DCSSI (Direction Centrale de la SSI), qui travaille sous l'autorité du Secrétariat Général de la Défense Nationale (SGDN) français. La DCSSI, parmi ses missions, assurait en France la fonction d'autorité nationale de régulation pour la SSIC (Sécurité des Système de l'Information et de la Communication) ; elle assurait la mise à jour régulière de la méthode EBIOS et animait différents sujets autour de cette méthode. A présent, tout cela est mis sous la tutelle de l'ANSSI.

Appliqué à un système d'information, le cadre EBIOS permet :

- d'identifier les risques qui pèsent sur le système d'information (combinaison d'un ou de plusieurs événements redoutés et d'un ou de plusieurs scénarios de menace) ;

- d'estimer leur niveau de gravité (hauteur des impacts) et de vraisemblance (possibilité qu'ils se réalisent), de les cartographier et prendre des décisions en conséquence ;
- de choisir les mesures nécessaires et suffisantes en termes de prévention, de protection et de récupération (restauration après sinistre).

EBIOS se présente sous la forme d'un guide composé de cinq sections, permettant d'apprécier et de traiter les risques relatifs à la SSI. Cette référence SSI a été conçue dans le but d'être déployée en interne (par un analyste ou une équipe) sans nécessité d'une intervention de spécialistes externes.

Nous résumons son principe général, comme suit :

- identifier les actifs (les biens et services) à protéger,
- analyser les conséquences d'incidents sur ces actifs,
- analyser les vulnérabilités des architectures techniques pour choisir les objectifs de sécurité appropriés pour minimiser les risques.

Le cadre EBIOS a principalement été conçu de manière à permettre la rédaction d'une FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité). Ce document est obligatoire dans le cas de systèmes traitant des informations classifiées de défense, et reste recommandé le cas échéant. Ceci conforte EBIOS dans sa position de méthode majeure de la gestion des risques en France.

L'ANSSI insiste beaucoup sur la compatibilité du cadre EBIOS avec les normes internationales telles que les Critères Communs (ISO/IEC 15408), la famille de normes ISO 27 Milles (notamment, ISO 27001, ISO 27002 et ISO 27005), ce qui renforce sa crédibilité. L'ANSSI accompagne EBIOS d'un outil gratuit qui facilite son utilisation et d'autres travaux qui permettent de couvrir le plus large spectre de la sécurité des systèmes d'information.

#### 2.3.2.2 La démarche inhérente au cadre EBIOS

Le contenu du cadre de sécurité EBIOS est bien focalisé sur la gestion des risques, où l'accent est mis sur la partie analyse des risques. Ce cadre de sécurité commence à l'analyse du contexte et se termine à l'énoncé des exigences de sécurité fonctionnelles. Il est très complet et peut être accéléré par l'utilisation des diverses listes et bases de connaissance tout en restant exhaustif et flexible. Dans les documents relatifs à EBIOS, les points qui peuvent être modifiés suivant les caractéristiques de l'organisation étudiée sont précisés.

Le cadre de sécurité EBIOS est composé de cinq étapes de base.

**Etape 1 : Etude du contexte**

- ✓ Etude de l'organisme
- ✓ Etude du système cible
- ✓ Détermination de la cible de l'étude sécurité

**Etape 2 : Expression des besoins de sécurité**

- ✓ Réalisation des fiches de besoins
- ✓ Synthèse des besoins de sécurité

**Etape 3 : Etude des menaces**

- ✓ Etude des origines des menaces
- ✓ Etude des vulnérabilités
- ✓ Formalisation des menaces

**Etape 4 : Identification des objectifs de sécurité**

- ✓ Confrontation des menaces aux besoins
- ✓ Formalisation des objectifs de sécurité
- ✓ Détermination des minimums de sécurité

**Etape 5 : Détermination des exigences de sécurité**

- ✓ Détermination des exigences de sécurité fonctionnelle,
- ✓ Détermination des exigences de sécurité d'assurance.

Cette dernière étape va permettre l'adéquation avec la norme ISO 15408.

L'articulation entre les cinq étapes de la démarche est visible en Figure 2.8.

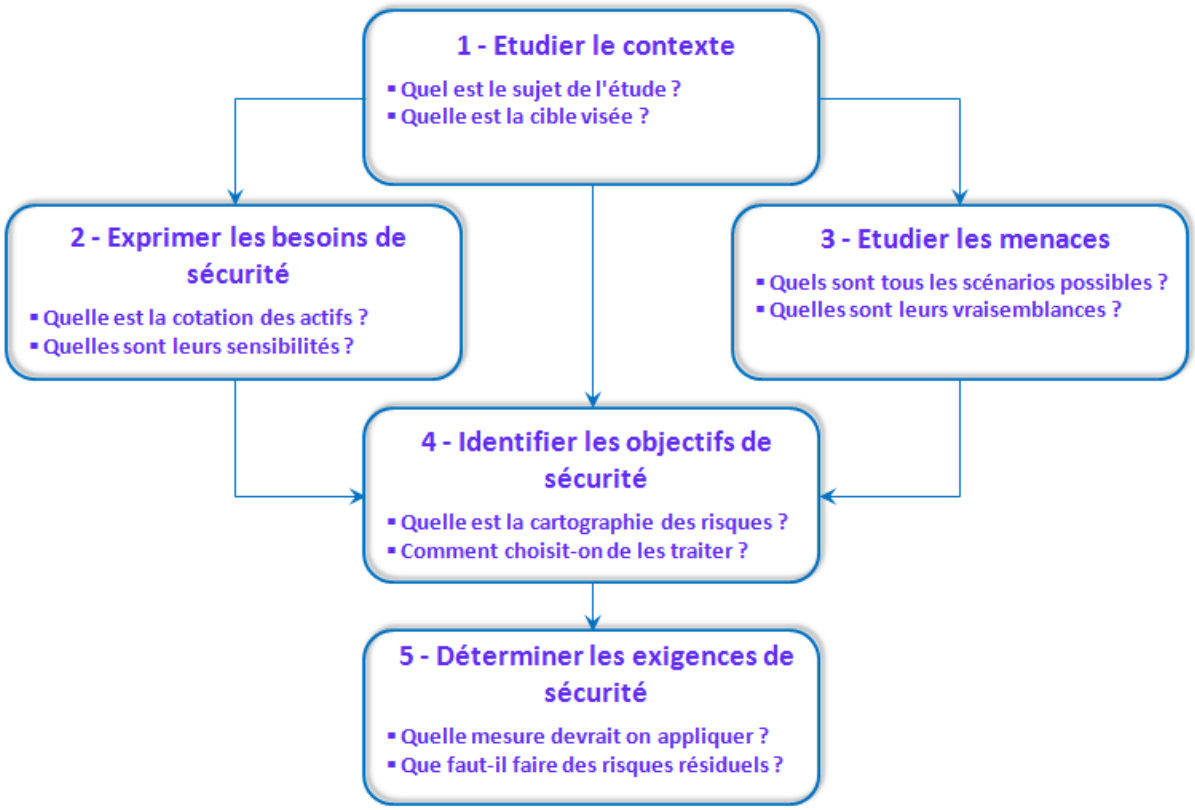


**Figure 2.8** : Schéma illustré de la démarche du cadre EBIOS inspiré de [EBIOS, 2016]

### 2.3.3 Synthèse sur les principaux cadres existants et leurs manquements

Les systèmes d'information sécurisés doivent fonctionner de manière fiable et sûre malgré les erreurs aléatoires, les perturbations techniques et les attaques malveillantes. Par le schéma de la Figure 2.9, nous illustrons la vision classique de la sécurité des systèmes d'information.

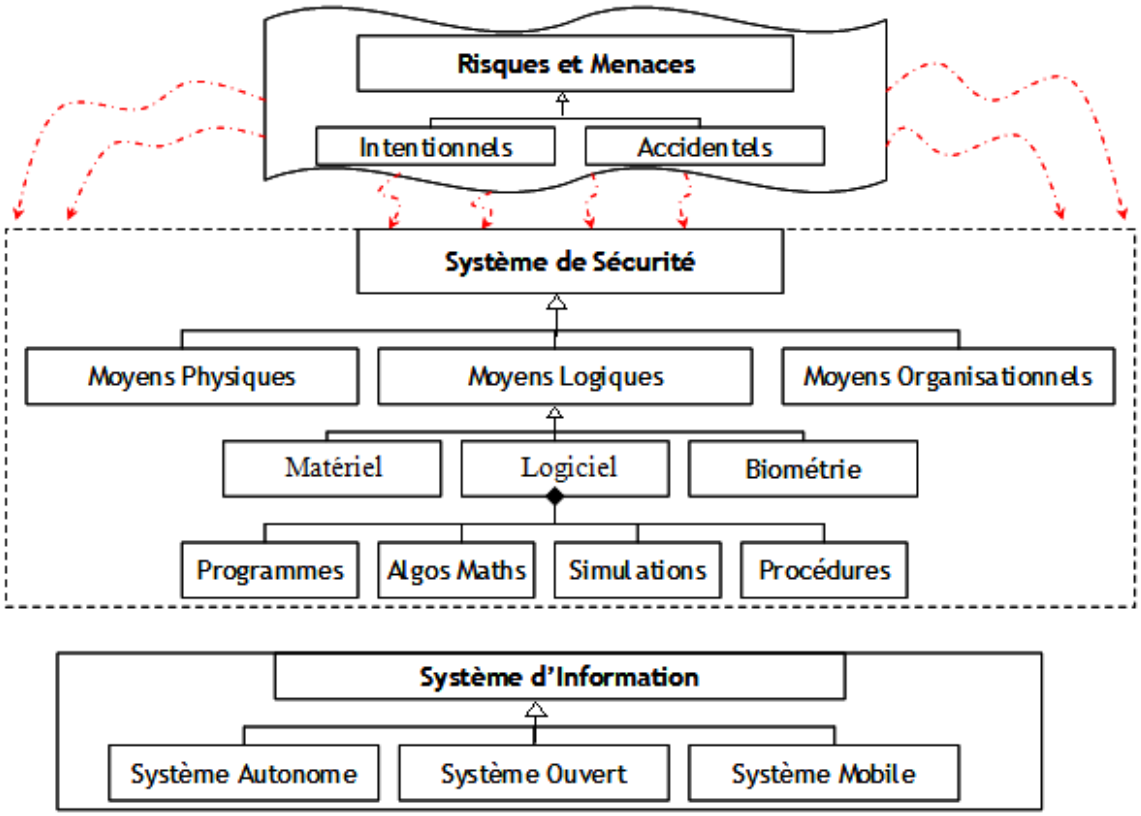


**Figure 2.9** : Vision classique de la sécurité des systèmes d'information

L'approche classique de la sécurité des systèmes d'information est essentiellement orientée Risques. Les risques et menaces peuvent être d'ordre intentionnel ou non. Les risques accidentels peuvent provenir d'une intempérie, une catastrophe naturelle, un dysfonctionnement ou une erreur humaine. 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 ;
- Robuste, 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.

La plupart des cadres de sécurité des systèmes d'information utilisent une approche de risques de sécurité des systèmes d'information des entreprises et organisations. 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, de par les applications d'entreprise ou les activités au quotidien des acteurs internes à l'entreprise ou à l'organisation. Les cadres devraient s'étendre vers une approche harmonieuse qui prend en compte l'ensemble des acteurs de l'entreprise (les responsables d'entreprise, les acteurs business, les spécialistes de la conformité et règlementation, les spécialistes de systèmes d'information, les spécialistes de la sécurité des systèmes d'information, les utilisateurs internes et externes). De même, les facteurs humains et les « *endpoints* » (les terminaisons[5]) devraient être pris en compte dans leur nouvelle réalité de mobilité, de BYOD[6] et de volatilité.

Dans l'optique d'améliorer la sécurité des systèmes d'information d'entreprise, Goudalo et Seret [Goudalo & Seret, 2008] ont proposé une approche méthodologique opérant sur le canevas d'adhésion de toutes les parties prenantes de l'organisation. De même les travaux de Clarke et Furnel [Clarke & Furnel, 2014] se rapportent à l'aspect humain dans le succès de la sécurité. Les systèmes dans les entreprises et industries sont utilisés par des humains même s'ils sont massivement automatisés. L'Interaction Homme-Machine est un facteur clé qui contribue à la sécurité et qui peut également la faire faillir. Ne serait-il pas la faiblesse de la sécurité des systèmes d'information ? Une ergonomie trop contraignante peut devenir une vulnérabilité de sécurité. Tel est le cas de certains systèmes de captcha[7] et de mots de passe. L'utilisabilité des systèmes de sécurité présente un caractère déterminant pour le succès de la sécurité. Yee propose des patterns d'utilisabilité qui sont adaptés à la conception des systèmes de sécurité pour des fonctions spécifiques [Yee, 2002]. D'un autre point de vue, une interface ergonomique mal adaptée constituerait une source de mauvais usage, mauvaise utilisabilité et par conséquent une source potentielle de failles, d'erreurs ou de sécurité.

Les travaux de Goudalo [Goudalo, 2011] ont défini la sécurité des systèmes d'information des entreprises et des organisations, comme étant :

[5] *Les appareils, les terminaux, les systèmes et les serveurs cibles.*

[6] *BYOD - Bring Your Own Device (apportez vos appareils personnels), tendance de plus en plus fréquente.*

[7] *Dispositifs permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur.*

- Une démarche globale qui met en œuvre tout ce qui est nécessaire pour protéger les biens des entreprises et des organisations et leur fonctionnement, et pour les accompagner à répondre efficacement aux enjeux auxquels elles (les entreprises et les organisations) sont confrontées.
- Une gestion harmonisée des risques qui pourraient advenir à tout moment pendant le cycle de vie des projets, que ces risques soient aussi bien accidentels qu'intentionnels, et aussi bien internes (endogènes) qu'externes (exogènes).
- Une science transversale qui s'intègre dans le fonctionnement et la structure traditionnels des entreprises et organisations et y amène un raffinement qui permet d'assurer la productivité et qui accompagne dans la création de valeur (augmentation de valeur).
- Un projet « vivant » qui couvre toute l'entreprise (dans un repère Espace/Interactivité, Productivité et Temps) et qui nécessite la participation de tous les acteurs de l'entreprise où elle est appliquée, ainsi que des spécialistes aussi bien pointus en expertise sécurité, en management et communication, et des spécialistes à compétences transverses couvrant différents domaines.

Malgré tout cela, la sécurité zéro risque n'existe, quelles que soient les solutions de sécurité mises en œuvre et quel que soit le niveau d'utilisabilité qu'elles présentent. Un risque pourra survenir. En cas d'occurrence du risque, il serait judicieux d'avoir la capacité de restaurer un état de service convenable sans grands préjudices.

Dans les travaux actuels, nous nous proposons :

- d'étendre le concept de la sécurité avec les apports de l'utilisabilité et de la résilience
- de traiter les trois concepts de façon conjointe dans l'ingénierie avancée de la sécurité des systèmes d'information.

# Chapitre 3 : Fondations préalables à notre méthodologie d'ingénierie avancée

La méthodologie d'ingénierie ICSUR devant opérer sur la sécurité, l'utilisabilité et la résilience de façon conjointe, ce chapitre présente les fondamentaux sur ces trois notions et leurs métriques respectives. Ce chapitre présente également une analyse critique sous l'angle d'approches conjointes à ces trois notions (sécurité, utilisabilité et résilience) et une synthèse sur les systèmes sociotechniques. Nous terminons ce chapitre avec une conclusion qui sert de transition sur la contribution de cette thèse.

## 3.1. Fondements et Métriques de la sécurité des systèmes d'information

Dans cette section, nous présentons les principales propriétés de la sécurité et les indicateurs de mesure de sa qualité.

### 3.1.1 Les principes fondamentaux de la sécurité – les trois critères invariants de la sécurité

Les besoins de sécurité sont exprimés au travers des principes fondamentaux de la sécurité que nous désignons aussi par les trois critères invariants [Goudalo et Seret, 2008]. Nous en proposons une synthèse, ci-dessous.

- Confidentialité : L'information ne doit être, ni rendue accessible, ni divulguée, à un utilisateur, une entité ou un processus non autorisé. La confidentialité est la mesure du secret.
- Intégrité : L'information ne doit être modifiée, altérée ou détruite de manière non autorisée. L'intégrité garantit que l'information est exacte et fiable.
- Disponibilité : l'accès, par une entité, un utilisateur ou un processus autorisé, aux services offerts par le système, doit toujours être possible. Les opérations destinées à occuper illégalement du temps et des ressources de traitement doivent être détectées. La disponibilité

garantit que les informations et les services sont disponibles en temps et en heure suivant les SLA[8].

A ces derniers, sont rajoutés différents attributs et propriétés de sécurité tels que preuve, trace, non-répudiation (NP), identification, authentification que nous suggérons de rassembler pour assurer le concept de l'imputabilité [ISO/CEI 27000, 2016], [Fayon et Tartar, 2014].

Les critères de sécurité caractérisent les contraintes ou propriétés sur les actifs d'entreprise, décrivant leurs besoins de sécurité. Les enjeux d'entreprise peuvent être d'ordres humain, financier, image de marque, règlementaire et légal. La cotation des actifs d'entreprise sont définis, par rapport aux enjeux de l'entreprise, suivant les critères de sécurité. La Figure 2.8 illustre le principe de cotation des actifs d'entreprise.

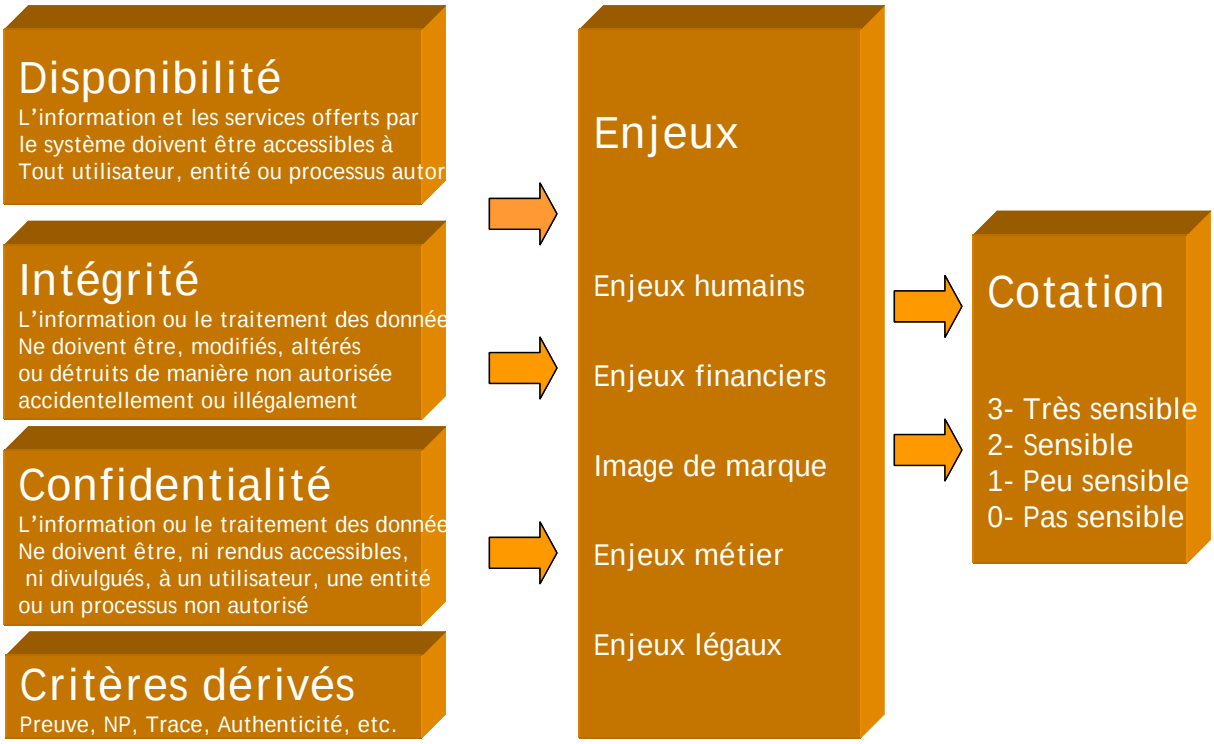


**Figure 3.1** : Cotation des actifs de l'entreprise – critères de sécurité

*In fine*, le résultat de la cotation d'un actif peut varier de « Pas sensible », jusqu'à « Très sensible ». Pour passer du niveau le plus banal au niveau le plus critique, nous représentons les différentes valeurs sur quatre niveaux.

[8] *Désignation usuelle des contrats de niveau de service, SLA - Service Level Agreement*

A titre d'illustration des sciences sous-jacentes à la sécurité et à ses propriétés, nous proposons d'approfondir l'un des trois critères invariants, le cas du critère de confidentialité.

### 3.1.2 Le critère de confidentialité

Dans cette section, nous indiquons les aspects scientifiques et formels sous-jacents au critère de confidentialité. Les outils mathématiques, informatiques et de télécommunication que nous utilisons encapsulent ces théories et principes scientifiques.

#### 3.1.2.1 Définition et concept général

Dans les systèmes d'information des entreprises et des organisations, d'une part il est géré, traité et stocké des données classées à différents niveaux de confidentialité. D'autre part il est nécessaire d'assurer la confidentialité de ces données vis-à-vis des utilisateurs ayant différents niveaux d'habilitation, différents niveaux de fonction et différents niveaux de compétence. Il s'agit du contexte de sécurité multi-niveaux.

Pour répondre à cette problématique, nous distinguons deux catégories de politiques de sécurité : les politiques de contrôle d'accès discrétionnaire (*discretionnary access control*) et les politiques de contrôle d'accès obligatoire (*mandatory access control*). Dans une politique de sécurité discrétionnaire, il existe pour chaque objet, une autorité qui décide au cas par cas (à discrétion) des droits d'accès (lecture, écriture, exécution, destruction et autres) de chaque sujet sur chaque objet. Elle est basée sur l'identité de chaque usager. Dans une telle politique, chaque sujet a, en plus de ses droits d'accès aux objets, le droit de transmettre ses droits comme il l'entend à d'autres utilisateurs du SI. Par contre, dans une politique de contrôle d'accès obligatoire, les droits de transmission n'existent pas. Les politiques de contrôle d'accès obligatoire sont basées sur des règles, où l'accès à un objet par un sujet n'est possible que si certaines règles sont vérifiées. Généralement, ces règles s'appuient sur une comparaison des attributs de sécurité des objets et des sujets. Une politique de contrôle d'accès discrétionnaire est souvent insuffisante car la sécurité du SI ne peut pas reposer seulement sur la confiance portée aux usagers.

Comme il est synthétisé dans le travail de Frédéric Cuppens [Cuppens, 1997], les notions d'objet et de sujet sont généralement introduites dans la définition de la politique de sécurité de SI. Un objet correspond à une entité passive qui contient ou qui reçoit de l'information. L'accès à un objet implique l'accès à l'information qu'il contient. Toute entité du SI peut être vue

comme un objet, tout dépend du niveau de détail de l'étude. Un bit, un octet, une structure, un fichier (exécutable ou non), un répertoire, un n-uplet d'une relation de base de données relationnelle, toute une base de données ou tout un disque pourront être vus comme un objet.

Un sujet correspond à une entité active du SI qui provoque un flux d'information d'un objet vers un autre ou qui change l'état courant du système. Il peut s'agir d'un utilisateur et d'un processus agissant pour le compte d'un utilisateur.

Les règles en vigueur pour tous les documents du département américain de la défense (DOD), connues sous les noms de « *Military Security Policy* » (politique de sécurité militaire) et « *Multi Level Security Policy* » (politique de Sécurité Multi Niveaux), spécifient que tout objet possède une classe de sécurité (classification) et que tout sujet possède un niveau d'autorisation (confiance) [DOD, 1983]. Les classes de sécurité et les niveaux d'autorisation sont des entités de même nature qui sont composées de deux éléments :

- un niveau de sensibilité appartenant à une échelle, donc un ensemble totalement ordonné ; par exemple, « Public, Diffusion Restreinte, Confidentiel, Secret » ou bien « Non-Classifié, Confidentiel, Secret, Top-Secret »
- et un ensemble de domaines (ou *compartiments* en anglais), comme OTAN, Nucléaire, Finance. Cet ensemble peut être vide. Les domaines sont indépendants les uns des autres et peuvent être munis d'une relation d'ordre partiel.

La classe de sécurité et le niveau d'autorisation sont définis comme un couple (s, c), où s - est le niveau de sensibilité et c - est un ensemble de domaines. L'ensemble de ces couples est muni d'une relation d'ordre partiel, appelée « DOMINER ».

Un exemple d'expression de propriété de confidentialité pourrait se présenter comme suit : « un sujet ne peut connaître l'information contenue dans un objet que si l'habilitation de ce sujet ‘’domine’’ le niveau de classification de l'objet ».

En réalité, un bon modèle doit être simple et facile à comprendre [Gasser, 1988]. On considère le plus souvent que les modèles complexes qui se perdent souvent dans trop de détails ne sont point exploitables. Pour des raisons d'efficacité, nous synthétisons, ci-dessous, des visions simples des différents modèles de confidentialité.

#### 3.1.2.2 Le Modèle de confidentialité dit à matrice d'accès (modèle HRU)

La première version de ce modèle a été donnée en 1971 par B. W. Lampson et publié plus tard en 1974 [Lampson, 1974]. En 1975, elle a été complétée par Harrison, Ruzzo et Ullman [Harrizon et al., 1976], d'où l'appellation modèle HRU.

Suivant le modèle HRU, le SI est constitué de deux composants : un ensemble d'objets et un ensemble de sujets les manipulant (voir définition dans la section précédente, §2.4.2.1 - Définition et concept général). Chaque sujet peut être vu comme un objet, car il pourrait être manipulé par un autre sujet (par exemple un processus peut exécuter un autre processus).

Le modèle est constitué d'une matrice d'accès, comme un tableau à deux dimensions dont une ligne par sujet et une colonne par objet et sujet. A chaque intersection, les modes d'accès entre le sujet et l'objet (ou sujet) correspondant sont précisés. Les droits d'accès les plus fréquemment rencontrés sont : Propriétaire, Lecture, Ajout, Ecriture, Exécution, Contrôle.

Le contenu de la matrice à un instant donné représente l'état du système à cet instant. Il existe un ensemble fini de règles qui spécifient dans quelles conditions on peut modifier le contenu de la matrice et passer ainsi à un nouvel état du SI. Ces règles se traduisent par un ensemble de fonctions de transformation qui sont constituées de primitives. Dans le travail de référence [Harrizon et al., 1976], six primitives sont proposées :

- Donner un droit r à un sujet s sur un objet o,
- Oter un droit r à un sujet s sur un objet o,
- Créer un sujet s,
- Créer un objet o,
- Détruire un sujet s,
- Détruire un objet o.

Les fonctions de transformation, autorisées dans le SI, sont formées par un enchaînement de ces six primitives en fonction des règles précisées.

La forme générale d'une fonction de transformation est la suivante :

NomFonction (listeSujets, listeObjets)

SI // Ensemble des conditions à remplir

ALORS // Liste des primitives

FIN

Une règle spécifiant que le propriétaire d'un objet peut accorder des droits en lecture sur cet objet, ferait créer la fonction de transformation suivante :

AccorderLecture (S1, S2, O)

SI S1 a le droit « Propriétaire » sur O

ALORS Donner le droit « Lecture » à S2 sur O

FIN

Ce modèle permet de décrire de façon simple les règles régissant l'accès aux objets par les sujets.

Par rapprochement à l'Ingénierie des SI, de ce modèle nous mettons en évidence les notions suivantes :

- les notions d'état du SI et de changement d'états,
- les notions d'actions concrètes sur un objet identifié et la notion de succession d'actions,
- les notions de règles, de condition d'exécution sur les actions et de contraintes sur les fonctions de transformation.

#### 3.1.2.3 Le modèle de Bell et La Padula

Ce modèle de référence a été proposé en 1973 par Bell et La Padula [Bell et La Padula, 1973] [Bell et La Padula, 1975]. Pour Bell et La Padula, le SI est constitué d'objets et de sujets (voir définition plus haut, cf. § 3.1.2.1 et §3.1.2.2). Ce modèle est basé sur le contrôle d'accès, muni d'une fonction de transformation. Trop contraignant à mettre en application dans un système réel, le modèle BLP nécessite un assouplissement, allant jusqu'à la notion de sujet digne de confiance.

Le modèle BLP est composé de :

- le contrôle d'accès discrétionnaire,
- le contrôle d'accès obligatoire,
- le et de règles de transformation.

*Dans le contrôle d'accès discrétionnaire* : Une matrice d'accès (sujet, objet) est définie. Les types de droits possibles sont semblables à ceux cités pour le modèle HRU.

*Le contrôle d'accès obligatoire* est affecté à chaque sujet et à chaque objet un niveau de sensibilité et un ensemble de domaine (voir définition plus haut, cf. § 2.4.2.1). L'accès par un sujet à un objet est possible si les règles suivantes sont respectées :

- Un sujet a accès en lecture à un objet si la classe de sécurité du sujet domine (est supérieure ou égale) à celle de l'objet. C'est la condition *Read-Down* ou *No-Read-Up* (Condition de Sécurité simple)
- Un sujet a accès en ajout à un objet si la classe de sécurité de l'objet domine celle du sujet. C'est la condition *Write-Up* ou *No-Write-Down*

L'ensemble de ces deux conditions vérifiées dans un SI lui confère la propriété de confinement, encore appelée *star property* (propriété étoile). Donc, un sujet a accès à un objet en écriture et en lecture si les classes de sécurité de l'objet et du sujet sont les mêmes. Cette condition est trop contraignante pour être exploitée dans un système réel. Dans la littérature, BLP ne précise aucune condition concernant l'accès en exécution.

Un ensemble de *fonctions de transformation* permet de passer d'un état sécurisé à un autre sécurisé (par modification de la matrice d'accès et/ou une classe de sécurité d'un sujet). Les fonctions définies par BLP sont :

- initialisation du type d'accès entre un sujet et un objet (*get*),
- suppression d'un droit d'un sujet sur un objet (*release*),
- suppression par le propriétaire d'un droit qu'il a transmis à un autre sujet (*rescind*),
- activation d'un objet (*create*),
- désactivation d'un objet (*delete*).

Bell et La Padula précisent que chacune de ces fonctions doit respecter la propriété de sécurité simple et la propriété de confinement. Ainsi elles assurent une transition vers un état sûr.

Il est également introduit le principe de tranquillité, suivant lequel aucune fonction de transformation ne permet de modifier la classe d'un objet.

La création d'un objet se fait en deux temps : dans un premier temps l'ajout du nouvel objet dans l'ensemble des objets, et dans un second temps l'activation de l'objet. Lorsqu'un objet est créé, sa classe de sécurité est initialisée à celle du sujet qui l'a créé.

**Assouplissement du modèle BLP.**

Un assouplissement au modèle BLP rend possible le transfert d'information entre deux sujets de différentes classes. La propriété étoile interdit à un sujet d'une classe donnée de transmettre de l'information à des sujets de classes inférieures. Pour répondre à un besoin réel et fréquent de la gestion des SI, il a été introduit la notion de « déclassification » qui permet à un sujet de diminuer son niveau de sensibilité jusqu'au niveau inférieur nécessaire pour réaliser le dialogue avec des sujets de classes inférieures. Cela est assuré par la fonction de transformation : modification par un sujet de son propre niveau de sécurité courant (fonction « change »).

*Notion de sujet digne de confiance.* Pour la raison précédemment indiquée, le modèle BLP, dans l'état, est trop contraignant pour être mis en œuvre. Bell et La Padula ont introduit la notion de sujet digne de confiance. Ces sujets sont autorisés à faire des accès aux objets, violant la propriété étoile. Un sujet digne de confiance peut faire ce qu'il veut dans le SI sous réserve que les propriétaires des objets lui aient conféré les droits d'accès qui conviennent.

La véritable vulnérabilité du modèle BLP est liée au problème de canaux cachés. Les tentatives de solutions au problème de transmission illicite d'information sont apportées par les modèles de contrôle des flux d'information.

#### 3.1.2.4 Le modèle de contrôle de flux d'information

Le principe des modèles de contrôle de flux est fondé sur l'analyse des dépendances entre les objets au cours du temps. Les modèles de contrôle de flux permettent de définir à quelles conditions l'observation effectuée par un sujet est autorisée ou non. Les travaux de Cuppens [Cuppens, 1993] regroupent les modèles de contrôle de flux selon deux tendances :

- les modèles de causalité, suivant lesquels un sujet public ne peut observer un objet que si la valeur de cet objet est déterminée par des objets publics. Il s'agit d'un raisonnement sur les permissions explicites. Frederic Cuppens y introduit la notion de temps, prenant en compte les transmissions indirectes d'informations par construction de canaux cachés temporels.
- Les modèles de non-inférence et de non-déduction, suivant lesquels un sujet public ne peut observer un objet que si la valeur de cet objet n'est pas déterminée par des objets de niveau de sensibilité plus élevé. Il s'agit d'un raisonnement sur les interdictions explicites.

### 3.1.3 Métriques et Indicateurs de suivi de la sécurité

Nous définissons les indicateurs de suivi de la sécurité, en introduisant la notion de qualité de sécurité. Selon une première approche, la qualité est assimilée à l'ensemble des exigences fonctionnelles et non fonctionnelles [Bernardez, 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 sécurité, nous utilisons une décomposition de la qualité sous la forme de modèle de qualité. Un méta-modèle associé à la qualité de sécurité est présenté dans la Figure 3.2.

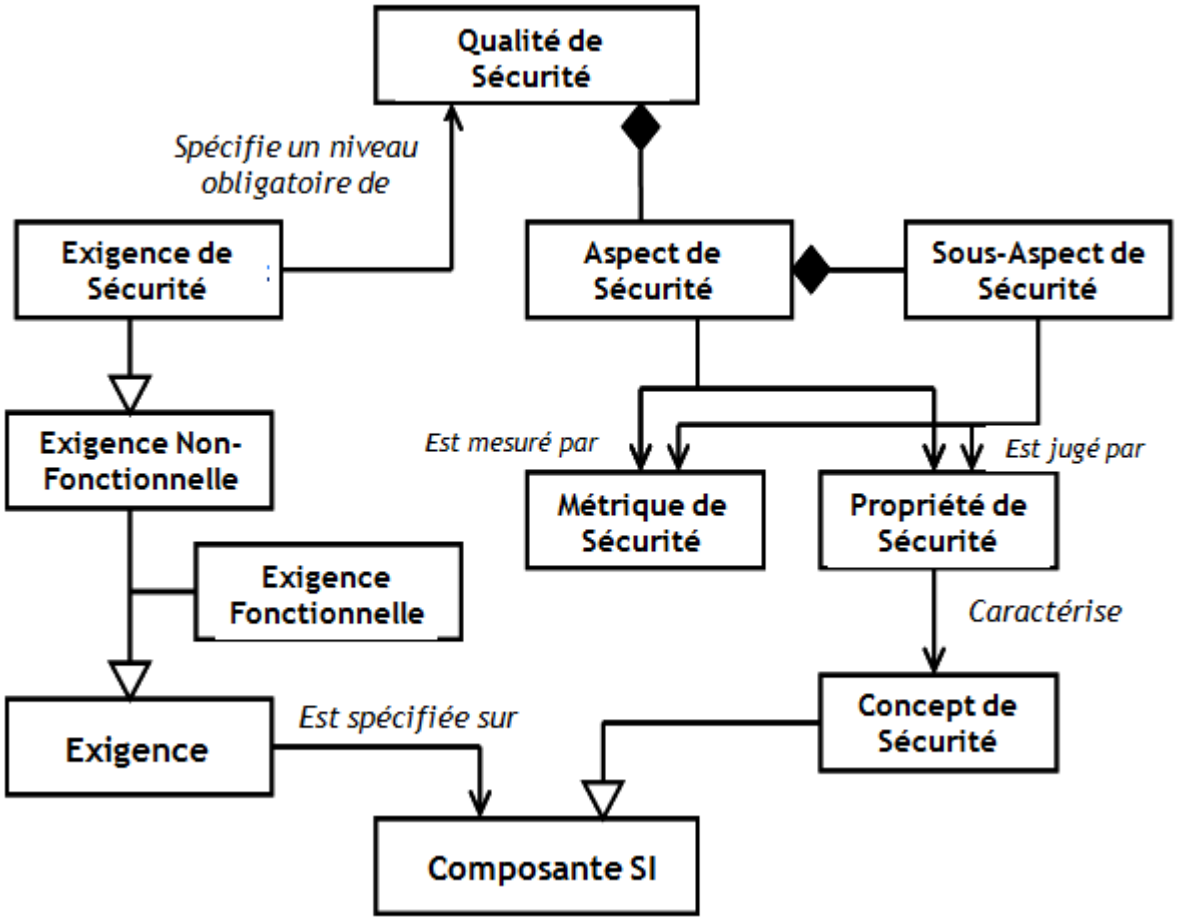


**Figure 3.2** : Méta-modèle de la qualité de sécurité (inspiré de [Goudalo & Seret, 2009])

Dans le cadre de travaux précédents (sur l'extension d'UML avec des profils de sécurité [Goudalo & Seret, 2008]), 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).

Nous avons ressorti principalement 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 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 La Padula [Bell et La Padula, 1975] et repris dans les travaux de Frederic Cuppens [Cuppens, 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 : « 0 », « 1 », « 2 » ou « 3 », quel que soit le critère choisi (sensibilité, confiance ou efficacité). Quelques exemples sont fournis ci-dessous :

- Un système de contrôle d'accès avec badges biométriques, dans la mesure où il est bien géré, un tel système 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 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). *Nota Bene* : Nous précisons qu'il s'agit d'un cas bien maîtrisé qui ne peut survenir par hasard dans une vraie entreprise. Ce cas a juste servi d'illustration.

Nous étendrons ce même principe de système métrique des indicateurs de suivi de la sécurité pour notre proposition d'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience (§3.3.4 - Système de métriques homogènes).

Les cadres de sécurité des systèmes d'information sont bien formalisées et documentées ([ISO 27032, 2012], [ISO 2700x, 2010] et [EBIOS, 2016]), par-dessus des considérations mathématiques inhérentes aux propriétés fondamentales de la sécurité ([Cuppens, 1997], [Harrizon et al., 1976] et [Bell D.E.et La Padula, 1975]). Cela explique, en partie, pourquoi les projets de sécurité sont souvent bien réussis en soit, et ils ne laissent pas de doutes sur l'avènement des problèmes énormes. Mais la réalité est que les systèmes d'information des entreprises et des organisations sont composés de services techniques et de services fonctionnels qui sont orchestrés pour faire fonctionner les processus métier avec des interventions humaines. La sécurité des systèmes d'information devrait adresser chacune de ces briques en particulier et leurs fonctionnements ensemble pour répondre aux exigences des entreprises et des organisations. Aussi bien au niveau de chaque brique (et des infrastructures logicielles et matérielles qui l'ont composée, de même que l'organisation autour) qu'au niveau du fonctionnement des briques ensemble, afin d'assurer la confidentialité, l'intégrité et la disponibilité sur les informations et les traitements du SI.

Les démarches de mise en application des cadres de gouvernance des systèmes d'information devraient s'étendre sur la problématique de la sécurité SI. Sans vouloir faire une extrapolation, les cadres de gouvernance d'entreprise devraient aussi intégrer les risques de sécurité des systèmes d'information. Ainsi il apparaîtrait clairement que la sécurité des systèmes d'information des entreprises et organisations ne peut plus être traitée dans un silo. Il faudrait considérer l'ensemble du contexte technologique, socio-économique et concurrentiel dans lequel opère l'entreprise ou l'organisation. Quoiqu'il en soit la technologie devrait soutenir les stratégies et objectifs d'entreprise, l'organisation et les personnes devraient être prises en compte à travers l'ingénierie de l'utilisabilité (qui sera abordée en section 3.3). En cas de péril ou perturbation, l'ingénierie de la résilience (qui sera abordée en section 3.2) devrait garantir le respect et la satisfaction des exigences de qualité de services.

## 3.2. Fondements et Métriques de la Résilience des systèmes d'information

Dans cette section, nous présentons les principales caractéristiques de la résilience et les indicateurs de mesure de sa qualité.

### 3.2.1 Fondements et concepts de la 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, 2016]. En rapport à la préoccupation de l'accident [Hollnagel, 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 » [Ruault et al., 2009], [Manciaux et al., 2001].

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 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 Encyclopedia of Philosophy, 2016]. Nous inspirant de Laprie [Laprie, 2008], nous conclurions 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, …). Un système résilient doit être doté des fonctions de résilience.

### 3.2.2 Fonctions de résilience

Luzeaux 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) » [Luzeaux, 2011].

Woods [Woods, 2015] a défini quatre principaux axes sous le concept de la résilience :

- rebond (suite à 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 a indiqué avoir défini ces quatre concepts en vue d'une ingénierie éventuelle de la résilience dans les systèmes et réseaux dans le futur.

Les travaux de thèse de Jean-René Ruault portent sur la résilience et ses fonctions, tout en proposant une architecture, ainsi qu'un processus à mettre en œuvre pour contribuer à la résilience (dans le cas d'un système critique à longue durée de vie) [Ruault, 2015].

### 3.2.3 Métriques de la résilience

Khan et ses collègues [Khan et al., 2015] ont identifié trois catégories de métriques de la résilience qui sont de nature *Proactive, Résistive et Réactive* respectivement. La première catégorie mesure la résilience des systèmes d'information de façon proactive. Se basant sur les informations disponibles au sujet des scénarios d'attaques possibles et des capacités des attaquants, les systèmes d'information peuvent être résilients de façon proactive, d'une telle sorte que les attaques ne puissent causer aucun dommage. Selon les auteurs, la résilience proactive est habituellement obtenue par la tromperie et la dissuasion. La deuxième catégorie de métriques se réfère à la capacité des systèmes d'information à résister à une attaque en cours. La troisième catégorie de métriques se réfère aux situations dans lesquelles l'attaque ou le dommage est déjà causé, ainsi l'objectif se recentre sur les services devant être fournis par le système d'information. Les auteurs ont proposé un cadre de l'ingénierie de la cyber-résilience qui prend en compte quatre concepts : le modèle représentatif d'un réseau logique ou physique ; les attaques et propriétés caractérisant le réseau ; les métriques de résilience pour mesurer la résilience du réseau de façon proactive, résistive et réactive ; l'axe de résilience pour indexer la capacité du modèle de réseau à résister aux attaques ou aux propriétés. Le quatrième concept est la valeur résultante du calcul, dont les trois premiers concepts sont les entrées.

Ouedraogo et ses collègues [Ouedraogo et al., 2013] ont travaillé sur les métriques de la résilience, en proposant une architecture fonctionnelle d'apprentissage à partir des indicateurs de résilience et leurs évolutions. Les auteurs présentent différentes mesures de la résilience au regard des niveaux de services rendus et au regard des délais de recouvrement suite à chaque perturbation. Les auteurs ont également rappelé les travaux de Wang et de ses collègues [Wang et al., 2010] spécifiques aux systèmes d'information, prenant en compte l'importance de chaque fonction assurée par le système d'information, la durée de recouvrement prévue dans les exigences de QoS (*Quality of Services*) au regard de la durée réellement nécessaire pour recouvrer chaque fonction. Ouedraogo et ses collègues ont rappelé aussi les travaux de Pérez-Espana et Sanchez [Pérez-Espana et Sanchez, 2001] sur la résilience des systèmes écologiques et qui portent sur l'opposé de la tangente du rapport entre la résistance et le temps de récupération d'une perturbation.

De cela, que dirait-on de la résilience d'un système qui a subi un évènement perturbateur et qui s'est vite recouvré pour fournir les services avec respect des termes de qualité de services, par

rapport à un système qui a subi un grand nombre d'évènements perturbateurs et qui s'est comporté aussi bien que le précédent système affecté par un seul évènement, fournissant les services avec respect des termes de qualité de services (QoS) ? Quelle réponse aurait-on donnée si le deuxième système s'était recouvré plus lentement que le premier ou s'il n'avait pu se recouvrer à temps afin d'honorer ses exigences à fournir les services avec respect des termes de QoS ? Le débat au sujet des métriques de la résilience porterait-il sur le volet nombre d'évènements perturbateurs ou bien sur le volet respect des exigences de QoS ? Dans le cadre du domaine cyber, plus spécialement les systèmes d'information des entreprises et organisations pour ce qui nous concerne, la recherche et les métriques de la résilience devraient être portées à minima sur les deux volets de façon simultanée. Il serait plus objectif, plutôt réaliste, de considérer à la fois, les évènements perturbateurs (leurs natures, nombres, intensités, fréquences, période de continuité), la vitesse de recouvrement, les impacts sur les exigences de QoS. Voilà l'une de nos motivations à traiter la résilience et la sécurité de façon conjointe dans les systèmes d'information des entreprises et organisations. Nous revenons plus en détail sur ces aspects dans le chapitre de proposition (analyse conjointe, section 4.3 du chapitre suivant).

## 3.3. Fondements et Métriques de l'Utilisabilité dans les systèmes d'information

Dans cette section, nous présentons les principales caractéristiques de l'utilisabilité et les indicateurs de mesure de sa qualité.

### 3.3.1 Fondements de l'Utilisabilité

L'utilisabilité est clairement définie par la norme ISO 9241-11 [ISO 9241-11, 1998] 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 [ISO 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, les versions plus récentes de la norme ([ISO/IEC FDIS

9126-1, 2000], [ISO/IEC 25000, 2014]) décrivent 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. Mais qu'en est-il des phases amont du produit (telles que la conception et la mise en œuvre) ? Cette absence de réponse sur les phases amont constitue des champs que doit explorer l'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience (cf. chapitre 4).

### 3.3.2 Des catégories de l'utilisabilité

Nigel Bevan [Bevan, 2001] a revu les définitions de l'utilisabilité en rappelant comment les standards sont élaborés. Dans ses travaux, l'auteur a pris en compte des standards relatifs à l'utilisation en contexte, à l'interface et l'interaction de logiciel, à l'interface de matériel, à la documentation, au processus de développement, à la capabilité organisationnelle au sujet de l'utilisabilité, et bien d'autres standards connexes comme sur l'ergonomie, l'accessibilité et le conseil sur les exigences de tâche. L'auteur a décrit les standards de l'utilisabilité et de l'IHM en quatre catégories : la catégorie de l'utilisation du produit, du système ou du service (efficacité, efficience, satisfaction de l'utilisateur dans un contexte particulier d'utilisation), telle la qualité de l'utilisation ; celle de l'interface utilisateur et interaction avec le produit, du système ou du service, telle la qualité de l'objet lui-même ; celle du processus utilisé pour développer le produit, du système ou du service, telle la qualité du processus de développement ; et enfin la catégorie de la capacité d'une organisation à mettre en œuvre une conception centrée utilisateur, telle la capabilité organisationnelle.

### 3.3.3 Métriques de l'utilisabilité

Le rapport technique adossé à la norme ISO 9126 [ISO/IEC DTR 9126-4, 2001] contient des exemples de métriques pour l'efficacité, l'efficience (productivité / sûreté) et la satisfaction. La conception orienté utilisateur se réfère non seulement aux spécifications des exigences de l'utilisabilité, mais aussi à la vérification du respect des exigences à travers des tests d'utilisabilité. Les résultats des tests d'utilisabilité peuvent être documentés en utilisant le format industriel commun pour les rapports de tests d'utilisabilité.

Se basant sur les normes ISO 9241-11 [ISO 9241-11, 1998], Macleod et ses collègues ont proposé la méthode MUSiC [Macleod et al., 1997], pour mesurer l'utilisabilité. Cette méthode est organisée en huit activités : Définir le produit à tester ; Définir le contexte d'utilisation ; Spécifier les conditions d'utilisabilité ; Préciser le contexte de l'évaluation ; Concevoir une évaluation ; Effectuer les tests utilisateur et recueillir des données ; Analyser et interpréter les données ; Produire un rapport d'utilisabilité. Dans leurs travaux [Seffah et al., 2006], Seffah et ses collègues revisitent les différents modèles, méthodes et standards existants, puis proposent le modèle consolidé QUIM (*Quality in Use Integrated Measurement* - Mesure intégrée de la qualité). Ce dernier opère sur 10 facteurs d'utilisabilité décomposés en un total de 26 critères mesurables qui sont eux-mêmes décomposés en 127 paramètres spécifiques. James Lewis, dans [Lewis, 2014], a présenté les controverses et les principales orientations des recherches scientifiques sur l'utilisabilité ; il a indiqué que l'utilisabilité a des racines récentes dans la psychologie expérimentale, la mesure et les statistiques, et qu'elle s'étend notamment vers la conception centrée utilisateur et l'expérience utilisateur.

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.

En somme, le principal objectif de l'utilisabilité est que le produit (système ou service) soit efficace, efficient et satisfaisant pendant l'utilisation dans les contextes prévus. Une condition préalable à cela est que l'interface et l'interaction soient appropriées. Cela requiert un processus de conception centré utilisateur qui, pour être atteint de manière cohérente, requiert une capabilité organisationnelle à supporter une conception centrée utilisateur. Notre contribution

à l'ingénierie conjointe de la sécurité sous-tend cette capabilité organisationnelle (voir la section 4.3.1 - Eléments d'Analyse conjointe de la sécurité, de la résilience et de l'utilisabilité, dans le chapitre suivant).

## 3.4. Analyse critique sous l'angle d'approches conjointes

Dans les sections précédentes (3.1, 3.2 et 3.3), nous avons présenté l'état de l'art des concepts de la résilience, de l'utilisabilité, de la sécurité, des indicateurs de suivi pour ces trois domaines (notions). Dans la section 2.3, nous avons présenté les cadres de la sécurité des systèmes d'information. Les travaux sont généralement centrés sur un domaine ; il nous semble donc important d'effectuer une étude critique sous l'angle d'approches conjointes qui opèrent sur plusieurs domaines à la fois.

A ce sujet, le livre de Clarke et Furnell [Clarke & Furnel, 2014] présente 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-Cambacedes [Piètre-Cambacèdés, 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, pour traiter les compromis fondamentaux entre robustesse, résilience et sécurité des systèmes [Zhu et Basar, 2015]. Dans [Giani et *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. Grâce à cela, les chercheurs déterminent 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 réaliste 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 cyber terrorisme dans un délai allant 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 cyber sécurité rentre dans le dispositif de la loi de programmation militaire [ANSSI, 2016]. Au-delà d'Ebios ([EBIOS, 2016], [ANSSI, 2017c]), 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.

A 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.

Avant de conclure ce chapitre sur l'état de l'art, nous présentons dans la section suivante le concept des systèmes sociotechniques que nous avons utilisé de façon essentielle dans l'élaboration de notre ingénierie avancée de la sécurité.

## 3.5. Systèmes sociotechniques

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]. Dan Sperber et Deidre 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 cybernétiques.

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. 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, 2014].

## 3.6. Synthèse et conclusion du chapitre

Nous sommes à une croisée des chemins où plusieurs cadres, référentiels, normes et bonnes pratiques devraient pouvoir être combinés dans un but de contribuer à en tirer meilleur avantage pour l'ingénierie avancée de la sécurité des systèmes d'information. En effet, les différents

points que nous avons évoqués dans ce chapitre constituent les fragments de méthodes, cadres et référentiels qu'il s'agit de rassembler pour élaborer notre méthodologie d'ingénierie avancée de la sécurité des systèmes d'information. Notre proposition vise à traiter conjointement la sécurité, l'utilisabilité et la résilience.

L'ingénierie logicielle et l'ingénierie des systèmes d'information des entreprises et organisations ont bien évolué depuis quelques décennies et sont soutenues par des démarches méthodologiques éprouvées et des outillages. Nous nous en inspirerons au mieux pour élaborer notre contribution et suggérer un dénouement au verrou scientifique que constitue aujourd'hui la cyber sécurité qui souffre d'un mal profond et qui y engendre des pertes énormes (enjeux financiers, image de marque, enjeux humains, enjeux métier, enjeux légaux et règlementaires).

La méthodologie d'ingénierie avancée de la sécurité que nous déployons dans les présents travaux de thèse est conçue sur le processus d'ingénierie des méthodes, comportant deux étapes principales : la ré-ingénierie des méthodes existantes sous forme modulaire et l'ingénierie des méthodes situationnelles par composition. Notre démarche est inspirée des travaux de Colette Rolland [Rolland, 2005] qui propose le cycle d'ingénierie des méthodes schématisé dans la Figure 3.3.

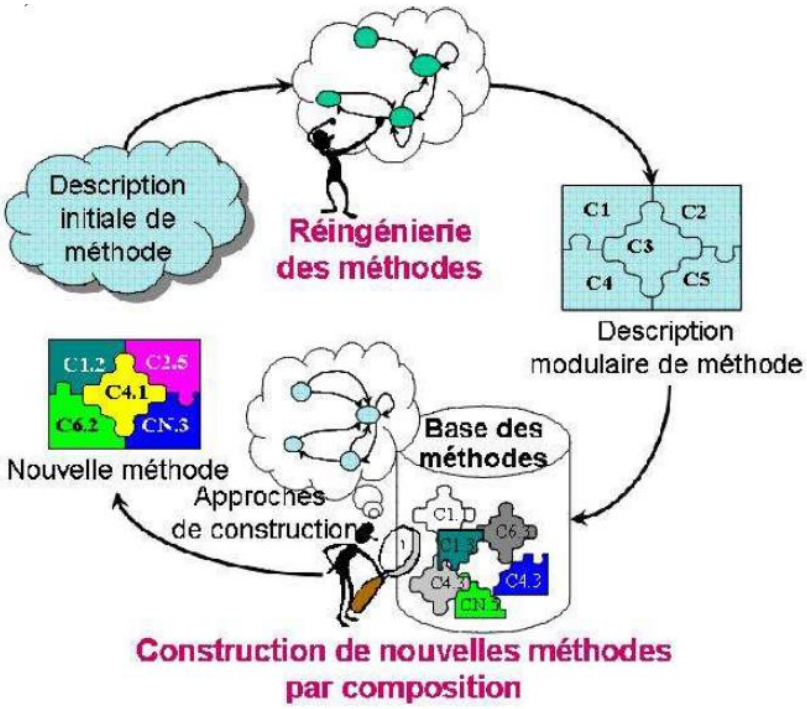


**Figure 3.3** : Cycle d'ingénierie des méthodes [Rolland, 2005]

Nous nous sommes donné comme challenge de définir une méthodologie d'ingénierie Avancée de la Sécurité des Systèmes d'Information, par combinaison et assemblage des :

- percées de l'ingénierie logicielle et de l'ingénierie des systèmes d'information,
- cadres et ingénierie de la sécurité ;
- cadres et ingénierie de l'utilisabilité ;
- cadres et ingénierie de la résilience ;
- retours d'expérience sur la réussite de grands projets stratégiques et sensibles pour les systèmes d'information des entreprises et organisation.

Les cadres de sécurité des systèmes d'information et nos connaissances heuristiques de la sécurité des entreprises et organisations constitueront les bonnes pratiques et les lignes directrices auxquelles nous appliquerons des fragments de méthodes provenant de divers cadres et ingénieries reconnus.

Dans la section suivante, nous suggérons notre méthodologie d'ingénierie avancée de la sécurité qui opère de manière conjointe sur la sécurité, l'utilisabilité et la résilience. La section d'analyse conjointe (4.3) exploite et étend l'état de l'art, 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 70, 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]. A la fin des années 80, les informaticiens travaillant dans le domaine de la conception orientée objet ont découvert les travaux effectués par Christopher Alexandre et les ont adaptés au génie logiciel [Gamma et *al.*, 1995] et [Salloway & Trott, 2002]. Schumacher [Schumacher, 2003] a fait valoir que l'ingénierie de la sécurité peut tirer bénéfice de l'utilisation des patterns, mais il ne parvint pas à présenter des patterns spécifiques pour atteindre cet objectif. Open Group a édité un livre sur les design patterns de la sécurité [Blakley, 2004], mais n'a pas adressé l'alignement entre la sécurité et l'utilisabilité. Parmi les nombreux chercheurs qui ont travaillé sur la conception de sécurité utilisable, Kai-Ping Yee [Yee, 2002] a proposé une liste de lignes directrices pour résoudre certains problèmes spécifiques dans la conception de sécurité utilisable : chemin de

moindre résistance, autorisation active, révocabilité, visibilité, conscience de soi, chemin de confiance, expressivité, limites pertinentes, identifiabilité et prévoyance.

Notre proposition de méthodologie d'ingénierie avancée de la sécurité est décrite dans le chapitre suivant.

# Chapitre 4 : Contribution à une méthodologie d'Ingénierie Conjointe de la Sécurité, de l'Utilisabilité et de la Résilience (ICSUR)

## 4.1. Introduction

De nombreux progrès sont réalisés en termes de sécurité des systèmes d'information, aussi bien dans la communauté académique que dans l'industrie. Les pratiques et normes internationales ont évolué. Cependant les problèmes de sécurité persistent et causent des incidents graves voire dangereux pour les individus, les entreprises et les organisations. 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 cadres méthodologiques d'ingénierie, et l'ingénierie de la sécurité devra s'améliorer dans un cycle vertueux. Plusieurs alternatives pourraient être explorées, afin de faire face à ce défi qui persiste malgré les travaux de recherche et les budgets colossaux déployés par les entreprises, les organisations et les Etats. Nous avons effectué le choix de développer une méthodologie d'ingénierie avancée qui vise à prendre en compte conjointement la sécurité, l'utilisabilité et la résilience. De nos jours, les activités de conception de produits (systèmes et services) devraient arbitrer constamment avec les principes de « time to market », l'immédiateté, la performance, la sécurité, la fiabilité, la robustesse, la flexibilité, l'adaptabilité, l'utilisabilité, le respect de la vie privée, la confidentialité, la traçabilité, l'imputabilité, la transparence, la conformité à diverses règlementations et lois, … (sans exhaustivité). Tout cela, afin de répondre aux préoccupations de toutes les parties prenantes. Cet objectif est pareil pour les activités des étapes en aval et en amont de la conception.

Pour répondre à ces réalités pragmatiques des entreprises et organisations, nous proposons une méthodologie d'ingénierie avancée, appelée ICSUR (Ingénierie Conjointe de la Sécurité, de l'Utilisabilité et de la Résilience). Celle-ci est basée sur des références de divers domaines.

- Les standards et les bonnes pratiques de la sécurité : [ISO/IEC 2700x, 2010], [ISO/IEC 27032, 2012], [ITSEC et ISO/IEC 15408, 2005], [ANSSI, 2016], [CLUSIF, 2016], [NIST, 2016], [ISACA, 2016].

- Les fondements de la sécurité : [Lampson, 1974], [Bell et La Padula, 1973], [Cuppens, 1997], [Goudalo & Seret, 2009], [EBIOS, 2016], [ISO/CEI 27000, 2016].
- Les fondements de l'utilisabilité ([ISO 9241-11, 1998], [Bevan, 2001], [Seffah et al., 2006], [ISO/IEC 25000, 2014], [Lewis, 2014], [Bevan et al., 2015].
- Les fondements de la résilience : [Laprie, 2008], [Luzeaux, 2011], [Palin, 2013], [Ouedraogo et al., 2013], [Ruault, 2015] [Woods, 2015], [Khan et al., 2015], [ReSIST, 2016].
- Les meilleures pratiques et retour d'expériences en architecture d'entreprise : [TOGAF 9.1, 2016], [Praxeme, 2016], [Ceisar, 2016].
- Les meilleures pratiques et retour d'expériences en ingénierie des Systèmes d'Information : ([McDavid, 1999], [Longépé, 2002], [Club Urba, 2003], [Zachman, 2003], [Rolland, 2005], [Brown, 2005], [Giraudin, 2007].

Notre méthodologie d'ingénierie avancée de la sécurité 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. Elle adresse principalement la sécurité, mais de façon conjointe avec l'utilisabilité et la résilience des systèmes d'information. Dans ce chapitre, nous proposons d'élaborer une approche systémique, de large couverture et innovante qui opère sur plusieurs 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. Nous suggérons trois contributions à travers lesquelles nous nous appuyons sur les paradigmes des systèmes sociotechniques, afin d'élaborer une ingénierie conjointe opérant, d'une part sur la sécurité, l'utilisabilité et la résilience des systèmes d'information, et d'autre part sur leurs corrélations réciproques.

Notre première contribution positionne les systèmes sociotechniques par rapport aux systèmes d'information bien connus. Grâce à ce nouveau modèle, les principales parties prenantes sont mises en évidence, de même que leurs responsabilités, leurs rôles, leurs centres d'intérêts, leurs relations mutuelles et leurs préoccupations. De façon plus explicite, nous analysons tout cela au regard des principaux enjeux et objectifs de l'entreprise ou de l'organisation concernée.

Notre deuxième contribution présente le développement du modèle conceptuel avancé qui soutient les paradigmes et les artéfacts mis en exergue grâce à l'approche des systèmes

sociotechniques. Tel un modèle avancé d'entité-relation et de datagramme, notre modèle conceptuel opère conjointement sur les principaux concepts d'actifs d'entreprise, de risques d'incidents, de solutions, de métriques. Grâce à cela, la moindre dissonance entre la valeur de l'actif, la catégorie de risque et la nature de la solution devrait être perceptible et traitée harmonieusement, dans une démarche d'amélioration continue.

Notre troisième contribution présente le développement de la démarche d'amélioration continue, telle une ingénierie avancée. Comme un « actigramme » en dichotomie avec le datagramme, il élabore les activités, les actions et les interactions conduisant à traiter la sécurité, la résilience et l'utilisabilité de façon conjointe. Nous recourons aux modèles de conception pour définir les résultats de notre troisième contribution ; ils sont basés sur les patrons de conception (design patterns).

## 4.2. Le positionnement du SST (Système Sociotechnique) dans la nouvelle industrie des services numériques, sous le regard de la sécurité et de l'expérience utilisateur

Dans cette section, nous suggérons de positionner les systèmes sociotechniques au regard des systèmes d'information des entreprises et organisations. Il apparaît que les systèmes sociotechniques comportent les concepts classiques des systèmes d'information, et en plus l'ensemble des environnements sociaux relatifs aux systèmes d'information concernés. Ces environnements sociaux comprennent à la fois les mondes cybernétiques et physiques.

### 4.2.1 Concepts de systèmes et approches sociotechniques

Les concepts essentiels de systèmes sociotechniques sont présentés dans la section 3.5 de l'état de l'art. Dans cette section, nous les appréhendons au regard des approches sociotechniques de la vie. Les propagations d'incidences entre le monde cyber et le monde physique sont prises en compte dans les environnements sociaux :

- Une querelle lors d'une rencontre entre deux personnes peut s'étendre tout de suite sur les réseaux sociaux aux vues et aux sus de milliers voire de millions de personnes en quelques minutes. Les clients et les employés mal considérés n'hésitent pas aujourd'hui à le faire savoir, plutôt certains peuvent avoir pour réflexe de chercher des ruses afin de

nuire dans le monde cyber (ternir l'image, perpétrer des tentatives d'intrusion ou de vandalisme dans les systèmes, vendre des informations sensibles).

- Des différends et des injures sur les réseaux sociaux (monde cyber) conduisent parfois les protagonistes à des rencontres pour des règlements de compte dans le monde physique.
- De même, nous assistons aujourd'hui à des milliers de cas de vrais mariages et construction de familles dans le monde physique, suite à des rencontres dans le monde cyber tels que les réseaux sociaux. C'est aussi le cas des embauches de collaborateurs (dans le monde physique), suite à des rencontres, échanges et discussions dans les forums, sur les réseaux sociaux (dans le monde cyber).

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 section suivante notre représentation du système sociotechnique.

### 4.2.2 Représentation de système sociotechnique et ses composantes

La section précédente a présenté le concept des systèmes et approches sociotechniques. 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 ou TI) 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 (ce qui nous sera utile dans la suite de cette thèse). La Figure 4.1 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.

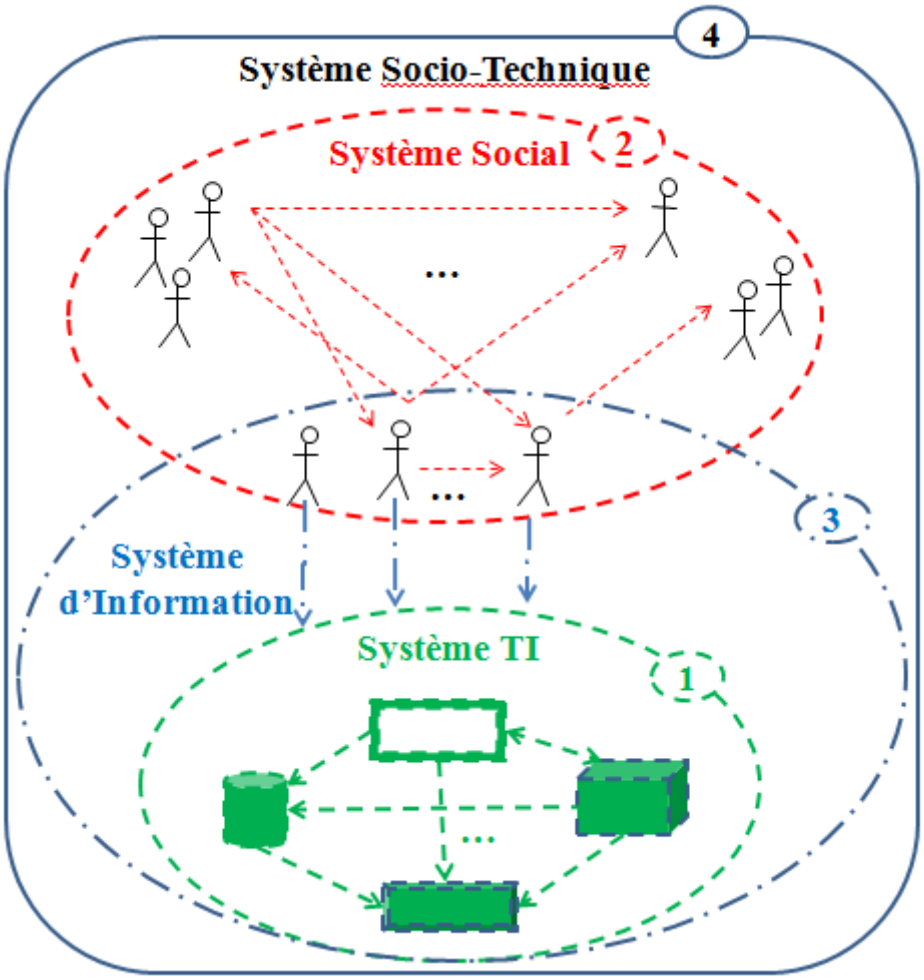


**Figure 4.1** : **Représentation de système sociotechnique [Goudalo & Kolski, 2016]**

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 les

informations sont accédées. Ainsi, par 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.

Ce défi scientifique tel un nœud complexe pourrait se dénouer 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.

### 4.2.3 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[9]. Dans le même temps, les utilisateurs adoptent un comportement ubiquitaire et présentent une volatilité élevée, avec les attentes insaisissables. Une véritable confiance pour une bonne expérience utilisateur s'avèrerait nécessaire pour le succès des systèmes sociotechniques, dans notre ère de l'industrie des services [IBM, 2014], [KPMG, 2014] et [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 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

[9] *Services de valeur - Services contribuant de façon essentielle à la chaîne de valeur (cf. Chaîne de valeur [Porter, 1986] et [Chaptal de Chanteloup, 2015]).*

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 [Sasse, 2007], l'expérience utilisateur prend en compte tous les critères d'utilisabilité avec des facteurs additionnels [Cranor & Blase, 2015]. Birge souligne le manque de recherche sur la conception de solutions techniques pour la communication et pour les technologies de l'information dans le domaine de "l'expérience utilisateur et la confiance" (Trust and User eXperience - TUX) [Birge, 2009]. Dans [Tullis et Albert, 2013], les auteurs étendent l'utilisabilité vers le concept d'expérience utilisateur et indiquent comment le quantifier, notamment avec les technologies récentes. La norme 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 somme, l'amélioration de l'expérience utilisateur instille les améliorations simultanées et optimales de différents critères comme 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 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 aux 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].

## 4.3. 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. L'idée-force est que 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.

### 4.3.1 Eléments d'Analyse conjointe de la sécurité, de la résilience et de l'utilisabilité

Dans cette section, nous effectuons une analyse de chacun des trois aspects (sécurité, utilisabilité et disponibilité) et de ses corrélations. Chacun de ces trois aspects a été défini dans l'état de l'art.

#### Aspects sécurité et corrélations

Dans toutes les normes de sécurité (locales et internationales), les trois critères invariants sont les mêmes : la Confidentialité, l'Intégrité et la Disponibilité. A 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 3.1.1). Dans les systèmes sociotechniques, et notamment pour le domaine des systèmes médicaux, les attributs de respect de la vie privée et ceux de la confiance (*Trust*) se joignent indéniablement à la sécurité.

Westin dans son livre remarquable "de la vie privée et la liberté" ouvrant le champ moderne du droit et de la vie privée, définit la vie privée comme « la demande des individus, des groupes et des institutions afin de déterminer eux-mêmes quand, comment et dans quelle mesure les informations à leur sujet peuvent être communiquées à d'autres » [Westin, 1968]. Alain Westin ajoute que « chaque individu est constamment engagé dans le processus d'ajustement personnel dans lequel il équilibre le désir d'intimité avec le désir de la divulgation et de la communication". Nous utilisons la *Privacy* à la fois comme la confidentialité et l'intégrité des

informations concernant les aspects particuliers des individus, des groupes et des institutions dans la société.

Dans ses supports de cours [Cranor, 2005], [Cranor, 2006] et [Cranor & Blase, 2015], Cranor définit différents points de vue sur la *Privacy* : la vie privée qu'est un accès limité à soi (la mesure dans laquelle nous sommes connus pour les autres et la mesure dans laquelle les autres ont un accès physique à nous) ; la *Privacy* comme un contrôle de l'information (nous devons contrôler tout ce qui est au-delà de la limite de ce que les autres ont le droit de savoir de nous, ce qui implique l'autonomie individuelle, nous pouvons contrôler l'information d'une manière significative). La présence de règles et politique de respect de la vie privée (*Privacy policy*) renforce la confiance des consommateurs.

Rousseau et ses collègues [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 pas 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 4.1, 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 les incidents tels que les attaques de sécurité au mieux. Dans la perspective de gérer tout type d'incidents, nous mettrons en œuvre dans la section 4.3 une ingénierie avancée de la sécurité qui inclut la résilience et l'utilisabilité.

| 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 (*Public Key Infrastructure*), Protection des traces, Signature numérique, Solution AAA (*Authentication Authorization Accounting*). |
| 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 (*Distributed Denial Of Service*). |
| 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 (*Virtual Private Network*). |
| 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. |

**Tableau 4.1** : Impacts de sécurité et solutions correspondantes

### Aspects utilisabilité et corrélations

La garantie de l'utilisabilité permet aux utilisateurs d'atteindre leurs objectifs et satisfaire à leurs besoins dans un contexte particulier d'utilisation. Le contexte d'utilisation prend en compte les utilisateurs, les tâches, les équipements et les environnements physiques et sociaux qui peuvent tous influer sur la facilité d'utilisation d'un service (produit ou système).

La norme ISO 9241-11 explique les bénéfices de la mesure de l'utilisabilité en termes de performance des utilisateurs et de satisfaction de ceux-ci [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. Shackel [Shackel, 2009] évalue l'utilisabilité sur la base de trois critères : 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 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.

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'utilisabilité, la norme 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 pas 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. La maturité acquise au fil des décennies renforce le concept et nous évaluons la facilité d'utilisation. Comme indiqué dans le chapitre précédent, une simple mesure de l'utilisabilité ne peut plus suffire. Nous devons trouver le moyen 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 4.2 une synthèse des objectifs d'utilisabilité, des risques potentiels et de solutions d'utilisabilité (sans souci d'exhaustivité, mais plutôt de représentativité).

| **Objectifs de l'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 recherche de contournement | Recherche d'amélioration de l'expérience utilisateur dès les phases amont |

**Tableau 4.2** : Impacts d'utilisabilité et solutions correspondantes

### Aspects résilience et corrélations

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 & Välikangas, 2003] et [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 (liée au 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. 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 la survivabilité dans les IST) [ReSIST, 2016], et les travaux de la Commission Européenne sur les questions de la résilience (voir [European Commission, 2010, 2012, 2013]).

Des travaux de Laprie [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 4.3 une synthèse des objectifs de la résilience, des techniques et des solutions (là aussi sans souci d'exhaustivité, mais plutôt de représentativité).

| Objectifs de Résilience | Techniques de résilience | Solutions de résilience |
|---|---|---|
| Eviter des 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 |
| Garantir la persistance de la prestation de services de confiance | Evaluation et vérification | Prévision des incidents et éradication de leurs causes |
| 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 |

**Tableau 4.3** : Techniques et moyens de garantie de la résilience

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 conditions difficiles 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 de mettre en place des solutions de mitigation (atténuation) des impacts de tout risque d'incident entraînant des conditions difficiles ou des changements.

A 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 nationales et transfrontalières, avec des impacts socio-économiques et géopolitiques accrus) ;
- Sophistication des attaques de sécurité (de très fortes motivations et 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 ; tendance au 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 [Weiser, 1999] [Laprie, 2008]. 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.

### 4.3.2 Modèle conceptuel résultant de l'analyse conjointe

La Figure 4.2 présente le modèle conceptuel qui est le résultat de l'analyse conjointe de la sécurité, de l'utilisabilité et de la résilience (sa légende est fournie en Figure 4.3). Ses éléments constitutifs sont détaillés dans les sections suivantes : §4.3.3 et §4.3.4.

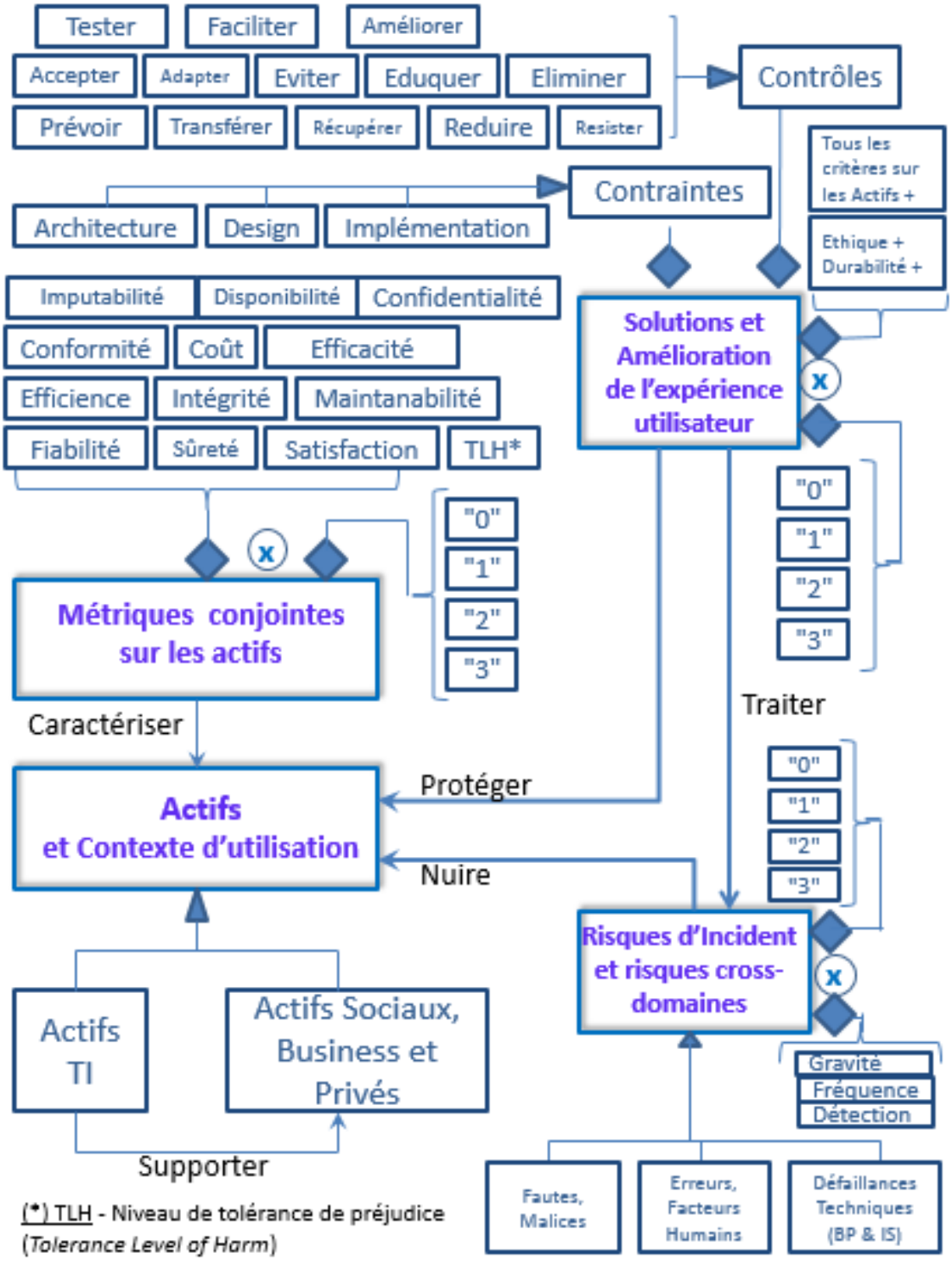


**Figure 4.2** : Modèle conceptuel de l'ingénierie conjointe, inspiré de [Goudalo et al., 2017b]

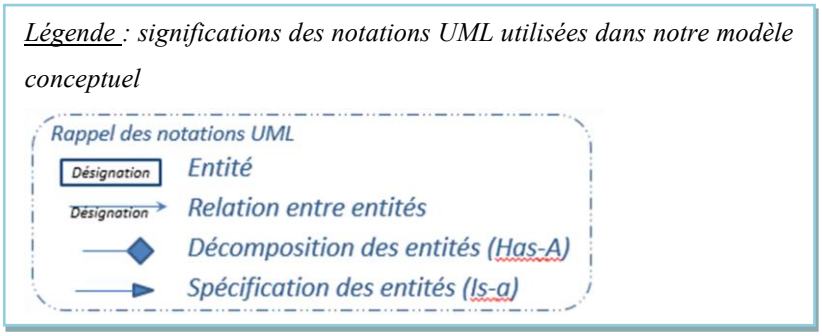


**Figure 4.3** : Légende accompagnant le modèle conceptuel de l'ingénierie conjointe

### 4.3.3 Concepts et Sémantiques

Les trois principaux concepts du modèle conceptuel proposé sont : les Actifs, les Risques d'incidents et les Solutions. Dans cette section, nous élucidons leurs définitions et leurs sémantiques dans les trois paragraphes §4.3.3.1, §4.3.3.2 et §4.3.3.3, respectivement.

#### 4.3.3.1 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. 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 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 (TI, SI et SST) qui soutiennent d'autres types d'actifs.

La Figure 4.4 indique un aperçu du modèle conceptuel recentré sur les actifs.

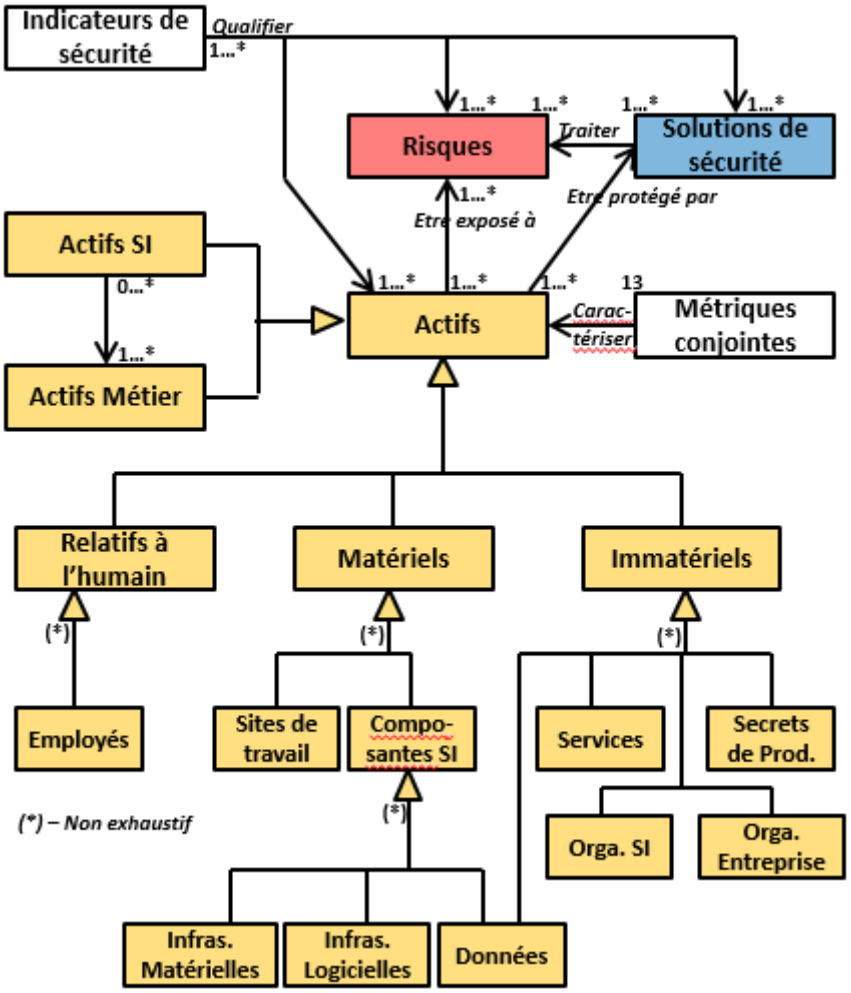


**Figure 4.4** : **Modèle conceptuel des actifs**

Les actifs sont caractérisés par les métriques conjointes sur les trois concepts (actifs, risques, solutions). Les métriques conjointes sont un produit cartésien de critères qualitatifs de la « Sécurité étendue » et de critères quantitatifs de la sécurité. Le produit cartésien avec des données non numériques (symboliques) est habituel dans la discipline de l'analyse des données symboliques [Diday, 2008].

- Les critères qualitatifs sont simultanément opérés sur les trois axes de la sécurité étendue : la sécurité de l'information, l'utilisabilité et la résilience. Il en ressort les treize critères suivants : Confidentialité, Conformité, Coût, Disponibilité, Efficacité, Efficience, Fiabilité, Imputabilité, Intégrité, Maintenabilité, Satisfaction, Sûreté, TLH (*Tolerance Level of Harm* - Niveau de Tolérance de Préjudice).
- Les critères quantitatifs étant les mesures homogènes définies conjointement sur les actifs, les solutions et les risques, afin de les piloter tous les trois de façon harmonieuse. Ces mesures sont « 0 – Très Faible ou Sans objet », « 1 – Faible », « 2 - Fort » et « 3 – Très Fort

». Exprès, nous avons exclu « Moyen » pour éviter les approximations non fondées. Par expérience, pour ne pas effectuer les calculs et mesures appropriés, la tentation pousse à choisir « Moyen ».

#### 4.3.3.2 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.

Dans le modèle conceptuel suggéré, à l'instar de l'actif, le risque est caractérisé par un produit cartésien de critères qualitatifs (Indice de gravité, Indice de fréquence, Indice de détection) et de critères quantitatifs (mesures homogènes de « 0 » à « 3 »).

#### 4.3.3.3 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, cross-domaines. 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 autres : Accepter, Adapter, Améliorer, Eduquer, Eliminer, Eviter, Faciliter, Prévoir, Récupérer, Réduire, Résister, Tester, Transférer.

Dans le modèle conceptuel suggéré, à l'instar de l'actif et du risque, les solutions sont caractérisées comme un produit cartésien de critères qualitatifs et de critères quantitatifs (mesures homogènes de « 0 » à « 3 »). Les solutions étant également des actifs d'entreprise, leurs critères qualitatifs regroupent tous les critères qualitatifs relatifs aux actifs, en plus

d'autres critères qualitatifs comme le respect des règles déontologiques et éthiques, la maintenabilité, la reproductibilité.

### 4.3.4 Système de métriques homogènes

Dans cette section, nous définissons un système de métriques homogènes sur les actifs, les risques et les solutions. 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. A l'instar du système métrique de suivi des indicateurs de la sécurité présenté dans la section 3.1.3, nous proposons ici un système métrique homogène, opérant sur trois axes majeurs de notre modèle conceptuel : les actifs, les risques d'incident 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 4.2 (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 et simplicité de manipulation, nous proposons de normaliser les valeurs en quatre catégories : "Non applicable ou Très Faible - 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. De la même

façon, ces quatre niveaux de risques d'incidents sont les suivants : "Sans objet ou Très Faible - 0", "Faible - 1", "Elevé - 2" et "Très élevé - 3".

- Quant aux solutions, nous proposons quatre niveaux normalisés 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 normalisés de solutions restent les mêmes : "Sans objet ou Très Faible - 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 et au moyen d'outils appropriés. Le développement de ces heuristiques et le choix des outils appropriés font l'objet des actes (activités et/ou tâches) de l'ingénierie avancée de la sécurité.

Nous proposons de présenter dans la section suivante l'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques.

## 4.4. La méthodologie ICSUR pour les SST

Encore aujourd'hui, nous rencontrons trop souvent des systèmes de sécurité (cf. §1.2) qui ne sont pas faciles d'utilisation et qui ne présentent pas non plus une appétence naturelle aux parties concernées [Hansen *et al.,* 2011]. Les principaux utilisateurs qui utilisent 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 de présenter les actes de sécurité avancée de notre approche d'amélioration de l'expérience pour l'ensemble des parties prenantes du système sociotechnique, sur la base des patrons de conception. Les patrons de conception (*design patterns*, patterns de conception ou patrons) ont été introduits dans la section l'état de l'art (cf. fin de §2.9). Cette approche sociotechnique opère sur l'interdépendance entre la sécurité, l'utilisabilité et la résilience. Nous en présentons un synoptique dans la section suivante.

### 4.4.1 Synoptique de la méthodologie d'ingénierie avancée

Nous voulons nous adapter à l'évolution perpétuelle des conditions d'utilisation (volatilité des utilisateurs, hostilité des contextes concurrentiels et sociaux, modification fréquente des règlementations) et faire face aux problèmes d'utilisabilité. Trois étapes constituent la synoptique de notre méthodologie d'ingénierie avancée, opérant conjointement sur la sécurité, l'utilisabilité, la résilience et sur leurs corrélations réciproques. Ces trois étapes sont : Définir le système sociotechnique, Identifier et analyser les risques d'incident et Définir les solutions basées sur l'amélioration de l'expérience utilisateur qui répondent aux préoccupations de toutes les parties prenantes.

La Figure 4.5 illustre le processus sous-jacent.

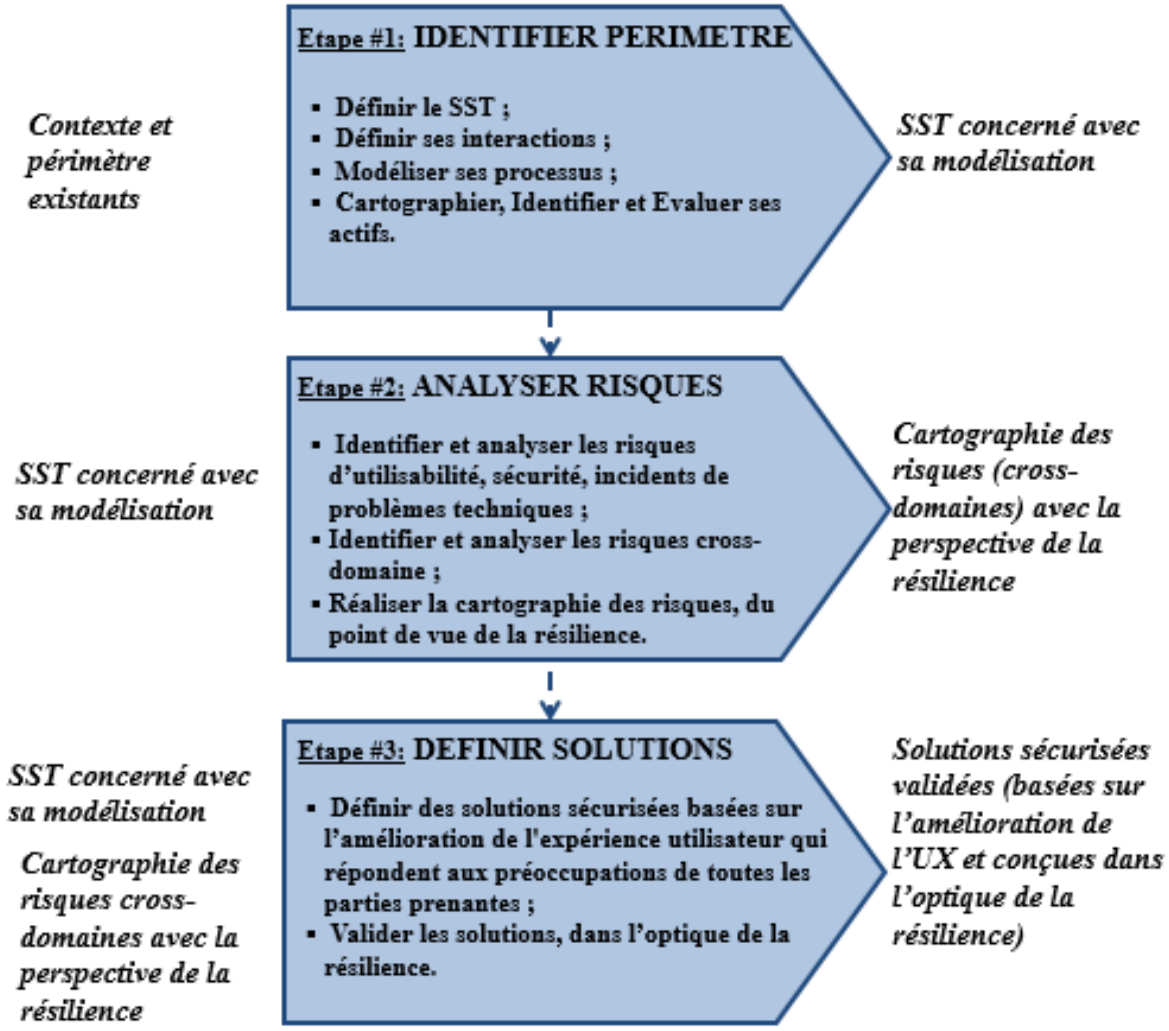


**Figure 4.5** : Méthodologie d'ingénierie conjointe de la sécurité de l'utilisabilité et de la résilience, inspiré de [Goudalo et al., 2017c]

Les trois étapes de la méthodologie sont développées ci-dessous.

### 4.4.2 Etape #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-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. Nous effectuons les tâches, ci-dessous :

- Enumérer les principaux actifs (matériels, physiques, logiciels, humains, documentaires et immatériels) ; les actifs peuvent être également des données, des services, des procédures et processus d'entreprise.
- Spécifier les contextes d'utilisation de chaque actif et le responsable de chaque actif principal. Ce responsable devrait savoir l'usage qui est fait sur chaque actif de son périmètre de responsabilité, l'utilité de chaque actif, sa valeur intrinsèque et les conséquences d'une corruption éventuelle sur n'importe quel actif de son périmètre.
- Déterminer la valeur intrinsèque des actifs, leur sensibilité pour l'entreprise, conformément à la stratégie d'entreprise et aux exigences de conformité règlementaire et légale.
- Classifier les actifs et déterminer leurs cotations, suivant les critères de sécurité, d'utilisabilité et de résilience. La dépendance fonctionnelle entre les actifs doit être prise en compte.
- Exprimer les besoins et les exigences sur les actifs, suivant la perspective de la sécurité, l'utilisabilité et la résilience, avec pour principal principe d'arbitrage l'amélioration de l'expérience utilisateur pour l'ensemble des parties prenantes.

### 4.4.3 Etape #2 – Effectuer l'analyse de risques cross-domaines du système sociotechnique

Cette étape produit la liste des problèmes potentiels. Il est possible de recourir à plusieurs types de 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]. La littérature scientifique présente beaucoup de travaux en analyse de risques ; les entreprises utilisent différents outils d'analyse de risques en fonction de leur taille et de leur secteur d'activité. A cette étape de notre approche, nous pouvons utiliser les méthodes et outils d'analyse de risques en place, les étendre et les adapter. Nous définissons les risques d'incident incluant, 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 certains aspects. Cette étude met en évidence les relations de proximité et d'interdépendance entre l'IHM, le respect de la vie privée et la sécurité. A cette partie, 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.

Nous synthétisons cette deuxième étape en cinq points :

- Identifier et analyser les risques d'utilisabilité ;
- Identifier et analyser les risques de sécurité ;
- Mettre en évidence les risques d'incidents de problèmes techniques (défaillances, erreurs de conception, incohérence procédurale, …) ;

- Identifier et analyser les risques cross-domaines (sécurité, utilisabilité et résilience ensemble), en tenant compte de la propagation de risques ;
- Effectuer la cartographie globale des risques, suivant la double perspective de la résilience (détecter tout ce qui empêcherait de garantir la qualité de services) et de l'amélioration de l'expérience utilisateur (détecter tout ce qui constituerait des irritants).

L'analyse des risques n'est pas une activité évidente. Pour terminer la description de cette deuxième étape, nous aimerions rappeler les tâches élémentaires suivantes qui font la différence dans une analyse des risques :

- Identifier les vulnérabilités inhérentes à chaque actif.
- Identifier les menaces auxquelles chaque actif est exposé.
- Estimer la probabilité intrinsèque d'occurrence de chaque menace.
- Etudier les impacts d'occurrence de chaque menace, et la propagation possible (avec une extrapolation tenant compte des attaques de rebond et de la dépendance fonctionnelle entre les actifs).
- Estimer la probabilité d'occurrence de chaque menace, cette fois-ci en tenant compte du contexte réel, à savoir les mesures existantes dans leur environnement d'exécution. En d'autres termes, définir la probabilité d'occurrence réelle.
- Évaluer le niveau global de risque auquel chaque actif est exposé en tenant compte de chacun des éléments obtenus ci-dessus.

Pour ce qui concerne notre méthodologie d'ingénierie avancée, chacune de ces tâches élémentaires prend en compte conjointement la sécurité, l'utilisabilité, la résilience. Bien que les outils techniques et les méthodes opérationnelles d'analyse de risque utilisent des dizaines d'indicateurs, nous proposons dans notre méthodologie d'ingénierie de normaliser les indicateurs résultants.

Comme nous verrons dans la section suivante, pour définir les solutions adéquates, nous recourons au principe d'arbitrage relatif à l'amélioration de l'expérience utilisateur pour chacune des parties prenantes.

### 4.4.4 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 au risque de créer de nouvelles vulnérabilités, ne boycottent ce qui est mis en œuvre au risque d'impacter la performance et la qualité de service.

Nous notons quatre types de traitement des risques : acceptation des risques, évitement des risques, réduction des risques et de transfert des risques. 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 tâches 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].

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 (cf. §3.6, dans le chapitre précédent). 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 d'architecture de résilience des systèmes, du point de vue de la sûreté et de la sécurité [Ruault et *al.*, 2016].

## 4.5. Synthèse et conclusion du chapitre

La considération de systèmes sociotechniques marque la véritable portée du numérique dans les activités socioéconomiques. Toutes les sphères sont concernées : la vie privée, les activités professionnelles, les organisations d'Etat, les entreprises de toutes tailles, les opérateurs de divertissement comme les opérateurs d'importance vitale. En début de ce chapitre de proposition, nous avons positionné les systèmes sociotechnique au regard des systèmes d'information, des systèmes sociaux et des systèmes de technologies de l'information.

Ensuite dans notre proposition, nous avons effectué des analyses sur chacun des trois aspects : la sécurité, l'utilisabilité et la résilience avec leurs corrélations réciproques. Les résultats de ces analyses sont synthétisés dans des tableaux présentant les objectifs, les impacts potentiels et les solutions associées (voir Tableaux 4.1, 4.2 et 4.3).

A l'issue de ces trois analyses, nous avons proposé un modèle conceptuel qui traite conjointement la sécurité, l'utilisabilité et la résilience avec leurs corrélations réciproques et qui opère sur l'amélioration de l'expérience utilisateur pour l'ensemble des parties prenantes. Il s'agit du modèle conceptuel de l'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience.

Enfin, nous avons présenté le processus de cette ingénierie avancée de la sécurité, au travers de sa synoptique et de ses actes de sécurité. Cette ingénierie avancée présente un double avantage, d'une part en opérant conjointement sur la sécurité, l'utilisabilité et la résilience, et d'autre part en recherchant systématiquement l'amélioration de l'expérience utilisateur.

Dans la section suivante, nous suggérons de dérouler une étude de cas qui illustrera la méthodologie d'ingénierie avancée que nous avons élaborée.

# Chapitre 5 : Etude de cas d'illustration de la méthodologie ICSUR

## 5.1. Introduction

L'étude de cas, appelée FI MedLab, est en relation avec le système d'information d'un laboratoire d'analyses médicales, en s'inspirant de celle décrite dans [Goudalo et Kolski, 2016]. La crédibilité des laboratoires médicaux est primordiale pour la santé et la sécurité des patients compte tenu de la nature des services fournis par ces laboratoires. La norme internationale en usage aujourd'hui pour l'accréditation des laboratoires médicaux est ISO 15189 [ISO 15189, 2012]. Un laboratoire d'analyses médicales effectue des tests sur des échantillons cliniques afin d'obtenir des informations sur la santé d'un patient concernant le diagnostic, le traitement et la prévention des maladies. Ces informations sont très sensibles à la sécurité, toute erreur peut avoir un impact direct sur la sécurité des patients, la vie privée et la réputation du laboratoire.

Aujourd'hui, la plupart des laboratoires médicaux disposent d'un système d'information. Ce dernier permet de recueillir des données sur les patients, les registres de tests médicaux et l'interprétation des résultats des tests. Le système d'information assure l'archivage, le stockage, le transfert et les échanges de données relatives aux principales activités du laboratoire médical. 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 forte 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. Par exemple, l'accès au système d'information peut être retardé par la nécessité d'une authentification sûre pour garantir que l'utilisateur est légitime, avant de fournir le niveau d'accès demandé au système du laboratoire médical. Certaines informations doivent être rapidement disponibles à un médecin dans le cas d'une situation d'urgence, mais elles ne doivent pas être communiquées à grande échelle, car il s'agit des données de santé et de la vie privée. La divulgation de ces informations est une infraction punissable, dans de nombreux pays, par exemple l'article 226-22 du Code pénal français.

Il en est de même pour les opérations de saisie de données médicales ou privées dans le système. Des erreurs éventuelles causées par un problème d'ergonomie de saisie de données engendreraient un impact fatal sur l'intégrité des données, qui est une mesure clé de sécurité dans la santé et le respect de la vie privée.

Dans les paragraphes suivants, nous déroulerons les trois principales étapes de la méthodologies ICSUR, tout en nous basant sur les éléments d'analyse conjointe (de la sécurité, l'utilisabilité et la résilience) et de modèle conceptuel (d'actifs, de risques et de solutions).

## 5.2. Etape #1 – Identifier le périmètre du système sociotechnique concerné

A cette étape de définition du périmètre du système sociotechnique, nous identifions et délimitons les processus d'entreprise concernés, avec les interactions. Qu'ils soient en consultation simple ou en consultation et modification / création, les principaux actifs qui entrent dans l'exécution des processus sont identifiés et leurs cotations sont définies.

### 5.2.1 Les processus d'entreprise

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, 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 5.1 synthétise trois processus métier de Fi MedLab et leurs activités.

| | |
|---|---|
| **1-** | **Préparer les analyses médicales** |
| *1.1-* | *Gérer le dossier patient (Créer, Mettre à jour ou Archiver) (voir Tableau 4.3)* |
| 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 médicaux (voir Tableau 4.3)* |
| 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 4.3)* |
| 3.4- | Archiver les résultats |

**Tableau 5.1** : Trois processus métier (*business processes*) de FI MEDLAB

La Figure 5.1 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 développerons dans l'analyse des risques.

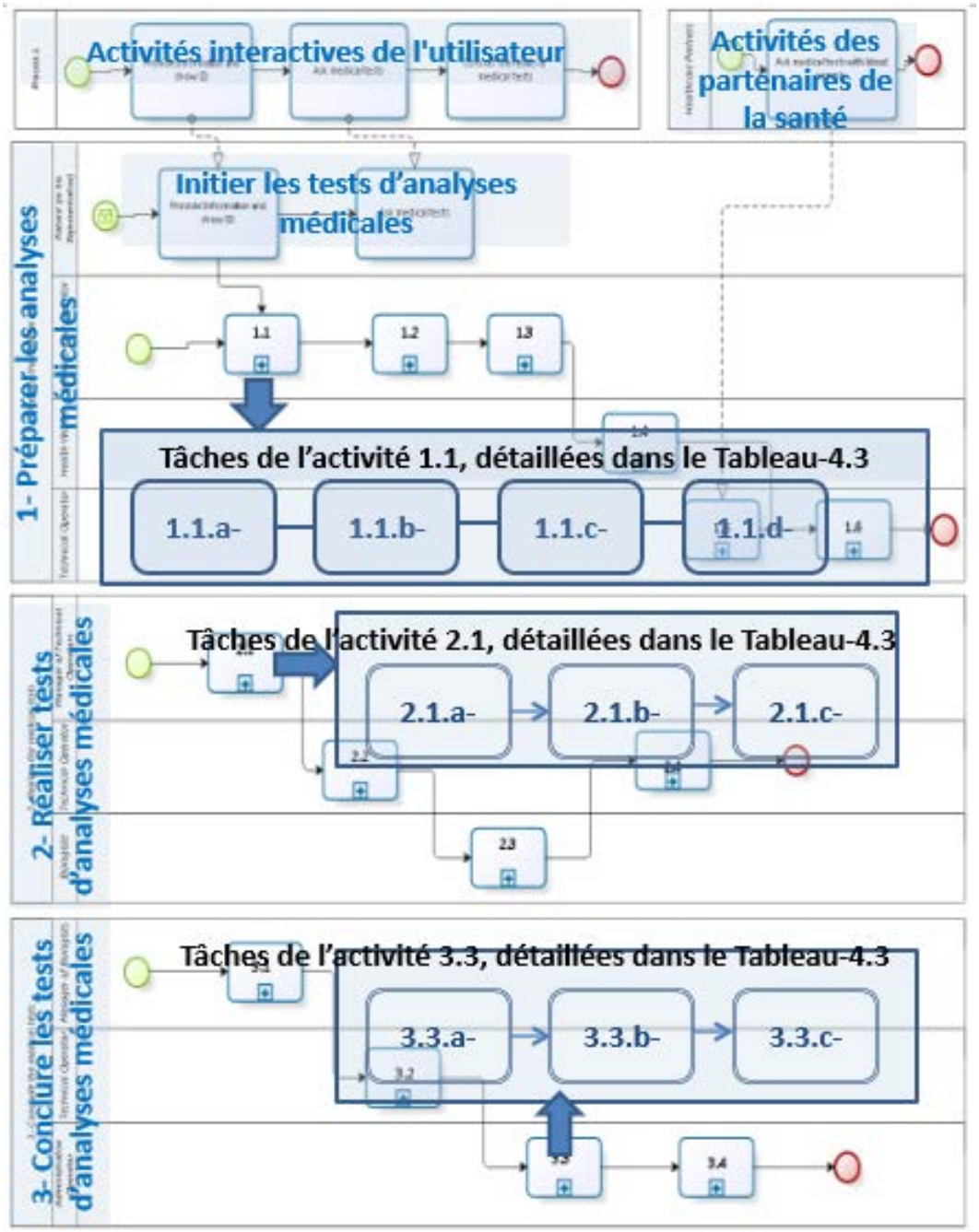


**Figure 5.1** : Modélisation des processus métier (avec mise en évidence des tâches ayant des problèmes potentiels)

### 5.2.2 Les actifs et leur cotation

Certains opérateurs ont accès à certains types d'informations, mais pas à d'autres. Cela dépend d'une part du niveau de sensibilité de l'information, et d'autre part du niveau d'autorisation et de l'authentification de chaque utilisateur. Ainsi, au sein des organisations, des groupes d'utilisateurs ayant des rôles et responsabilités respectifs doivent être définis.

La sensibilité de l'information est déterminée lors de la cotation des actifs, à l'instar du dispositif de cotation des actifs d'entreprise (illustré sur la Figure 3.1 pour les critères invariants de la sécurité, dans le troisième chapitre). Au regard des 13 critères de l'analyse conjointe de la sécurité, de l'utilisabilité et de la résilience, le tableau 5.2 présente trois actifs concernés par les activités opérationnelles avec leurs cotations respectives :

- Dossier du patient (l'opérateur administrative de FI MedLab entre des informations dans le système sociotechnique FI MedLab, pour la création et / ou la mise à jour du dossier du patient) ;
- Résultats d'analyses médicales (après analyse médicale et validation, le résultat est communiqué de trois façons - envoyé au médecin traitant, envoyé au patient par courrier électronique, mis à disposition sur le site sécurisé de FI MeddLab) ;
- Devices / Appareils médicaux (le gestionnaire allume et initialise les appareils médicaux, les étalonne afin de procéder aux analyses médicales).

L'activité de cotation est effectuée en ateliers (travail collaboratif) entre les responsables sécurité et les responsables métier (Analystes métier ou *Business Analyst*)[10]. Cette activité est sous la responsabilité du propriétaire des actifs. Le tableau de cotation est considéré comme la principale entrée (Input – Données fournies pour réaliser les autres activités de sécurité). Les valeurs de ce tableau sont basées sur les réalités de l'entreprise (ou de l'organisation concernée), dans son environnement socio-économique, concurrentiel, réglementaire et/ou légal.

Considérant par exemple le critère d'imputabilité, il est impératif (extrêmement) de tracer et d'identifier avec précision et rigueur qui a effectué quoi, quand, de quelle façon et pour quelle raison sur les appareils médicaux. A cause de cela, la métrique d'Imputabilité est "TRES ELEVEE, EXTREMEMENT" (3) pour les appareils médicaux. De la même façon la métrique d'Imputabilité est "ELEVEE" (2) pour les résultats d'analyse et pour les dossiers patients. On suppose que, dans le cadre de cette étude de cas, selon une démarche collaborative, la même chose a été reproduite pour les douze autres critères (cf. Tableau 5.2).

[10] *Dans le chapitre suivant, une première prise de hauteur relativement aux acteurs de la démarche d'ingénierie de la sécurité, valable aussi bien pour ICSUR que pour une de ses éventuelles évolutions dans le cadre de perspectives de recherche, est fournie en section 6.3.*

| **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 tolerance des prejudices - *Tolerance Level of Harm*) | "2" | "2" | "3" |

**Tableau 5.2** : Trois actifs sélectionnés et leurs métriques

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

Le tableau 5.3 présente la description détaillée de trois des sous-processus indiqués dans le tableau 5.1 (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.

| | |
|---|---|
| ***1.1-*** | ***Gérer le dossier patient (Créer, Mettre à jour ou Archiver)*** |
| | *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 saisit les informations dans le système sociotechnique 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. |
| ***2.1-*** | ***Mettre en marche et calibrer les appareils médicaux*** |
| | *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. |
| ***3.3-*** | ***Communiquer les résultats*** |
| | *En entrée : Résultats validés et interprétés.* |
| | *En sortie : Résultats communiqués, par trois canaux (envoyés au médecin concerné, envoyé au patient par courriel, 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 charge les résultats sur le site web sécurisé de FI MedLab. |

**Tableau 5.3** : Trois activités détaillées

Les risques d'incidents sont dus aux problèmes d'utilisabilité, de sécurité, de défaillance technique et à l'interdépendance entre eux. Les utilisateurs ont besoin d'accéder à des actifs du système (services, données et produits), en fonction de leur rôle et leur fonction. Toutefois la

modalité d'accès à cet actif dépend du contexte de la tâche à opérer (pression intérieure / extérieure, le délai court, ...), la qualité du dispositif de sécurité, son adéquation à la tâche et de son contexte.

Nous investiguons, ci-dessous, les trois scénarios sélectionnés pour illustration [Goudalo & Kolski, 2016].

- *Scénario T1 :* Le patient donne son adresse électronique professionnelle. Il ne remarque pas que les résultats de ses analyses médicales seront envoyés à cette adresse et l'opérateur administratif n'indique pas cette précision utile pour le patient. Lorsque les résultats sont effectivement envoyés au patient, ce dernier est absent et son assistant gère le courriel, comme tout autre courriel professionnel du patient. Ceci est un problème sérieux en termes de respect de la vie privée et de confidentialité que nous détectons au cours de cette phase. Ce scénario traite de la confusion entre l'information professionnelle et personnelle, dans la boîte de courriers électroniques professionnels. L'assistant peut ouvrir la boîte de courriers électroniques et lire les courriels, étant donné que ces courriels sont censés être professionnels.
- *Scénario T2 :* Le directeur des opérations techniques se confronte à de sérieuses difficultés à se faire accepter par le système d'authentification biométrique. Le système de caméra est mal positionné pour ce gestionnaire sportif qui mesure 1.92m (pour information, la hauteur moyenne de ses collègues est 1,76 m). Le gestionnaire n'est pas à l'aise dans une telle situation ; il n'arrive pas à trouver sa bonne inclinaison pour être authentifié. Dans ce contexte, il exécute la procédure de secours ; il se connecte dans le système et active les dispositifs électroniques. Les appareils sont initialisés, mais ne chargent pas la signature du chef biologiste (qui interprète la validation biologique des tests). Il n'y a pas eu d'alertes. Le gestionnaire ne remarque pas l'erreur car il est stressé et comme il n'y a pas eu d'alerte, il a supposé que la procédure de secours se soit bien déroulée. Dans ce scénario, nous sommes confrontés initialement à un problème d'utilisabilité et d'ergonomie, d'abord sur les procédures internes du système et d'autre part, sur les interfaces utilisateur de communication. Ce problème crée la vulnérabilité de sécurité sur tous les tests médicaux qui seront effectués au cours de la journée. Il n'y a pas de traçabilité et aucun respect de l'intégrité sur l'interprétation et la validation des résultats des tests médicaux. Le dispositif de sécurité ne correspond pas à la tâche et aux utilisateurs. L'utilisateur contourne le dispositif de sécurité, en utilisant une procédure de secours. De plus, il n'y a pas d'alarme informant le contournement de cette barrière contournement. Ce genre de comportement

correspond aux règles de contournement de barrières. Il s'agit d'une question cruciale de la sécurité.

- *Scénario T3 :* Le patient est en vacances lorsque les résultats d'analyses médicales sont prêts. De son lieu de vacances, il décide d'accéder au site Web sécurisé de FI MedLab. Il reçoit un message demandant d'entrer le code qui vient d'être envoyé à son téléphone via SMS. Cela peut conduire à trois problèmes :
    - Un problème de respect de la vie privée - Le lieu de vacances pourrait être une « information non publique », mais trouvée facilement par le système de sécurité du site Web de FI MedLab, ce qui pourrait conduire à des rumeurs potentielles sur la réputation du patient ;
    - Un problème de confiance - une catégorie de patients pourrait dire : « J'ai très confiance dans le système FI MedLab, car je ressens que mes données y sont bien protégées par des systèmes à la pointe de la technologie », une autre catégorie de patients pourrait dire : « Je n'ai pas confiance dans le système FI MedLab, je me sens espionné même jusqu'à mon lieu de vacances » ;
    - Un problème du confort et de la simplicité en raison de la vérification supplémentaire.

  Ce scénario traite du contexte de la tâche, à savoir, le lieu de vacances. En outre, le service d'envoi de SMS est en panne. Le SMS n'a jamais atteint sa destination et le patient n'a pas pu accéder à ses résultats médicaux sur le site Web de FI MedLab depuis son lieu de vacances (contrairement à ce qui a été promis).

Nous synthétisons les trois risques d'incidents et leurs métriques dans le Tableau 5.4.

A l'instar des métriques sur les actifs, nous avons défini des métriques homogènes sur les risques, variant de "0" (le moins élevé) à "3" (le plus élevé). La valeur résultante de risque dépend essentiellement de la gravité de l'impact, de la fréquence de l'occurrence, au regard de l'ensemble des sous-facteur. Dans le tableau 5.4, nous avons défini six sous-facteurs qui concourent aux métriques résultantes sur chacun des trois risques.

L'activité d'évaluation des métriques de risques est effectuée en atelier avec les responsables de sécurité, les responsables métier et les responsables de risque (*risk manager*). Les métriques résultantes de risque sont sous la responsabilité du principal responsable des risques.

Prenant par exemple le scénario T2 sur le système d'authentification biométrique, compte tenu de la description ci-dessus, le risque d'utilisabilité est "Extrêmement ELEVE" (3), le risque de

sécurité est "ELEVE" (2), le risque de défaillance nul "Pas de Défaillance" (0), il n'y a "Aucun Impact" sur le "Dossier Patient" (0), l'impact sur le "Résultat d'analyse médicale" est "ELEVE", l'impact sur les "Appareils médicaux" est "Très ELEVE". D'où la valeur "3" pour la métrique résultante qui est effectivement "Très ELEVEE".

Le même raisonnement s'applique aux scénarios d'incident T1 et T3.

| **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 trois scénarios | | |

**Tableau 5.4** : Risques d'incident et leurs métriques

## 5.4. Etape #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 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 son représentant). Le Tableau 5.5 présente la solution élucidée par l'expert en ingénierie avancée de la sécurité pour ce problème.

| ***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 sociotechnique et qui les concernent. Cela nécessitera un soutien et une pédagogie individualisés. Sur le plan opérationnel, nous pouvons mettre des prospectus et des terminaux d'information (interactifs et captifs) dans le hall d'entrée (ou salle d'accueil).<br>Une solution alternative devrait être "d'envoyer tous les courriers des résultats via paquet postal Recommandé Accusé/Réception".<br>Une autre solution plus technique consiste à :<br>- ajouter une étiquette « 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 ;<br>- utiliser du courriel sécurisé et chiffré. |
| *Conséquences* | La principale conséquence de ce design pattern est que la confidentialité et le respect de la vie privée seront bien respectés, sans entrainer un impact négatif sur l'utilisabilité. |

**Tableau 5.5** : Solution de design pattern pour le problème T1

Dans le scénario T2, le problème est plus complexe avec plusieurs dimensions :

- T2.1- Mauvaise utilisabilité du système d'authentification biométrique ;
- T2.2- Non-efficacité de la procédure de secours ;
- T2.3- Non maîtrise de la procédure de secours par le gestionnaire ;
- T2.4- Contournement de barrière non géré de façon efficace.

Les solutions élucidées pour les quatre scénarios T2.1, T2.2, T2.3 et T2.4 sont respectivement présentées dans les tableaux : Tableau 5.6, Tableau 5.7, Tableau 5.8 et Tableau 5.9.

| ***Solution de design pattern pour le problème T2.1*** | |
|---|---|
| *Nom* | Anticipation |
| *Description du problème* | Mauvaise utilisabilité du système d'authentification biométrique |
| *Description de la solution design pattern* | Repositionnement de la caméra et reconfiguration du système d'authentification biométrique, afin de tenir compte de tous les collaborateurs de l'équipe, susceptibles de s'y authentifier.<br>Les personnes concernées ont besoin d'utiliser des solutions sécurisées, de façon simple et efficiente. |
| *Conséquences* | L'utilisation simple et efficace des solutions de sécurité est une étape primordiale, pour assurer la sécurité dans le contexte de système sociotechnique. La conséquence de ce design pattern est d'apporter ce résultat. |

**Tableau 5.6** : Solution de design pattern pour le problème T2.1

| ***Solution de design pattern pour le problème T2.2*** | |
|---|---|
| *Nom* | Tests de vérification réguliers des procédures |
| *Description du problème* | Non efficacité de la procédure d'urgence. |
| *Description de la solution design pattern* | La fréquence des tests de vérification des procédures, de même que leurs résultats devront être intégrés dans les systèmes de contrôle et d'audit. |
| *Conséquences* | Ce problème est bien connu dans les problématiques de sûreté des systèmes critiques. La répétition des exercices de vérification développe la confiance des opérateurs et en cas de défaillance du système, ils savent appliquer la procédure d'urgence de façon adéquate. Tester régulièrement les procédures d'urgence est une façon d'améliorer l'expérience utilisateur des opérateurs. La conséquence de ce design pattern est d'apporter ce résultat. |

**Tableau 5.7** : Solution de design pattern pour le problème T2.2

| ***Solution de design pattern pour le problème T2.3*** | |
|---|---|
| *Nom* | Exercice d'entrainement des personnes concernées |
| *Description du problème* | Manque de maîtrise de la procédure d'urgence, de la part du manager. |
| *Description de la solution design pattern* | Entrainer et former toutes les personnes aux procédures et opérations auxquelles elles seront confrontées.<br>Ces activités d'entrainement, notamment sur les procédures d'urgence, devraient être intégrées dans les systèmes de contrôle et d'audit. |
| *Conséquences* | Ce problème est bien connu dans les systèmes critiques. L'entrainement et la formation des utilisateurs contribuent à améliorer leur expérience utilisateur. La conséquence de ce design pattern est d'apporter ce résultat. |

**Tableau 5.8** : Solution de design pattern pour le problème T2.3

| ***Solution de design pattern pour le problème T2.4*** | |
|---|---|
| *Nom* | Détection et alerte en cas de franchissement de barrière |
| *Description du problème* | Pour cause de problème d'utilisabilité, le dispositif de sécurité a été contourné, en utilisant une procédure alternative. |
| *Description de la solution design pattern* | L'utilisation des dispositifs de sécurité doit être monitorée, afin d'alerter l'administrateur du système de sécurité, en cas de franchissement de barrière. Dans cette optique, l'administrateur de sécurité peut améliorer l'utilisabilité du dispositif de sécurité et l'adapter au contexte d'usage. |
| *Conséquences* | C'est aussi un problème bien connu dans les systèmes critiques et de tels patterns devront être respectés. La conséquence de ce design pattern est d'enrichir le système de gestion de la sécurité, afin que cette dernière soit adaptée aux différents cas d'usage pour améliorer l'expérience utilisateur. |

**Tableau 5.9** : Solution de design pattern pour le problème T2.4

Dans le scénario T3, nous sommes confrontés à plusieurs problèmes encore :

- T3.1- Problème de ressenti d'atteinte à la vie privée ;
- T3.2- Problème de confiance « subjective » ;
- T3.3- Problème de confort et de simplicité.

A cela nous rajoutons un problème technique sur le service d'envoi de SMS qui aurait être provoqué par une attaque réussie. Une solution de secours ou de la haute disponibilité serait

convenable. Le plus important encore, aurait été l'anticipation de l'effet déceptif (non confort) pour l'utilisateur. La recherche d'une meilleure expérience utilisateur apporte une réponse efficace à l'ensemble de ces trois points (Tableau 4.10).

| ***Solution de design pattern pour le problème T3 (T3.1, T3.2, T3.3)*** | |
|---|---|
| *Nom* | Sensibilisation et pédagogie |
| *Description du problème* | Utilisateur en situation de panique et de stress. |
| *Description de la solution design pattern* | Former l'utilisateur et lui procurer suffisamment d'instructions durant les phases amont, lui permettent de comprendre les différents modes de fonctionnement du système sociotechnique, afin d'effectuer des actions de façon avisée. |
| *Conséquences* | A l'ère de l'industrie des services, un accompagnement personnalisé avec une bonne pédagogie constitue une bonne façon d'améliorer l'expérience utilisateur. La conséquence de ce design pattern est d'apporter ce résultat. |

**Tableau 5.10** : Solution de design pattern pour le problème T3

Ces scénarios représentatifs montrent réellement comment les problèmes d'utilisabilité impactent la sécurité, et inversement. Nous avons élucidé des solutions à base de design patterns, en identifiant les processus métier et en étayant les activités, les rôles et les tâches des utilisateurs, ainsi que leurs besoins (d'information privée ou, au contraire, l'incapacité d'accéder à ces informations privées), les réels contextes d'utilisation et d'autres problèmes d'utilisabilité. Ces modèles de conception sont la clé de voûte des systèmes sociotechniques résilients. Ensemble, ils intègrent les problématiques de sécurité et d'utilisabilité, puis en cas de problème la résilience assure la continuité de service de confiance justifiable.

Le Tableau 5.11 synthétise l'évaluation des métriques relatives aux solutions élucidées.

La métrique résultante des solutions de sécurité est décomposée en dix-sept sous-facteurs. Quand ces derniers sont applicables pour une solution, il faut vérifier si la solution proposée les respecte ou pas (OUI / NON). Même si les solutions sont essentiellement élaborées par les responsables de sécurité, cette activité de métriques sur les solutions de sécurité est effectuée dans le respect des stratégies et cibles d'entreprise (Architecture d'Entreprise et Risques d'entreprise). Cette activité est effectuée en ateliers avec les responsables de sécurité, les

responsables des cibles d'entreprise, les responsables de risque d'entreprise et le représentant de la finance d'entreprise (de type GRCA – Gouvernance, Risque, Conformité et Assurance).

Voici quelques interprétations sur le calcul de la métrique résultante des solutions :

- Considérant la solution proposée pour le scénario T1, elle répond positivement aux vérifications de quatorze sous-facteurs et elle n'est pas applicable à trois sous-facteurs. Aucun sous-facteur ne ressort de vérification négative. Sa métrique résultante est "EFFICACE" (2).
- Considérant la solution proposée pour le scénario T2, elle répond positivement aux vérifications de dix-sept sous-facteurs sur dix-sept au total. Sa métrique résultante est "Très EFFICACE" (3).
- Considérant la solution proposée pour le scénario T3, elle répond positivement aux vérifications de douze sous-facteurs et elle n'est pas applicable à cinq sous-facteurs. Aucun sous-facteur ne ressort de vérification négative. Sa métrique résultante est "EFFICACE" (2).

| **Caractéristiques** | **Solution pour le scénario T1** | **Solution pour le scénario T2** | **Solution pour le scénario T3** |
|---|---|---|---|
| Contrainte d'Architecture | *NA*[11] | Oui | Oui |
| Contrainte de Conception | Oui | Oui | Oui |
| Contrainte d'Implémentation | Oui | Oui | Oui |
| Contrôle d'Acceptation | Oui | Oui | *NA* |
| Contrôle d'Adaptation | Oui | Oui | Oui |
| Contrôle d'Amélioration | Oui | Oui | Oui |
| Contrôle d'Education | Oui | Oui | *NA* |
| Contrôle d'Elimination | Oui | Oui | Oui |
| Contrôle d'Evitement | Oui | Oui | Oui |
| Contrôle de Facilité | Oui | Oui | *NA* |
| Contrôle de Prévision | Oui | Oui | Oui |
| Contrôle de Récupération | *NA* | Oui | *NA* |
| Contrôle de Réduction | Oui | Oui | Oui |
| Contrôle de Résistance | *NA* | Oui | Oui |
| Contrôle de Test | Oui | Oui | Oui |
| Contrôle de Transfert | Oui | Oui | *NA* |
| Contrôle de Test | Oui | Oui | Oui |
| **Métrique sur la solution** | **"2"** | **"3"** | **"2"** |

**Tableau 5.11** : Caractéristiques des solutions et leurs métriques

[11] *NA - Non Appliquée (la solution n'est pas applicable au sous-facteur concerné)*

## 5.5. Synthèse et conclusion du chapitre

Dès lors que la maturité de la sécurité des banques et des établissements financiers commence à s'améliorer, des malversations sont de plus en plus fréquentes dans le domaine médical et de santé. De surcroit ce domaine utilise de plus en plus d'appareils connectés, ce qui augmente la surface d'exposition aux risques d'incident d'erreurs, de défaillances et de malversation.

L'étude de cas porte sur le domaine de santé et illustre la méthodologie ICSUR, en parcourant toutes les étapes de façon pédagogique. 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. Nous avons retenu trois actifs majeurs (dossier du patient, résultats d'analyses médicales et appareils médicaux) dont nous avons défini la cotation suivant les 13 critères de l'analyse conjointe de la sécurité, de l'utilisabilité et de la résilience. 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 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. Cette étude de cas est une illustration, afin de démontrer l'opportunité d'une telle méthodologie d'ingénierie, de même que sa faisabilité.

Il serait judicieux de trouver un financement et de constituer une équipe étoffée afin de travailler sur un véritable cas, en situation. Les résultats serviront aussi bien pour la science que pour le domaine médical et de santé. Les points de discussions sont présentés dans le chapitre suivant.

# Chapitre 6 : Discussions et Eléments d'appréciation

## 6.1. Discussions sur la proposition

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 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 méthodologie 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. En parallèle, 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 restaurer un état sûr après un accident ou une faute intentionnelle [Laprie, 2008] et [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 méthodologie d'ingénierie avancée baptisée ICSUR (Ingénierie Conjointe de la Sécurité, de l'Utilisabilité et de la Résilience) qui permet de traiter de façon conjointe la sécurité, l'utilisabilité et la résilience dans les systèmes d'information d'entreprise.

## 6.2. Eléments d'appréciation de la proposition

Notre proposition d'ingénierie avancée n'a pas pour objectif de remplacer les 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 (Etape # 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 de 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. Cela se justifie par deux raisons. Premièrement, nous nous sommes donnés pour objectif de démontrer l'opportunité et la faisabilité de la méthodologie ICSUR dans le cadre de ce premier travail, et à présent, l'Etape #2 d'analyse de risques cross-domaines peut s'interfacer avec des outils existants d'analyses de risques (qu'ils soient basés sur les mathématiques, les probabilités et/ou les statistiques). Deuxièmement, lors des futurs travaux de développement et d'industrialisation de la méthodologie ICSUR, nous serons amenés à outiller la méthodologie, entre autres avec les implémentations de 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 continue de l'expérience utilisateur inhérente à tous les scénarios de risques identifiés préalablement (en Etape # 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 (soit par l'atténuation des dommages, inhibition de propagations, diminution des occurrences, correction des vulnérabilités, sensibilisation des utilisateurs, 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 méthodologie d'ingénierie avancée qui traite la sécurité, l'utilisabilité et la résilience, de façon conjointe.

## 6.3. Relations des acteurs pour l'ingénierie avancée de la sécurité

Afin d'initier l'une de nos perspectives de recherche, nous proposons de présenter ici nos réflexions sur les acteurs de l'ingénierie avancée de la sécurité, leurs rôles et leurs interactions. Cette section est inspirée de [Goudalo et al., 2017]. Cette première proposition concerne aussi bien la méthodologie ICSUR que d'éventuelles évolutions de celle-ci.

### 6.3.1 Les principaux acteurs

Compte tenu de la définition de la méthodologie ICSUR, et des points rencontrés dans le déroulement du cas d'étude, nous retenons les acteurs suivants qui sont présentés dans le Tableau 6.1.

| Identifiant | Désignation de l'acteur | Commentaires / Observations |
|---|---|---|
| i. | Sponsor | Le représentant des hauts responsables (de l'organisation ou l'entreprise) sur l'initiative de sécurité avancée |
| ii. | Propriétaires des actifs | Un actif doit avoir un et un seul propriétaire (il se peut que le sponsor soit aussi propriétaire de certains actifs) |
| iii. | Analystes métier | Experts du domaine métier |
| iv. | Chargé de risques et conformité | Responsable GRC (Gouvernance Risque et Conformité), expert des lois et des règlementations |
| v. | Chargé de la sécurité sur l'initiative de sécurité avancée | Responsable risque de sécurité sur l'initiative |
| vi. | Chargé de l'utilisabilité sur l'initiative de sécurité avancée | Responsable Utilisabilité sur l'initiative |

| | | |
|---|---|---|
| vii. | Chargé de la résilience sur l'initiative de sécurité avancée | Responsable Résilience sur l'initiative |
| viii. | Les autres chargés de … sur le projet | Chargé de la technologie informatique, chargé des appareils médicaux, etc. (selon le domaine d'application). |
| ix. | Responsable de l'initiative dans l'entreprise | Responsable du management de l'initiative, comme projet ou chantier, rend compte au sponsor, organise et anime les comités. |
| x. | Représentants clients | Représente l'intérêt des utilisateurs finaux (externes) et connait bien leurs contextes d'utilisation |
| xi. | Représentant des opérateurs et utilisateurs internes | Connait bien les contextes d'utilisation et les enjeux des utilisateurs internes et opérateurs |
| xii. | Responsable de l'organisation ou l'entreprise | Le CEO/DG (*Chief Executive Officer* / Directeur Général) ou son représentant en fonction de la portée du projet |
| xiii. | Comité de pilotage de la sécurité de l'organisation ou l'entreprise | Le CISO/RSSI (*Chief Information Security Officer* / Responsable de Sécurité des SI) et une équipe transverse, en fonction de la portée du projet |
| xiv. | Comité de pilotage de l'IT de l'organisation ou l'entreprise | Le CIO/DSI (Chief Information Officer / Directeur des SI) et une équipe transverse, en fonction de la portée du projet |

**Tableau 6.1** : Acteurs de l'initiative d'ingénierie de la sécurité avancée, inspiré de [Goudalo et al., 2017]

### 6.3.2 Les rôles

Nous recourons à la matrice de RASCI, aussi désignée par matrice de RACI ou RACI tout simplement [Clet et al., 2013], pour définir les rôles entre les acteurs et parties prenantes. Avant d'élaborer la synergie entre les acteurs, à travers la matrice RASCI, nous définissons chacun des rôles imputables.

- R : Responsable (*Responsible*), la personne qui réalise l'action ou la tâche proprement dite. Ce rôle peut être partagé, et même, déléguée.
- A : Approbateur (*Accountable*), la personne qui approuve et qui porte la responsabilité que l'action ou la tâche est effectivement réalisée. Cette responsabilité ne peut être déléguée. Elle fait office d'autorité à tous les niveaux les plus bas et est impliquée à des niveaux supérieurs.
- C : Consulté (*Consulted*), la personne qui est consultée avant la réalisation de l'action ou de la tâche. Ceci implique une communication bidirectionnelle.
- I : Informé (*Informed*), la personne qui est informée après la réalisation de l'action ou de la tâche.

Dans le cadre des processus opérationnels et techniques, on y rajoute le rôle du Support (S) et on parle du RASCI. Le RASCI (ou le RACI) est utilisé, afin d'éviter les problèmes fondamentaux avec un processus où des personnes erronées sont impliquées et/ou personne n'en est vraiment responsable.

### 6.3.3 Les interactions entre les acteurs

Nous proposons de présenter les interactions entre les acteurs, en fonction de leurs rôles et au regard des quatre activités suivantes issues de la méthodologie d'ingénierie avancée ICSUR :

- Définir le périmètre du système sociotechnique ***(1)***
- Définir les actifs majeurs et leur cotation ***(2)***
- Analyser les risques d'incident et les scénarios associés ***(3)***
- Elaborer les solutions adéquates ***(4)***

Le tableau 5.2 présente les relations et les rôles des acteurs sur chacun de ces quatre points.

| **Les acteurs** | | **RASCI – Rôles des acteurs par activités** | | | |
|---|---|---|---|---|---|
| **Identifiant** | **Désignation de l'acteur** | ***(1)*** | ***(2)*** | ***(3)*** | ***(4)*** |
| i. | Sponsor | R | I | I | C |
| ii. | Propriétaires des actifs | I | R | S | C |
| iii. | Analystes métier | S | S | R | S |
| iv. | Chargé de risques et conformité | I | S | R | C |

| | | | | | |
|---|---|---|---|---|---|
| v. | Chargé de la sécurité sur l'initiative de sécurité avancée | I | S | R | R |
| vi. | Chargé de l'utilisabilité sur l'initiative de sécurité avancée | I | S | R | R |
| vii. | Chargé de la résilience sur l'initiative de sécurité avancée | I | S | R | R |
| viii. | Les autres chargés de … sur le projet | I | S | S | C |
| ix. | Responsable de l'initiative dans l'entreprise | A | A | A | A |
| x. | Représentants clients | I | S | S | C |
| xi. | Représentant des opérateurs et utilisateurs internes | I | S | S | C |
| xii. | Responsable de l'organisation ou l'entreprise | I | I | I | C |
| xiii. | Comité de pilotage de la sécurité de l'organisation ou l'entreprise | I | I | S | C |
| xiv. | Comité de pilotage de l'IT de l'organisation ou l'entreprise | I | I | S | C |

**Tableau 6.2** : Relations et rôles des acteurs de la sécurité, inspiré de [Goudalo et al., 2017]

Cette proposition n'est qu'un prélude de l'une de nos perspectives. Nous espérons avoir l'opportunité de l'enrichir lors d'un véritable projet de mise en œuvre globale de notre méthodologie d'ingénierie avancée, opérant de façon conjointe sur la sécurité, l'utilisabilité et sur la résilience.

# Conclusion générale

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, à l'heure actuelle et pour les générations à venir. Une autre forme d'ingénierie de sécurité avancée doit être conçue pour faire face à ce nouveau dilemme. 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].

De la position des entreprises et organisations, les travaux de recherche du présent mémoire adressent les besoins cruciaux de la sécurité de l'information pour lesquels nous sommes tous concernés. Les contributions suggérées constituent l'un des volets de cette ingénierie avancée de la sécurité, à l'ère de l'économie numérique.

Nous nous sommes proposés de traiter la sécurité de l'information au moyen d'une approche d'ingénierie qui réunit toutes les parties prenantes de l'organisation. Cette approche d'ingénierie est une méthodologie innovante baptisée ICSUR et fonctionne sur les processus d'entreprise (processus métier, *business processes*), leur décomposition et variantes opérationnelles, afin de : 1) découvrir les principaux actifs dans leur contexte d'utilisation, 2) identifier la valeur réelle et la sensibilité des actifs avec leurs interdépendances, 3) 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.

La méthodologie ICSUR d'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. Notre méthodologie d'ingénierie trouve son inspiration dans les percées et succès qu'ont connu l'ingénierie logicielle et l'ingénierie des systèmes d'information, au fil des décennies. Dans l'état de l'art nous les avons présentés. Nous y avons présenté également les fondements de chacun des trois aspects : sécurité, utilisabilité et résilience. Nous avons conclu l'état de l'art avec une analyse critique des travaux scientifiques portant sur deux de ces aspects. Nous n'avons identifié dans la littérature aucun travail qui porte conjointement sur les trois aspects. La méthodologie ICSUR est donc une réponse pertinente à ce besoin et une étude de cas a démontré la faisabilité de son application. De nombreux points restent néanmoins à approfondir, ce qui a fait l'objet d'une discussion sur les perspectives éventuelles des travaux de recherche dans le dernier chapitre de ce mémoire.

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. Nous suggérons d'explorer également l'ingénierie des connaissances, afin d'identifier les atouts qu'elle constituerait à ce nouvel objectif.

Malgré les différents outils proposés dans la littérature et dans l'industrie pour fournir des technologies de sécurité plus faciles à utiliser, malgré les valeurs ajoutées de notre méthodologie d'ingénierie avancée de la sécurité, d'autres défis sont encore nécessaires. Comment sensibiliser et transmettre efficacement le « bon sens » de l'utilisabilité comme un attribut inhérent de la sécurité ? Comment définir un cadre approprié qui facilitera une considération pondérée de la sécurité dans les réflexions, les décisions et les activités ? Comment outiller notre approche pour qu'elle se greffe facilement sur les méthodes et outils en place dans les entreprises et organisations, quels que soient leurs niveaux de maturité. Nous suggérons d'aborder ces questions à l'avenir, tout en élucidant une ingénierie à base de modèle de conception qui permettra d'intégrer explicitement les mesures de la confiance, du respect de la vie privée et d'autres critères subjectifs de mesure de l'expérience utilisateur pour toutes les parties prenantes.

# Bibliographie


[ACCESS-DEV, 2017] La gestion de projet : Méthodes classiques vs Méthodes agiles, ressource Internet http://www.access-dev.com/access-dev/la-gestion-de-projet-methodes-classiques-vs-methodes-agiles/ [dernier accès en juillet 2017].

[Adgeg, 2015] Adgeg G., 2015, 'Journée sur l'Internet des Objets et la Cybersécurité – Compte Rendu', Internet ressource http://blog.octo.com/journee-sur-linternet-des-objets-et-la-cybersecurite-compte-rendu/, [Dernier accès le 29/04/2017].

[Agile, 2017] Manifeste pour le développement Agile de logiciels, ressource Internet http://agilemanifesto.org/iso/fr/manifesto.html [dernier accès en juillet 2017].

[Alexander et al., 1977] Alexander C., Ishikawa S. & Silverstein, M., 1977, 'A Pattern Language: Towns, Buildings, Construction', Oxford University Press, New-York.

[Ambler, 1998] Ambler, S. W., 1998, "Process Patterns: building large scale systems using object technology", SIGS Books, Cambridge University Press, 1998.

[ANSSI, 2014] ANSSI, 2014, 'Résilience de l'Internet français', Internet resources http://www.ssi.gouv.fr/ [Accessed: 11/11/2015].

[ANSSI, 2016] ANSSI, 2016, '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].

[ANSSI, 2017] ANSSI, 2017, 'Comprendre et anticiper les attaques DDoS', Internet ressources https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf [Dernier accès 29/04/2017].

[ANSSI, 2017b] ANSSI, 2017, 'Risques liés à l'utilisation d'objets connectés sur un réseau d'entreprise', Internet ressources http://cert.ssi.gouv.fr/site/CERTFR-2016-ACT-006/ [Dernier accès 29/04/2017].

[ANSSI, 2017c] ANSSI (Agence nationale de la sécurité des systèmes d'information), 2017. L'agence française qui porte actuellement le cadre Ebios, Ressource Internet https://www.ssi.gouv.fr/, [Dernier accès 29/04/2017].

[Bell D.E.et La Padula, 1973] Bell D.E. and La Padula L.J., 1973, "Secure Computer Systems: Matematical foundations", Hanscom AFB. Bedford. MA. Rep. FSD-TR-73-278. vol.1, ESD/AFSC, 1973.

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

[Bernardez, 2005] Bernardez B., Duran A., Genero M., 2005, Metrics for use cases: a Survey of Current Proposals. In M. Genero, M. Piattini, and C. Colero Editors, Metrics for Software Conceptual Models, pages 59-98. Imperial College Press, 2005.

[Bevan, 2001] Bevan N., 2001, International Standards for HCI and Usability. International Journal of Human-Computer Studies archive, Volume 55 Issue 4, October 2001, pp. 533-552.

[Bevan, 2009] Bevan, N. 2009, 'Extending quality in use to provide a framework for usability measurement', In M. Kurosu (ed), Human centered design, HCII 2009, pp.13–22, Heidelberg, Germany, Springer-Verlag.

[Bevan et al., 2015] Bevan N., Carter J., Harker S., "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.

[Birge, 2009] 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, 2004] Blakley, B, Heath, C and 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].

[Braz, 2007] Braz, C, Seffah, A, Raihi, DM, 2007, “Designing a Trade-Off Between Usability and Security: A Metrics Based-Model”, In Proc. Interact, LNCS 4663, pp. 114–126.

[Boehm, 1976] Boehm, B. W., 1976, “A spiral model of software development”, ACM, SIGSOFT, vol. 11, 1976.

[Boehm, 1981] Boehm B.W., 1981, Software Engineering Economics. Englewoods Cliffs N.J. Prentice Hall.

[Boehm, 1988] Boehm B.W., "A Spiral Model of Software Development and Enhancement", Journal Computer Volume 21 Issue 5, May 1988, IEEE Computer Society Press Los Alamitos, CA, USA.

[Bonjean, 2013] Bonjean N., "Auto-organisation de fragments pour la conception de processus de développement", Thèse de doctorat UT3 Paul Sabatier, Toulouse, Juin 2013.

[Booch, 1991] Booch Grady, 1991, “Object Oriented Analysis and Design with Applications”, Benjamin/Cummings, 1991.

[Booch et al., 1998] Booch, G. Rumbaugh, J., Jacobson, I., 1998, “The Unified Modeling Language User Guide”, Addison-Wesley, 1998.

[Boulding, 1956] Boulding Kenneth, 1956, General Systems Theory, The Skeleton of Science. General Systems, Yearbook of the Society for General Systems Research, vol. 1, 1956.

[Brinkkemper et al., 1998] Brinkkemper S., Saeki M., Harmsen F., 1998, “Assembly Techniques for Method Engineering”, International Conference on Advanced Information Systems Engineering, (CAiSE’98), Italy, 1998.

[Brown, 2005] Brown T., 2005, “The Value of Enterprise Architecture”, ZIFA report, 2005.

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

[Chapelle et al., 2004] Chapelle, A., Crama, Y. Hubner, G., Peeters, J.P., 2004, Basel II and Operational Risk: Implications for risk measurement and management in the financial sector. Research series 200405-7, National Bank of Belgium.

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

[Chen, 1976] Chen Peter, 1976, The entity-relationship model: Toward the unified view of Data, ACM TODS, Vol 11, No 1, 1976.

[Choras et al., 2015] Choras, M., Kozik, R., Pilar, M., Bruna, T., Yautsiukhin, A., Churchill, A., Maciejewska, I., Eguinoa, I., and Jomni, A.,"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 & Furnel, 2014] Clarke, N. & Furnell, S. 2014, “8th Int’l Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)”, Nathan Clarke, Steven Furnell (eds.), Plymouth, UK, July 8-9, 2014. ISBN : 978-1-84102-375-5.

[Clet et al., 2013] Clet E., Maders H.P., Leblanc J., Goldfarb M. 2013, "Le métier de chef de projet", Editions Eyrolles, novembre 2013, Paris.

[Club Urba, 2003] Club Urba SI., 2003, "Pratiques de l’Urbanisme des Systèmes d’Information en entreprises", Publibook, 2003.

[CLUSIF, 2016] CLUSIF, 2016, La méthode méhari, Analyse des risques https://clusif.fr/mehari/ [Dernier accès en décembre 2016].

[Coakes, 2002] Coakes E. 2002, Knowledge Management: A Sociotechnical Perspective. In E. Cokes, D. Willis & S. Clarke (Eds.), Knowledge Management in the Sociotechnical World (Chapter 2, pp.4-14). London, Springer-Verlag.

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

[Cranor, 2006] Cranor, L 2006, "Usable Privacy and Security", Lorrie Cranor's courses, Internet resources http://cups.cs.cmu.edu/courses/ups-sp06/ [Accessed: 13/11/2015].

[Cranor & Blase, 2015] Cranor, L.F. & Blase, U. 2015, "Usable Privacy and Security", Lecturer materials, Courses January 2015, Carnegie Mellon University, CyLab. http://cups.cs.cmu.edu/courses/ups-sp14 [Accessed: 13/11/2015].

[Cuppens, 1993] Cuppens F., 1993, A Logical Analysis of Authorized and Prohibited Information Flows. IEEE Symposium on Security and Privacy, Oakland, 1993.

[Cuppens, 1997] Cuppens F., 1997, "Conception d'Applications Sécurisées". ONERA-CERT, Toulouse, 1997.

[DCSSI, 2009] 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].

[Diday, 2008] Diday E., 2008, "Comment extraire des connaissances à partir des concepts de vos bases de données ? les deux étapes de l'analyse des données symboliques.", Revue MODULAD, numéro 38.

[Deming, 1982] Deming, W. E., 1982, "Quality Productivity and Competitive Position". Massachusetts Institute Technology Eds, June 1982.

[DOD, 1983] DOD - Departement of Defense, 1983, "Trusted Computer System Evaluation Criteria". Technical Report CSC-STD-001-83, 1983.

[EBIOS, 2016] 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, 1967] Emery, E 1967, "The next thirty years: concepts, methods and anticipation", Human relations, #20, pp. 199-237.

[Engle et al., 1996] Engle, P. L., Castle, S., & Menon, P., "Child development: vulnerability and resilience". Social Science and Medicine, vol. 43, no. 5, 1996, pp. 621-635.

[European Commission, 2010] European Commission, "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] European Commission, "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," 2012.

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

[Evans et al., 1998] Evans A., France R., Lano K. et Rumpe B., 1998, "Developing the UML as a Formal Modelling Notation", Mulhouse 1998.

[Fayon et Tartar, 2014] Fayon D., Tartar M., 2014, "Transformation digitale : 5 leviers pour l'entreprise". Village Mondial, ISSN 2107-2620, ed Pearson Education France, 2014, ISBN 9782744066078.

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

[Filkins & Northcutt, 2016] Filkins B. & Northcutt S., 2016, Healthcare Provider Breaches and Risk Management Road Maps: Results of the SANS Survey on Information Security Practices in the Healthcare Industry, June 2016.

[French Penal Code, 2015] French penal code 2015, "De l'atteinte à la vie privée", article 226-1, [Accessed: 14/11/2015].

[Gamma et al., 1995] Gamma, E. Helm, R., Johnson, R., Vlissides, J., 1995, Design Patterns – Elements of Reusable Object-Oriented Software. Addison-Wesley, 1995.

[Gardarin et Valduriez, 1990] Gardarin G., Valduriez P., 1990, "SGBD avancés", éditions Eyrolles, Paris 1990.

[Gasser, 1988] Gasser M., 1988, Building a secure computer system, Van Hoostrand and Reinhold ed., 1988.

[Giani and al., 2009] Giani, A., Sastry, S., Johansson, K., and Sandberg, H., "The VIKING project: An initiative on resilient control of power networks," in Proc. Int. Symp. Resilient Control Syst., 2009, pp. 31–35.

[Giraudin, 2007] Giraudin Jean-Pierre. "Complexité des systèmes d'information et de leur ingénierie". e-TI - la revue électronique des technologies d'information, mai 2007, Internet Ressource www.revue-eti.net/index.php/eti/article/download/45/36, [Dernier accès 29/04/2017].

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

[Goudalo & Seret, 2009] Goudalo, W. & Seret, D., 2009, "The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes", SECURWARE 2009, 3rd Int'l Conf on Emerging Security Information, Systems and Technologies, IARIA, pp.105-113.

[Goudalo, 2011] 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, 2011, pp.44-50.

[Goudalo & Kolski, 2016] 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, pp. 400-411, ISBN: 978-989-758-187-8.

[Goudalo et al., 2016] 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.

[Goudalo et al., 2017] Goudalo W., Kolski C., Vanderhaegen F., 2017, Démarche d'ingénierie de la sécurité dans le management de projet : activités de sécurité et relations entre acteurs. Atelier "Sécurité des SI : technologies et personnes", Inforsid 2017, INFormatique des ORganisation et Systèmes d'Information et de Décision, Toulouse, France, juin.

[Goudalo et al., 2017b] Goudalo W., Kolski C., Vanderhaegen F., 2017b, 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. Ingénierie des Systèmes d'Information, 22 (1), pp. 65-107.

[Goudalo et al., 2017c] Goudalo W., Kolski C., Vanderhaegen F., 2017c, Towards Advanced Security Engineering for Enterprise Information Systems: Solving Security, Resilience and Usability Issues Together Within Improvement of User Experience. In Hammoudi S., Maciaszek L., Missikoff M., Camp

O., Cordeiro J. (Eds.), Enterprise Information Systems, ICEIS 2016, 291, Lecture Notes in Business Information Processing, Springer, pp. 436-459.

[Grundstein et Rosenthal-Sabroux, 2007] Grundstein M., Rosenthal-Sabroux C., Knowledge management system as a sociotechnical system. 2007. <hal-00948705> https://halshs.archives-ouvertes.fr/hal-00948705/document.

[Gzara, 2000] Gzara, L., Rieu, D., Tollenaere, 2000, “Patterns Engineering for Reuse at Product Information System Development”. Requirements Engineering Journal, Vol. 5, N°3, pp. 157-179, Springer-Verlag.

[Hafiz and Johnson, 2009] Hafiz M. and 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, Pages 61-67, IEEE Computer Society Washington, DC, USA.

[Hamel & Välikangas, 2003] Hamel G., Välikangas L., The quest for resilience. Harvard Business Review, Sept. 2003.

[Hansen et al., 2011] 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 2011, ACM New York, NY, USA.

[Hassine, 2005] Hassine, I., 2005, "Spécification et formalisation des démarches de développement à base de composants métier : la démarche SYMPHONY", Thèse d’informatique de l’Institut National Polytechnique de Grenoble, 2005.

[Henderson-Sellers et Edwards, 1990] Henderson-Sellers, B., Edwards, J-M., 1990, “The object-oriented software life cycle”. CACM, Vol. 33, 1990.

[Harrizon et al., 1976] Harrizon M.A., Ruzzo W.L. and Ullman J. D., 1976, Protection in operating systems, ACM, vol.19, n°8, pp. 461-471, Aug. 1976.

[Hedrick A., 2007] 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.

[Hertzum, 2007] Hertzum, M., Clemmensen, T., Hornbæk, K., Kumar, J., Qingxin, S. & Yammiyavar, P., 2007, “Usability constructs: A cross-cultural study of how users and developers experience their use of information systems”, In Proceedings of HCI International 2007, pp. 317–326, Beijing, China: Springer-Verlag.

[Hoagland, 1998] Hoagland J.A., Pandey R., Levitt K.N., 1998, Security Policy Specification Using a Graphical Approach, Department of Computer Science, University of California, Davis 1998.

[Hong et al., 1993] Hong S., van den Goor G. and Brinkkemper S., 1993, “A formal Approach to the Comparison of Object-Oriented Analysis and Design Methodologies”, in the Proceedings of the 26th Hawaii International Conference on System Sciences, January 1993, Vol 4, pp 689-698.

[Hollnagel, 2006] Hollnagel, E., Woods, D., D. & Leveson, N. 2006, “Resilience engineering. Concepts and precepts”, Ashgate, Aldershot.

[HSC, 2011] HSC, Hervé Schauer Consultants, 2011, "Normes en Sécurité", http://www.hsc.fr/ressources/presentations/normesISO-SSI2-11/normesISO-SSI2-11.pdf [Dernier accès en novembre 2016].

[IBM, 2014] IBM Corporation, 2014, “Understanding big data so you can act with confidence”, Doc. Ref. IMM14123USEN, June 2014, http://www-01.ibm.com, [Accessed: 13/11/2015].

[IRIS, 2016] IRIS (Infrastructure for Resilient Internet Systems) project. https://pdos.csail.mit.edu/archive/iris/ [accédé en septembre 2016].

[ISACA, 2016] ISACA – The provider of COBIT Framework (le fournisseur du Framework COBIT). http://www.isaca.org/ [Dernier accès en décembre 2016].

[ISO 9126, 1991] ISO/IEC, 9126, 1991, Software product evaluation - Quality characteristics and guidelines for their use.

[ISO/IEC FDIS 9126-1, 2000] ISO/IEC FDIS 9126-1, 2000, Software Engineering - Product quality - Part 1: Quality model.

[ISO/IEC DTR 9126-4, 2001] ISO/IEC DTR 9126-4, 2001, Software Engineering - Product quality - Part 4: Quality in use metrics.

[ISO 9241-110, 2006] ISO 9241-110, 2006, “Ergonomics of human-system interaction”, Part 110 Dialogue principles.

[ISO 9241-11, 1998] ISO 9241-11, 1998, Guidance on Usability.

[ISO 9241-12, 1998] ISO 9241-12, 1998, 'Ergonomic requirements for office work with visual display terminals (VDTs)', Part 12 Presentation of information.

[ISO 15189, 2012] ISO 15189, 2012, Laboratoires de biologie médicale -- Exigences concernant la qualité et la compétence.

[ISO/IEC 15408, 2005] ISO/IEC 15408, 2005, ITSEC (Information Technology Security Evaluation Criteria - Critères d'évaluation de la sécurité des systèmes informatiques) Critères Communs ; ISO/IEC 15408 : 2005.

[ISO/IEC 25000, 2014] ISO/IEC 25000, 2014, "Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Guide to SQuaRE".

[ISO/IEC 2700x, 2010] ISO/IEC 2700x, 2010, "Information Technology Security techniques".

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

[ISO/CEI 27000, 2016] ISO/CEI 27000, 2016, "Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Vue d'ensemble et vocabulaire".

[Jacobs, 2011] Jacobs, S., 2011, “Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance”. John Wiley & Sons, Inc.

[Jaeger T., 2016] Jaeger T., 2016, “Configuring Software and Systems for Defense-in-Depth”, in SafeConfig '16 Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Pages 1-1, Vienna, Austria — October 2016, ACM New York, NY, USA.

[Juels and Oprea, 2013] Juels A. and Oprea A., 2013, “New approaches to security and availability for cloud data”, in Magazine Communications of the ACM, Volume 56 Issue 2, February 2013, Pages 64-73, NY, USA.

[Karame G., 2016] Karame G., 2016, “On the Security and Scalability of Bitcoin's Blockchain”, in CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Pages 1861-1862, Vienna, Austria, October 24 - 28, 2016.

[Kaspersky Lab, 2015] Kaspersky Lab, 2015, "Enquête sur les risques informatiques mondiaux" http://www.kaspersky.fr/entreprise-securite-it/ [Dernier accès en septembre 2016].

[Khaitan et McCalley, 2015] Khaitan S.K. et McCalley J.D., 2015, “Design Techniques and Applications of Cyberphysical Systems: A Survey”, in IEEE Systems Journal, vol. 9, no. 2, pp. 350-365, June 2015.

[Khan et al., 2015] Khan Y.I., Al-Shaer E. et Rauf U., 2015, Cyber Resilience-by-Construction: Modeling, Measuring & Verifying. Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig'15), pp. 9-14, ACM New York, NY, USA 2015.

[Kolski et al., 2001] Kolski C., Ezzedine H., Abed M., 2001, Développement du logiciel : des cycles classiques aux cycles enrichis sous l'angle des IHM. In Kolski C. (Ed.), Analyse et Conception de l'IHM. Interaction Homme-machine pour les SI, vol. 1, Hermès, Paris, pp. 23-49.

[Korson et al., 1992] Korson T. et al., 1992, “Managing the transition to Object-Oriented Technology (Panel)”, in Proceedings of OOPSLA, October 1992.

[KPMG, 2014] KPMG International, 2014, 'Managing the data challenge in banking. Why is it so hard?', Document published on June 2014, http://www.kpmg.com, [Accessed: 13/11/2015].

[Kruchten, 1995] Kruchten, P., 1995, “The 4+1 View Model of Architecture”, IEEE Software 12 (6), pp. 42-50.

[Kumar et al., 2006] Kumar D., Ramakrishnan N., Helm R. F., Potts M., 2006, "Algorithms for storytelling", in, KDD '06 Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, Pages 604-610, Philadelphia, PA, USA, August 2006, ACM New York, NY, USA.

[Lampson, 1974] Lampson B.W., 1974, “Protection”, ACM, vol.8, n°1, pp. 18-24, Jan 1974.

[Laprie, 2008] 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.

[Larson, 2008] Larson, R.C. 2008, “Service science: At the intersection of management, social, and engineering sciences”, IBM Systems Journal, 47, pp. 41–51.

[Lemoigne, 1977] Lemoigne J. L., 1977 : "La théorie du système général – théorème de la modélisation", PUF, Paris, 1977.

[Les Echos, 2016] Les Echos, 2016, "Des hackers prennent en otage le système informatique d'un hôpital". Ressource Internet https://www.lesechos.fr/17/02/2016/lesechos.fr/021704417085_des-hackers-prennent-en-otage-le-systeme-informatique-d-un-hopital.htm [Dernier accès en septembre 2016].

[Les Echos, 2017] Les Echos, 2017, "Les demandes de rançons sur le web atteignent un niveau record". Ressource Internet https://www.lesechos.fr/tech-medias/hightech/0212019397891-les-demandes-de-rancons-sur-le-web-atteignent-un-niveau-jamais-vu-2082991.php, [Dernier accès en mai 2017].

[Lewis, 2014] Lewis, J.R., 2014, “Usability: Lessons Learned … and Yet to Be Learned”, International Journal of Human-Computer Interaction, 30:9, pp. 663-684.

[Lissandre, 1990] Lissandre M., 1990, "Maîtriser SADT", Armand Colin, 219 pages, ISBN 2200420226.

[Ltifi, 2011] Ltifi H., 2011, "Démarche centrée utilisateur pour la conception de SIAD basés sur un processus d'Extraction de Connaissances à partir de Données". Thèse de doctorat en Informatique, Université de Valenciennes et du Hainaut-Cambrésis, France & Université de Sfax, Tunisie (en co-tutelle).

[Longépé, 2002] Longépé C., 2002, “The Enterprise Architecture IT Project – the Urbanisation Paradigm”, Penton, 2002.

[Luzeaux, 2011] Luzeaux, D., 2011, “Engineering Large-Scale Complex Systems”, In Luzeaux D., Ruault J.-R. & Wippler J.-L. (eds.), Complex Systems and Systems of Systems Engineering, ISTE-Wiley, London, pp. 3-84.

[Macleod et al., 1997] Macleod M., Bowden R., Bevan N. and Curson I., 1997, “The MUSiC Performance Measurement Method”. Behaviour and Information Technology, 16.

[Mahatody et al., 2010] 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, 26 (8), pp.741-785.

[Mana et al., 2003] Mana A., Montenegro J.A., Sanchez F., Ray D., Yagüe M., 2003, “Integrating and Automating Security Engineering in UML”. University of Malaga, 2003.

[Manciaux et al., 2001] Manciaux M., Vanistendael S., Lecomte J., Cyrulnik B., 2001, "La résilience : état des lieux", dans La résilience : résister et se construire, sous la dir. de Michel Manciaux, Genève : Médecine & hygiène, 2001, pp. 13-20.

[Martin, 1982] Martin, J., 1982, "Application Developpement Without Programmers". Prentice-Hall. 1982.

[Martin, 1985] Martin, J., 1985, "Manifeste pour un système d'information". Les Editions d'Organisation.

[Martin, 1986] Martin J., 1986, "Information Engineering: An improved, automatable Methodology for the Design of Data Sharing Systems", Olle 1986.

[McDavid, 1999] McDavid D. W., 1999, "A standard for business architecture description in Enterprise Solutions Structure". IBM Systems Journal,Volume 38, Number 1, pp. 12-31, 1999.

[Minsky, 1968] Minsky M. L., 1968, "Matter, Mind and Models", in Semantic Information Processing, MIT Press, 1968.

[Munro D., 2015] Munro D., 2015, "Data Breaches in Healthcare Totaled Over 112 Million Records In 2015" www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#35f775697fd5 [Lastest access September 2016].

[Murphy and Murphy, 2013] Murphy D. R. and Murphy R. H., 2013, "Teaching Cybersecurity: Protecting the Business Environment", in InfoSecCD '13 Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference, Pages 88, Kennesaw GA, USA — October 12 - 12, 2013.

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

[Nanci et al., 1992] Nanci, D., Espinasse, B., Cohen, B., Heckenroth, H., 1992, "Ingénierie des systèmes d'information avec Merise – vers une deuxième génération". SYBEX, 1992.

[Nanci et Espinasse, 2001] Nanci D., Espinasse B., 2001, Ingénierie des systèmes d'information : MERISE, 2ème génération. Vuibert, Paris.

[Nijssen et Halpin, 1989] Nijssen G.M., Halpin T.A., 1989, "NIAM: Nijssen Information Analysis Methodology" 1989, ISBN:0-13-167263-0.

[Niknafs et Ramsin, 2008] Niknafs, A., Ramsin, R., 2008, "Computer-Aided Method Engineering: An Analysis of Existing Environments". Proc. 20th International Conf. Advanced Information Systems Engineering (CAiSE 2008), volume 5074 of the series Lecture Notes in Computer Science, pp. 525-540, France.

[NIST, 2016] NIST, 2016, "Cybersecurity Framework" https://www.nist.gov/cyberframework [Dernier accès en septembre 2016].

[OMG, 2005] OMG, 2005, "Model Driven Architecture - MDA", Object Management Group.

[OMG, 2008] OMG, 2008, "Software Processing Engineering Metamodel Spécification – SPEM", Object Management Group Internet ressource http://www.omg.org/spec/SPEM/2.0/ [Lastest access 04/29/20017].

[OMG, UML, 2016] OMG, UML, 2016, "Unified Modeling Language (UML) specification", version 2.x Reports Formal. http://www.omg.org/technology/documents/formal/uml.htm ; http://www.uml.org/#UML2.0 [Dernier accès, en décembre 2016].

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

[Palin, 2013] Palin, P.J., 2013, "Resilience: Cultivating the virtue", Internet resources http://www.hlswatch.com/2013/08/29/resilience-cultivating-the-virtue/ [Accessed: 11/11/2015].

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

[Pérez-Espana et Sanchez, 2001] Pérez-Espana H. et Sanchez A., 2001, An inverse relationship between stability and maturity in models of aquatic ecosystems. Ecol. Modelling 145, 189–196.

[Pièrre-Cambacèdés, 2010] Pièrre-Cambacèdés, L 2010, "Des relations entre sûreté et sécurité", Thèse de Doctorat in Software and Network, Paris.

[Ponemon Institute LLC, 2016] Ponemon Institute LLC, 2016, "2015 Cost of Data Breach Study: Global Analysis". Benchmark research sponsored by IBM, independently conducted by Ponemon Institute LLC, May 2016.

[Porter, 1986] Porter M., 1986, “L’avantage concurrentiel”. Paris, InterEditions.

[Praxeme, 2016] Praxeme institute 2016: Public methodology of Enterprise Architecture. Ressource Internet http://www.praxeme.org [Dernier accès en décembre 2016].

[PwC Etude Sécurité, 2016] PwC, 2016, "Turnaround and transformation in cybersecurity", Key findings from The Global State of Information Security® Survey 2016 www.pwc.com/gsiss.

[Ralité, 2001] Ralité J., 2001, “Ingénierie des méthodes à base de composants”, Université de Paris 1, Janvier 2001.

[Ralyté, 2001] Ralyté J., 2001, “Vue stratégique sur l’ingénierie des méthodes”, In INFORSID 2001, Martigny, Suisse, mai 2001, ISBN : 2-906855-17-0, pp. 43-66.

[Ralyté et al, 2008] Ralyté J., Deneckère R., Jamoussi Y., 2008, "Construction de méthodes par composition", in book : Ingénierie des méthodes : des nouvelles tendances de développement des applications informatiques, Chapter: Chapitre 7, Publisher: Centre de Publication Universitaire, Tunis, Editors: Naoufel Kraiem, Yassine Jamoussi, pp. 217-288, January.

[RAMBO, 2012] 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.

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

[ReSIST, 2016] ReSIST 2016, 'Resilience for Survivability in IST', A European Network of Excellence, http://www.resist-noe.org, [Dernier accès en septembre 2016].

[Rocques et Vallée, 2001] Rocques, P., Vallée, F., 2001, "UML en action – De l’analyse des besoins à la conception en Java". Eyrolles, 2001.

[Rolland et Prakash, 1996] Rolland C. et Prakash N., 1996, "A proposal for context-specific method engineering”, IFIP WG 8.1 Conference on Method Engineering, Chapman and Hall, pp. 191-208, Atlanta, Gerorgie, USA.

[Rolland et al., 1997] Rolland C., Brunet J., Sai Peck Lee, 1997, "Abstraction in an object-oriented analysis method”, Malaysian Journal of Computer Science, Volume 10, No 1, June 1997, pp. 53-63.

[Rolland, 2005] Rolland, C., 2005, "L’ingénierie des méthodes : une visite guidée", e-TI - la revue électronique des technologies d'information, Numéro 1, pp. 1-21, 2005.

[Romanosky, 2016] Romanosky, S., 2016, "Examining the Costs and Causes of Cyber Incidents". (http://cybersecurity.oxfordjournals.org/) [Lastest access in July 2017].

[Ross et Scholman, 1977] Ross D. T., Scholman U. E., 1977, "Structured analysis for Requirements Definition", IEEE Trans. Software Eng. Vol SE-3, No 1, 1977.

[Rousseau et al., 1998] Rousseau, D.M., Sitkin, S.B., Burt, R.S. & Camerer, C., 1998, "Not So Different After All: A Cross-Discipline View Of Trust", Academy of Management Review, vol.23, no.3, pp. 393-404.

[Royce, 1970] Royce, W.W., 1970, "Managing the development of large software systems". IEEE WESCON.

[Ruault et al., 2009] Ruault J.R, Luzeaux D., Colas C. et Sarron J.C., 2009, "Ingénierie système et résilience des systèmes sociotechniques", à la 5ème Conférence Annuelle d'Ingénierie Système AFIS 2009 "Ingénierie système et résilience des systèmes sociotechniques", Paris, Septembre 2009.

[Ruault, 2015] Ruault, J.R, 2015, "Proposition d'architecture et de processus pour la résilience des systèmes ; application aux systèmes critiques à longue durée de vie", Thèse de doctorat en Automatique, LAMIH, Université de Valenciennes et du Hainaut-Cambrésis, France.

[Ruault et al., 2015] Ruault, J.R, Kolski, C, Vanderhaegen, F. & Luzeaux, D., 2015, "Sûreté et sécurité : différences et complémentarités", Conférence C&ESAR 2015, Résilience des systèmes numériques, Rennes, France.

[Ruault et al., 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, pp. 2-12.

[Salehie et al., 2012] 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, pp. 165-170, Zurich, Switzerland, June 2012, IEEE Press Piscataway, NJ, USA.

[Salloway & Trott, 2002] Salloway, A. & Trott, J.R., 2002, "Design patterns par la pratique", Eyrolles, Paris.

[Sarbanes-Oxley Act, 2002] Congress of the United States. Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act), 2002, Pub. L. No. 107-204, 116 Stat. 745.

[Sasse, 2007] 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, no. 3, May/June 2007, pp. 78-81.

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

[Schneider, 1998] Schneider, F.B., 1998, "Trust in Cyberspace", Committee on Information Systems Trustworthiness, National Research Council, Washington, D.C.

[Schumacher, 2003] Schumacher, M., 2003, "Security engineering with patterns: origins, theoretical models, and new applications", Springer, 2003, LCNS 2754.

[Schwab, 2016] Schwab K., 2016, "Executive Chairman speech at 2016 annual World Economic Forum at Davos, Internet Resource https://www.weforum.org/agenda/2016/01/9-quotes-that-sum-up-the-fourth-industrial-revolution [Last accessed in July 2017].

[Scrum, 2017] The Scrum Guide, ressource Internet https://www.scrum.org/resources/scrum-guide [dernier accès en juillet 2017].

[Seffah et al., 2006] Seffah, A., Donyaee, M., Kline, R., B., Padda, H., K., 2006, "Usability measurement and metrics: A consolidated model", Software Quality Journal, vol. 14, pp. 159–178.

[SGDSN, 2017] SGDSN (Secrétariat général de la défense et de la sécurité nationale), 2017, "Le service d'Etat qui est responsable de l'Agence ANSSI", Ressource Internet http://www.sgdsn.gouv.fr/, [Dernier accès 29/04/2017].

[Shackel, 2009] Shackel, B., 2009, “Usability—Context, Framework, Definition, Design, and Evaluation”, Human Factors for Informatics Usability, B. Shackel and S. Richardson (eds.), Cambridge Univ. Press, pp. 21–37.

[Singh, 2013] Singh, MP 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.

[Smith et Smith, 1977] Smith J. M., Smith D. C. P., "Data Base Abstractions: Aggregation and Generalization", ACM TODS, Vol 2, No 2, 1977.

[Sperber et Wilson, 1995] Sperber, D, Wilson, D 1995, "Relevance: Communication and Cognition", 2nd Edition, ISBN: 978-0-631-19878-9, 338 pages, December 1995, Wiley-Blackwell.

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

[Symantec, 2017] Symantec 2017, "ISTR - Internet Security Threat Report", Rapport publié en avril 2017 https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf [dernier accès en mai 2017].

[Tullis and Albert, 2013] Tullis T. and Albert W., 2013, "Measuring the User Experience, Second Edition: Collecting, Analyzing, and Presenting Usability Metrics (Interactive Technologies)", Morgan Kaufmann; 2nd edition, July 2013.

[TOGAF 9.1, 2016] TOGAF 9.1, 2016, "Enterprise Architecture" - The Open Group's Architecture Forum https://www.opengroup.org/togaf/ [Dernier accès en juillet 2017].

[Trist et al., 1963] 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 Publications, London.

[Umhoefer et al., 2014] 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, [Lastest access in July 2017].

[Vanderhaegen, 2010] Vanderhaegen F., 2010, “Human-error-based design of barriers and analysis of their uses”, Cognition Technology & Work, 12(2), pp. 133-142.

[Vitali-Rosati, 2014] Vitali-Rosati M., 2014, “Pour une définition du "numérique"”, in E. Sinatra Michael, Vitali-Rosati Marcello (édité par), Pratiques de l’édition numérique, collection « Parcours Numériques », Les Presses de l’Université de Montréal, Montréal, p. 63-75, ISBN : 978-2-7606-3202-8 http://parcoursnumeriques-pum.ca/pour-une-definition-du-numerique [dernier accès, décembre 2016].

[Walden J., 2008] Walden J., 2008, “Integrating web application security into the IT curriculum” in SIGITE '08 Proceedings of the 9th ACM SIGITE conference on Information technology education pp. 187-192, Cincinnati, OH, USA — October 2008.

[Wang and al., 2010] Wang J.W., Gao F., Ip W.H., 2010, “Measurement of resilience and its application to enterprise information systems”. Enterprise Inf. Systems, 4(2), pp. 215–223.

[Weiser, 1999] Weiser M., 1999, "The Computer for the 21st Century". ACM SIGMOBILE Mobile Computing and Communications Review, 3(3) : pp. 3–11, 1999.

[Weske, 2012] Weske M., 2012, “Business Process Management: Concepts, Languages, Architectures”. ISBN 978-3-642-28616-2, Springer-Verlag Berlin Heidelberg.

[Westin, 1968] Westin A.F., 1968, “Privacy and Freedom”, 25 Wash. & Lee L. Rev. 166, http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 [Accessed: 13/11/2015].

[Wharton et al., 1994] Wharton C., Rieman J., Lewis C. & Polson P., 1994, “The cognitive walkthrough method: A practitioner’s guide”, In J. Nielsen & R. L. Mack (Eds.), Usability inspection methods, John Wiley & Sons, New York, pp.105-140.

[Winter, 2007] Winter, S, Wagner, S & Deissenboeck, F 2007, “A comprehensive model of usability”, In Engineering Interactive Systems, pp.106–122, Heidelberg, Germany: International Federation for Information Processing.

[Wirfs-Brock et Johnson, 1990] Wirfs-Brock R. J. and Johnson R. E., 1990, “Surveying Current Research in Object-Oriented Design”, Communications of ACM, Volume 33, No 9, pp. 104-124, September 1990.

[Woods, 2015] Woods D.D., 2015, “Four concepts for resilience and the implications for the future of resilience engineering”. Reliability Engineering and System Safety, 141 (2015), pp. 5–9, 2015.

[Yee, 2002] Yee, KP 2002, 'User Interaction Design for Secure Systems', Proc. 4th Int’l Conf. Information and Communications Security, Springer-Verlag, 2002, pp. 278–290.

[Yeo et al., 2014] Yeo M. L., Rolland E., Ulmer J. R., Patterson R. A., 2014, "Risk Mitigation Decisions for IT Security", in ACM Transactions on Management Information Systems (TMIS), Volume 5 Issue 1, April 2014, Article No. 5.

[Zachman, 2012] Zachman J.A., 2003, “The Framework for Enterprise Architecture”, ZIFA report.

[Zhu et Basar, 2015] 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", published in: IEEE Control Systems (Volume: 35, Issue: 1, Feb. 2015), pp. 46-65.

## Résumé

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 continuellement ; 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 ensemble, en améliorant l'expérience utilisateur. Notre objectif est de traquer et résoudre de façon conjointe les problèmes de la sécurité, de l'utilisabilité et de la résilience dans les systèmes d'information d'entreprise. Dans cette thèse, 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 nous recentrons 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. La thèse se termine par une discussion globale de l'approche, ainsi que par des perspectives de recherche.

**Mots clés :** Système d'information d'entreprise, Résilience de système, Sécurité de l'information, Utilisabilité, Expérience utilisateur, Système sociotechnique, Patron de conception.

## 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 doctoral thesis, we position sociotechnical systems in relation 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 thesis concludes with an overall discussion of the approach, as well as research perspectives.



## Key-words

Enterprise Information System, System Resilience, Information Security, Usability, User eXperience, Socio-Technical System, Design Pattern.