N°d'ordre: .....

République Algerienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la Recherche scientifique

Université Djillali Liabès de Sidi Bel Abbès
Faculté des Sciences Exactes
Département d'informatique
Laboratoire EEDIS

Thèse de Doctorat en Sciences

Filière : Informatique
Spécialité : Informatique

Par

CHERGUI Mohamed El Amine

Vers des processus métiers sécurisés dans le Cloud

Soutenue le .. .. 2021 devant le jury :

Dr.	TOUMOUH Adil	UDL SBA	Président du jury
Pr.	MALKI Mimoun	ESI SBA	Examinateur
Dr.	BERRABAH Djamel	UDL SBA	Examinateur
Dr.	AMAR BENSABER Djamel	UDL SBA	Examinateur
Pr.	BENSLIMANE Sidi Mohammed	ESI SBA	Directeur de thèse

Année Universitaire : 2020 - 2021

Remerciements

Mes remerciements s'adressent particulièrement à mon directeur de thèse le Pr. BENSLIMANE Sidi Mohammed, pour l'encadrement et pour la confiance qu'il m'a accordée. Ses remarques pertinentes, son occupation appréciable et ses judicieux conseils ont beaucoup contribué à améliorer la qualité de ce travail.

J'exprime mes vifs remerciements et mon respect aux membres du jury d'avoir accepté d'évaluer mon travail.

Je remercie aussi toute l'équipe pédagogique du département d'informatique de Sidi Bel Abbés.

Je profite de cette occasion pour exprimer ma reconnaissance et adresser mes remerciements les plus sincères à toute personne qui m'a aidé et contribuer à ce travail de recherche.

Enfin je dédie ce travail à ma famille, principalement mes parents, mes sœurs et mes amis/amies. Je les remercie tous pour leur apport moral et leur soutien.

ملخص

في سياق نمذجة الشركات، تعد نمذجة أساليب الأعمال هدفًا معقدًا ولكنه أساسي. BPMN هو المعيار لنمذجة أساليب الأعمال، هذه الأخيرة تكون قادرة على التحمل متطلبات الأمن من مرحلة النمذجة إلى المستوى المفاهيمي. من ناحية، BPMN لا يدعم تحديد متطلبات الأمن عند نمذجة عملية الأعمال. سيؤدي ذلك إلى زيادة ضعف النظام ويجعل تعديل الأمن النظام مستقبلا أكثر صعوبة، ومن ناحية أخرى، تُحدث الحوسبة السحابية ثورة في عالم المعلوماتية. وهو يتألف من الاستعانة بمصادر خارجية للبنية التحتية لتكنولوجيا المعلومات لمقدمي الخدمة المختصة. ينال مستخدمو الحوسبة السحابية الاستقلالية و أرغونوميا والبساطة ومع ذلك فإن الإستخدام الواسع للحوسبة السحابية يكشف عن مخاطر أمنية جديدة هي سبب التأخير في التبني الشامل لهذا الحل الجديد.

في هذه الأطروحة، سندرس تكامل متطلبات الأمن في أساليب الأعمال BPMN وسنقوم أيضًا بدراسة الأمن في السياق المحدد للحوسبة السحابية. سنعرض أحدث ما توصلت إليه التقنية حول الأساليب المختلفة للتعليقات التوضيحية المتعلقة بالأمن في أساليب الأعمال التي تستند إلى BPMN بالإضافة إلى أساليب التي تتناول موضوع الأمن في السحابة. بعد ذلك نقدم امتدادات BPMN . كلا من الامتدادات تتوافق مع آلية تمديد BPMN . الأول يستجيب للحاجة إلى إثراء معيار BPMN بأهداف أمنية مشتقة من أنطولوجيا الأمن السيبراني. و الثاني يأخذ الأمن في سياق محدد للحوسبة السحابية ، لقد قمنا بتوسيع الامتداد الأول مع تهديدات الحوسبة السحابية. أظهرت النتائج التجريبية على حالة استخدام حقيقية (عملية نموذجية لإدخال مريض إلى المستشفى) فاعلية الامتدادين المقترحين.

Résumé

Dans le contexte de la modélisation des entreprises, la modélisation des processus métiers constitue un objectif complexe, mais fondamental. Le BPMN (Business Process Model and Notation) est le standard pour la modélisation des processus métier. Les processus métiers doivent être en mesure de supporter les exigences de sécurité dès l'étape de modélisation au niveau conceptuel. Le BPMN ne prend pas en charge la spécification des exigences de sécurité lors de la modélisation des processus métier. Considérer les problématiques de sécurité à la fin du cycle de développement augmentera le risque de vulnérabilité du système et rendra difficile l'implémentation la sécurité. Le cloud computing est en train de révolutionner le monde informatique. Il consiste en l'externalisation des infrastructures informatiques vers des prestataires spécialisés. Les utilisateurs du cloud computing gagnent en autonomie, en ergonomie et en simplicité, cependant l'utilisation de plus en plus fréquente du cloud computing fait apparaître de nouveaux risques de sécurité qui sont la cause du retard de l'adoption massive de cette nouvelle solution.

Dans cette thèse, nous étudions l'intégration des exigences de sécurité dans les processus métiers BPMN ainsi que la sécurité dans contexte particulier du cloud computing. Nous proposons un état de l'art complet sur les différentes approches d'annotation de sécurité dans les processus métiers qui sont basé sur le BPMN ainsi que les approches qui traitent le sujet de sécurité dans le cloud. Par la suite nous proposons deux extensions conformes au mécanisme d'extension BPMN. Une première extension qui répond au besoin d'enrichir le standard BPMN avec les objectifs de sécurité qui sont dérivés de l'ontologie de la cybersécurité. La deuxième, prend en considération la sécurité dans le contexte spécifique du cloud computing avec la prise en charge des menaces du cloud computing. Les résultats expérimentaux sur un cas d'utilisation réel (processus typique d'admission d'un patient à un hôpital) sont présentés pour démontrer l'efficacité des deux extensions proposées.

Abstract

In the context of business modeling, business process modeling is a complex but fundamental goal. Business Process Model and Notation (BPMN) is the de facto standard for business process modeling. One of the most important aspect of business process models is security. Since most business processes revolve around the exchange of information, the security of such information assets becomes a critical factor for the success of the overall business process. Therefore, it is very important to capture the security requirements at conceptual level in order to identify the security needs in the first place. There is a need for an integrated tools and methodology that allows for specifying and enforcing compliance and security requirements for business process-driven enterprise systems. Furthermore, BPMN do not support the specification of security requirements along the business process modelling. This will increase the vulnerability of the system and make the future development of security for the system more difficult. Cloud computing is revolutionizing the computing world. It consists of the outsourcing of IT infrastructures to specialized service providers. Cloud computing users are gaining in autonomy, ergonomics and simplicity; however, the increasingly frequent use of cloud computing is revealing new security risks which are the cause of the delay in the mass adoption of this new solution.

In this thesis, we will study the integration of security requirements into BPMN business processes and we will also study security in the specific context of cloud computing. We provide a comprehensive state of the art for the different approaches that are based on BPMN that treat security annotation in business processes as well as approaches that address the topic of security in the cloud. Subsequently we offer two BPMN extensions. Both extensions comply with the BPMN extension mechanism. The first responds to the need to enrich the BPMN standard with security objectives that are derived from a cybersecurity ontology. The second, takes security consideration in the specific context of cloud computing, we have extended the first extension with cloud computing threats. In order to provide a commonly usable extension, these enhancements were implemented as BPMN metamodel extension. Experimental results on a real use case (typical process of patient admission to a hospital) are presented to illustrate the capabilities and the effectiveness of the proposed extensions.

Table des matières

Liste des figures

Liste des tableaux

Introduction

Contexte

Pour rester compétitives, les entreprises doivent faire face à de nombreux défis : externalisation, innovation, sécurité, les coûts de fonctionnement et recentrage sur le cœur métier en sont quelques-uns. Alors que le marché devient de plus en plus concurrentiel et imprévisible, de telles stratégies visent à rendre une entreprise plus efficace dans la délivrance des services afin de répondre au mieux la demande. En effet, le consommateur veut des services simples et fiables, tout en ayant des besoins très changeants. Les entreprises doivent répondre à ces exigences pour réussir à suivre les énormes variations des tendances du marché.

Pour répondre à ce besoin, il faut des systèmes d'information (SI) efficaces pour supporter de telles contraintes. Ceci est rendu possible par le développement de nouvelles technologies tel que « cloud computing » et l'optimisation des processus métiers. Les activités d'une entreprise peuvent être gérées de manière automatique afin d'améliorer l'efficacité de l'exécution des processus métier. Les sociétés modernes, adopte souvent des méthodes de gestion des processus métier pour définir les exigences fonctionnelles de l'entreprise. Les modèles de processus métier sont utilisés pour les besoins de communication entre les experts système et les experts métier pour combler le fossé. Les processus métier modernes combinent des tâches manuelles avec des tâches automatisées (par exemple, implémentées par des services web ou des micros services).

Le « cloud computing » permet de contribuer à l'adaptation des systèmes d'information au nouvel environnement assez turbulent dans lequel évoluent les organisations. Basée sur la notion de distribution de ressources, apparue dans les années 90, l'idée consiste à exploiter la puissance de calcul ou de stockage de serveurs distants par l'intermédiaire d'un réseau, assurant un partage aux moindres coûts des ressources pour l'entreprise. Conscientes des opportunités qu'offrent les systèmes d'informations basés sur les services cloud, les entreprises manifestent un intérêt croissant pour l'adoption de ce concept, ce qui constitue un important changement de paradigme des systèmes informatiques, jusque-là constitués de serveurs situés au sein même de l'entreprise.

En conséquence, l'interruption de l'activité, les données ou les processus devient un vrai problème pour toute l'entreprise. Le contexte veut qu'un petit changement à n'importe quel point de la chaîne de services, affectera le processus globalement. Surtout dans des environnements cloud, des problèmes tels que la non disponibilité d'une infrastructure, le vol ou la perte de données doivent être considérés lors d'une externalisation d'applications métiers.

Parfois, l'intégralité du savoir-faire et les données d'une entreprise sont gérées par une entité externe. Et vu que la chaîne de service complète n'est pas totalement sous contrôle d'un participant et ne peut être gérée indépendamment par un seul acteur. Traiter ces risques est primordiale, c'est seulement en anticipant de possibles défaillances qu'il est possible de garantir le fonctionnement du service. Donc vaut mieux, identifier les risques de sécurités à la phase de modélisation afin d'annoter directement les processus métier avec les concepts de sécurités.

Problématique

Le passage au Cloud dans une organisation présente une série de défis. La sécurité, reste obstacle majeur pour le passage à l'environnement cloud et l'externalisation. L'intégration des annotations de sécurité et de conformité directement dans les processus métier constitue une préoccupation majeure pour le développement et l'exécution dans les systèmes basés sur les processus métier.

En outre, les annotations de sécurités ont été reconnues comme une préoccupation importante pour les développeurs ainsi que pour les utilisateurs. Il ressort donc que l'association entre les processus métier et la sécurité est inévitable. Des études empiriques, ont démontré que les experts du domaine métier, peuvent spécifier des exigences de sécurité à un niveau élevé d'abstraction. Le problème, de nombreuses méthodes de développement de logiciels traitent souvent la sécurité à la fin.

La nécessité d'une approche d'annotation des concepts de sécurités est reconnue par plusieurs auteurs, qui sont aussi d'accord que les exigences de sécurités doivent être représentées dans le processus métier dès la phase de modélisation. Leur approche, cependant, ne prennent pas en considération tous les aspects de sécurités et ne respectent pas le mécanisme d'extension du méta-modèle. Ainsi donc, l'annotation des concepts de sécurités dans les processus métier devient une activité complexe d'où l'émergence de nouveaux challenges. Surtout dans le Cloud, où les exigences de sécurité sont importantes plus que dans un système classique.

Comment faire pour spécifier d'une façon simple les annotations de sécurité durant la phase de modélisation ?

L'approche doit se baser sur un langage familier pour l'utilisateur et proposer des simples annotations graphiques pour représenter les concepts de sécurité. En se basant sur des standards existants. A quelques exceptions près, la plupart des méthodes ne propose pas une représentation graphique formelle des concepts de sécurité.

Quels sont les concepts de sécurité qu'on va inclure ?

La sécurité des systèmes d'information vise plusieurs objectifs. Les approches actuelles de sécurité sont construites de manière non systématique, sans aucune preuve empirique pour justifier le choix des concepts retenus. L'approche, doit regrouper tous les concepts de sécurité en se basant sur une ontologie claire pour éviter la confusion entres les objectifs de sécurité.

De quelle façon on peut développer une extension complétement compatible avec le BPMN ?

Le BPMN supporte un mécanisme d'extension par addition afin de garantir la validité du modèle généré par extension. La quasi-totalité des approches de sécurité n'utilisent pas ce mécanisme d'extension.

Objectifs et contribution

L'approche qu'on devra proposer un ensemble complet des concepts de sécurité avec des représentations graphiques, pour permettre aux experts de sécurité d'annoter d'une façon complète les processus métier. Notre approche doit respecter aussi le mécanisme d'extension du BPMN, pour faciliter l'intégration dans les différents outils. Ceci permettra d'anticiper la plupart des risques lors de la phase de modélisation.

— Nous avons élaboré une revue de littérature pour évalué les extensions de sécurité BPMN existantes.

— Nous avons proposé une première extension du BPMN qui se base sur une ontologie d'exigences de la cybersécurité. Notre solution propose un ensemble complet de concepts de sécurité et permet d'introduire les exigences de sécurité à un stade de développement relativement précoce pour concevoir des systèmes d'informations sécurisés. Nous avons développé une application Web qui permet l'annotation facile des concepts de sécurité et nous avons illustré l'usage avec un cas d'utilisation (admission d'un patient à un hôpital).

— Nous avons proposé une seconde approche qui répond aux besoins spécifiques de la sécurité dans le contexte du cloud computing. Pour illustrer la modélisation des menaces du cloud computing, nous avons repris le même processus d'admission du patient à un hôpitale, en supposant que l'exécution ça se passe dans le cloud. Les expérimentations ont montré que notre extension augmente la compréhension des concepts de sécurité intégrés par rapport au BPMN standard. Les participants à cette expérimentation ont également indiqué que la conception de processus sécurisés via notre extension était préférable aux approches adhoc.

Organisation

Cette thèse se compose de cinq chapitres, à savoir :

Dans Le *premier chapitre*, nous verrons les techniques de modélisation des entreprises telles que BPMN et autre.

Le *deuxième chapitre* introduit des notions de base sur les concepts utilisés tout au long de cette thèse ainsi que les différents modèles du Cloud Computing.

Dans le *troisième chapitre* nous présentons les principes généraux de la sécurité informatique ainsi que la modélisation des menaces dans l'environnement du Cloud Computing.

Le *quatrième chapitre* dresse un état de l'art sur les extensions BPMN de sécurité ». Au niveau de ce chapitre, nous faisons une synthèse des approches déjà existantes, pour pouvoir par la suite dégager les limites de chacun de ces types d'approches.

Dans le *cinquième chapitre*, nous introduisons notre extension BPMN pour annoter facilement les concepts de sécurités et les menaces du Cloud Computing dans les processus métiers. Nous présentons notre outil ainsi que les cas usages utilisés pour illustrer l'utilisation de notre extension afin de valider notre approche.

Une conclusion résume en fin les principales leçons tirées de ce travail et les perspectives futures.

1 Modélisation des entreprises et processus métier

1.1 Introduction

De nos jours, le fonctionnement des organisations est basé sur le concept de processus métier. Le besoin d'adaptation rapide des entreprises à de nouveaux contextes du marché offrant aux clients de meilleurs services plus complets dans les plus brefs délais, ainsi que les évolutions des techniques et des nouvelles technologies. Ainsi, afin d'améliorer leurs performances, garantir la qualité de leurs services, réduire leurs coûts de fonctionnement, les organisations doivent veiller au bon fonctionnement et à l'optimisation de leurs processus. Face à tous ces facteurs complexes, il faut une bonne cartographie de la vue métier du Système d'Information (SI). De nouveaux paradigmes sont apparus tel que l'approche processus pour essayer de répondre aux exigences des entreprises imposées par les changements fréquents de l'environnement et des contraintes citées au-dessus.

L'utilisation de l'approche processus permet de maîtriser le fonctionnement d'une entreprise dans un contexte d'alignement continu des objectif métiers de l'entreprise avec son système d'information en intégrant les aspects organisationnels humains et technologiques.

Dans ce chapitre nous passerons en revue les principales techniques de modélisation des processus d'entreprise, pour mieux appréhender la notion de processus métiers.

1.2 Modélisation des entreprises

Une entreprise est une structure économique et sociale composée de gens et de processus dans le but de fournir des produits et des services à des clients [Vernadat, 1996]. Le modèle est "une représentation d'une abstraction d'une partie du monde réel, exprimée dans un langage de représentation".

En effet, le terme de modèle fait partie du langage commun mais sa signification n'est pas consensuelle. Ainsi, en peinture le modèle est le sujet qui sera traduit en peinture, il correspond donc à la réalité. Dans certains domaines techniques, le terme de modèle signifie le langage utilisé pour représenter la réalité (ex. : le modèle entité-relation en génie des systèmes d'information) [Benabdejlil, 2016].

Cette représentation est construite, vérifiée, analysée et manipulée pour maîtriser la réalité et mieux la comprendre. Le langage peut être :

— formel (ex informatique)

— semi-formel (ex graphique normalisé)

— informel (langage naturel)

[Moigne, 1999] définit la modélisation comme "l'action d'élaboration et de construction intentionnelle, par composition de symboles, de modèles artefacts susceptibles de rendre intelligible un phénomène perçu complexe, et d'amplifier alors la capacité de raisonnement de l'acteur projetant une intervention délibérée au sein du phénomène ; raisonnement visant notamment à anticiper les conséquences, tant synchroniques que diachronique, de ces projets d'actions possibles. ". Un modèle possède alors une syntaxe prédéfinie et chaque élément du modèle véhicule une sémantique particulière.

Selon [Zaidat, 2005] : "le processus de modélisation dans les entreprises est une tâche très complexe. Il consiste à décrire un agencement d'un nombre d'éléments important dont la nature est différente. La réalisation de ce processus requiert l'utilisation de techniques de modélisation appropriées. C'est dans ce sens que les architectures de référence ont proposé des cadres de modélisation pour la conduite du processus de modélisation ".

"La modélisation des entreprises concerne la représentation et la spécification des différents aspects des opérations des entreprises. L'aspect fonctionnel décrit ce qu'on doit faire et dans quel ordre. L'aspect informationnel décrit quels sont les objets utilisés ou traités. L'aspect ressource décrit qui "fait" les choses et selon quelle politique. Et enfin, l'aspect organisationnel décrit la structure organisationnelle dans laquelle les choses seront-elles faites" [Vernadat, 1996]. Le but de la modélisation des entreprises est d'aboutir à une spécification qui soit une représentation simplifiée de sa réalité passive ou active.

1.3 L'approche processus dans les organisations

L'approche processus adoptée par la norme ISO9001 :2015 a pour objectif de satisfaire le client de manière efficace. Pour qu'une organisation fonctionne efficacement, elle doit s'assurer que ses processus soient gérés de manière à satisfaire les besoins et attentes de ses clients [ISO, 2015]. La norme de management de la qualité donne des recommandations en matière d'organisation qui doivent permettre à une entreprise de maîtriser la qualité de ses produits et de satisfaire ses clients [Brandenburg et Wojtyna, 2006]. L'approche processus est une méthode d'analyse ou de modélisation. Elle consiste à décrire de façon méthodique une organisation ou une activité, généralement dans le but d'agir dessus [Brandenburg et Wojtyna, 2006]. L'approche processus désigne aussi l'application d'un système de processus au sein d'une organisation, ainsi que l'identification, les interactions et le management de ces processus.

L'un des avantages de l'approche processus est la maîtrise permanente qu'elle permet sur les relations entre les processus au sein du système de processus, ainsi que sur leurs combinaisons et interactions. Une organisation doit établir, documenter, mettre en œuvre, entretenir et améliorer en continu ses processus conformément aux exigences de la norme ISO. Ainsi, selon [ISO, 2015], l'organisation doit :

— identifier les processus nécessaires au système de management de la qualité et leur application dans tout l'organisme ;
— déterminer la séquence et l'interaction de ces processus ;
— déterminer les critères et les méthodes nécessaires pour assurer l'efficacité du fonctionnement et de la maîtrise de ces processus ;
— assurer la disponibilité des ressources et des informations nécessaires au fonctionnement et à la surveillance de ces processus ;
— surveiller, mesurer et analyser ces processus ;
— mettre en œuvre les actions nécessaires pour obtenir les résultats planifiés et l'amélioration continue de ces processus. »

L'approche processus consiste à décrire de façon méthodique une organisation ou un ensemble d'activités en processus, de façon à organiser sa contribution à la satisfaction des clients. Ainsi la production d'un produit est un processus qui fait intervenir différentes entités d'une organisation. L'importance de l'approche qualité et de la satisfaction du client ont mené à cette définition de processus "orientés client" par nature inter-fonctionnelle, donc transversale à l'organisation et soutenus par la mise en place des technologies de l'information et de la communication [Gaubert-Macon, 2006]. La norme ISO 9001, recommande à l'entreprise d'identifier et décrire les processus nécessaires à la réalisation de ces produits et ensuite assurer le bon fonctionnement et l'amélioration continue de chaque processus [Brandenburg et Wojtyna, 2006].

1.4 Types de processus

La norme AFNOR de juin 2000 sur le management des processus propose trois grandes familles [Cattan, 2000] :

- **Les processus métiers** (de réalisation ou opérationnels) : ils contribuent directement à la réalisation du produit, depuis la détection du besoin client jusqu'à sa satisfaction. Ils regroupent des activités liées au cycle de vie du produit : recherche de nouveaux produits, conception, achats et approvisionnements, logistique, production, commercialisation, etc. Ils ont pour but de participer à la réalisation d'un produit ou d'un service pour un client

- **Les processus de support** (dits aussi processus de soutien) : ils contribuent au bon déroulement des processus de réalisation en leur apportant les ressources nécessaires. Bien que ne créant pas de valeur directement perceptible par le client, ils sont nécessaires au fonctionnement permanent de l'organisation et de sa pérennité. Selon l'activité de l'organisation et sa stratégie, les processus de support peuvent être considérés comme des processus de réalisation et réciproquement. C'est le cas, par exemple, de la gestion des ressources humaines, des achats/approvisionnements, de la logistique, etc. Ils ont pour but de fournir les moyens nécessaires à tous les autres processus.

- **Les processus de direction** (dits aussi processus de management ou de pilotage) : ils contribuent la détermination de la politique et au déploiement des objectifs dans l'organisation. Sous la responsabilité totale de l'équipe dirigeante, ils permettent d'orienter et d'assurer la cohérence des processus de réalisation et de support. Ils ont pour but de piloter tous les autres processus en transformant des informations (venant des processus ou de l'extérieur) en directives. Parmi les processus de direction on peut citer :

— L'élaboration de la stratégie de l'organisation
— Le management de la qualité de l'organisation
— La communication interne et mobilisation du personnel

Les entrées des processus de direction proviennent, en grande partie, des processus de réalisation, sous forme d'indicateurs, de tableaux de bord, de résultats financiers, mais aussi sous forme de remontée de problèmes [Brandenburg et Wojtyna, 2006].

Le schéma suivant illustré par la figure 1.1 donne une vision globale des types de processus et de leurs interactions :

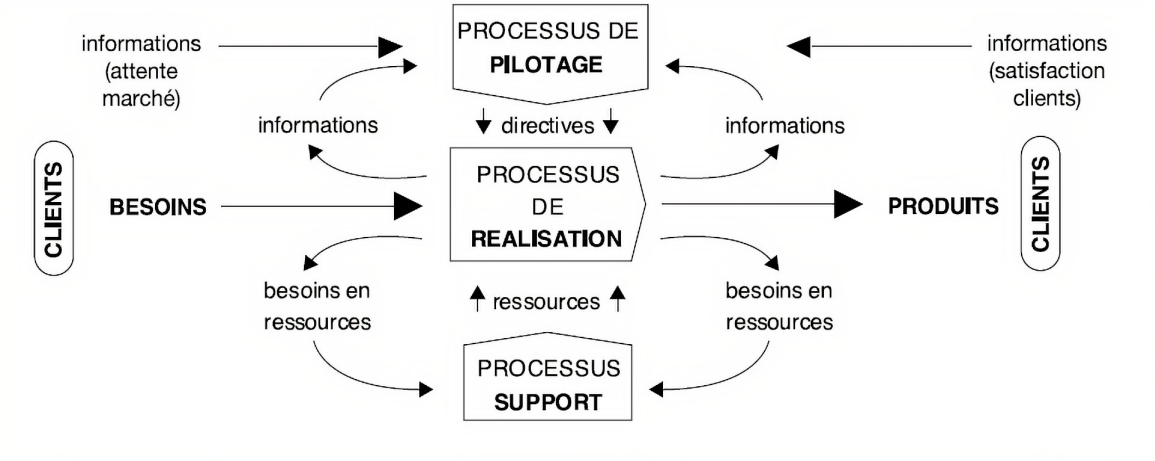


FIGURE 1.1 – *Typologie des processus [Brandenburg et Wojtyna, 2006]*

1.5 DÉFINITION DE PROCESSUS

L'ISO 9001 :2015 [ISO, 2015], définit un « processus » comme « un ensemble d'activités corrélées ou interactives qui transforment des éléments d'entrée en éléments de sortie ». Les entrées d'un processus proviennent soit de l'extérieur, soit d'un autre processus (processus amont). Tout comme ses sorties vont soit vers l'extérieur, soit vers un processus aval [Brandenburg et Wojtyna, 2006].

Dans ce contexte, un processus constitue l'ensemble des moyens et des activités mis en œuvre par l'entreprise depuis l'expression d'un besoin client jusqu'à la satisfaction de ce besoin. Le client est l'origine (la cause) et le destinataire (la finalité) du processus [Debauche et Mégard, 2004].

Un processus possède donc les caractéristiques suivantes [MANSOURI, 2009] :

— Représente une vue dynamique de l'organisation (Possède un but).
— Possède une entrée et une sortie.
— Est composé de sous-processus, puis d'activités qui sont les éléments d'action atomiques. Une activité exprime la transformation d'une ressource d'entrée en une ressource de sortie.

— Un graphe d'activités, qui représente l'enchaînement des activités nécessaires à la réalisation de l'objectif.
— Ajoute de la valeur aux biens ou aux services ;
— Des rôles, qui expriment l'organisation dans le processus.
— Une fonction de transition, qui contrôle le déroulement du processus.
— Des ressources, qui peuvent être des moyens, des informations ou des outils utilisés par une activité.
— Peut impliquer plusieurs unités fonctionnelles.
— S'exécute généralement horizontalement à travers une organisation verticale.

D'autres définitions introduisent la notion de processus métier :

Dans [Gillot, 2008], « un processus métier est un enchainement ordonné d'activités, qui se déroulent en série ou en parallèle, qui sont exécutées par des personnes ou par des applications et qui aboutissent à un résultat attendu. Un processus se caractérise par un événement déclencheur en entrée, suivi d'activités permettant de construire le résultat final».

Dans [Morley et al., 2005], « un processus métier est un ensemble d'activités, entreprises dans un objectif déterminé. La responsabilité d'exécution de tout ou partie des activités par un acteur correspond à un rôle. Le déroulement du processus utilise des ressources et peut être conditionné par des événements, d'origine interne ou externe. L'agencement des activités correspond à la structure du processus ». Ces processus métier sont le sujet de notre étude. La figure 1.2 et la figure 1.3 montrent des exemples de processus Métiers :

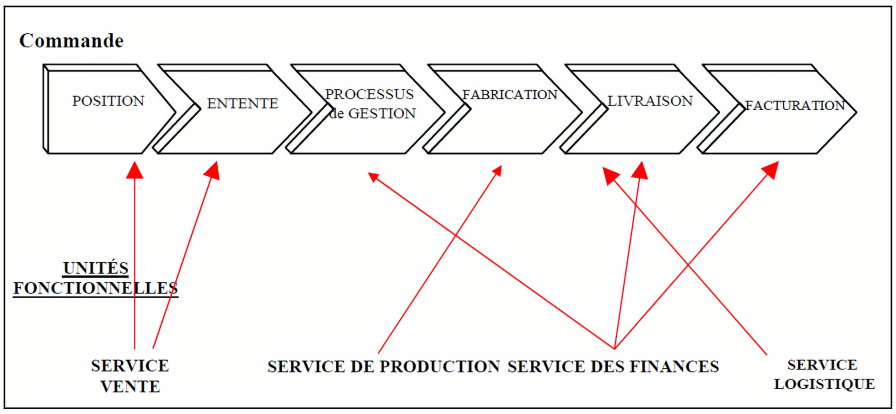


FIGURE 1.2 – *Processus de gestion de commandes [MANSOURI, 2009]*

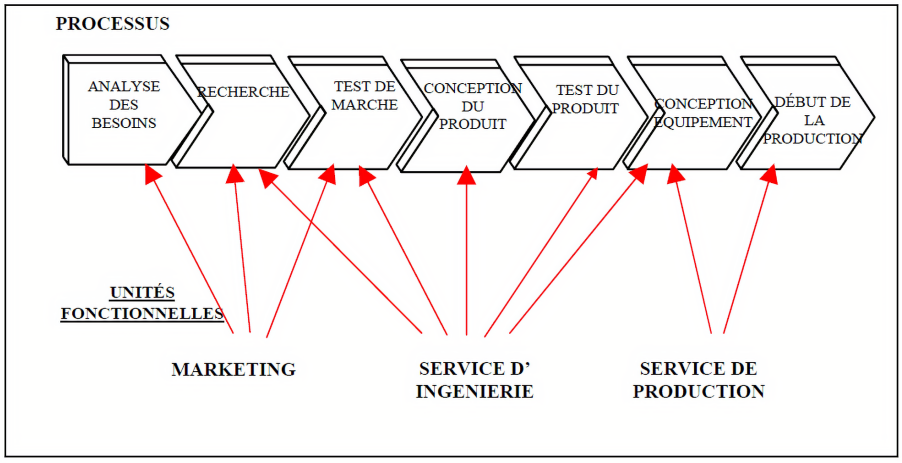
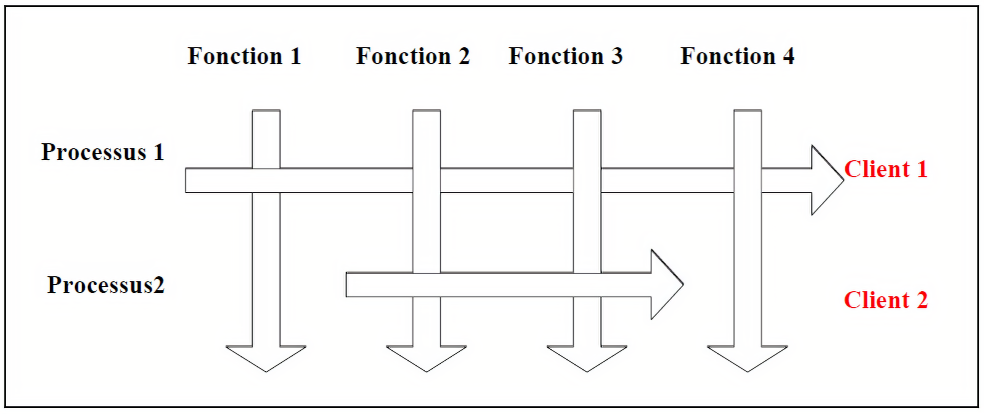


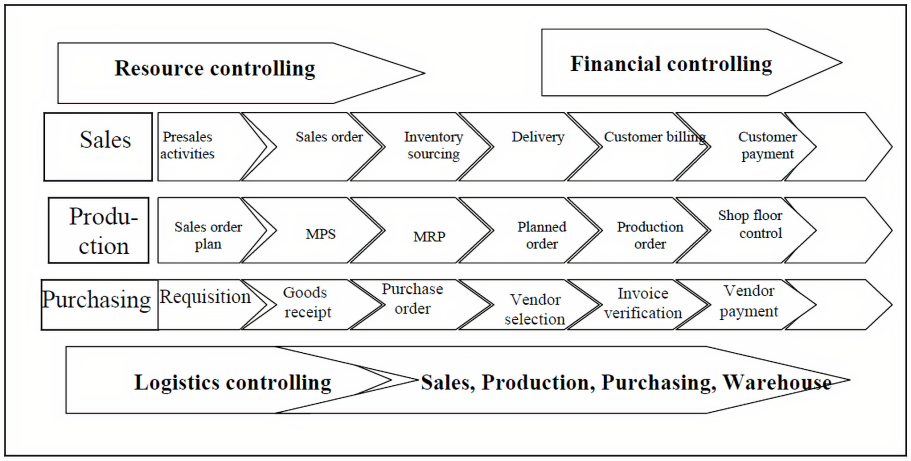
FIGURE 1.3 – *Processus de développement d'un nouveau produit [MANSOURI, 2009]*

Les processus d'une organisation s'étendent de façon fonctionnelle sur plusieurs services ou départements. Ils sont interdépartementaux et représentent la carte fonctionnelle de l'entreprise (figure 1.4 et figure 1.5) :



(a)

FIGURE 1.4 – *Entreprise vue par ses processus [Talbot, 2003]*



(b)

FIGURE 1.5 – *Exemple d'organisation d'une entreprise [Talbot, 2003]*

1.6 Modélisation des processus

Dans le contexte de la modélisation des entreprises, la modélisation des processus métiers constitue un objectif complexe, mais fondamental. Généralement, une procédure d'entreprise est transverse à l'entreprise. Elle concerne plusieurs unités organisationnelles qui impliquent des processus métiers différents. C'est pourquoi la modélisation des architectures des processus métiers assiste la compréhension des interdépendances entre les services métiers des unités organisationnelles d'une entreprise [Dussart et al., 2004]. L'aspect fonctionnel est au cœur des autres vues des entreprises. Elle consiste à représenter la structure et le fonctionnement de l'entreprise.

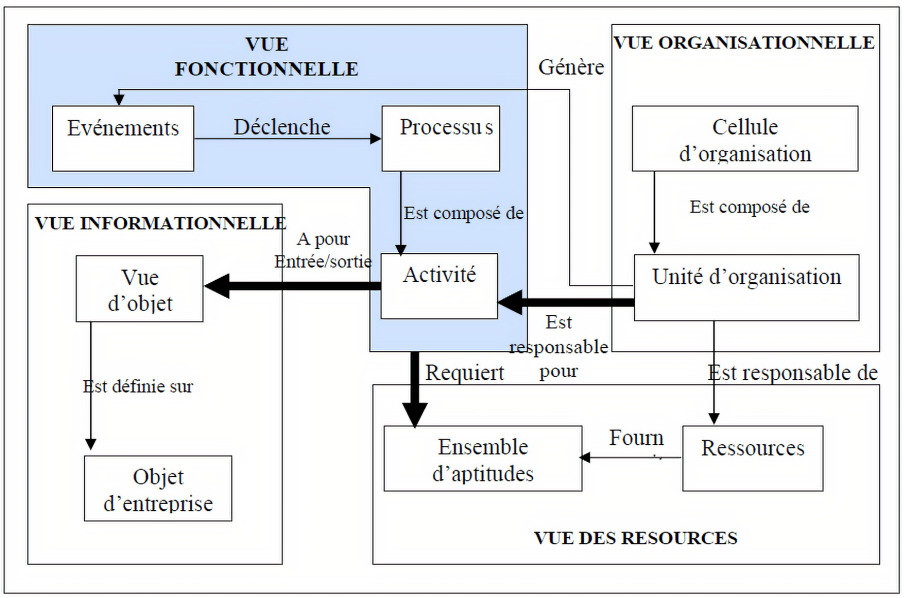


FIGURE 1.6 – *Modélisation des entreprises [Touzi, 2007]*

En effet, la vue fonctionnelle est la seule vue qui est connectée à toutes les autres vues (figure 1.6). L'élément activité de cette vue assure cette connexion avec les autres vues : une activité a pour entrée/sortie des objets (vue informationnelle), il existe une unité d'organisation (vue organisationnelle) de l'entreprise, responsable de l'activité et l'activité requiert pour son exécution un ensemble d'aptitudes fournies par des ressources (vue des ressources) de l'entreprise. Si nous devons caractériser un modèle d'entreprise et nous poser la question de la vue sur laquelle s'appuyer pour commencer cette caractérisation, la réponse est certainement la vue fonctionnelle [Touzi, 2007].

1.7 Représentation des processus

La modélisation des processus métier est au cœur même de la démarche d'analyse dynamique d'une organisation. Que ce soit dans le cadre d'une démarche d'amélioration ciblée ou d'une réorganisation plus globale, la modélisation des processus permet de formaliser le fonctionnement précis d'une organisation en utilisant un langage standard et aisément compréhensible [Morley et al., 2005]. Il est possible d'avoir autant de représentations d'un existant que de points de vue envisagés, il n'existe pas de représentation unique ou universelle d'une même réalité métier. Ces représentations peuvent varier selon le type de représentation choisi, le point de vue envisagé, le niveau de détail, etc.

La richesse sémantique, offerte par les techniques et outils de modélisation organisationnelle de l'entreprise, facilite ainsi une perception commune des processus métiers orientée "amélioration" ponctuelle ou continue.

La modélisation des processus a beaucoup d'avantages pour les entreprises qui cherchent à améliorer leurs performances. On peut citer selon [Gaibor et Oswaldo, 2011] :

- Faciliter la communication en utilisant un langage commun
- Meilleure compréhension de l'existant
- Documentation du processus métier
- Améliorer la situation actuelle
- Expérimenter et simuler de nouvelles situations et de nouveaux concepts et leurs impacts sur l'organisation
- Automatiser le processus

Bien que la modélisation des processus métiers ait beaucoup d'avantages, elle l'est rarement faite. Et si c'est le cas, elle ne l'est pas bien faite. Ceci est dû à la nature complexe et floue des processus métiers qui les différencie des autres projets d'ingénieurs qui se font de manière bien structurée [MANSOURI, 2009]. L'architecture, qui est le haut niveau de la conception fonctionnelle des processus métiers est plus un art qu'une science [Dufresne et Martin, 2003]. Cette complexité extrême des processus métiers est due à plusieurs raisons [Dufresne et Martin, 2003] :

- Ils requièrent plusieurs domaines de connaissance.
- Ils opèrent dans des échelles de temps " largement différentes".
- Ils sont souvent indépendants.
- Les gens ont besoin d'années d'entraînement pour les comprendre ou comprendre "leur raison d'être"
- Ils ont beaucoup " de modification non- contrôlées"

1.8 Techniques de modélisation des processus métiers

Nous présentons dans cette section deux catégories de formalismes de modélisation de processus, qui ne sont pas au même stade d'évolution [Touzi, 2007] :

- **Les formalismes primaires** : présentent uniquement une représentation comportementale (évènementielle) pour décrire les processus. Il s'agit de formalismes simples qui sont basés sur une approche élémentaire du processus. La modélisation du processus est alors réduite à cette vision : un enchaînement d'un ensemble d'activités.

- **Les formalismes évolués** : peuvent inclure, en plus, une représentation informationnelle (donnée) ou/et organisationnelle (acteurs). De plus, les formalismes évolués peuvent offrir une typologie riche d'activités, d'évènements, de contrôles de flux, etc. Ces formalismes peuvent être dédiés à des domaines particuliers : processus de système d'information : UML (Unified Modelling Language), processus métiers : BPMN (Business Process Management Notation), etc.

1.8.1 Organigrammes (Flowcharts)

Présentent probablement les premières notions de modélisation de processus. Ce sont des représentations graphiques d'une séquence logique d'activités : opérations, données, flux, équipements, etc. Les caractéristiques des organigrammes sont flexibles et simples [Touzi, 2007].

Adoptés par la communauté des programmeurs depuis longtemps, ils représentent probablement les premières tentatives de modélisation de processus. Leur symbolisation et leur sémantique se limitent aux structures de contrôle atomique disponibles aux programmeurs. C'est une façon typique de modélisation des structures d'organisation. Ce modèle illustre un aspect de la vue organisationnelle de l'entreprise. Dans l'organigramme sont représentées, en fonction des critères de structuration sélectionnés, les unités organisationnelles (en tant que responsables des tâches) créées et leurs relations. Les unités organisationnelles sont les responsables des tâches à accomplir pour atteindre les objectifs de l'entreprise.

L'organigramme est composé d'unités organisationnelles (formes ovales) et de postes de travail (formes rectangulaires). La modélisation de l'organigramme est le point de départ de la modélisation de l'entreprise. Elle permet de déclarer tous les acteurs des processus, et de réutiliser ces objets tout au long de la modélisation (figure 1.7). Ils ne sont pas assez expressifs pour modéliser des groupes de processus coopératifs [MANSOURI, 2009].

1.8.2 Les diagrammes des flux de données DFD (Data Flow Diagrams)

Le diagramme de flux de données (DFD) est une représentation graphique du flux des données dans un système d'information. Il permet de représenter les processus dans votre système de d'information du point de vue des données. Le diagramme de flux de données permet de visualiser le mode de fonctionnement du système, ce que le système accomplit

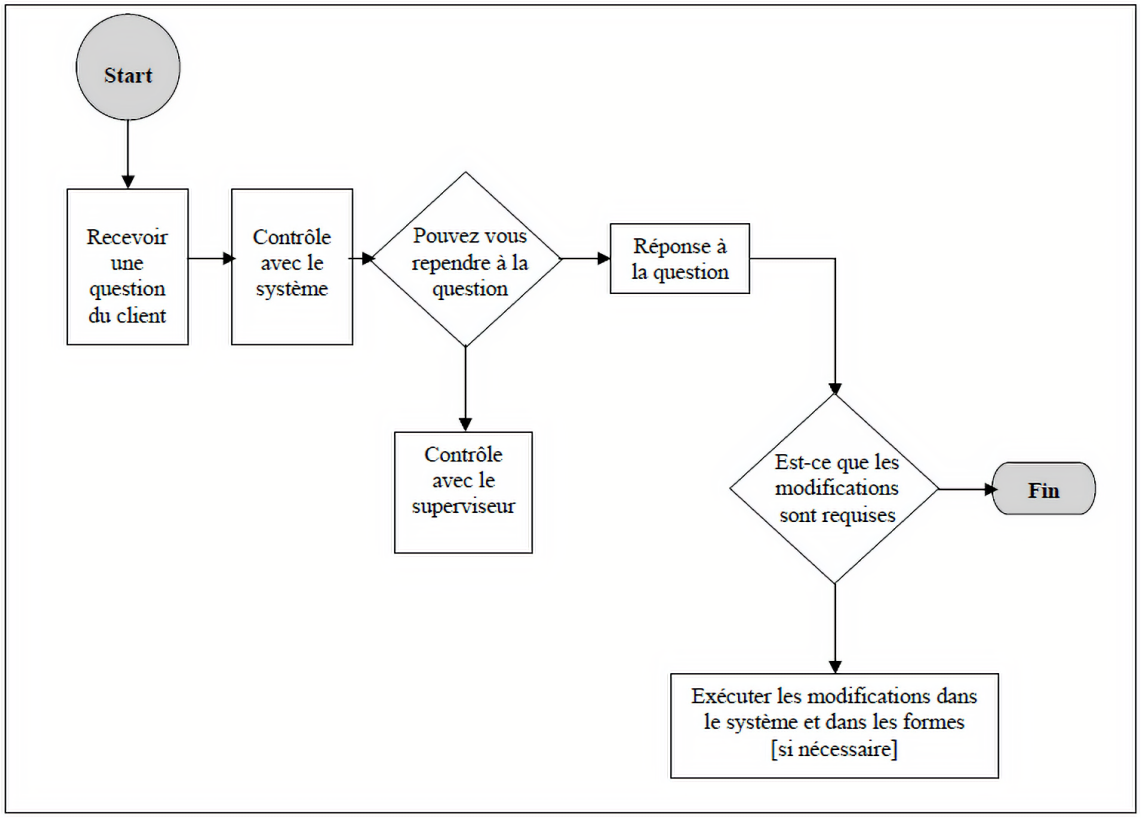


FIGURE 1.7 – *Exemple d'organigrammes [MANSOURI, 2009]*

et comment il sera mis en œuvre, puis comment il sera affiné avec des spécifications ultérieures.

Les DFDs s'intéressent au flux logique des données entre les différents processus du système plutôt qu'au flux de contrôle [Alter, 2002]. Les DFDs étaient les outils clés de modélisation dans les méthodes classiques de développement des systèmes d'information Merise et SADT [MANSOURI, 2009].

Les quatre symboles de base des DFDs sont : le carré représentant les sources et les destinations externes des données. Le rectangle arrondi, représentant les processus. Le dépôt de données est représenté par un rectangle ouvert. Une flèche étiquetée représente le flux de données comme illustré dans la figure 1.8.

C'est une méthode simple pour décrire les interrelations entre les traitements et l'information d'un système et communiquer cette description à des non-spécialistes. Elle est moins appropriée pour décrire les processus manipulant principalement des produits physiques ou comportant plusieurs points de décision (figure 1.9).

1.8.3 IDEF

IDEF est un groupe de méthodes de modélisation du fonctionnement d'entreprise. IDEF a été créée par l'US AIR FORCE et elle est actuellement développée par le <Knowledge Based Systems >. Initialement développée pour les environnements manufacturiers,

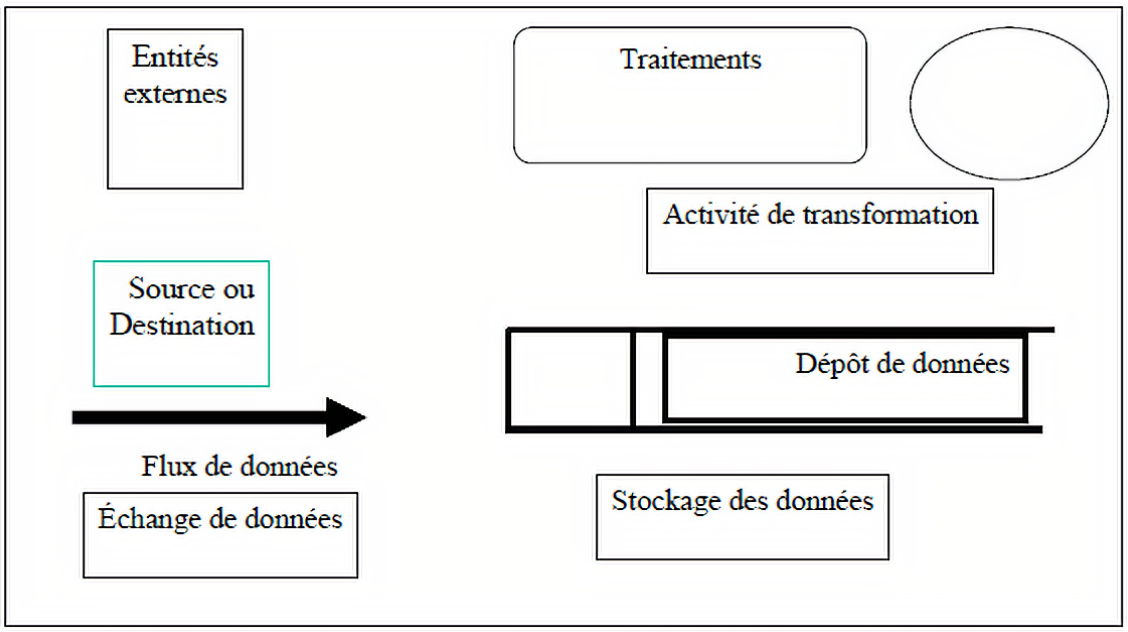


FIGURE 1.8 – *Symboles de base des DFDS [MANSOURI, 2009]*

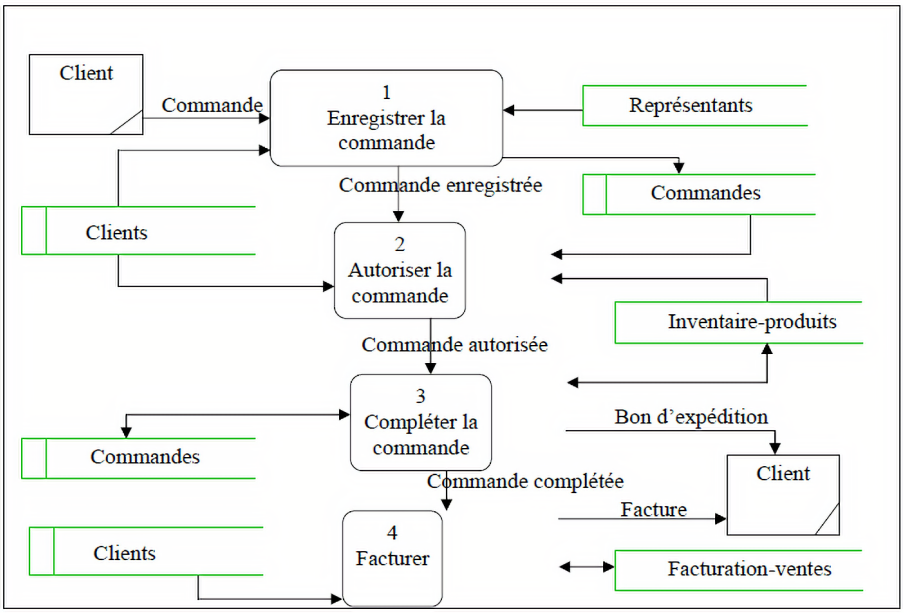


FIGURE 1.9 – *Traitement des commandes de la clientèle représenté par un DFD [MANSOURI, 2009]*

les méthodes IDEF ont été adaptées à une utilisation large et en particulier, au système d'information.

Seize méthodes, de IDEF0 à IDEF14 (en incluant IDEF1X), ont été développées dans le but de modéliser tout type d'information à travers le processus de modélisation. Ces méthodes sont utilisées pour une description graphique des systèmes, une analyse des modèles et comme support d'aide de passage d'un modèle à un autre [Zaidat, 2005]. Nous donnerons les grandes lignes de IDEF0, IDEF2, et IDEF3.

IDEFo

Également connu sous le nom de Structured Analysis and Design Technique (SADT). IDEFo a une structure hiérarchique, grâce à laquelle même les modèles les plus complexes restent clairs, étant donné que les détails sont représentés à différents niveaux. IDEFo est donc souvent utilisé pour représenter des processus. Un grand désavantage de cette technique cependant, est qu'elle ne permet pas la modélisation du temps ni de représenter les relations logiques (relations ET et OU). IDEFo peut traiter des modèles volumineux, mais l'utilisateur n'en a aucune vue générale sur le déroulement. Cette technique n'est donc pas appropriée pour optimaliser le processus de développement de produits.

Le concept de base d'IDEFo est l'activité. Une activité dans ce langage peut être une fonction, un processus, un ensemble de tâches, etc. Chaque activité peut être décomposée en d'autres activités. La figure 1.10 présente le construct graphique associe à l'activité d'IDEFo [Zaidat, 2005]. Une approche IDEFo plus complète peut être représentée de la manière illustrée par la figure 1.11.

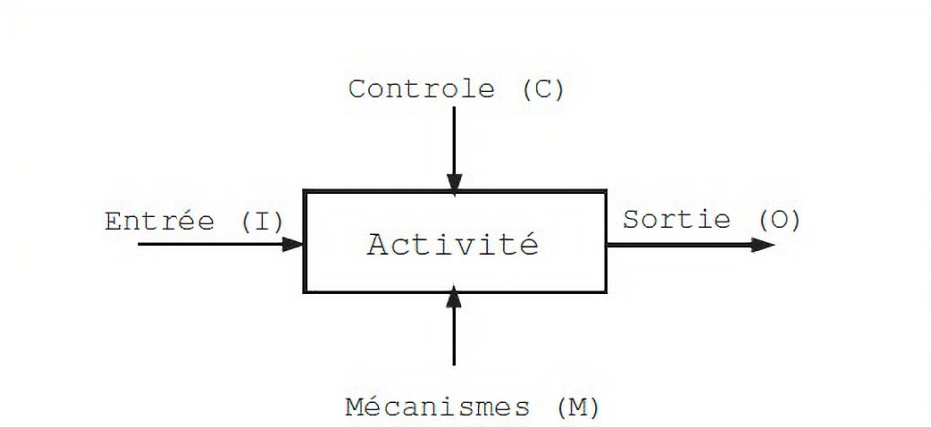


FIGURE 1.10 – *Le modèle SADT/IDEFo [Zaidat, 2005]*

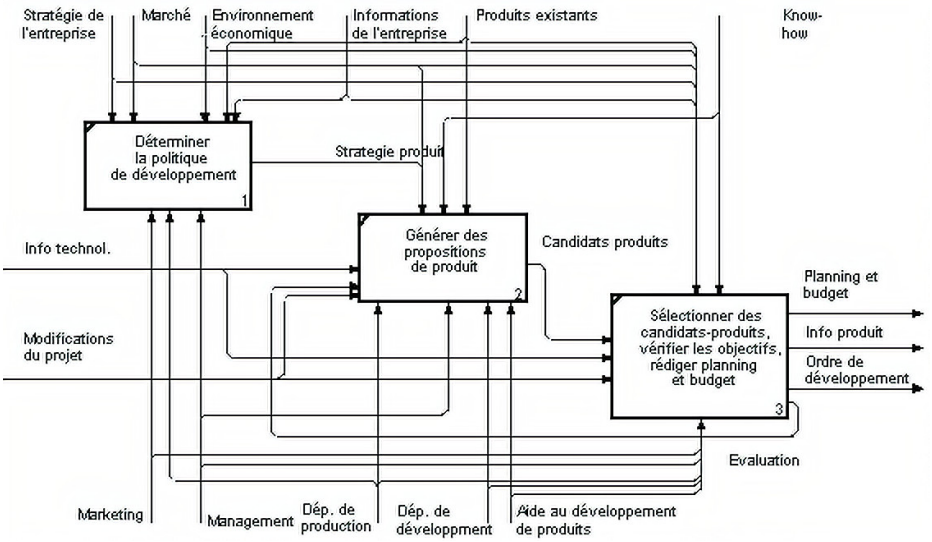


FIGURE 1.11 – *Modélisation IDEFo [Heguy, 2018]*

La principale force de IDEF0/SADT est son niveau de détail et sa simplicité. Son point faible est aussi sa simplicité avec une syntaxe assez pauvre (pas d'origine ni destination des infos par exemple). Le second problème est qu'il n'existe pas de point d'arrêt dans la modélisation, on peut descendre très bas en niveaux de détails [Heguy, 2018].

IDEF1

La méthode IDEF1 a été conçue pour développer des modèles reflétant l'intégration de l'ensemble des informations de l'entreprise ; point de vue informationnel. L'approche d'IDEF1 généralement utilisé pour :

— identifier quelle information est actuellement géré dans l'organisation
— déterminer quels sont les problèmes identifiés lors de l'analyse des besoins qui sont causés par le manque de gestion de l'information appropriée
— préciser quelles informations seront gérées dans la phase mise en œuvre.

La méthode IDEF1 offre un ensemble de règles et procédures pour la création des modèles informationnels. Elle incorpore les graphiques, le texte et les formes nécessaires pour la meilleure description du modèle. Il existe deux composants fondamentaux dans cette représentation [MANSOURI, 2009] :

– les diagrammes : les caractéristiques du modèle informationnel, représentées selon un ensemble de règles et de procédures,

– le dictionnaire : chaque élément du modèle est décrit textuellement pour obtenir une définition explicite.

IDEF2

IDEF2 est un langage de modélisation du comportement d'un système de production basé sur le concept des files d'attente, dérivé du langage SLAM. C'est une méthode complémentaire à SADT qui vise à répondre aux lacunes du point de vue analyse des aspects dynamiques d'un système. IDEF2 est basée sur 4 modèles [MEGARTSI, 1997] :

— Modèle du système physique.
— Modèle du flux des entités.
— Modèle de gestion des ressources.
— Modèle de contrôle du système.

IDEF2 aborde donc de façon privilégiée les vues informationnelles et ressources sur des niveaux d'abstraction proches de l'exécution. Les résultats obtenus par l'étude d'IDEF2 au travers de la simulation correspondent à des cas de fonctionnement particuliers, aucune généralisation sur le système modélisé n'est possible.

IDEF3

La méthode IDEF3 est proposée en 1992 pour dépasser les limites d'IDEF0 en matière de modélisation du comportement de l'entreprise, donc la représentation des processus opérationnels.

IDEF3 représente les modèles sous la forme de flux de processus et de diagrammes de changement d'état des objets associés. Le langage de modélisation est graphique et chaque processus est considéré comme une tâche à réaliser. Un objet est une abstraction qui représente une entité physique de l'environnement réel modélisé ou un concept qui intervient dans la description d'un processus [MEGARTSI, 1997]. IDEF2 et IDEF3 représentent donc le point de vue dynamique. A la différence d'IDEF0, les flèches sont des liens de séquence comme dans BPMN et non des flux avec des noms des éléments supportés par les flux, comme on peut le voir dans la figure 1.12.

Les concepts utilisés pour décrire le flux de processus sont les suivants [MEGARTSI, 1997] :

— Unités de comportements ou processus.
— Les fonctions.
— Les liens.
— Les référents.

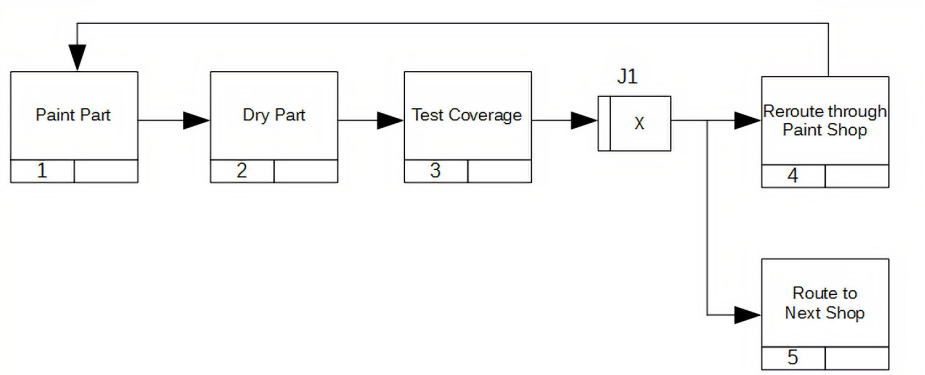


FIGURE 1.12 – *Modèle de flux de processus de IDEF3 [Heguy, 2018]*

IDEF3 est une méthode intéressante par rapport à la description de flux de processus, mais la richesse de ses outils ne lui permet pas de décrire simplement et formellement une condition sur l'exécution d'un processus, toute information additionnelle est traitée sous forme de commentaire.

1.8.4 Réseau de Pétri (RdP)

Parmi les formalismes utilisables pour décrire les systèmes à événements discrets, les réseaux de Petri jouent un rôle important car ils sont capables de modéliser des propriétés telles que synchronisation, parallélisme, conflits, mutuelle exclusion et partage de ressources [Dhouibi, 2005].

Les réseaux de Petri (RdP) constituent, depuis leur introduction en 1964 par Carl Adam Petri, un puissant outil graphique de représentation des phénomènes et mécanismes séquentiels, de modélisation des systèmes à événements discrets. Les modèles obtenus, outre l'expression graphique de la structure des systèmes, permettent une analyse de leurs propriétés [Dhouibi, 2005] :

— les propriétés dynamiques intéressantes du système : bornitude, absence de blocage, invariants, réversibilité, ...
— La représentation du processus : un comportement donné d'un processus en modélisant le fait que les ressources sont partagées, que des priorités interviennent, qu'il peut y avoir présence d'une gamme de fabrication,...
— Les objectifs de production : le processus doit obéir à des critères liés aux coûts de fonctionnement et à sa rentabilité et devra être optimisé : ressources minimales nécessaires, taux de production, production au plus tard pour limiter les stocks de pièces, périodicité du système,...

Cet outil de modélisation a le double avantage d'être graphique et mathématique, atouts qui enthousiasment aussi bien les théoriciens que les praticiens [Bourjij, 1994] :

— l'aspect graphique clarifie et synthétise la représentation du système modélisé (visualisation), le déplacement de marques dans les places simulant la dynamique de celui-ci
— l'aspect mathématique permet de poser les équations d'état du système et d'analyser ce dernier par l'algèbre linéaire ou la théorie des graphes

Il est composé par un ensemble de places représentées par des cercles, un ensemble de transitions représentées par des barres et deux applications ayant comme ensemble d'arrivée l'ensemble des entiers naturels :

$$R = <P, T, Pre, Post>$$

où :

— P est un ensemble fini de places,
— T est un ensemble fini de transitions,
— $Pre : P \times T \rightarrow N$ est l'application places précédentes,
— $Post : P \times T \rightarrow N$ est l'application places suivantes

Fortement utilisé dans le domaine industriel, il sert à traiter les problèmes de synchronisation d'activités. Les notions graphiques sont : les places (nœuds), les arcs (flèches) et les transitions (contrôles). Les places correspondent aux activités des processus modélisées.

Les arcs sont associés aux évolutions du processus et des flux d'informations. Les transitions représentent les évènements ou les conditions à vérifier pour avancer dans le processus (figure 1.13).

Les RdP peuvent être très utiles en automatique, notamment par la simplicité de leur représentation des systèmes et la diversification des outils mathématiques associés. Le

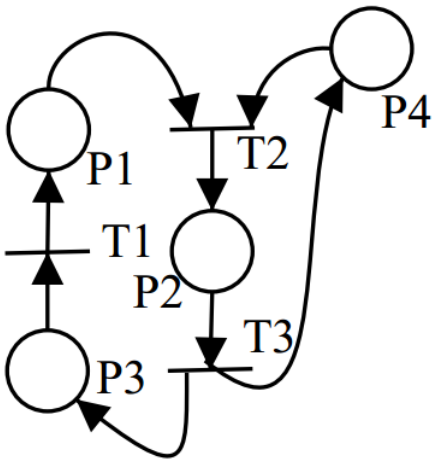


FIGURE 1.13 – *Exemple d'un Réseau de Petri*

champ d'utilisation des RdP couvre un large éventail de disciplines. L'apport des RdP est très important dans la conception, l'analyse et le diagnostic des systèmes. Cependant, la représentation graphique n'est valable que pour des systèmes de petite dimension sinon, la lisibilité du graphe est compromise [Bourjij, 1994].

1.8.5 La méthode GRAI

GRAI, acronyme de Graphes à Résultats et Activités Inter reliées a été développé par Breuil, Doumeingts et Pun au laboratoire GRAI, université de Bordeaux, au début des années 80. Le modèle conceptuel GRAI est un système hiérarchisé décomposé en trois sous-systèmes [MEGARTSI, 1997] :

— Le système physique (machines, hommes, matières premières) décomposé en centres de charges. Ces centres se présentent sous la forme d'îlots de fabrication définis par des techniques de groupement.

— Le système de décision, décomposé en niveaux de décisions caractérisés par un horizon de prise de décision et une période de temps au bout de laquelle les décisions prises sont remises en question.

— Le système d'information qui sert de liaison entre le système de décision et le système physique.

— L'ensemble constitué par le système de décision et le système d'information forme le système de pilotage de production.

La grille GRAI permet de différencier les liaisons de dépendance fonctionnelle (double flèche, transmission d'une consigne ou d'un objectif) des liaisons informationnelles (simple flèche, transmission d'un flux informationnel) entre centres de décisions (figure 1.14).

Les réseaux GRAI représentent le fonctionnement de tout ou une partie d'un centre de décision d'une grille GRAI. Le processus de prise de décision peut être représenté grâce à des activités de décision ou d'exécution. Toutefois, le réseau GRAI s'avère complexe

pour représenter plusieurs activités dans le même modèle. De plus, il ne permet pas de représenter une vue comportementale [Heguy, 2018].

Pour compléter la grille, la mise en œuvre de la décision est détaillée en réseau d'activités. Ce réseau (figure 1.15) permet de différencier les activités "d'exécution" de celles de "décision".

Au début des années 90, la méthode GRAI a donné naissance à la méthodologie GIM (GRAI Integrated Methodology). La méthodologie GIM s'appuie sur le modèle conceptuel de référence qui décompose une entreprise en trois sous-systèmes : le système physique, le système d'information et le système décisionnel. Elle analyse l'entreprise par quatre vues de modélisation qui sont : information (données/connaissances), décision (chaine d'activités et centres décision), physique (ressources) et fonction (décomposition fonctionnelle) [Zaidat, 2005].

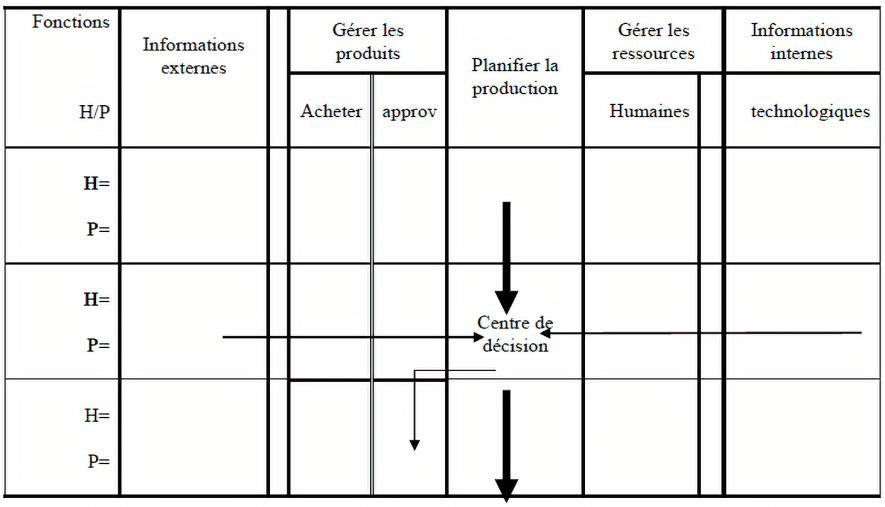


FIGURE 1.14 – *La grille de GRAI [MEGARTSI, 1997]*

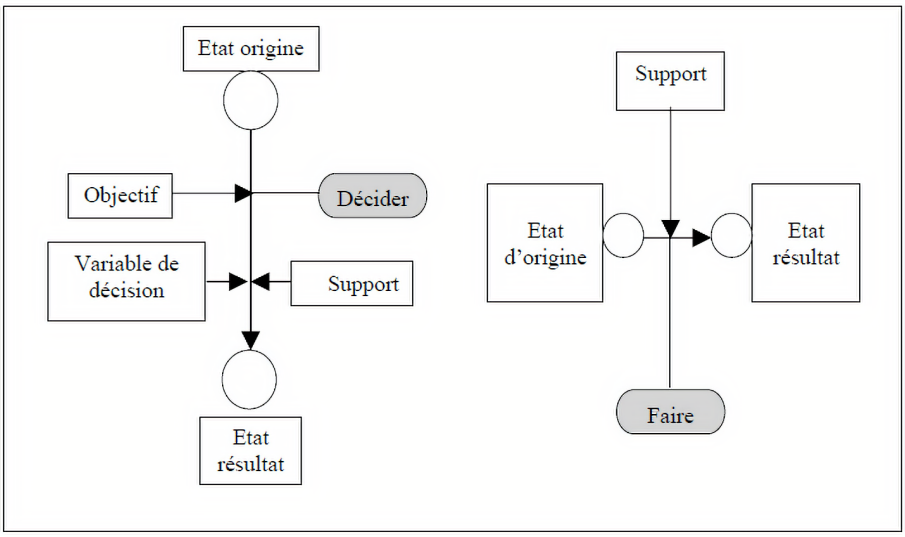


FIGURE 1.15 – *Réseau GRAI, activité de décision et activité d'exécution [MEGARTSI, 1997]*

1.8.6 CIMOSA

CIMOSA (Open System Architecture for CIM) est une architecture de référence des systèmes ouverts pour la productique, développée par le Consortium AMICE dans le cadre du programme ESPRIT (Projets No. 688, 5288 et 7110). CIMOSA a pour but de fournir un support tout au long du cycle de vie du système CIM, en particulier pour [Zaidat, 2005] :

— la définition précise des objectifs de l'entreprise et des stratégies manufacturières.

— la configuration et l'exploitation du système CIM (Computer intergrated manufacturing) en réponse à ses objectifs.

— la gestion du système dans un contexte en changement perpétuel.

La méthodologie CIMOSA repose sur une séparation entre l'environnement de l'ingénierie et l'environnement opérationnel de l'entreprise. Son édifice comprend [MEGARTSI, 1997] :

1. Un cadre de modélisation (incluant une architecture de référence qui fournit une intégration conceptuelle par unification sémantique).
2. Une infrastructure intégrante (permettant l'intégration physique et l'intégration des applications).
3. Un cadre méthodologique (couvrant le cycle de vie du système de production et assurant la cohérence de l'ensemble).

Le but du cadre de modélisation de CIMOSA ou CUBE CIMOSA est de fournir un cadre conceptuel, une méthode et des outils de modélisation pour assister l'utilisateur dans le développement du modèle particulier, propre à son entreprise. Il est composé de deux parties : Une architecture de référence, générique et réutilisable dans différents projets et une architecture particulière propre à l'entreprise. Le cadre de modélisation développé dans CIMOSA comme illustré dans la figure 1.16 s'articule autour de trois axes de modélisation orthogonaux :

— L'axe de généricité qui suggère de construire le modèle particulier de l'entreprise à partir de modèles partiels, eux-mêmes exprimés en termes de construction générique de base.

— L'axe de génération qui propose de modéliser d'abord les besoins de l'entreprise. Il est appelé aussi axe des vues (fonctionnelle, informationnel, ressources et organisation).

— L'axe de dérivation qui invite à modéliser d'abord les besoins de l'entreprise, puis les spécifications de conception et enfin la description de l'implantation.

CIMOSA fournit un ensemble très riche de concepts de base dans son langage de modélisation, couvrant les quatre vues mentionnées ci-dessus. Le modèle de CIMOSA est basé sur les concepts d'événements, de processus, d'activités, et d'opérations. La méthodologie CIMOSA apporte une réponse originale au problème d'intégration globale en fournissant une infrastructure intégrante et propose une modélisation cohérente de l'entreprise, depuis l'expression précise des besoins jusqu'à une description conforme de l'implantation mais la représentation textuelle préconisée par CIMOSA pendant l'analyse

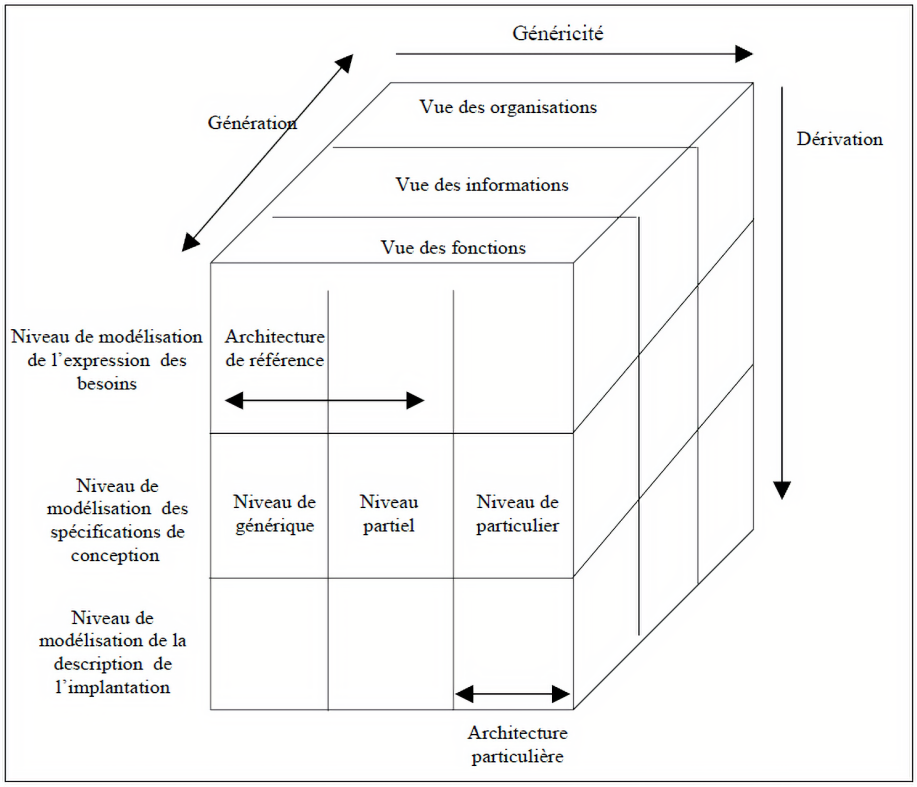


FIGURE 1.16 – *Le cadre de modélisation de CIMOSA [MEGARTSI, 1997]*

comportementale ne permet pas de visualiser facilement le comportement d'un processus. Cependant, l'absence de formalisme graphique de représentation ne permet pas une visualisation claire des échanges de données pour un public non technicien. CIMOSA n'offre aucun moyen de représenter l'interopérabilité [Heguy, 2018].

1.8.7 PERA

PERA (Purdue Entreprise Reference Architecture) est une méthodologie complète d'ingénierie des environnements industriels. PERA est une architecture de référence développée par le professeur Williams, de Purdue University. Elle est une méthodologie d'ingénierie complète, destinée aux environnements industriels et tertiaires.

Son objectif est d'établir les bases pour le traitement des fonctions mises en œuvre par l'être humain dans le domaine de l'intégration des entreprises.

La description des tâches et des fonctions de l'entreprise est décomposée en deux grands courants [MEGARTSI, 1997] :

— Le courant des informations.
— Le courant de la production.

Dans le modèle de PERA, les classes des fonctions concernant la décision, le contrôle et l'information sont regroupées dans un seul courant appelé fonction d'information.

- Pendant l'implémentation, les deux courants cités ci-dessus sont réaménagés dans trois jeux d'implémentation de tâches et de fonctions :

1. Les activités de l'être humain qui sont :
   — Activités d'information.
   — Activités de production.
2. Les activités d'information non effectuées par l'être humain.
3. Les activités de production non effectuées par l'être humain.

Différemment de CIMOSA qui définit quatre vues : fonctionnelle, informationnelle, ressources et organisationnelle, PERA se focalise sur seulement deux vues : Une vue fonctionnelle et une vue d'implémentation.

Le paradigme de modélisation dans PERA s'organise autour de la représentation des tâches du système d'information, de la production et celles effectuées par l'être humain de l'entreprise modélisée. Le schéma de représentation de la connaissance des tâches citées ci-dessus est similaire à celui utilisé dans IDEF. Il comporte des entrées prenant en compte le temps, des paramètres de validation, processus de transformation, sorties et mémorisation des entités. Les points forts de la méthodologie PERA sont son cycle de vie et son aspect pratique. Son cycle de vie est qualifié d'exhaustif. C'est une démarche qui prend en compte les aspects réels d'application d'une méthodologie [MEGARTSI, 1997].

La méthodologie définit toutes les phases du cycle de vie d'une entité industrielle depuis sa conceptualisation jusqu'à sa mise en opération en passant par les phases de conception. La figure 1.17 précise l'architecture de la méthodologie, organisée suivant le cycle de vie de toute entité industrielle. Les numéros indiquent les différentes étapes de la [Abdmouleh, 2004].

1.8.8 GERAM

La norme ISO 15704 a généralisé les résultats scientifiques importants issus des développements d'architectures de référence et de méthodologies pour l'ingénierie d'entreprise (CIMOSA, PERA et GRAI-GIM) dans la formalisation de GERAM. GERAM n'est pas une nouvelle architecture de référence mais une organisation et une intégration des connaissances développées dans les architectures de références citées [Zaidat, 2005]. Une telle connaissance traite les méthodes et les outils requis. GERAM a plusieurs objectifs, nous citerons [MEGARTSI, 1997] :

— Fournir un environnement de modélisation consistant qui va mener éventuellement à un code exécutable par l'ordinateur.
— Promouvoir une ingénierie pratique pour des structures réutilisables des modèles standards.
— Se munir d'une méthodologie détaillée pour l'utilisation, de laquelle le développement personnel de tout type d'entreprise puisse facilement découler.
— Donner le meilleur traitement possible des capacités d'une entreprise d'un point de vue des systèmes.

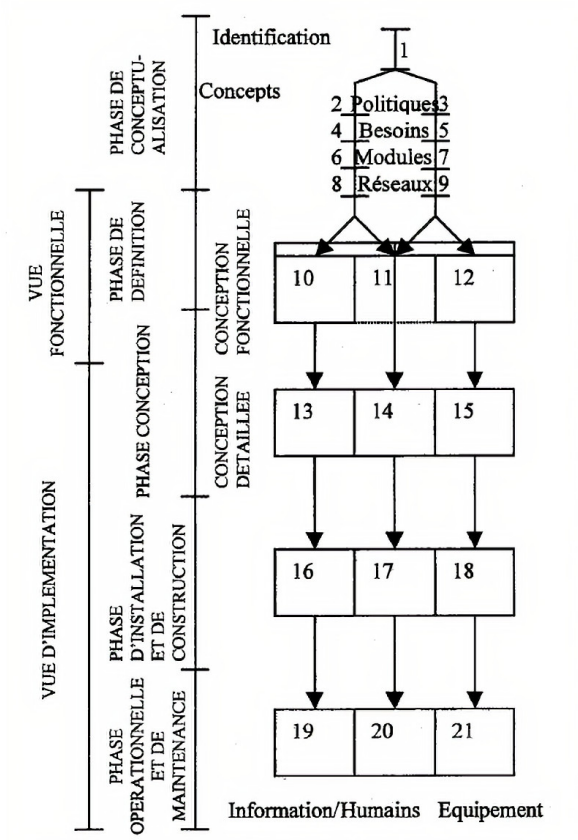


FIGURE 1.17 – *Structure de l'architecture PERA [Abdmouleh, 2004]*

— Etre générique à tout type d'entreprise sans se soucier de la complexité de l'industrie et de ses applications.
— Fournir une unification des perspectives pour la production, traitements, développement de l'entreprise et une gestion stratégique.

GERAM est basée sur un modèle graphique matriciel du cycle de vie d'une entreprise, utilisé comme base pour la comparaison et l'évaluation des compétences de chacune des architectures étudiées. Ce modèle a été structuré pour inclure une présentation des capacités et points forts des architectures. GERAM reste une coque vide qui n'offre pas son propre langage de modélisations, sauf ceux fournis par les autres méthodes.

1.8.9 Diagrammes d'enchaînement de processus d'ARIS

ARIS (Architecture of Integrated Information Systems) a été développée dans les années 1990 par le professeur August-Wilhelm SCHEER. Elle a été proposée pour les phases d'analyse et de définition des besoins d'un système d'information de gestion [A. Scheer et Kruse, 1994]. ARIS définit Trois vues : la vue fonctionnelle, la vue informationnelle et la vue organisationnelle. Chaque vue va répondre à une question liée au processus modélisé [Heguy, 2018] :

— Fonctions : « What ? » : par quoi est réalisé le processus. Pour y répondre, on peut utiliser un diagramme en arbre représentant les activités de l'entreprise ;

— Organisation : « Who ? » : chaque processus va être géré par un ou plusieurs acteurs. Ils peuvent donc être représentés sous la forme d'un organigramme, détaillant l'entreprise, les services, les responsables de chaque service, etc. de manière hiérarchique ;

— Produits/Services : « Why ? » : pour quelle raison ce processus existe-t-il, à quoi sert-il. On détaille à cette étape les produits et/ou les services concernés par ce processus, via un diagramme en arbre par exemple ;

— Données : « Which information ? » : quelles seront les informations nécessaires pour réaliser ce processus. Pour y répondre, nous pouvons utiliser l'ERM (entity-relationship model, ou modèle entité-association) ;

— Contrôle : « How ? » : comment sera géré le processus. Pour cela, il est possible d'exploiter l'EPC (Event-driven Process Chain, ou chaînes de processus événementielles).

Chaque vue est traitée à part, et les relations entre les trois vues sont représentées par des contrôles de flux. La vue de processus dans cette méthode est basée sur les diagrammes d'enchaînement de processus ou (Process Chain Diagram (PCD) .

Les PCD peuvent exister sous deux formes : Tableau ou Diagramme. Le Tableau réunit les entités provenant des différents modèles de vue, ce qui permet d'offrir une représentation "étendue" des processus de l'entreprise. Il permet de séparer les concepts (Évènement, Fonction, Données, Système applicatif et unité d'organisation) et de les présenter dans des couloirs. Cette représentation offre une vue générale de la composition structurelle des processus et de leurs relations avec les autres vues de l'entreprise. Le Diagramme reprend exactement les mêmes concepts, mais avec une représentation "à plat " [Touzi, 2007].

1.8.10 La Chaîne de Processus Evénementielle (CPE)

Les fonctions et les évènements permettent de représenter les processus sous la forme d'Event Driven Process Chain. Tout comme ARIS, EPC est issue des travaux d'August-Wilhelm SCHEER. D'autres modèles sont proposés par cette méthode dont une vue plus globale des processus permettant de représenter la chaîne de valeur (Value Chain) [Heguy, 2018].

Les diagrammes de chaîne de processus événementielle ou Chaîne de processus événementielle (EPC) représentent les processus métier de l'organisation avec un formalisme défini. La figure 1.18 illustre les éléments de notation. Chaque diagramme EPC comporte des éléments visuels signifiant une logique particulière. Un modèle EPC représente alors un processus métier comme une succession de fonctions et d'événements.

La modélisation d'un processus métier avec un diagramme EPC est constituée d'éléments graphiques représentant les fonctions, les événements, les opérateurs logiques et des objets divers comme les ressources employées. Une chaîne de processus événementielle comprend [MANSOURI, 2009] :

— **L'enchaînement des fonctions** (représentées par des parallélogrammes) dans le sens du processus de l'entreprise.

— **Les événements déclencheurs** et résultats (représentés par des rectangles) pour chaque fonction. La désignation d'un événement doit comprendre à la fois l'objet support ('patient') et l'information de changement d'état de cet objet ("arrivé"). Comme les événements définissent l'état ou la condition qui déclenche une fonction ainsi que l'état qui en marque l'achèvement, les nœuds de départ et d'arrivée d'une telle CPE sont toujours des événements.

Dans l'exemple de la figure 1.19, il existe une connexion ET par une règle ET entre les événements de départ. Cela implique que le processus activer phase de fabrication ne peut être lancé que lorsqu'il existe une gamme opératoire et lorsque les ressources nécessaires ont été vérifiées. Pour que le processus soit lancé, il faut que les deux événements aient déjà eu lieu. Le deuxième cas représente une connexion OU exclusive (OU exclusif) à l'aide d'une règle XOR. Le résultat de la fonction Vérifier l'offre du fournisseur peut être l'acceptation ou le refus de l'offre. Les deux cas de figure ne peuvent toutefois pas se présenter en même temps. Outre ces deux cas et la connexion au sens d'un 'OU exclusif', il peut aussi exister des relations plus complexes. Dans ce cas, une règle générale peut être représentée dans la CPE qui sera plus amplement détaillée sous forme de diagramme de règles [Ari, 2016].

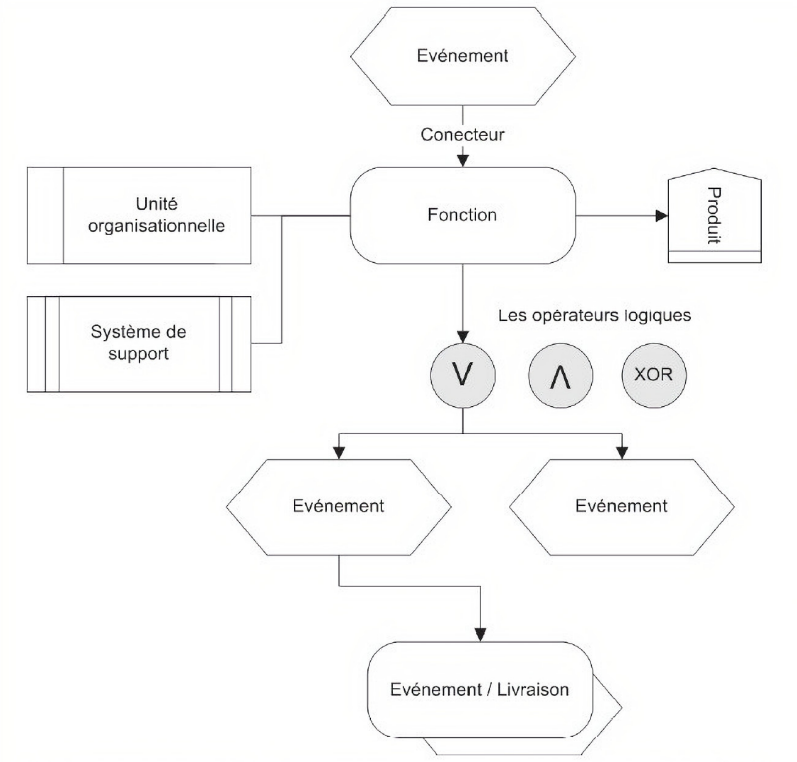


FIGURE 1.18 – *Éléments de la notation EPC [Briol, 2008]*

Selon [Briol, 2008], pour l'élaboration des diagrammes EPC, il faut considérer cinq règles :

— Le processus commence toujours avec un événement.
— Le processus se termine toujours avec un événement.
— Les fonctions et événements sont alternés.
— Les fonctions et événements disposent d'une entrée et d'une sortie.
— Un événement est un élément passif sans capacité de décision.

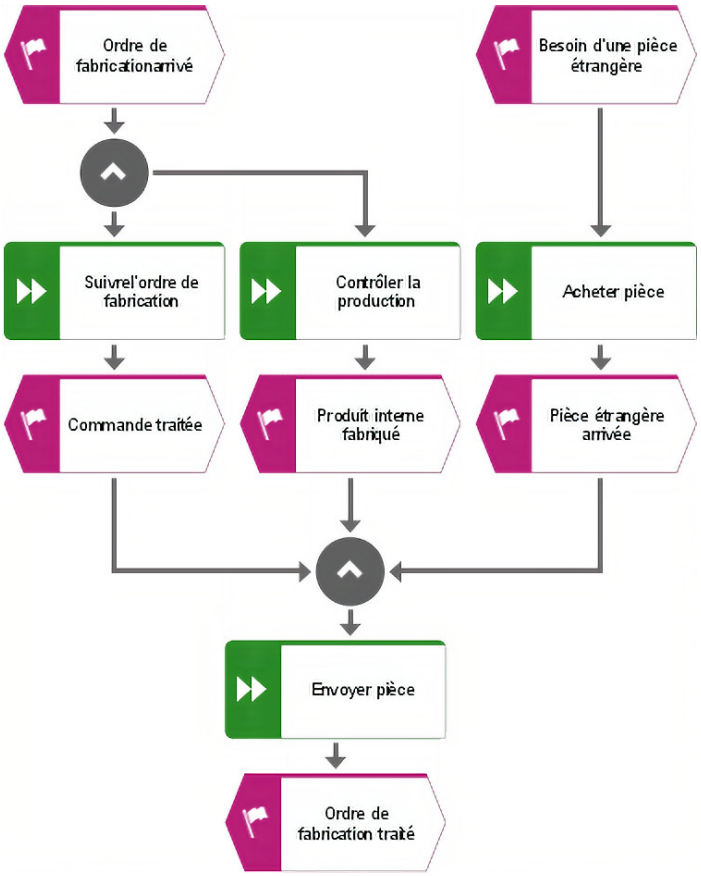


FIGURE 1.19 – *Exemple de CPE [Ari, 2016]*

1.8.11 BPMN

En 2000, un consortium d'entreprises impliquées dans le développement du commerce électronique, s'est donné pour objectif de définir un langage de description des processus métiers, qui puisse en traduire la complexité tout en restant accessible. Cela a donné lieu à un formalisme orienté activité, BPMN, en partie inspiré d'UML, et qui en 2005, a été adopté par l'OMG comme UML l'avait été quelques années auparavant. BPMN est une notation, c'est-à-dire un ensemble de symboles permettant de représenter des processus métiers sous forme graphique. Par rapport aux langages antérieurs, on peut relever que le diagramme d'activités d'UML a été une source d'inspiration, mais BPMN a eu un apport majeur dans la représentation des différents échanges entre processus. Il a, en effet, été conçu pour pouvoir modéliser des processus privés (internes à une entreprise) comme des processus publics (qui impliquent deux ou plusieurs organisations)[Morley et al., 2011].

La version BPMN 2.0 vient remédier aux problèmes d'exécution des modèle BPMN. Dans cette version BPMN évolue vers un schéma d'échange standard basé sur XML permettant l'échange de modèles exécutables. BPMN 2.0 a vocation de devenir un langage de modélisation exécutable en remplacement de BPEL. Plus précisément, BPMN 2.0 ajoute par rapport à la version 1.2 les points suivants [Ben Said, 2017] :

— Un méta-modèle normalisé et un format de sérialisation pour BPMN, qui permet aux concepteurs d'échanger des modèles BPMN entre les outils de différents fournisseurs.

— Une sémantique d'exécution normalisée pour BPMN, qui va permettre aux fournisseurs logiciels d'implémenter des moteurs d'exécution interopérables pour les processus métier.
— Un processus de transformation détaillé de BPMN pour WS-BPEL, montrant l'alignement de BPMN avec les outils et les normes existants.
— Une définition d'un nouveau type de diagramme, nommé chorégraphie, permettant de se focaliser sur les interactions entre les partenaires d'un processus inter-organisationnel.
— Certains éléments de modélisation supplémentaires pour des processus, telles que les tâches manuelles et les tâches humaines.

De plus, BPMN 2.0 est une notation ouverte et extensible par les concepteurs et les outils de modélisation. En effet, BPMN 2.0 offre un mécanisme d'extension permettant l'adjonction de nouveaux éléments (ayant une représentation graphique particulière) et / ou attributs (informations caractérisant un élément). Cependant, ces extensions ne doivent pas changer les représentations (les formes) définies en standard. Parmi les mécanismes d'extension offerts par BPMN, nous pouvons citer [Ben Said, 2017] :

— L'utilisation de marqueurs (indicateurs) pour décrire un type particulier ou bien une information spécifique d'un élément existant dans le standard.
— L'adjonction de nouvelles formes graphiques pour satisfaire un besoin spécifique. Les éléments ajoutés sont considérés comme des artefacts.
— La coloration des éléments graphiques ou bien le changement de leurs styles de trait pour introduire une sémantique particulière qu'on associe à un élément de la notation standard. Par exemple, elle permet de distinguer les informations produites des informations consommées en utilisant deux couleurs différentes.

BPMN (Business Process Modeling Notation) est une notation qui permet de décrire les processus métier. Un diagramme BPMN a des éléments graphiques qui permettent de modéliser les activités, les flux, les relations, les données des processus, leurs interactions, etc [Gaibor et Oswaldo, 2011].

L'objectif principal de l'effort de BPMN était de fournir une notation qui soit facilement compréhensible par tous les utilisateurs métiers, depuis les analystes qui créent les premières ébauches des processus, jusqu'aux développeurs techniques responsables de l'implémentation de la technologie qui va s'acquitter de ces processus, et, enfin, les gens d'affaires qui vont gérer et contrôler ces processus.

La BPMN sera également soutenue par un modèle interne qui permettra la génération d'exécutables sous le format BPEL (business Process Exexutable Langage). Ainsi, BPMN veut créer un pont standard pour l'écart entre la conception et la mise en œuvre des processus métiers [Touzi, 2007].

Un processus modélisé en BPMN est un graphe qui contient des noeuds reliés par des arcs. Ils peuvent appartenir à des conteneurs et sont annotés par des artefacts. Les nœuds sont les objets de flux (object flows). Les éléments de base de représentation graphique avec BPMN sont de trois types [MANSOURI, 2009] :

— les conteneurs (point de vue organisationnel) qui sont les couloirs ("pool") et les bandes ("lane"). Ce sont des partitions du processus qui relèvent d'un acteur ou d'une entité organisationnelle particulière.
— Les noeuds du graphe (point de vue fonctionnel) représentent les activités ("activities", symbole rectangulaire), les évènements ("events", symbole circulaire) et les branchements conditionnels ("gateways ", symbole losange).
— Les arcs (point de vue informationnel) représentent les flux d'information. Il en existe trois types : les flux de contrôle séquentiel, qui caractérisent une communication interne (dans un même couloir ou une même bande, "sequenceflow", trait plein), les flux de message, qui caractérisent une communication interconteneurs ("message flow", trait pointillé) et les associations ("Association", trait incliné). Cette dernière est utilisée, par exemple, pour associer un élément de documentation d'une entité, pour identifier des données en tant qu'entrées ou sorties d'une activité ou pour associer une compensation à une activité, etc.

Les évènements dans BPMN sont typés et à chaque type correspond un symbole particulier normalisé : début et fin, arrivée d'un message, échéance d'une temporisation, exception, nécessité de mettre en œuvre une compensation (défaire ce qui a été fait précédemment pour revenir à un état stable). La figure 1.20 reprend les symboles utilisés. L'exemple de modélisation du proccesus de commande de pizza est illustré dans la figure 1.21.

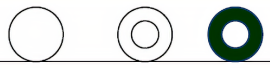
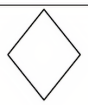
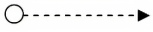
Objet	**Symbole**
Evénement (Event)	
Activité (Activity)	
Branchement sequentiel (Gateway)	
Flux séquentiel (Sequence Flow)	
Flux de messages (Message Flows)	
Associations	

FIGURE 1.20 – *Symbolisation BPMN [Touzi, 2007]*

En résumé, les points forts du formalisme BPMN sont [Touzi, 2007] :

— Une notation intuitive et plus ergonomique à l'usage des acteurs de l'organisation et de la gestion d'entreprise.
— Un vocabulaire riche et adapté aux besoins de conception de processus métiers complexes –ensemble de concepts et de relations – rigoureusement défini pour fournir un socle robuste à l'outillage des approches processus.

— Un lien fort avec le format d'échange BPEL.

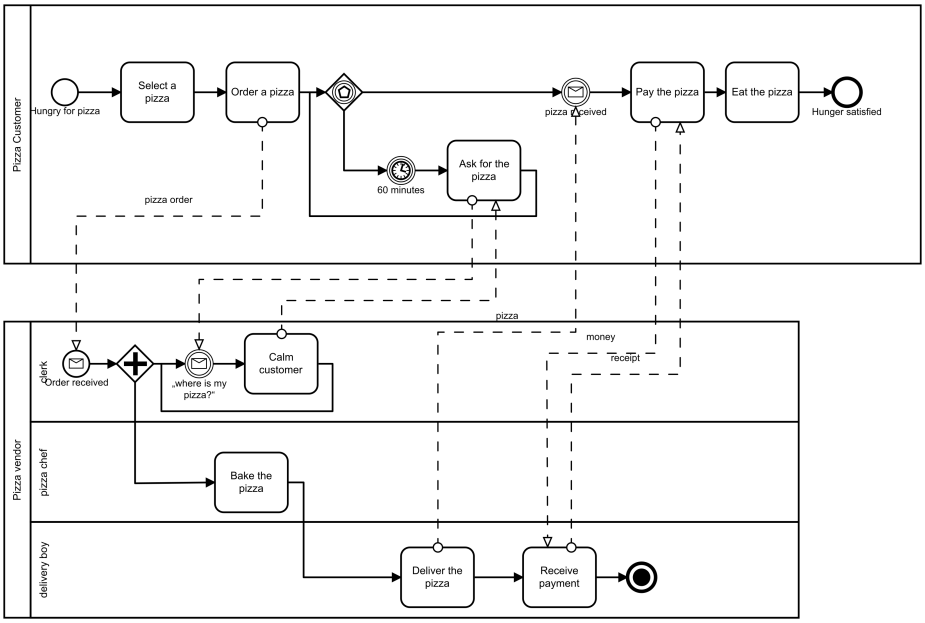


FIGURE 1.21 – *Exemple d'un processus BPMN*

Le principal objectif de la norme BPMN pour modéliser les processus est d'être compréhensible par les multiples utilisateurs du processus : les acteurs, les concepteurs mais aussi les spécialistes informatiques chargés de les intégrer dans les BPMS. En effet, ce type de modèle permet ensuite de facilement générer un diagramme exécutable par des BPMS [Froger, 2020].

1.8.12 Unified Modelling Language : UML

"UML est un langage pour spécifier, visualiser, construire, et documenter les artefacts des systèmes logiciels, ainsi que pour la modélisation d'entreprise et des systèmes non logiciels" [www.omg.org].

Comme son nom l'indique, ce langage est né de la fusion de plusieurs langages de modélisation, issus notamment de la méthode de Grady Booch particulièrement adaptée à la conception et à l'implémentation, de la méthode OOSE (Object Oriented Software Engineering) de Ivar Jacobson : qui permettait essentiellement l'expression des besoins, et de la méthode OMT (Object Modelling Technique) de James Rumbaugh : pour l'analyse et applications orientées données. En 1994 Rumbaugh rejoint Booch chez Rational, puis en 1995 Jacobson rejoint Rational et le 14 Novembre 1997 : UML est adopté par l'OMG (Object Management Group).

UML était initialement un ensemble de diagrammes permettant de représenter un système informatique pour les développeurs travaillant avec une approche orientée objet. Après son évolution en 2004 vers la version UML2, ce langage de modélisation a été utilisé pour décrire un système d'information, notamment au niveau du cahier des charges [Morley et al., 2011].

UML s'appuie sur un métamodèle, un modèle de plus haut niveau qui définit les éléments d'UML. UML propose des diagrammes avec lesquels il est possible de modéliser divers aspects d'un processus métier. La figure 1.22 montre les différentes étapes par lesquelles est passé UML :

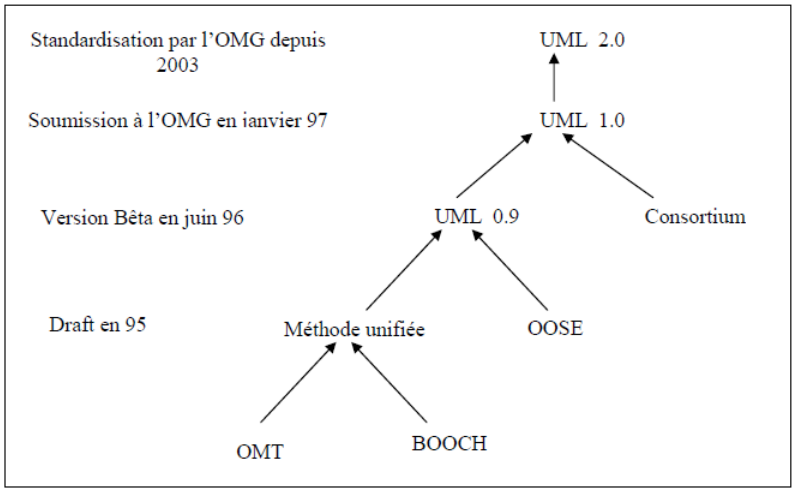


FIGURE 1.22 – *Evolution de UML [MANSOURI, 2009]*

UML présente un ensemble assez riche de diagrammes permettant de décrire les besoins des utilisateurs, ainsi que les propriétés statiques et dynamiques du système. On peut distinguer deux catégories de diagrammes UML (figure 1.23) :

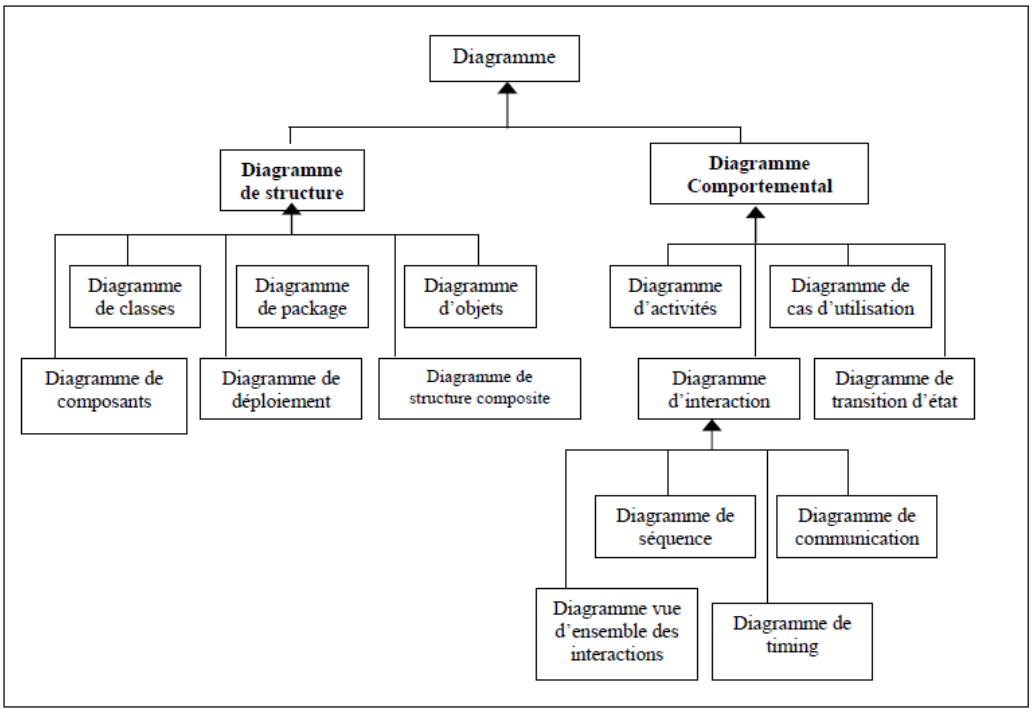


FIGURE 1.23 – *Diagrammes UML [MANSOURI, 2009]*

Diagrammes décrivant l'aspect structurel du système [MANSOURI, 2009] :

— les diagrammes de classes : expriment de manière générale la structure statique d'un

système, en termes de classes et de relations entre ces classes. De plus, ils présentent un ensemble d'interfaces et de paquetages, ainsi que leurs relations.

— les diagrammes d'objets : sont des graphes d'instances qui incluent les objets et les valeurs de données. Un diagramme d'objets statiques est une instance d'un diagramme de classes, présente un snapshot de l'état détaillé d'un système à un instant donné.

— les diagrammes de cas d'utilisation : représentent la structure des grandes fonctionnalités nécessaires aux utilisateurs du système. Ils assurent la relation entre l'utilisateur et les objets que le système met en œuvre en décrivant, sous forme d'actions et de réactions, le comportement d'un système du point de vue utilisateur.

— les diagrammes de composants : présentent les dépendances entre les composants logiciels. Ils incluent les classificateurs (i.e. classes) qui spécifient les composants, et les artefacts qui les implémentent, tels que les fichiers de code source, de code binaire, exécutables ou scripts.

— les diagrammes de déploiements : présentent la configuration des éléments de traitement en temps d'exécution, ainsi que les composants logiciels, les processus et les objets qui les exécutent.

Diagrammes décrivant l'aspect comportemental du système [Morley et al., 2011] :

— Le diagramme de collaboration : (figure 1.24) permet de mettre en évidence et de formaliser les interactions entre les différents objets du système étudié. Les objets émetteurs ou récepteurs de messages ne sont pas exclusivement des instances d'entité mais peuvent être des acteurs. Les messages peuvent être décrits par leur nom, une séquence, des arguments, un résultat attendu, une synchronisation, une condition d'émission.

— Le diagramme de séquence : (figure 1.25) est une variante du diagramme de collaboration qui permet de mieux visualiser la séquence des messages par une lecture de haut en bas. L'axe vertical représente le temps et l'axe horizontal représente les objets qui collaborent.

— Le diagramme d'activité : (figure 1.26) permet de représenter la dynamique du système d'information. Le diagramme d'activité est attaché à une classe-processus, acteur ou entité, ou bien à un cas d'utilisation ou à une opération. C'est un graphe orienté qui décrit un enchaînement de traitements (flot de contrôle). L'enchaînement des activités peut être soumis à des branchements conditionnels ou à des synchronisations. La visualisation des couloirs d'activités permet de représenter la répartition de la responsabilité des activités entre les différents acteurs. Les activités sont reliées par des transitions qui sont déclenchées par des événements. Une transition peut être assortie d'une condition de garde qui bloque la transition si elle n'est pas vérifiée.

— Le diagramme d'états-transitions : (figure 1.27) a comme objectif de représenter des traitements en les positionnant par rapport à une classe et plus précisément à des états d'une classe. Ce diagramme fait ainsi apparaître l'ordonnancement des différents travaux. Ce diagramme utilise le concept d'état qui est une situation durable dans laquelle peuvent se trouver les objets d'une classe, et le concept de transition qui est une relation entre deux états signifiant qu'un passage de l'un à l'autre est possible. Un processus peut ainsi être représenté comme une classe, dont les états correspondent aux activités du processus.

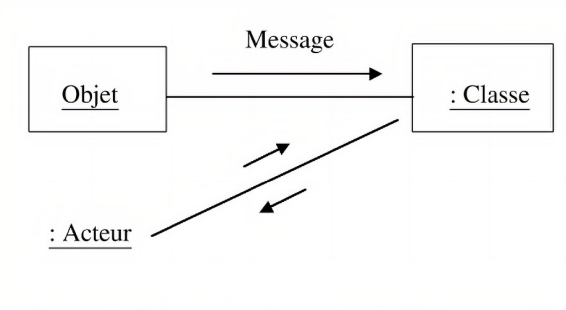


FIGURE 1.24 – *Le diagramme de collaboration UML [Morley et al., 2011]*

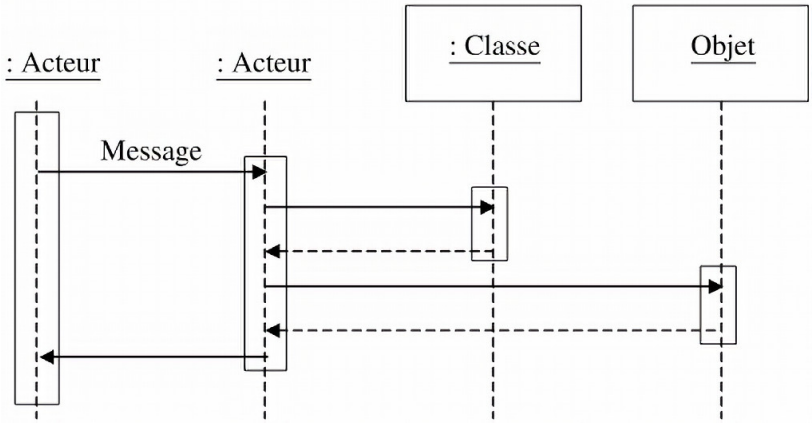


FIGURE 1.25 – *Le diagramme de séquence UML [Morley et al., 2011]*

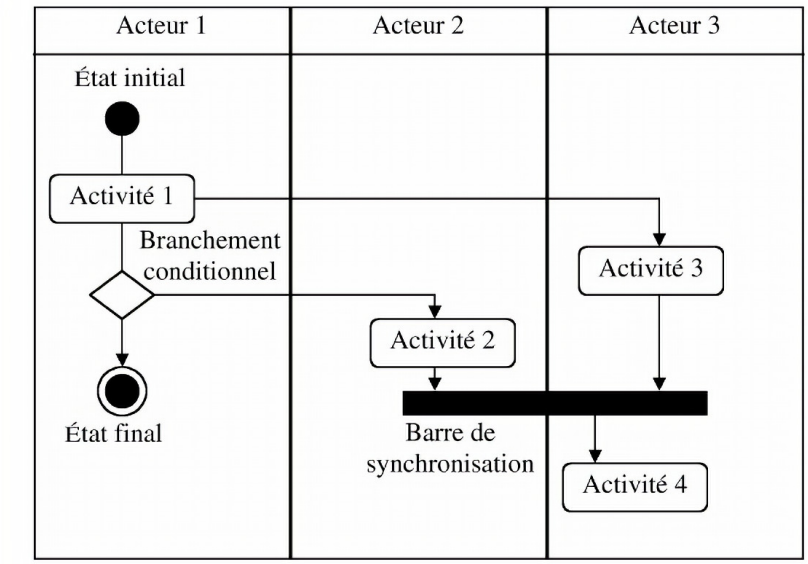


FIGURE 1.26 – *Le diagramme d'activité UML [Morley et al., 2011]*

Les diagrammes de séquence, d'activité et d'état transition sont les plus utilisés pour la modélisation des processus métiers.

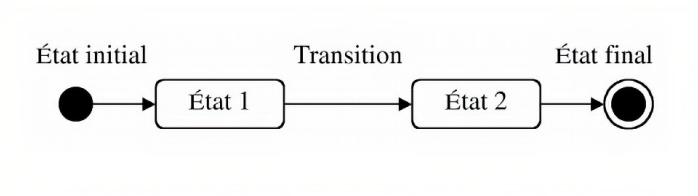


FIGURE 1.27 – *Le diagramme d'états-transitions UML [Morley et al., 2011]*

1.9 CONCLUSION

Le but de ce chapitre était de donner une idée sur les entreprises ainsi leur modélisation. Nous avons présenté les approches importantes de modélisation associées essentiellement aux systèmes d'information et aux entreprises. Nous avons mis l'accent sur la notion de processus et le rôle crucial que jouent les processus métiers dans la prospérité des entreprises d'aujourd'hui. Il faut accorder une attention particulière lors de leur modélisation afin d'éviter l'introduction précoce des erreurs.

Cloud Computing 2

2.1 Introduction

L'informatique suit un cycle régulier de centralisation/décentralisation depuis 1960 avec le langage de prédilection qui est le Cobol. Les premiers systèmes utilisés en sociétés étaient des mainframes sur gros système (IBM ou Bull) après par la suite il y a eu l'émergence des architectures client/serveur.

L'émergence du Cloud Computing comme une suite logique dans l'informatique est passée par plusieurs étapes [Déon, 2015] et [Plouin, 2016].

1980-1989 : avec les développements en puissance et en fiabilité des ordinateurs, toutes les pratiques de conception, de fabrication, de commercialisation, de publication, de communication ont été envahies et transformées par l'informatique. Après 1985, on voit la mise en place de la micro-informatique avec ces nouveaux métiers. L'architecture client/serveur a été massivement utilisée dans la plupart des systèmes d'information.

1990-1999 : à partir des années 1990, les architectures web ont conduit à la recentralisation de la logique de traitement sur des serveurs centraux. Les réseaux (Web, mail, chats) accroissent fortement la demande, durant cette période est marquée par la mise en réseau des PC, serveurs et imprimantes des entreprises, par l'arrivée de Windows 3.1 suivi de la version réseau, par des environnements de développement intégré. C'est également le temps des expérimentations d'accès Internet sur ligne analogique et des tests avec le premier navigateur (Netscape) qui ont permis l'usage d'applications à l'échelle de l'internet grâce aux standards HTTP et HTML. Le nombre de fournisseurs d'accès Internet est en pleine évolution, les fournisseurs de modems RTC connaissent une réussite. Au milieu des années 1990, deux révolutions technologiques vont bouleverser le quotidien avec l'arrivée d'Internet pour le grand public et les entreprises et l'arrivée du téléphone mobile.

2000-2009 : cette période voit l'arrivée de la virtualisation, un tournant dans le monde du système. Le terme web 2.0 a été créé en 2005 par Tim O'Reillly : selon lui, le web 2.0 consiste à considérer le web comme une plateforme. Le web 2.0 repose sur le concept de l'intelligence collective. Il y a eu l'émergence de plusieurs outils durant cette période comme les blogs, les wikis et plus largement les site web qui incitent à la participation. Le mouvement du web 2.0 est basé sur des applications web plus ergonomiques, plus facile à utiliser grâce entre autres le HTML 5 et des API ouvertes (Application Programming Interface).

2010-2014 : ce quinquennat a vu l'émergence d'une notion fondamentale, le Cloud Computing, qui va bien au-delà de la synthèse des mouvements précédents. En proposant l'hébergement des services sur des plateformes accessibles depuis l'Internet, le Cloud Computing est l'aboutissement de l'ensemble des mouvements précédents.

2015-aujourd'hui : cette période actuelle est synonyme de simplification, de disponibilité, de sécurité, d'innovation digitale, d'open data, de monétisation d'API et d'automatisation. Tout va vite avec les GAFA (Google, Amazon, Facebook, Apple). Les entreprises ils commencent à comprendre que le numérique doit faire partie de la stratégie globale et que c'est un catalyseur de progrès qui va transformer le métier en profondeur avec des clients naturellement intégrés dans le SI de l'entreprise. Internet of Things, considéré comme la troisième évolution de l'Internet, baptisé Web 3.0 sera partout avec de plus en plus des objets connectés

Ce chapitre du Cloud Computing a pour objectif de décrire les concepts de base, les challenges actuels et à venir en matière de Cloud Computing ainsi que les transformations futures de l'IT.

2.2 Définition du Cloud Computing

Il existe de nombreuses définitions des services de Cloud Computing et il y a peu de consensus d'une définition universelle. Dans ce qui suit, nous citons quelques définitions. Selon [Foster et al., 2008, Buyya et al., 2009, Höfer et Karagiannis, 2011], qui se basent sur une vision rapprochée de Grid Computing, le Cloud Computing se base principalement sur le paradigme de l'informatique distribuée à grande échelle afin d'assurer un service à la demande accessible à travers Internet. Une autre définition, proposée dans [Ahmed et al., 2012] et qui est plus abstraite, définit le Cloud Computing par l'utilisation des ressources informatiques qui sont offertes en tant que service à travers un réseau (typiquement Internet). Une troisième définition, élaborée par un groupe de travail de la commission européenne [Schubert et al., 2010], considère le Cloud Computing comme un environnement de stockage et d'exécution élastique de ressources informatiques impliquant plusieurs acteurs, connectés par Internet. Cet environnement délivre un service mesurable, à la demande, à granularité variable et qui implique des niveaux de qualité de services. Cette définition a été étendue dans [Schubert et Jeffery, 2012] en prenant en considération les différents acteurs de l'écosystème Cloud Computing (fournisseur, développeur, utilisateur).

Cependant, la définition proposée par la National Institute of Standards and Technology (NIST) dans [Mell et Grance, 2011], est la définition la plus largement acceptée aujourd'hui, défini le Cloud Computing comme un modèle qui permet un accès réseau pratique et sur demande à un pool partagé de ressources informatiques configurables (par exemple, des réseaux, des serveurs, du stockage, des applications et des services) qui peut être rapidement approvisionné et disponible sans trop d'efforts de gestion ou d'interaction d'opérateurs. Ce modèle de Cloud favorise la disponibilité et est composé de cinq caractéristiques essentielles, de trois modèles de service et de quatre modèles de déploiement. Ces éléments sont énumérés par la suite.

Sur un plan plus technique, on peut considérer que le Cloud Computing est une évolution des technologies de virtualisation. La virtualisation permet de donner plus d'agilité aux centres de données, grâce aux trois propriétés suivantes [Plouin, 2016] :

— Mutualisation des ressources : la virtualisation permet d'affecter les ressources d'une même machine à plusieurs applications.
— Abstraction sur la localisation : l'application est « quelque part » sur l'une des machines constitutives de la plateforme de virtualisation. Si cette plateforme utilise des mécanismes de réplication sur des Datacenters distants, les risques de désastre (incendies, inondations) sont couverts par la distribution multisite.
— Élasticité : il est possible d'allouer des ressources supplémentaires à une application proche de la saturation, dans les limites physiques de la plateforme. Cette propriété est particulièrement importante : en effet, si la plateforme dispose de grandes ressources de puissance inutilisées, on peut affecter en quelques instants des capacités supplémentaires à une application. Elle permet aussi d'optimiser l'usage des ressources, en évitant le syndrome de la machine utilisée à 20 % de ses capacités (un cas classique avec une machine hébergeant un serveur HTTP).

Le Cloud Computing reprend ces propriétés, mais à une plus grande échelle :

— Dans le cadre des plateformes de Cloud Computing publiques (Google, Amazon, etc.), la mutualisation de ressources se fait à l'échelle de plusieurs milliers d'entreprises. On dispose donc de bénéfices liés au facteur d'échelle.
— L'abstraction sur la localisation est à l'échelle de plusieurs continents dans le cadre des Clouds publics : la garantie sur l'intégrité des données est donc supérieure à celle d'un centre de données utilisant deux sites distants de quelques kilomètres. On retrouve ici le caractère ubiquitaire des ressources évoquées dans le paragraphe précédent.
— Avec des plateformes de plusieurs dizaines milliers de serveurs, les Clouds publics proposent une réserve de puissance et donc une élasticité exceptionnelle.

Le Cloud Computing ajoute d'autres propriétés à celles de la virtualisation :

— Le Pay As You Go : les utilisateurs paient les ressources qu'ils utilisent en fonction de leur consommation réelle et précise. Peu de DSI savent aujourd'hui mesurer précisément la consommation informatique de telle ou telle application. Les acteurs du Cloud savent le faire.
— Le Self-Service : l'équipe de développement peut demander l'allocation de ressources via un portail web. Ces ressources seront mises à sa disposition de manière automatique quelques minutes plus tard.
— Les API ouvertes : les plateformes Cloud proposent des interfaces techniques accessibles à distance qui permettent de les intégrer avec le système d'information ou bien de piloter les services à distance.

Sur la base de cette définition, le Cloud offre deux grandes familles de services :

— Des services de fourniture d'application en location, appelés SaaS. Ces services sont généralement facturés au nombre d'utilisateurs actifs.

— Des services techniques de plateforme d'exécution en location, appelés PaaS et IaaS. Ces services sont facturés selon les ressources techniques consommées.

La figure 2.1, illustre les propriétés et les services du Cloud Computing.

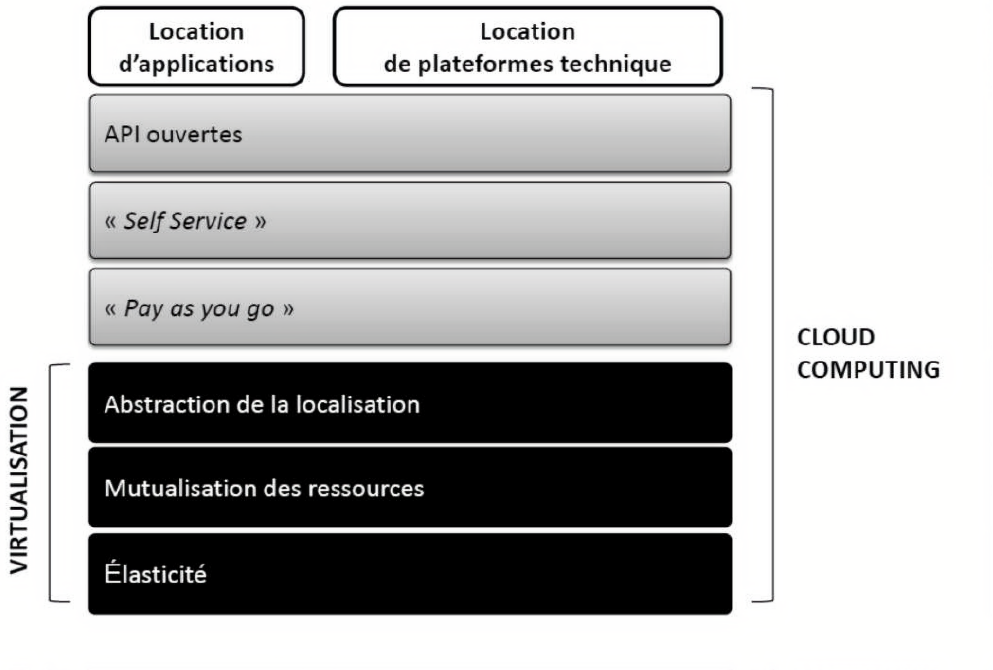


FIGURE 2.1 – *Une définition pragmatique du Cloud Computing [Plouin, 2016]*

Le concept de Cloud Computing englobe les concepts de Software as a Service (SaaS), de Platform as a Service (PaaS), et d'Infrastructure as a Service (IaaS) que nous allons présenter dans la suite. Le terme as a Service évoque bien un service, dans le sens où le fournisseur vend une fonction opérationnelle, et non des composants techniques nécessitant une compétence informatique.

2.3 Caractéristiques

Selon le NIST, le Cloud Computing doit posséder 5 caractéristiques essentielles :

— **Libre-service à la demande** Un utilisateur peut allouer unilatéralement des ressources informatiques (serveurs, réseau, stockage, environnement d'exécution, application) au besoin, de façon automatique et sans nécessité d'interaction humaine avec chaque fournisseur de services.

— **Large accès réseau** Les ressources Cloud Computing sont disponibles à travers le réseau et accessibles via des mécanismes standards qui favorisent leurs utilisations à partir des appareils clients hétérogènes, voire légères (ex ordinateurs portables, téléphones, tablettes).

— **Mise en commun des ressources** Les ressources informatiques du fournisseur Cloud Computing sont mutualisées pour servir plusieurs clients en utilisant un modèle multi-tenant. Ces ressources, physiques ou virtuelles, sont allouées et libérées

dynamiquement selon la demande du consommateur. Généralement, l'utilisateur n'a ni le contrôle ni la connaissance de l'emplacement exact des ressources allouées. Dans certains cas, il peut choisir l'emplacement géographique à un niveau haut (ex par pays, continent ou data-center).

— **Une souplesse rapide** Les ressources sont allouées et libérées d'une façon élastique, idéalement d'une façon automatiquement, pour s'adapter rapidement à la demande qu'elle soit croissante ou décroissante. Pour le consommateur, les ressources disponibles à l'allocation apparaissent comme illimitées et peuvent s'allouer à tout moment.

— **Services mesurés** Toutes les ressources allouées peuvent être surveillées et contrôlées afin de mesurer leurs consommations avec un niveau d'abstraction approprié selon le type du service (ex stockage, temps de calcul, bande passante).

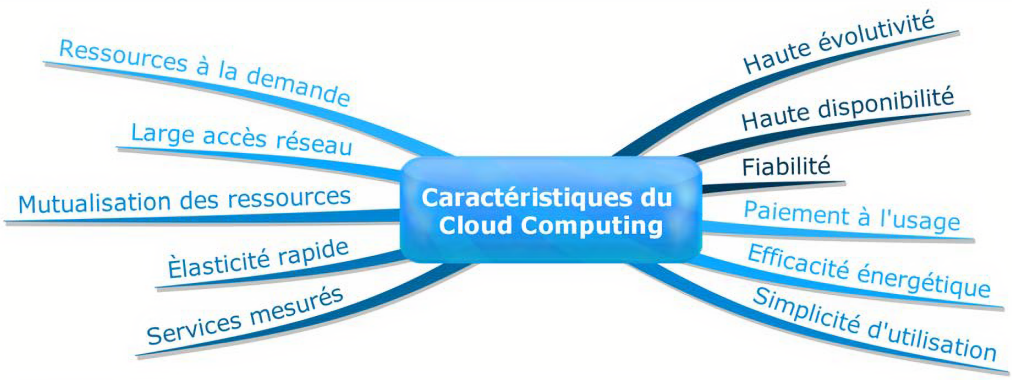


FIGURE 2.2 – *Caractéristiques du Cloud Computing [Medhioub, 2015]*

En plus des cinq caractéristiques définies par NIST, il y a d'autres caractéristiques [Medhioub, 2015] :

— **Haute évolutivité** Les services de type Cloud Computing devraient être évolutifs et doivent satisfaire toute demande de croissance de la part des utilisateurs selon le besoin des services et des ressources allouées. Cette évolutivité doit se faire d'une façon automatique et en cours d'exécution.

— **Haute disponibilité** La haute disponibilité des ressources Cloud Computing est primordiale. Par exemple, l'accès réseau aux ressources doit être assuré à plein temps sans aucune interruption.

— **Haute fiabilité** Toutes les ressources Cloud Computing doivent être d'une grande fiabilité. Par exemple, la probabilité de perte de donnée doit être quasi nulle.

— **Paiement à l'usage 'Pay as you Go'** La philosophie de facturation des ressources Cloud Computing se base sur l'usage. L'idée est que l'utilisateur ne paye que ce qui a consommé.

— **Efficacité énergétique** Malgré que cette caractéristique n'ait pas été unanimement adoptée, mais la diminution de l'énergie consommée par les ressources Cloud Computing est d'une grande importance et sa prise en considération ne cesse de croître. En effet, l'efficacité énergétique contribue à diminuer les coûts.

— **Simplicité d'utilisation** L'allocation, la gestion et l'utilisation des ressources Cloud Computing doivent être simples. Idéalement, elles doivent se faire à travers des interfaces et des Application Programming Interfaces (APIs) efficaces et génériques.

La figure 2.2 schématise les caractéristiques du Cloud Computing.

2.4 Acteurs

L'écosystème du Cloud Computing est composé principalement par cinq acteurs majeurs [Medhioub, 2015] :

- **Cloud Provider :** Le fournisseur des ressources Cloud Computing. Il est responsable de fournir un service Cloud Computing qui satisfait les caractéristiques définies précédemment, tout en respectant les Service Level Agreements (SLAs) établies avec les autres acteurs (en particulier le Cloud Consumer). Le Cloud Provider a comme activité l'allocation, l'orchestration et la gestion des ressources qu'il offre tout en assurant le bon niveau de sécurité.
- **Cloud Consumer :** L'utilisateur des ressources Cloud Computing. Cet utilisateur peut être un utilisateur final ou un développeur selon le type du service Cloud alloué. Cet utilisateur peut être une personne, un groupe de personnes, les petites et moyennes entreprises, les multinationales ou les gouvernements.
- **Cloud Carrier ou Network Provider :** Le fournisseur de réseau est l'intermédiaire qui assure principalement la connectivité entre les ressources Cloud Computing et la liaison entre les acteurs de l'écosystème Cloud Computing (en particulier entre le Cloud Provider et le Cloud Consumer). Cet utilisateur peut jouer un simple rôle d'acheminements des paquets, comme il peut jouer un rôle plus important en offrant des fonctionnalités avancées dans le réseau. Ces fonctionnalités sont basées sur des SLAs établies avec les autres acteurs de l'écosystème.
- **Cloud Broker :** Le courtier Cloud est un intermédiaire qui négocie la relation entre les Cloud Providers et les Cloud Consumers. Il peut offrir de nouveaux services qui simplifient les tâches de gestion du Cloud Consumer. Ce dernier peut demander les ressources Cloud Computing auprès du Cloud Broker au lieu du Cloud Provider directement. Pour récapituler, le Cloud Broker peut assurer l'orchestration, l'agrégation et l'arbitrage des services Cloud Computing.
- **Cloud Auditor :** L'auditeur Cloud s'occupe de la vérification et l'audition des services Cloud Computing. Il évalue les services offerts par les Cloud Providers, Cloud Carriers et Cloud Brokers du point de vue performances et sécuritaires. Le but principal est de vérifier que les fournisseurs respectent bien les SLAs qu'ils proposent.

2.5 Classification

2.5.1 Quatre types de Cloud

Il faut distinguer plusieurs types de Cloud Computing (par abus de langage, il s'agira de Clouds dans la suite de cette thèse) - figure 2.3 :

Cloud privé

Il s'agit d'une plate-forme de ressources (hosts, RAM, CPU, mémoire, machines virtuelles, middleware, services applicatifs...) qui est dans l'entreprise. Le Cloud privé est administré généralement par l'équipe IT (besoin de compétence système et réseau) interne.

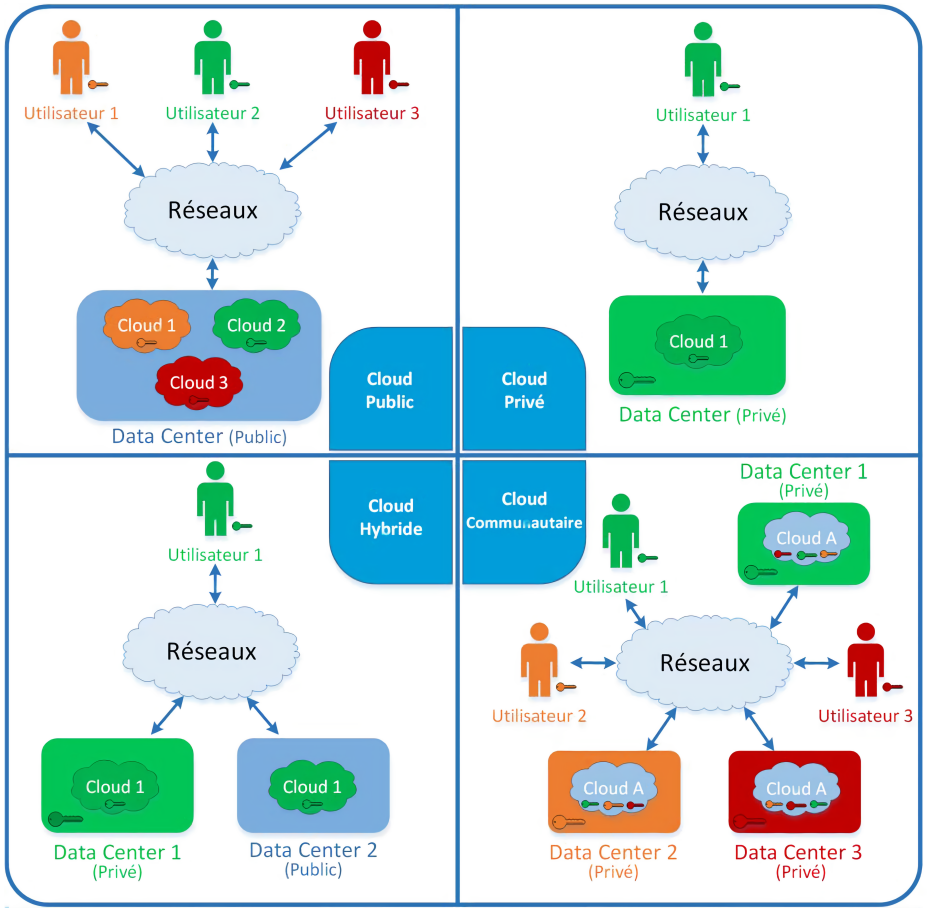


FIGURE 2.3 – *Modèles de déploiement Cloud [Medhioub, 2015]*

Le Cloud privé s'adresse aux grandes entreprises et grosses PMI/PME car il nécessite un investissement important en moyens humains et financiers. Il doit donc répondre au préalable à une étude d'opportunité et à une mesure de ROI (retour sur investissement). [Déon, 2015] Dans ce type de déploiement, l'infrastructure est gérée avec des solutions (Open Source ou propriétaire) de type Cloud pour offrir les ressources et services par le biais d'interface Cloud [Medhioub, 2015]

Cloud public

Dans un Cloud Public, le fournisseur gère l'infrastructure et offre ses services aux utilisateurs Cloud grand public d'une façon complètement ouverte. Les ressources informatiques sont partagées entre les utilisateurs [Medhioub, 2015]. Il s'agit ici de disposer d'une plate-forme de Cloud totalement en dehors des murs de l'entreprise. Cette dernière y accède donc via une simple ligne Internet (et souvent un accès VPN pour plus de sécurité). Les plates-formes de Cloud public sont généralement "multi-tenants", c'est-à-dire mutualisées pour plusieurs clients. Par exemple, sur un ensemble de hosts physiques, il est possible de créer un cluster de virtualisation disponible pour de nombreux clients : les ressources physiques sont partagées mais les VM sont bien spécifiques à chaque client [Déon, 2015].

Cloud Hybride

Dans un Cloud Hybride, les ressources peuvent être allouées à partir d'un Cloud Privé et d'un Cloud Public. C'est un environnement qui combine les deux modèles Public et Privé. Comme utilisation de ce type de Cloud Hybride, il est possible de stocker et gérer les données confidentielles dans l'environnement privé et celles qui sont moins confidentielles dans un Cloud Public [Medhioub, 2015]. Le Cloud hybride est utilisé aussi pour des usages de débordement de la production (quand l'entreprise ne dispose plus d'assez de ressources en interne et surtout qu'elle n'est pas capable d'en mettre de nouvelles rapidement à disposition des utilisateurs) [Déon, 2015].

Cloud Communautaire

Dans un Cloud Communautaire, l'infrastructure de Cloud est provisionnée à l'usage exclusif d'une communauté d'utilisateurs, par exemple les organismes gouvernementaux. L'infrastructure peut être détenue, gérée et exploitée par un ou plusieurs des organismes de la communauté, un tiers, ou une combinaison d'entre eux [Medhioub, 2015]. Les types de Clouds communautaires les plus connus sont [Déon, 2015] :

— Les Clouds universitaires (exemple : UnivCloud) permettant des services d'enseignement à distance de type MOOC (Massive Open Online Course), de la visioconférence, du tutorat à distance, de la messagerie, des bureaux virtuels, des connexions avec les services administratifs, etc.).
— Les Clouds de voyage (exemple : Amadeus) permettant de mettre en relation agences de voyage, compagnies aériennes, hôtels...
— Les Clouds santé permettant l'interconnexion d'établissements hospitaliers, éditeurs de logiciels pour professionnels de santé, laboratoires pharmaceutiques.

2.5.2 Les trois modèles du Cloud Computing

Afin de mieux définir la classification selon le type du service Cloud Computing et comme illustré dans la figure 2.4, un environnement informatique standard peut être composé par plusieurs couches qui partent du bas niveau (le matériel physique) vers le haut niveau (l'application à utiliser). Ces couches sont : Calcul, Réseau, Stockage, Virtualisation, Système d'exploitation, Intergiciel, Environnement de développement, Environnement d'exécution, Données et Applications. La classification selon le type du service correspond au niveau de responsabilité dans la gestion de ces couches que ce soit par les fournisseurs ou par les utilisateurs. Traditionnellement, toutes les couches sont gérées par l'utilisateur lui-même. Avec le Cloud Computing, l'utilisateur n'a plus en charge la totalité des couches et en fonction du niveau des sous-ensembles de couche nous distinguons le type de service [Medhioub, 2015].

Le cloud désigne une informatique externalisée vers l'Internet. Il offre des possibilités de location d'applications et de plateformes techniques. Il repose sur la virtualisation, le Pay As You Go, le Self Service, et les API ouvertes. Il englobe les concepts de SaaS, PaaS et IaaS. Il constitue une évolution logique de l'ouverture des entreprises vers l'Internet [Plouin, 2019].

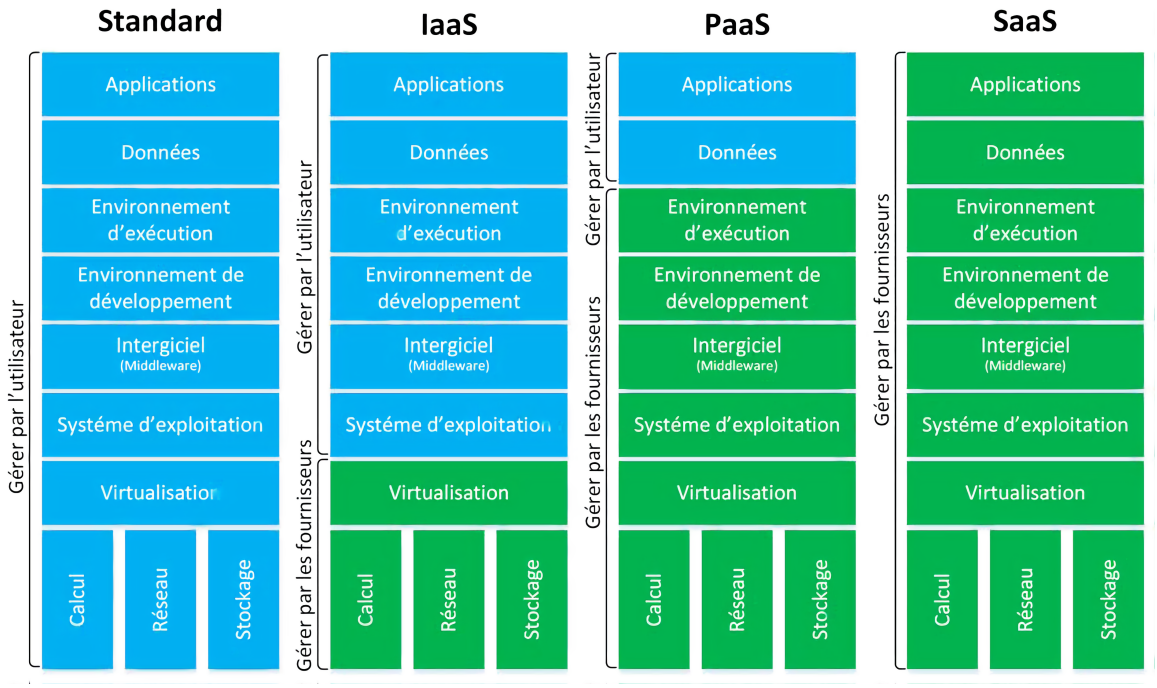


FIGURE 2.4 – *Types de service Cloud Computing [Medhioub, 2015]*

SaaS

SaaS signifie Software as a Service, c'est-à-dire un logiciel fourni sous la forme de service. Il s'agit donc de location d'application opérationnelle, clef en main, et non d'achat de logiciel informatique, à installer soi-même sur une machine. Les SaaS s'adressent donc aux utilisateurs finaux [Plouin, 2016]. Les services de type SaaS correspondent tout simplement à des applications prêtes à l'utilisation offertes à la demande. L'utilisateur n'a qu'à utiliser le service Cloud Computing offert. Il n'a rien à gérer et c'est le fournisseur qui a toute la responsabilité de maintenir le service en gérant toutes les couches [Medhioub, 2015]. La figure 2.5 schématise le SaaS.

La différence entre SaaS et logiciel est essentielle. En effet, les SaaS proposent des logiciels opérationnels, prêts à l'emploi, sans passer par une étape d'installation, et sans aucune tâche de maintenance. Les SaaS sont exécutés sur des plateformes conçues pour une utilisation simultanée par un grand nombre de collaborateurs qui travaillent dans de nombreuses entreprises différentes. Ces plateformes sont mises à disposition par des acteurs (comme Google ou Salesforce) [Plouin, 2016].

PaaS

PaaS signifie Platform as a Service ou plateforme sous forme de service. Il s'agit de location de plateforme technique, permettant l'exécution de code développé en spécifique. Les PaaS s'adressent donc aux développeurs [Plouin, 2016]. Les services PaaS correspondent principalement à des environnements de développement offerts à la demande. L'utilisateur n'a plus en charge que les couches de données et d'applications. Pour ce faire, il y a utilisation des librairies, langages et outils offerts par le fournisseur pour structurer

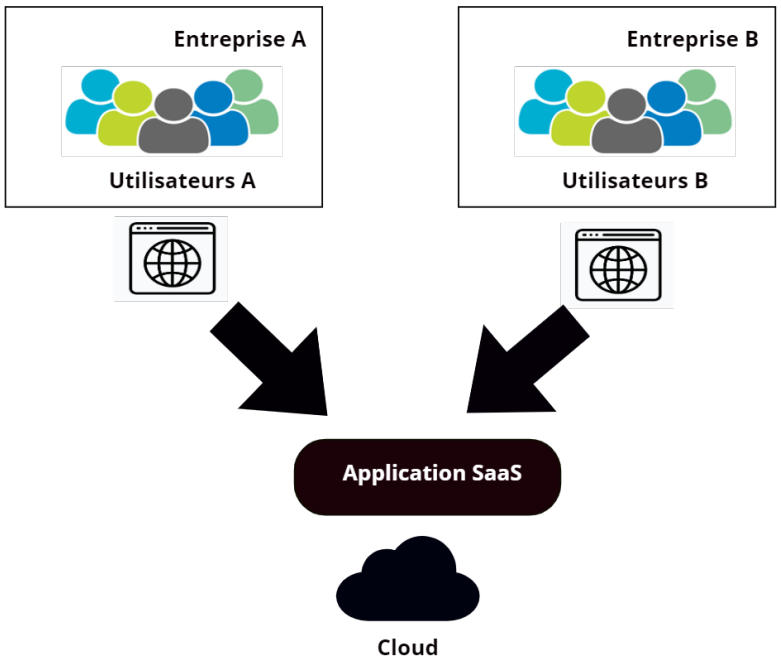


FIGURE 2.5 – *Vision générale des SaaS*

ses données et développer ses applications [Medhioub, 2015]. Cette plateforme peut être utilisée pour exécuter des sites web, des SaaS, ou tout développement spécifique issu de l'entreprise. Ces développements spécifiques doivent respecter le langage de développement et l'architecture de la plateforme PaaS [Déon, 2015].

Dans l'approche PaaS, l'opérateur ne fournit pas seulement un environnement d'exécution déporté, mais aussi un ensemble de services d'infrastructures. La plate-forme PaaS propose ainsi [Plouin, 2016] :

— Un portail de Self Service : pour souscrire au service, administrer et surveiller son application.
— Un service d'exécution d'applications : qui permet d'exécuter des applications écrites dans les langages autorisés par la plateforme, et un service de persistance de données qui permet de stocker des données structurées ou des fichiers.
— Le Pay As You Go : en général, les PaaS sont facturées à l'entreprise selon la consommation de CPU, réseau (bande passante, volume, etc.) et espace disque.
— Des API ouvertes : elles permettent l'intégration de l'application hébergée sur la PaaS avec le SI, ainsi que sa surveillance.
— Des architectures « multi-tenants » , dédiées à un usage en ligne : comme les SaaS, les PaaS sont liées à l'environnement de l'opérateur et ne peuvent pas être « déménagées » simplement sur un serveur Windows ou Linux en entreprise.

La figure 2.6 ci-dessous résume les différentes couches du PaaS :

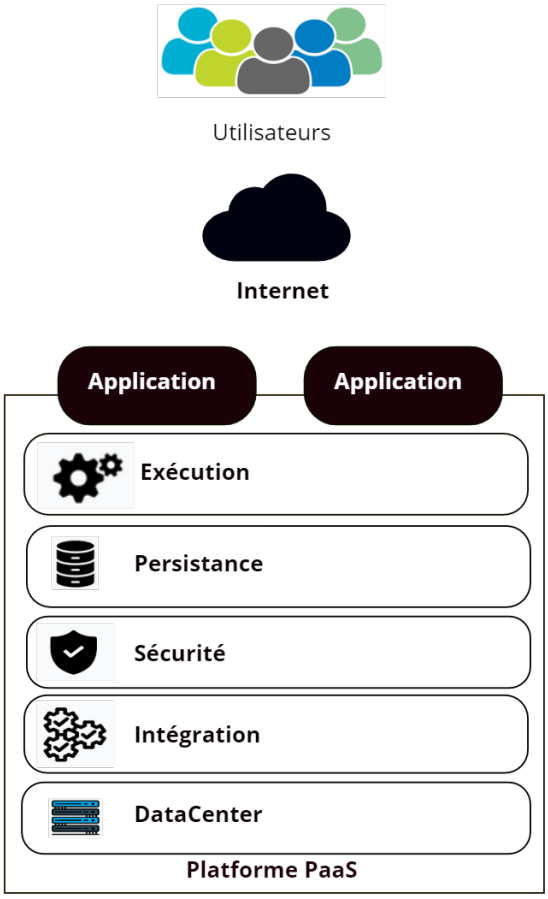


FIGURE 2.6 – *Les plateformes PaaS*

IaaS

IaaS signifie Infrastructure as a Service ou infrastructure sous forme de service. Il s'agit de location de plateforme technique, permettant l'exécution d'architectures applicatives complètes, comprenant base de données, serveur d'application, etc. Les IaaS s'adressent donc aux équipes d'exploitation [Plouin, 2016].

Les services Cloud Computing de type IaaS correspondent à des ressources infrastructures offertes à la demande (Figure 2.7). Ces ressources sont des ressources de calculs, de stockage ou de réseau et peuvent être soit virtuelles, soit physiques. Le fournisseur a la gestion des couches Calcul, Stockage, Réseau et Virtulisation. L'utilisateur des ressources IaaS est responsable de la gestion de toutes les couches à partir et au-dessus du système d'exploitation. L'utilisateur n'a ni le contrôle, ni la gestion, ni la visibilité de l'infrastructure sous-jacente [Medhioub, 2015]

L'infrastructure en tant que service (IaaS pour Infrastructure as a Service) a été introduite au début des années 2000 par Amazon pour régler des problèmes de charge de commandes sur son site web lors des fêtes de Noël. Amazon a ensuite mis en place sa propre solution de Cloud Computing dont un des premiers services a été EC2 (Elastic Compute Cloud) et dont la version beta est sortie durant l'été 2006 (presque une décennie déjà). L'idée est ici de fournir de la puissance IT à partir d'une interface web : concrè-

tement la possibilité pour un particulier ou une entreprise de commander des machines virtuelles, de pouvoir les instancier ou les arrêter et de payer à l'usage. Le IaaS apporte donc plusieurs concepts [Déon, 2015] :

— Interface web de commande (portail d'accès à un catalogue de services).
— Choix de type de configuration (CPU, RAM ou disque).
— Location et paiement à l'usage.
— Provisionning/déprovisionning de machines virtuelles : soit un système d'exploitation seul sur lequel le client peut installer tout applicatif en totale autonomie, soit un serveur avec des composants déjà installés appeler les COTS (commercial-off-the-shelf) comme le middleware.

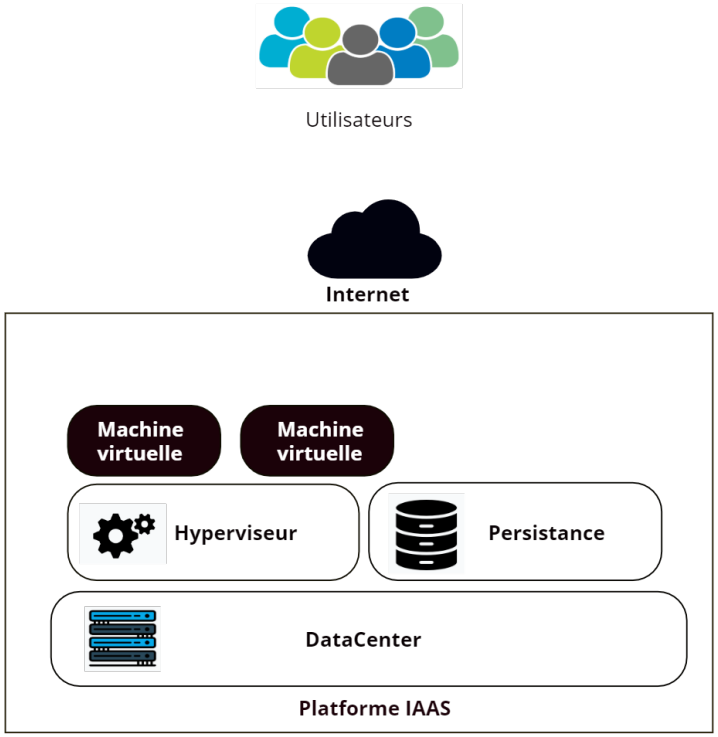


FIGURE 2.7 – *Les infrastructures IaaS*

XaaS

L'acronyme XaaS fait référence à l'expression Everything-as-a-Service (Tout en tant que Service). Cette expression désigne les différents modèles du Cloud Computing « en tant que service ». Chacune des nouvelles abréviations peut être vues comme un sous-ensemble d'un ou plusieurs des trois types de base. Parmi ces abréviations, nous citons quelqu'une d'entre elles dans le tableau 2.1.

APaaS	Application Platform as a Service
BaaS	Backup as a Service
BaaS	Backend as a Service
CaaS	Communication as a Service
DaaS	Data as a Service
DBaaS	Database as a Service
DCaaS	Data Center as a Service
DPaaS	Database Platform as a Service
DRaaS	Disaster Recovery as a Service
HaaS	Hardware as a Service
HPCaaS	High Performance Computing as a Service
IDaaS	Identity as a Service
IPaaS	Integration Platform as a Service
MaaS	Monitoring as a Service
MQaaS	Message Queues as a Service
NaaS	Network as a Service
PRaaS	Process as a Service
RaaS	Resource as a Service
SECaaS	Security as a Service
STaaS	Storage as a Service
XaaS	Everything as a Service

TABLE 2.1 – *Les abréviations des services dans le Cloud [Plouin, 2016]*

2.6 AVANTAGES ET OBSTACLES

Le Cloud Computing est généralement associé à une multitude d'avantages qui créent l'unanimité parmi les professionnels de l'entreprise. Plusieurs travaux ont listé ces avantages [Schubert et al., 2010, Mirashe et Kalyankar, 2010, Rajan et Jairath, 2011, Gai et Li, 2012, Medhioub, 2015] :

— Facilité de déploiement
— Réduction des coûts d'infrastructure.
— Réduction des coûts de développement.
— Réduction des coûts des logiciels.
— Des ressources et services plus rapide à allouer et plus simple à utiliser.
— Accès aux ressources plus flexible.
— Meilleure utilisation, plus efficace, des ressources.
— Augmentation de la puissance de calcul.
— Grande capacité de stockage (quasi illimitée).
— Moins de problèmes d'entretien.
— Gestion des mises à jour plus simple et rapide.
— Pas de perte de données.
— Tout est considéré comme un service défini par un SLA.
— Infrastructure allouée et disponible juste à temps.

Le Cloud Computing n'a pas que des avantages, il possède quelques inconvénients qui sont abordés dans [Armbrust et al., 2010, Gai et Li, 2012, Michael Armbrust et Patterson, 2009, Medhioub, 2015]. Parmi ces obstacles, il y a :

— Le Lock-in des données.
— Dépendance à un prestataire
— Confidentialité des données.
— Chiffrement des données.
— Nécessité d'un accès réseau constant.
— Mauvais fonctionnement avec les connexions à basse vitesse.
— Faible niveau de la qualité de service dans le réseau.
— Risque d'engorgements lors des transferts de données.
— Problème d'interopérabilité.
— Problème de portabilité.
— Faible contrôlabilité.
— Manque de fonctionnalités d'audit.
— Des contrats de service SLAs non normalisés.

2.7 Les challenges dans le Cloud Computing

Le Cloud Computing est devenu une préoccupation de toutes les sociétés pour leurs systèmes informatiques. Pour évaluer l'impact que le cloud peut avoir sur les entreprises, il est important d'évaluer d'un point de vue critique les challenges de recherche dans le Cloud. Dans cette partie, nous résumons quelques enjeux de recherche dans le cloud computing [Yassa, 2014] :

— **Migration des données entre les environnements non standards :** La plupart des fournisseurs de services de cloud computing utilisent des applications cloud propriétaires. Ces applications ne sont pas interopérables, ce qui rend très difficile pour les utilisateurs de faire passer leurs données à un autre fournisseur de cloud ou de revenir à leurs machines.
— **Sécurité de données et confidentialité :** Dans le cloud computing, les données doivent être transférés entre les dispositifs de l'utilisateur et les Datacenter des fournisseurs de services de cloud computing, ce qui les rendra cible facile pour les pirates. La sécurité des données et la confidentialité doivent être garanties, que ce soit sur le réseau ou encore dans les Datacenter de cloud où elles seront stockées.
— **Migration de machines virtuelles :** La virtualisation peut offrir des avantages importants dans le cloud computing en permettant la migration de machine virtuelle pour équilibrer la charge de travail entre les Datacenter. Elle permet un approvisionnement robuste et très réactif dans les Datacenter. Les principaux avantages de la migration de VM est d'éviter les points chauds (hot spots). Toutefois, cela n'est pas simple à réaliser. Actuellement, la détection de points chauds et l'initiation d'une migration manque de souplesse pour répondre aux changements brusques de charge de travail.

— **Consolidation de serveurs :** La consolidation de serveurs est une approche efficace pour maximiser l'utilisation des ressources, tout en minimisant la consommation d'énergie dans un environnement de cloud computing. La technologie de migration de VM est souvent utilisée pour consolider les machines virtuelles se trouvant sur plusieurs serveurs sous-utilisés sur un seul serveur, de sorte à mettre ces derniers en mode d'économie d'énergie. Le problème de la consolidation optimale des serveurs est un problème d'optimisation NP-complet. Pour les ressources du serveur qui sont partagées entre les machines virtuelles, comme la bande passante, la mémoire cache et les E/S disques, consolider au maximum un serveur peut entraîner la congestion des ressources quand une machine virtuelle change son utilisation de ressource sur le serveur. Par conséquent, il est parfois important d'observer les fluctuations des traces de VM et d'utiliser cette information pour une consolidation efficace de serveurs.

— **Gestion de l'énergie :** Améliorer l'efficacité énergétique est un autre enjeu majeur dans le cloud computing. Il a été estimé que le coût de l'alimentation et du refroidissement compte pour 53% des dépenses de fonctionnement total des Datacenter. En 2006, les Datacenter aux États-Unis ont consommé plus de 1,5% de l'énergie totale produite dans l'année, et le pourcentage devrait croître de 18% par an. Ainsi, les fournisseurs d'infrastructure doivent prendre des mesures pour réduire la consommation d'énergie. L'objectif est non seulement de réduire le coût de l'énergie dans les Datacenter, mais aussi pour répondre aux réglementations gouvernementales et aux normes environnementales.

— **Ordonnancement :** L'ordonnancement est un enjeu important qui influence considérablement les performances de l'environnement de cloud computing. Il existe plusieurs niveaux d'ordonnancement dans le cloud, notamment : l'ordonnancement au niveau application et l'ordonnancement au niveau infrastructure. Le premier consiste en l'ordonnancement (affectation) des tâches composant les applications des utilisateurs sur les services IaaS ou HaaS du cloud, et le deuxième niveau concerne l'affectation de machines virtuelles sur les infrastructures physiques (machines physiques) du cloud. Les deux niveaux d'ordonnancement sont des problèmes complexes.

2.8 Conclusion

Dans ce chapitre, on a vu les aspects fondamentaux du Cloud Computing, les modèles de déploiement ainsi que les caractéristiques essentielles. Cloud Computing est encore un paradigme en évolution qui se base sur de nombreuses technologies existantes. Une brève rétrospective de l'histoire de l'informatique nous a aidé à bien comprendre les évolutions et le besoin du Cloud Computing. Le Cloud il est de plus en plus adopté dans les sociétés mais il reste encore quelques challenges et lacunes comme on a pu le voir comme la sécurité. Le prochain chapitre va traiter la problématique de la sécurité dans le Cloud.

Gestion de la sécurité 3

3.1 Introduction

De plus en plus d'entreprises utilisent des applications web pour exploiter des données privées, telles que des données bancaires ou des informations personnelles. Toutes ces données représentent un attrait considérable pour un attaquant. Une fuite de données due à un piratage a un impact majeur sur l'image d'une entreprise. Ces dommages se matérialisent bien souvent par des pertes financières importantes, à tel point que le Forum économique mondial (World Economic Forum) a placé la cybersécurité en tête de sa dernière liste de risques mondiaux dans le Global Risks Report 2019 [1], en annonçant que la cybersécurité était la plus grande menace qui pèse sur l'économie mondiale. La mise en place de pratiques de développement sécurisées au sein d'une entreprise peut représenter un budget considérable. Toutes les entreprises ont des actifs qu'elles doivent protéger. Ces actifs peuvent être des équipements physiques tels que des serveurs, mais aussi des données que l'entreprise doit protéger. C'est pour cette raison que les entreprises doivent mettre en place une politique de gestion des risques, comprenant la gestion de la responsabilité de la sécurité de l'entreprise. Cependant, cette politique ne sera pas la même en fonction de la valeur des actifs.

Dans ce chapitre, nous étudions d'abord les concepts liés à la sécurité, après nous abordons la gestion de la sécurité et le besoin d'avoir un cadre pour la définition d'une politique de sécurité globale. Nous présentons la technique de modélisation des menaces que nous allons utiliser par la suite dans notre approche. Nous nous intéressons ensuite, aux défis de la sécurisation dans le cloud computing.

NSIT [Pub, 2004] définit la sécurité comme étant « la protection de l'information et des systèmes d'information contre tout accès et utilisation non autorisés, divulgation, perturbation, modification ou destruction ». Selon C. Alberts, « la sécurité revient à déterminer ce qui doit être protégé et pourquoi, ce qui a besoin d'être protégé et comment le protéger tant qu'il existe » [Christopher Alberts, 2002]. Ces définitions nous montrent que la sécurité d'un système revient à la définition de ce système et à l'identification de la portée de la sécurité sur la totalité des composants formant le système.

La sécurité représente la « satisfaction des besoins de sécurité des biens essentiels » selon [De la Défense Nationale, 2004]. Les besoins de sécurité créent des objectifs de sécurité à atteindre et conduisent à mettre en place des mesures pour améliorer la sécurité

1. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

d'un système [Bou Nassar, 2012]. Dans ce qui suit, nous traitons les objectifs de sécurité, les mesures de sécurité et les stratégies de développement de systèmes sécurisés.

3.2 Les objectifs de sécurité

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité informatique vise généralement ces principaux objectifs qui peuvent être appliqués pour garantir la sécurité d'une application ou d'une infrastructure :

— L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être.
— La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
— La disponibilité, permettant de maintenir le bon fonctionnement du système d'information.
— La non répudiation, permettant de garantir qu'une transaction ne peut être niée.
— L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

3.2.1 La confidentialité

La confidentialité a été définie par l'Organisation internationale de normalisation (ISO) comme « le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé », et est une des pierres angulaires de la sécurité de l'information. La confidentialité est l'une des raisons d'être des cryptosystèmes, rendus possibles dans la pratique par les techniques de la cryptographie moderne.

Les données protégées doivent être accessibles qu'à ceux (les acteurs ou les systèmes) qui sont autorisés [Zissis et Lekkas, 2012]. Avec, le Cloud Computing la menace de la protection des données augmente, en raison du nombre d'acteurs, d'appareils et d'applications impliqués, ce qui entraîne une augmentation du nombre de points d'accès. La délégation du contrôle des données entraîne un risque accru car les données deviennent accessibles à un nombre accru d'acteurs [Zissis et Lekkas, 2012]. Pour résumer, c'est l'assurance que les personnes non autorisées n'accèdent pas à des informations sensibles.

3.2.2 La disponibilité

L'objectif de la disponibilité est de garantir l'accès à un service, à une information ou à une ressource à tout moment pour les personnes autorisées. La disponibilité est assurée techniquement en assurant la protection des ressources et de s'assurer que ces biens fonctionnent correctement. Toutefois, il ne faut pas oublier que la disponibilité est aussi assurée en mettant en place des procédures et des politiques de sécurité. En effet, les dénis de service (indisponibilité du service) sont causés par les attaques malveillantes qui peuvent résulter de la non-application des politiques et des procédures de sécurité

[Bou Nassar, 2012]. En bref, c'est l'assurance qu'il n'y a pas de perturbation d'un service ou de l'accessibilité aux données.

3.2.3 L'intégrité

D'après l'agence nationale de la sécurité des systèmes d'information (ANSSI) [De la Défense Nationale, 2004], l'intégrité est la propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée. Pour assurer l'intégrité de l'information en transit, on peut utiliser des mécanismes de signature électronique. L'intégrité de l'information au repos est assurée en utilisant des mécanismes de signature de cette information d'une part et en vérifiant par des mécanismes de détection d'intrusion que les systèmes hébergeant l'information fonctionnent d'une façon fiable d'autre part. L'intégrité permet donc, d'être sûr que les données sont fiables et n'ont pas été modifiées par des personnes non autorisées.

3.2.4 Les objectifs dérivés

La non répudiation

La non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues [Yacine Challal and Hatem Bettahar, 2008]. Cet objectif garanti qu'aucun des correspondants ne pourra nier la transaction.

L'authentification

L'accès aux ressources d'un système d'information par une entité, se décompose en trois sous-processus, l'authentification, l'identification et le contrôle d'accès. L'authentification désigne le processus visant à confirmer qu'un utilisateur est bien légitime pour accéder au système. Cet objectif permet de valider l'identifiant d'un utilisateur ou d'un service. L'authentification est une fonction que les fournisseurs de services offrent pour garantir que les utilisateurs accédant aux ressources (par exemple, les applications, le contenu Web, etc.) sont autorisés à le faire. Pour s'assurer qu'un utilisateur n'est pas un imposteur, les fournisseurs de services (par exemple, les serveurs Web) demandent généralement le nom d'utilisateur et le mot de passe d'un utilisateur pour prouver son identité avant d'autoriser l'accès aux ressources. L'authentification unique (SSO) est un mécanisme de contrôle d'accès qui permet à un utilisateur de s'authentifier une fois et d'accéder aux ressources logicielles sur plusieurs systèmes [Chang et al., 2014].

L'autorisation

L'autorisation est utilisée pour déterminer les autorisations accordées à un utilisateur déjà authentifié. C'est une mesure qui consiste à vérifier si l'utilisateur est autorisé à accé-

der aux ressources particulières ou non. L'autorisation se produit après l'authentification, lorsque l'identité de l'utilisateur est connue. En se basant par la suite sur ses habilitations le système déterminer si la ressource est accessible ou non.

Audit

Un audit de sécurité de l'information est un audit sur le niveau de sécurité de l'information dans une organisation. L'objectif c'est de vérifier le bon fonctionnement du système et de détecter les problèmes de sécurité et de conformité selon la politique de sécurité de la société.

3.3 La gestion de la sécurité

3.3.1 Sécurité des systèmes d'information

Il est nécessaire de poser les bases de la sécurité organisationnelle. En effet, la sécurité technique est un des maillons de la chaîne de la sécurité et non la chaîne en tant que telle.

On appelle système d'information (SI) l'organisation des ressources permettant de gérer l'information au sein des entreprises. Son directeur, nommé DSI (directeur des systèmes d'information), a la lourde tâche d'aider les entreprises dans l'accompagnement digital des choix stratégiques de l'entreprise ou bien dans l'orchestration de l'ensemble physique (backup, stockage, réseau) et logique (logiciel) de celle-ci.

Le monde devenant de plus en plus informatisé, les SI s'agrandissent. Afin de gérer et établir des règles, il est nécessaire de mettre en place de la gouvernance.

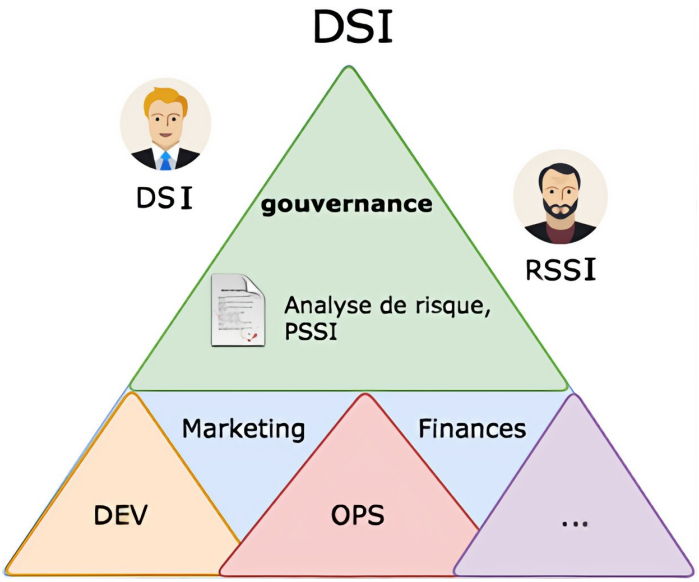


Figure 3.1 – *La gouvernance d'un système d'information [Thémée et Hennecart, 2017]*

La gouvernance est l'art et la manière de gérer un SI en établissant des obligations, procédures ou référentiels tels que COBIT et ITIL. Les décideurs tels que le DSI et le RSSI

(responsable de la sécurité des systèmes d'information) sont en charge de la gouvernance d'un SI figure 3.1. Contrairement au DSI, le RSSI est responsable de la sécurité, de l'intégrité et de la disponibilité de l'entreprise. Au-delà de la gestion de l'équipe sécurité au quotidien,intégrer et surveiller la sécurité du parc informatique, il est chargé d'instaurer la sécurité au niveau organisationnel et fonctionnel. Pour ce faire, il va se charger d'analyser les risques et d'identifier les besoins de l'entreprise en matière de sécurité de l'information. Une fois les exigences établies, il pourra créer une politique de sécurité du système d'information (PSSI) stipulant les règles à respecter au sein de l'entreprise pour tous les utilisateurs en matière de sécurité [Thémée et Hennecart, 2017].

3.3.2 Les mesures de sécurité

Les mesures de sécurité représentent les différentes solutions de sécurité qui pourront être mises en place pour atteindre les objectifs de sécurité. L'ontologie de sécurité NRL-SO [Kim et al., 2005] classifie les mesures de sécurité en trois types, les protocoles, les mécanismes et les politiques de sécurité :

1. Les protocoles de sécurité sont définis comme une série d'étapes permettant de réaliser une tâche bien définie [Bou Nassar, 2012]. Ces protocoles peuvent être associés aux protocoles fonctionnels qu'ils supportent comme des protocoles de sécurité associés aux protocoles de routage (IPsec est associé à IP), de transport (SSL/TLS est associé à TCP) ou d'application (DNSsec associé à DNS).
2. Les mécanismes de sécurité représentent la mise en œuvre des protocoles. Nous pouvons trouver des mécanismes de sécurité réseaux (VPN), des mécanismes systèmes, des mécanismes de services (Web Application Firewall) [Kim et al., 2005].
3. Les politiques gouvernent les mécanismes et les protocoles en spécifiant les règles de sécurité à appliquer. Différents types de politiques de sécurité peuvent être définis [Bou Nassar, 2012] :
   - Les politiques de sécurité métier sont définies par les responsables métier. Dans cette catégorie, on trouve par exemple les politiques spécifiant les droits d'accès à l'information.
   - Les politiques de sécurité applicative et architecturale sont définies par les architectes logiciels. Ces politiques sont utilisées dans la conception des applications. Par exemple, ces politiques intègrent la définition des rôles qui donnent des droits à l'invocation d'opérations dans une application.
   - Les politiques de sécurité opérationnelles sont définies par les administrateurs réseaux. Ces politiques sont utilisées dans la gestion de l'infrastructure technique comme par exemple la définition du nombre de tentatives de connexion sur un système informatique.

Afin de choisir les meilleures mesures de sécurité à mettre en place, il faut faire une veille sur les mesures de sécurité existantes et choisir parmi ces mesures celles qui sont les plus adéquates au contexte métier et technologique de l'entreprise. Par exemple, les mesures de sécurité suivantes pourront être mises en place pour assurer la confidentialité des données [Bou Nassar, 2012] :

- Des politiques spécifiant les droits d'accès aux données.

— Des mécanismes de chiffrement ou des mécanismes d'authentification et d'autorisation (Mandatory Access Control « MAC » [Samarati et de Vimercati, 2000], Role Based Access Control « RBAC » [Ferraiolo et al., 1995])
— Des protocoles de chiffrement tels que les protocoles SSL/TLS pour les données en transit. Assurer la confidentialité des données revient à choisir une ou plusieurs de ces instances, à les combiner en fonction des contextes métier et technologique de l'entreprise.

3.3.3 Les politiques de Sécurité

Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Une politique de sécurité représente le cœur de la sécurité d'un système d'information. Elle spécifie les contraintes à haut niveau d'un système. La définition d'une politique de sécurité adoptée en général est une spécification d'objectifs de sécurité qui explicitent ce qu'un système doit respecter. Celles-ci définissent ce qui est permis ou interdit dans l'utilisation et l'accès au système. Dans la plupart des cas, les politiques considèrent implicitement que tout ce qui n'est pas autorisé, est interdit. Cependant, dans certains cas, il peut être utile d'expliciter ce qui est interdit. Il est donc souvent indispensable, et c'est ce qui se fait en pratique, de vérifier ou de garantir des interdictions autant que des autorisations. Les politiques doivent être précises, non ambiguës, explicites, cohérentes et consistantes. Par exemple la politique, associée à un composant du type firewall, décrit les configurations du firewall, les permissions d'accès des utilisateurs et le contrôle du flot de données [Obeid, 2018].

Une politique de sécurité est décrite par des objectifs de sécurité. Ces objectifs sont regroupés en trois grandes classes : confidentialité, intégrité et disponibilité. Chaque objectif représente les conditions que le système doit respecter pour rester dans un état considéré comme sûr. Une définition incorrecte, ou l'application partielle d'une politique, peut entraîner le système dans un état non sûr [Obeid, 2018]. Une politique de sécurité n'implante pas seulement des restrictions et des contrôles, elle est définie d'une manière abstraite où les règles sont établies sans tenir compte des mécanismes d'implantation [Anderson et al., 2001]. Une formalisation permet le dialogue entre des concepteurs, des développeurs et des experts du domaine lors de la construction et la validation d'un système à sécuriser. Pour s'assurer d'une bonne définition des politiques de sécurité, il faut s'assurer que celles-ci soient cohérentes. Ceci signifie que les politiques sont consistantes et n'ont aucun conflit. En outre, ces politiques doivent être complètes en couvrant tous les cas et toutes les possibilités [Obeid, 2018].

3.3.4 Méthodes classiques et méthodes agiles

La méthode traditionnelle dite en cascade (Waterfall) a pour particularité d'être décomposée en plusieurs phases. Une fois une phase terminée, il est possible de passer à l'autre phase et ainsi de suite.

La figure 3.2 illustre le modèle en cascade d'un cycle de développement Waterfall.

La phase Exigences correspond généralement à l'analyse des besoins clients alors que la phase Conception correspond plutôt à la réflexion autour de l'architecture de l'applica-

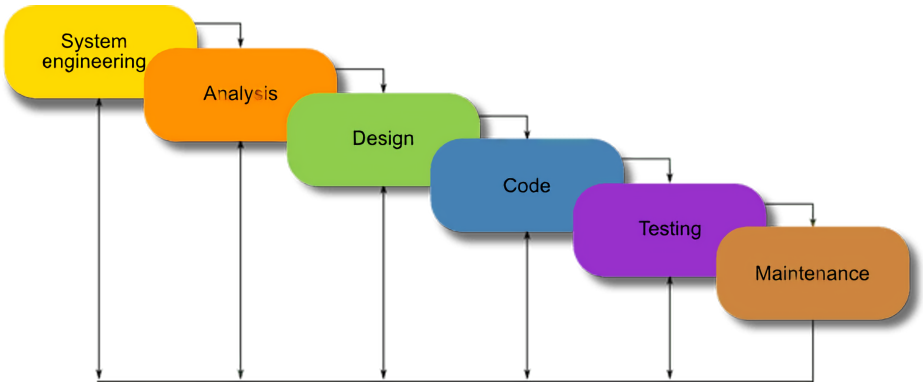


FIGURE 3.2 – *Modèle en cascade [Powell-Morse, 2016]*

tion et à la façon d'arriver au résultat escompté. La phase Code se charge du développement logiciel et la phase Test permet de vérifier la qualité et sécurité de celui-ci.

Même si cette méthode paraît concrète et logique, elle peut avoir quelques défauts comme [Anagnostopoulos, 2020] :

— Le modèle en cascade fonctionne sur l'hypothèse que toutes les exigences du client peuvent être collectées dès le début, en particulier avant le début de la phase de mise en œuvre du projet.

— A cause de la nature séquentielle du modèle, il peut y avoir un changement des exigences entre le moment du recueil du besoin et celui de l'implémentation.

— Le cout du changement est considérable vers la fin, donc ça nécessite des développements spécifiques.

Pour pallier ces problématiques, les méthodes agiles sont utilisées dans la plupart des organisations, des sociétés du monde logiciel et du DevOps. La figure 3.3 est une illustration représentant les itérations agiles.

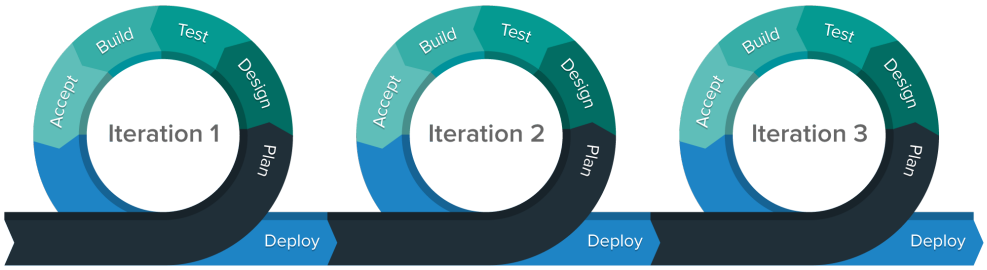


FIGURE 3.3 – *Les itérations agiles [PivotalTracker, 2020]*

Le modèle d'amélioration itérative décrit dans le diagramme suivant a été proposé en 1975 par Basili et Victori2lin pour tenter d'améliorer certaines des mises en garde du modèle en cascade.

Contrairement au Waterfall, les méthodes agiles se base sur une approche itérative. En reconnaissant que les exigences peuvent potentiellement changer pour les projets de longue durée, le modèle préconise d'exécuter un ensemble de cycles d'évolution ou d'itérations [Anagnostopoulos, 2020]. Ce qui veut dire que l'ensemble des phases du cycle de développement sont répétées plusieurs fois. Ce qui permet les avantages suivants [Anagnostopoulos, 2020] :

— Une amélioration continu du produit en se basant sur les retours des utilisateurs.
— Une visibilité sur l'avancement du projet.
— Un gain en qualité du code et du projet globalement. La dette technique a un impact certain sur la vitesse de l'équipe de développement, car les membres doivent souvent interrompre leur travail pour corriger les bogues potentiellement critiques qui ont été introduits lors des précédentes itérations.

L'agilité permet un gain de temps considérable grâce aux itérations successives mais l'équipe de développement néglige souvent la sécurité. Avec la relecture du code et les pratiques de codages on peut diminuer le nombre de bogues et d'erreurs mais ce n'est pas suffisant pour répondre à toutes les exigences de sécurité. La sécurité n'est pas une priorité dans ce genre d'approche parce que l'objectif principal c'est la livraison des fonctionnalités qui sont embarqués dans l'itération. Il est donc important de mettre en place un cycle de développement sécurisé.

3.3.5 DevSecOps

Une organisation est communément segmentée en plusieurs pôles d'activités, dont deux sont étroitement liés à l'intégration et à la livraison des applications. Le pôle développement (Dev) dont l'objectif est de créer, développer les applications et le pôle opérationnel (Ops) qui a pour mission d'intégrer les applications, gérer les serveurs et administrer le parc informatique.

Le DevOps décrit des approches d'accélération des processus selon lesquels une nouvelle fonctionnalité par exemple passe de la phase de développement à celle du déploiement dans un environnement de production où elle peut apporter de la valeur à l'utilisateur rapidement. Ces approches nécessitent que les équipes de développement et d'exploitation communiquent fréquemment entre elles et abordent leur travail en gardant à l'esprit celui de leurs collaborateurs. Le DevOps a pour fonction de rassembler les deux pôles (Dev et Ops) en se basant sur des méthodes agiles.

L'illustration ci-dessus (La figure 3.4) montre une chaîne DevOps classique permettant le déploiement d'une application avec des outils utilisés par les développeurs et d'autres intégrés par des administrateurs systèmes (Ops).

L'avantage de ce modèle est la rapidité de déploiement pour la mise en production d'une application. En effet, l'orchestration de ce processus permet l'exécution des différentes phases nécessaires pour la mise en production d'une application (test, déploiement, monitoring) de manière automatique. Se pose alors la question de la sécurité. Depuis quelques années, un mouvement appelé DevSecOps a pour objectif la réflexion autour de la sécurité du DevOps. Celui-ci étant un modèle récent, la sécurité autour de ce mouvement n'a pas encore beaucoup de retours d'expérience. Cependant, la plupart des experts du sujet sont unanimes sur l'utilisation des cycles de développement sécurisé comme modèle de sécurité sur le DevOps [Thémée et Hennecart, 2017]

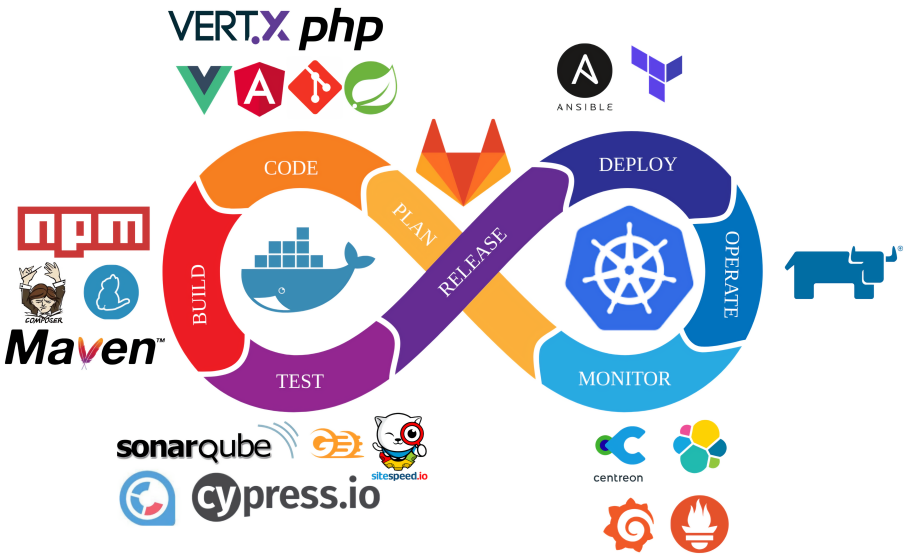


FIGURE 3.4 – *Chaîne DevOps classique [Aukfood, 2020]*

3.4 Les normes et référentiels

3.4.1 ISO/IEC 27034

Il existe un grand nombre de normes internationales concernant une multitude de branches métier. Les plus célèbres sont les normes ISO (International Organization for Standardization).

Les avantages des normes internationales sont nombreux ; elles assurent généralement le bon fonctionnement d'un service et permettent la certification des entreprises, ce qui est un gage de qualité dans certains métiers. Parmi les normes les plus pratiquées figurent les séries ISO/IEC 27000 et ISO/IEC 31000 relatives au management de la sécurité de l'information. ISO/CEI 27000 est une norme de sécurité de l'information publiée conjointement en mai 2009 et révisée en 2012, 2016 et 2018 par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI, ou IEC en anglais), faisant partie de la suite ISO/CEI 27000. Sans entrer dans les détails, ces normes ont pour objectif d'améliorer la protection contre le vol, l'altération et la perte de données, et de maîtriser le risque au sein d'un système d'information. Ci-après, quelques exigences de l'ISO/IEC 27001 et 27002 (Table 3.1) :

Les items cités ci-dessus montrent bien l'intérêt d'intégrer la mise en place d'un cycle de développement sécurisé au sein des systèmes d'information des entreprises.

La norme ISO/IEC 27034 a quant à elle l'objectif d'aider les organisations à mettre en place de la sécurité de façon transparente tout au long du cycle de vie d'une application. Elle s'intègre parfaitement avec les normes ISO/IEC 27001 et ISO/IEC 27002. Ci-dessous, la relation entre les normes ISO/IEC 27000 La figure 3.5 :

Index	Titre	Description
A.14.2.1	Politique de développement sécurisé	Des règles de développement des logiciels et des systèmes doivent être établies et appliquées au développement de l'organisation.
A.14.2.4	Restrictions relatives aux changements apportés aux progiciels	Les modifications des progiciels ne doivent pas être encouragées, doivent être limitées aux changements nécessaires et tous les changements doivent strictement être contrôlés.
A.14.2.7	Développement externalisé	L'organisation doit superviser et contrôler l'activité de développement du système externalisé.
A.14.2.6	Environnement de développement sécurisé	Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système.

TABLE 3.1 – *Quelques exigences de l'ISO/IEC 27001 et 27002 [ISO, 2018b]*

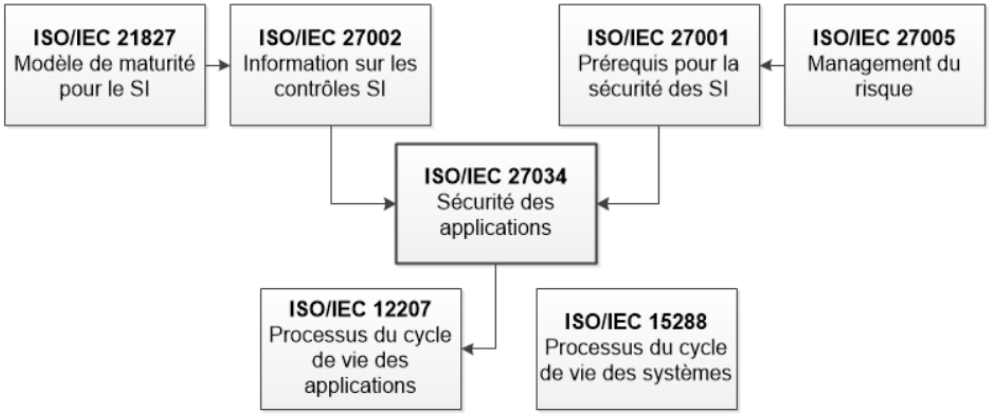


FIGURE 3.5 – *La relation entre les normes ISO/IEC 27000 [ISO, 2018a]*

Nous pouvons constater que l'ISO/IEC 27034 est une suite logique de la politique de sécurité de l'information, d'après l'organisme ISO. Voici ce que contient la norme avec ses différents points (Table 3.2) :

Partie de la norme	Titre	Publication
ISO/IEC 27034-1 :2011	Aperçu et concept de la sécurité des applications	Publié
ISO/IEC 27034-2 :2015	Cadre normatif d'une organisation	Publié
ISO/IEC 27034-3	Processus de la sécurité d'une application	Brouillon
ISO/IEC 27034-4	Validation de la sécurité d'une application	Abandonnée
ISO/IEC 27034-5	Protocoles et contrôles pour la structure des données	Brouillon
ISO/IEC 27034-6	Études de cas	Brouillon
ISO/IEC 27034-7	Assurance pour la sécurité applicative	Brouillon

TABLE 3.2 – *La norme ISO/IEC 27034 [ISO, 2011]*

Les sept parties de la norme représentent concrètement les différents points à aborder lors de la mise en place d'un cycle de développement sécurisé au sein d'une organisation.

Malgré cela, l'ISO/IEC 27034 n'est pas encore suffisante car seulement deux parties sont publiées par le comité et d'autres outils abordent de façon plus pragmatique et avec plus de maturité ces mêmes sujets.

3.4.2 PCI-DSS et PA-DSS

La norme Payment Card Industry Data Security Standard (PCI DSS) est une norme établie pour toutes les entreprises qui traitent des données bancaires. La sécurisation des données bancaires met l'accent sur la sécurité lors de la transmission, du traitement et du stockage des données. De plus en plus de plateformes web et de solutions de stockage gèrent les applications pour les entreprises, il est essentiel que le fournisseur soit également conforme à la norme PCI DSS. Son but est la mise en place de bonnes pratiques en matière de protection des données stockées sur les cartes bancaires pour les différents acteurs tels que les banques, commerçants, sociétés e-commerce et hébergeurs de solutions bancaires.

PCI-DSS comporte douze exigences, dont [Thémée et Hennecart, 2017] :

— Installer et gérer une configuration de pare-feu pour protéger les données du titulaire,

— Chiffrer la transmission des données du titulaire sur les réseaux publics ouverts,

— Utiliser des logiciels antivirus et les mettre à jour régulièrement,

— Restreindre l'accès physique aux données du titulaire,

— Tester régulièrement les processus et les systèmes de sécurité.

Les exigences ci-dessus montrent le pragmatisme de la PCI-DSS et couvrent bien l'essentiel des différents aspects de sécurité d'un processus de paiement à l'intérieur d'un système d'information.

Une fois ces critères remplis, le commerçant (entreprise ayant la gérance des données bancaires) peut demander par une société agréée à être audité afin d'obtenir l'accréditation PCI-DSS, qui sera valable un an.

De façon évidente, les actions requises pour l'accréditation PCI-DSS ne sont pas les mêmes suivant les profils des organisations. Il existe quatre niveaux définis par PCI concernant le type d'activité, ci-dessous un tableau récapitulatif (Table 3.3) :

La norme PCI-DSS n'est donc pas un acquis car il est nécessaire de façon générale d'auditer le site web tous les ans tout comme il devra être effectué un scan de vulnérabilité tous les trimestres. Le conseil PCI a pensé aussi aux concepteurs de logiciels en introduisant la norme PA-DSS (Payment Application Data Security Standard) qui définit les procédures et exigences d'évaluation de sécurité d'applications de paiement. Contrairement au PCI-DSS, la PA-DSS se limite à l'application en elle-même et non pas à son environnement extérieur. La PA-DSS est issue de la PCI-DSS et donc, il n'est pas possible d'être certifié PCI-DSS avec seulement l'accréditation PA-DSS [Thémée et Hennecart, 2017].

Pour conclure, cette norme permet aux concepteurs de logiciels d'être accrédités afin de pouvoir vendre des logiciels avec les prérequis nécessaires en sécurité pour des systèmes de paiement.

Niveau	Type d'activité	Actions requises pour la conformité
1	Tout commerçant traitant plus de 6 millions de transactions Visa ou MasterCard par an. Tout commerçant ayant subi une compromission.	— Audit de sécurité sur site (ou SAQ pour Visa Europe) — Scan de vulnérabilité trimestriel (si commerce en ligne)
2	Tout commerçant traitant de 1 à 6 millions de transactions Visa ou MasterCard par an.	— Questionnaire d'autoévaluation annuel — Scan de vulnérabilité trimestriel (si commerce en ligne)
3	Tout commerçant traitant de 20 000 à 1 million de transactions Visa ou MasterCard par an.	— Questionnaire d'autoévaluation annuel — Scan de vulnérabilité trimestriel (si commerce en ligne)
4	Tout commerçant traitant moins de 20 000 transactions de commerce en ligne Visa ou MasterCard par an. Tous les autres commerçants traitant jusqu'à 1 million de transactions Visa ou MasterCard par an.	— Questionnaire d'autoévaluation annuel — Scan de vulnérabilité trimestriel recommandé (si commerce en ligne. Cela dépend de si les données sont capturées, stockées ou transmises par l'infrastructure du commerçant ou par un fournisseur de services.)

TABLE 3.3 – *Les quatre niveaux définis par PCI [Council, 2018]*

Voici les quatorze exigences demandées par PA-DSS [Council, 2018] :

— Ne pas conserver la totalité des données de bande magnétique, de code ou de valeur d'audit de carte
— Protéger les données du titulaire stockées
— Fournir des fonctions d'authentification sécurisées
— Enregistrer l'activité de l'application de paiement
— Développer des applications de paiement sécurisées
— Protéger les transmissions sans-fil
— Tester les applications de paiement pour gérer les vulnérabilités et maintenir leurs mises à jour
— Permettre la mise en œuvre de réseaux sécurisés
— Les données du titulaire ne doivent jamais être stockées sur un serveur connecté à Internet
— Faciliter l'accès à distance sécurisé à l'application de paiement

— Crypter le trafic sensible transitant par les réseaux publics
— Crypter tous les accès administratifs non console
— Maintenir un Guide de mise en œuvre de la norme PA-DSS pour les clients, les revendeurs et les intégrateurs
— Affecter des responsabilités vis-à-vis de la norme PA-DSS au personnel et maintenir des programmes de formation pour le personnel, les clients, les revendeurs et les intégrateurs

3.4.3 HIPAA

HIPAA, acronyme anglais de Health Insurance Portability and Accountability Act, est une loi votée par le Congrès des États-Unis en 1996 et qui concerne la santé et l'assurance maladie qui régit l'utilisation, le stockage et la diffusion de données médicales personnelles. La loi est applicable à toutes les entreprises ayant accès à de l'information sur la santé et particulièrement aux USA. Le département américain de la santé et des services sociaux (HHS) a l'obligation de publier et mettre à jour les exigences pour la conformité des échanges de données à travers les différents acteurs de la santé. Voici les cinq domaines d'application de HIPAA [Centers for Medicare & Medicaid Services, 1996] :

— Vie privée
— Régulation des transactions
— Règle d'identification unique
— Règle de pénalités
— Sécurité des données

3.4.4 GDPR (General Data Protection Regulation)

Le règlement sur la protection des données (RGPD, ou encore GDPR, de l'anglais General Data Protection Regulation), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Les principaux objectifs du RGPD sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement. Ces principes pourront être appliqués grâce à l'augmentation du pouvoir des autorités de contrôle. Voici quelques obligations [Voigt et Von dem Bussche, 2017] :

— Désigner un responsable (Data Protection Officer) des données personnelles dans les entreprises afin de garantir la mise en conformité et donc la sécurité.
— Contraindre les responsables du traitement des données à l'effacement de celles-ci sous certaines conditions. C'est le "droit à l'oubli" de l'utilisateur.
— Permettre à l'utilisateur de transférer ses données personnelles vers une autre organisation dans un format lisible. C'est la "portabilité des données".
— Obliger les entreprises à prendre en compte des exigences relatives à la protection des données personnelles dès la conception des applications (privacy by design).

— Notifier l'autorité nationale, par exemple la CNIL en France, lors d'une fuite de données dans les 72 heures.
— Pour les entreprises, prévoir et documenter une analyse de risque, une analyse des incidences sur l'activité (business impact analysis) et prévoir des mesures.

En cas de non-respect du RGPD, plusieurs sanctions peuvent être appliquées aux entreprises. Bien qu'il soit basé sur la législation de l'Union européenne, il concerne tous les pays car les applications web sont disponibles dans le monde entier. Les entreprises en dehors de l'UE qui font du business avec des entreprises européennes devront respecter le RGPD pour leurs applications web à destination du marché européen. En cas d'infraction importante et liée au non-respect du RGPD, l'amende administrative pouvant être appliquée peut atteindre jusqu'à 20 000 000 euros ou dans le cas d'une entreprise, l'amende correspond à 4 % du chiffre d'affaires mondial (le montant le plus important sera là aussi retenu). Les principaux objectifs du RGPD sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement.

3.5 Les guides et bibliothèques

3.5.1 MITRE CWE

Common Weakness Enumeration ou CWE est une liste des vulnérabilités que l'on peut rencontrer dans les logiciels. Cette liste est maintenue par l'organisme MITRE, le projet étant soutenu par la National Cyber Security Division et le Département de la Sécurité intérieure des États-Unis. Cette organisation à but non lucratif soutenue par la division cybersécurité des États-Unis (National Cyber Security Division) est surtout connue pour ses deux listes de diffusions, CVE (Common Vulnerabilities and Exposures) et CWE (Common Weakness Enumeration).

La première (CVE) une liste publique de failles de sécurité informatique trouvées par les organisations et personnes du monde de la sécurité informatique, le but étant de fournir un identifiant commun à une vulnérabilité, et de partager des connaissances afin d'améliorer la sécurité des applications. Lorsque l'on parle d'une CVE, on fait généralement référence à l'identifiant d'une faille de sécurité répertoriée dans cette liste.

La deuxième (CWE) est une liste ou un dictionnaire formel des faiblesses logicielles et matérielles courantes qui peuvent se produire dans l'architecture, la conception, le code ou la mise en œuvre et qui peuvent conduire à des vulnérabilités de sécurité exploitables. CWE a été créé pour servir de langage commun pour décrire les faiblesses de sécurité.

3.5.2 BSIMM

Il s'agit d'un modèle de maturité créé à partir des données réelles recueillies à partir de 120 initiatives de sécurité applicative. Le Building Security In Maturity Model (BSIMM) est le résultat de plusieurs années d'études dans le monde de la sécurité applicative. Le

modèle collecte toutes les observations à partir des évaluations BSIMM (analyses d'organisations individuelles) afin de fournir les meilleures pratiques. Le pool de données actuel s'est étendu à plus de 125 organisations, faisant du BSIMM un projet vraiment vivant qui s'adapte au fur et à mesure que les méthodologies de développement changent ou que de nouvelles menaces émergent.

Le BSIMM atteint sa 10e itération, il continue d'être une ressource importante pour toutes les personnes impliquées dans la sécurité des logiciels.

BSIMM ne nous dit pas comment faire mais apporte plutôt un moyen de comparaison afin d'analyser la maturité des applications en matière de sécurité. Le projet est porté par les sociétés Cigital et Fortify. Celles-ci se réunissent autour de groupes de travail nommés SSG (Software Security Group) qui ont pour mission l'interview des sociétés participantes et le report des différentes informations [Thémée et Hennecart, 2017].

Une fois l'analyse faite entre BSIMM et votre cycle de développement, on obtient un moyen de comparaison de la maturité de sécurité en termes de cycle de développement sécurisé. Un exemple d'analyse du framework BSIMM est illustré par la figure 3.6.

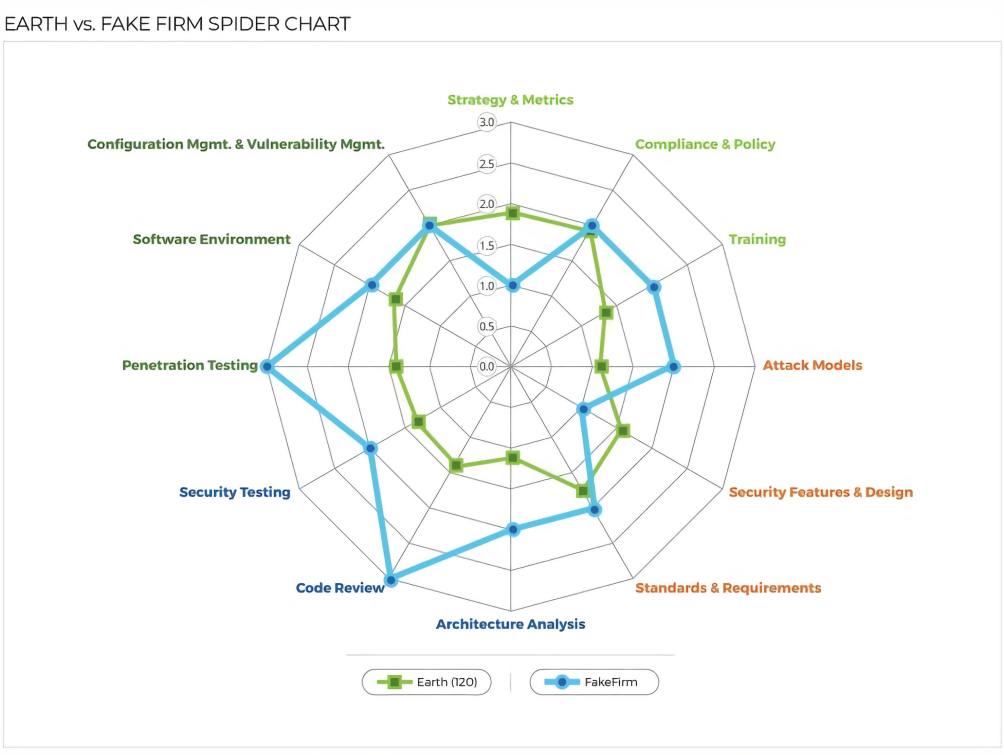


FIGURE 3.6 – *Le niveau de maturité d'une organisation après l'utilisation de BSIMM [Synopsys, 2018]*

3.5.3 OWASP

Open Web Application Security Project (OWASP) est une communauté en ligne travaillant sur la sécurité des applications Web. OWASP est une organisation à but non lucratif fondée en 2004 pour prévenir de manière proactive les attaques sur les applications web. Il s'agit du premier effort de normalisation des pratiques de développement sécu-

risé. En 2001, l'OWASP n'était pas une organisation officielle, mais plutôt un collectif qui préconisait des pratiques de développement sécurisé. Ce collectif a pris de l'ampleur et est devenu l'OWASP foundation en 2004, avec une norme éthique pour maintenir une neutralité et l'absence de pressions commerciales. L'OWASP n'est réglementée par aucune entreprise. Elle propose un référentiel neutre permettant d'accompagner les entreprises dans le processus de sécurisation ou d'audit de sécurité. Parmi les projets les plus connus, le TOP 10 OWASP a pour but d'évaluer les dix principaux risques pour la sécurité des applications web et préconise un développement logiciel sécurisé. Pour arriver à ce résultat, l'OWASP organise une enquête mondiale sur les différentes vulnérabilités relevées par les contributeurs de l'enquête et ainsi, établit un classement dont les items sont les suivants [Open Web Application Security Project, 2017] :

— Injection (SQL, LDAP, Xpath, etc.)
— Violation de gestion d'authentification et de session
— Cross-Site Scripting (XSS)
— Références directes non sécurisées à un objet
— Mauvaise configuration de sécurité
— Exposition de données sensibles
— Manque de contrôle d'accès au niveau fonctionnel
— Falsification de requête intersite (CSRF)
— Utilisation de composants avec des vulnérabilités connues
— Redirections et renvois non validés

3.6 Modélisation des menaces (threat modeling)

3.6.1 SDL de Microsoft

Le SDL (Security Development Lifecycle) de Microsoft est un processus de sept étapes aidant à la création d'un cycle de développement sécurisé. L'ensemble des étapes regroupent les différentes phases de sécurisation et les tâches à effectuer en matière de sécurité lors de la construction d'une application.

Voici une illustration par Microsoft des différentes phases du SDL Microsoft - La figure 3.7.

Les différentes étapes du SDL Microsoft [Thémée et Hennecart, 2017] :

— La première phase, nommée "sensibilisation" (training), a pour but de former les équipes et particulièrement les développeurs aux différentes vulnérabilités de sécurité, à l'analyse de code ainsi qu'à la modélisation des menaces pour une optimisation du code en matière de sécurité.
— La seconde phase "exigences" (requirements) définit les prérequis pour commencer la création d'un cycle de développement sécurisé comme établir les responsables de la sécurité sur le cycle de développement et du respect des données privées, définir les critères de sécurité demandés par l'organisation, et établir une gestion d'identification et de suivi des vulnérabilités.

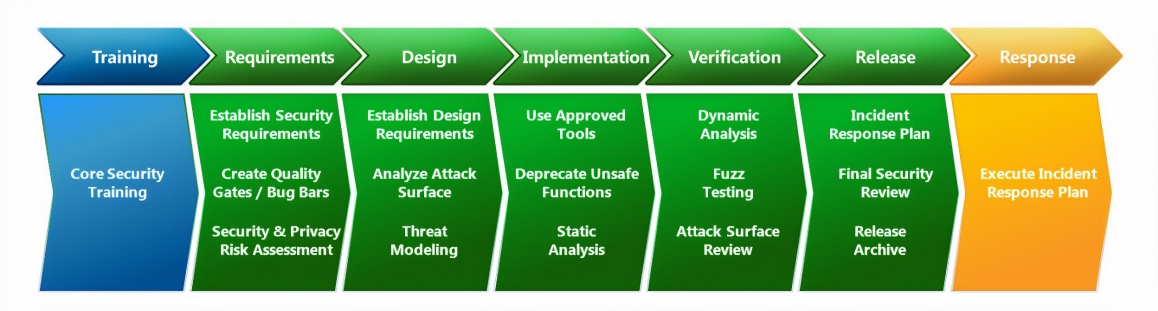


FIGURE 3.7 – *Les différentes phases du SDL Microsoft [Microsoft, 2012]*

— La phase "conception" (design) traite de la modélisation des menaces de l'application, l'objectif étant de déterminer la probabilité et les différentes menaces pouvant porter sur l'application. L'objectif est de trouver les différentes menaces et de les prévenir pour un gain de temps et d'argent pour l'organisation.

— La phase "implémentation" demande l'installation d'outils d'analyse statique de code afin de trouver des vulnérabilités dans le code de l'application ainsi que les fonctions prescrites par l'organisation avant la mise en production.

— La phase "vérification" nécessite le lancement d'outils de fuzzing permettant d'automatiser l'envoi de requêtes afin de trouver des différents bugs et potentielles failles sur l'application. Un test de pénétration peut aussi être engagé.

— L'avant-dernière phase, "diffusion" (release), s'oriente sur la création d'un plan de suivi des incidents afin d'organiser une action immédiate pour arrêter ou réduire l'impact de l'incident le cas échéant.

— Un passage en revue final est aussi conseillé. Celui-ci s'organise à travers l'analyse des exigences et prérequis demandés lors de la phase requirements, et l'analyse des bugs et vulnérabilités trouvés lors de la phase verification.

— Un archivage des différentes documentations, codes sources, procédures est également conseillé lors de cette phase.

— La dernière phase, nommée "response", est l'exécution du plan de réponse à incident prévu dans la phase précédente. Cette phase permettra d'ajouter des mises à jour de sécurité à l'application.

3.6.2 Présentation de la modélisation des menaces

Dans le domaine de la sécurité informatique, le modèle de menace est un processus par lequel des menaces potentielles, telles que les vulnérabilités structurelles peuvent être identifiées, énumérées et classées par ordre de priorité - du point de vue de l'hypothétique agresseur [Swiderski et Snyder, 2004].

Quels sont les risques potentiels pour mon architecture ? Quels sont les actifs à prioriser en termes de sécurité ? Ce sont là des questions qui pourraient représenter la modélisation de menaces. La figure 3.8 représente le processus classique :

La première phase du Threat modeling, Diagramme, consiste à décomposer l'application et son architecture à l'aide d'un diagramme dit DFD (Data Flow Diagram). Le but

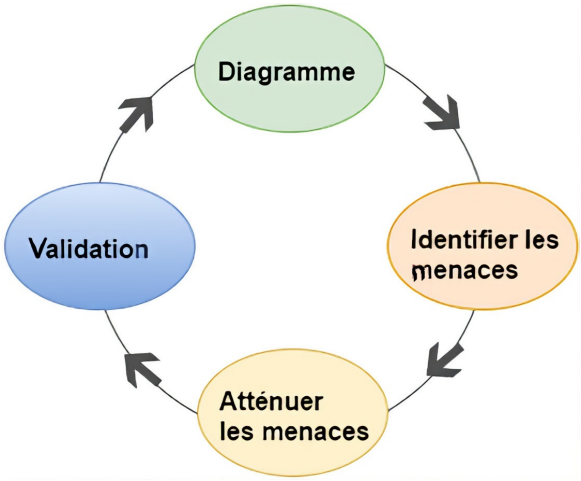


FIGURE 3.8 – *Le processus de modélisation des menaces [Thémée et Hennecart, 2017]*

est de déterminer les points d'entrée par lesquels un cybercriminel pourrait passer et le niveau de confiance de chacun.

La deuxième phase, Identifier les menaces, consiste à utiliser une méthodologie comme STRIDE ou PASTA qu'on va voir par la suite. Le but de cette étape est de trouver le type de menaces et de mesurer celles-ci pour chaque point d'entrée. La troisième phase, Atténuer les menaces, a pour fonction de déterminer les contre-mesures et contrôles de sécurité à mettre en place pour les menaces identifiées lors de la phase 2.

La dernière phase, Validation, consiste à faire valider les trois premières phases établies auparavant par les pairs et généralement, les managers en sécurité.

3.6.3 Diagramme de flux de données

Le Data Flow Diagram est un type de représentation graphique du flux de données à travers un système d'information. Cet outil est souvent utilisé comme étape préliminaire dans la conception d'un système afin de créer un aperçu de ce système d'information.

Il faut d'abord collecter les informations utiles qui vont permettre de créer une représentation visuelle de l'architecture et des processus internes de l'application. La figure 3.9, représente une modélisation des flux d'une application avec l'outil de modélisation des menaces de Microsoft.

3.6.4 Identification des menaces

Durant cette phase on peut employer plusieurs modèles mais le plus populaire reste le modèle STRIDE de Microsoft. STRIDE (pour Spoofing - Tampering - Repudiation - Information Disclosure - Denial of Service - Elevation of Privilege) est un modèle de classification de Menaces (Threats) développé par Microsoft. Voici une présentation de l'acronyme STRIDE [Contributor, 2018] :

Spoofing (Userpation) : on appelle "Usurpation (d'identité)" le fait qu'un pirate in-

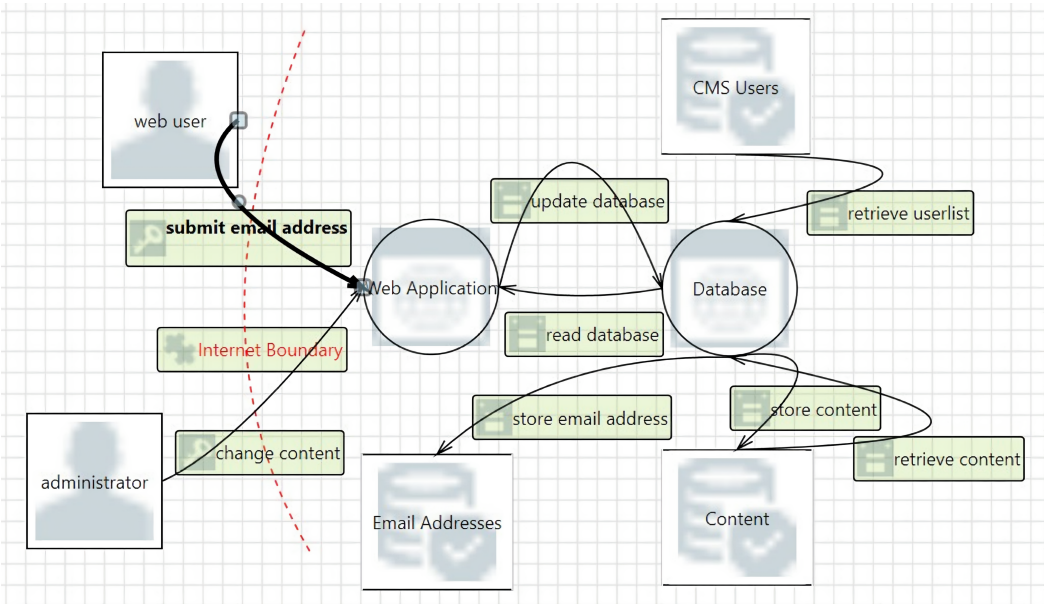


FIGURE 3.9 – *Exemple de modélisation d'un DFD*

formatique se fasse passer pour un autre utilisateur ou Device du réseau pour voler des données ou obtenir l'accès à des informations confidentielles (e.g : données financières). Les formes les plus courantes d'usurpation sont l'usurpation d'IP, l'usurpation d'e-mail et l'usurpation de DNS.

Tampering (Falsification) : falsifier signifie modifier ou supprimer une ressource sans autorisation. C'est le cas par exemple de l'altération d'une page Web par un utilisateur malveillant qui accède à un site et en modifie les fichiers. L'utilisation d'une attaque de script constitue un moyen de falsification indirect. Un utilisateur malveillant envoie du code (script) exécutable en le masquant comme entrée d'utilisateur d'un formulaire ou sous forme de lien

Repudiation (Répudiation) : la répudiation définit le comportement d'une personne qui nie malhonnêtement avoir reçu ou envoyé certaines informations au cours d'une transaction ou une communication au travers d'un réseau, alors que ce n'est pas le cas.

Information Disclosure (Divulgation de l'information) : la divulgation de l'information permet à un pirate informatique d'obtenir des informations "précieuses" sur votre système d'information, ou simplement sur une plateforme applicative spécifique (Web-Site, Web App...etc) : vol d'informations liées à un site Internet telles que la distribution de logiciels, les numéros de version et les niveaux de module de correction. Les informations collectées peuvent également comporter l'emplacement des fichiers de sauvegarde ou des fichiers temporaires.

Denial of Service (Déni de Service) : une attaque par Déni de Service a pour but de rendre indisponible un système informatique (WebSite, Application, Serveurs de données/fichiers...etc) et d'empêcher les utilisateurs légitimes du réseau de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (DDoS attack pour Distributed Denial of Service attack).

Elevation of Privilege (Elévation de privilège) : L'élévation de privilège consiste, pour un utilisateur malveillant, à obtenir un niveau d'autorisation plus élevé que celui qui lui est normalement attribué (passage d'un rôle "Standard User" à "Admin User /root". Par exemple, dans une attaque d'élévation de privilège réussie, un utilisateur malveillant parvient à obtenir des privilèges d'administrateur sur un serveur Web, d'application ou d'annuaire (LDPA /AD)ce qui lui permet de réaliser librement tous les ravages qu'il souhaite.

Chaque menace peut être atténuée par un contrôle (Table 3.4) :

Threat	**Desired property**
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

TABLE 3.4 – *Le modèle des menaces - STRIDE*

3.6.5 La phase d'évaluation des menaces

Il n'est pas toujours possible de traiter toutes les menaces identifiées parce pour certaines le changement et les éventuels dommages qu'elles entraînent sont minimes. Ainsi, cette phase permet d'évaluer les menaces précédemment identifiées en fonction du risque qu'elles représentent et de traiter en priorité celles qui présentent le plus grand risque, avant de résoudre les autres dans un second temps.

Pour mener à bien cette étape, il faut utiliser des critères précis qui permettent d'obtenir un calcul du risque qui soit consistent. DREAD, également tiré de la méthodologie SDL de Microsoft. Comme pour STRIDE, DREAD est un est un acronyme : chaque lettre correspond à l'une catégorie de risques suivantes - La figure 3.10 :

3.7 La sécurité dans le Cloud Computing

3.7.1 Définition

La sécurité dans le cloud est un sous domaine de cloud computing en relation avec la sécurité informatique. La sécurité du cloud peut être définie comme étant l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour protéger les données, les applications et l'infrastructure associée au cloud contre une faiblesse d'ordre logicielle ou matérielle qui peut être exploitée par une ou plusieurs menaces internes ou externes. La sécurité du cloud implique des concepts tels que la sécurité des réseaux et du matériel ainsi que les stratégies de contrôle déployées afin de protéger les données, les applications et l'infrastructure d'un environnement de cloud [Hamze, 2015].

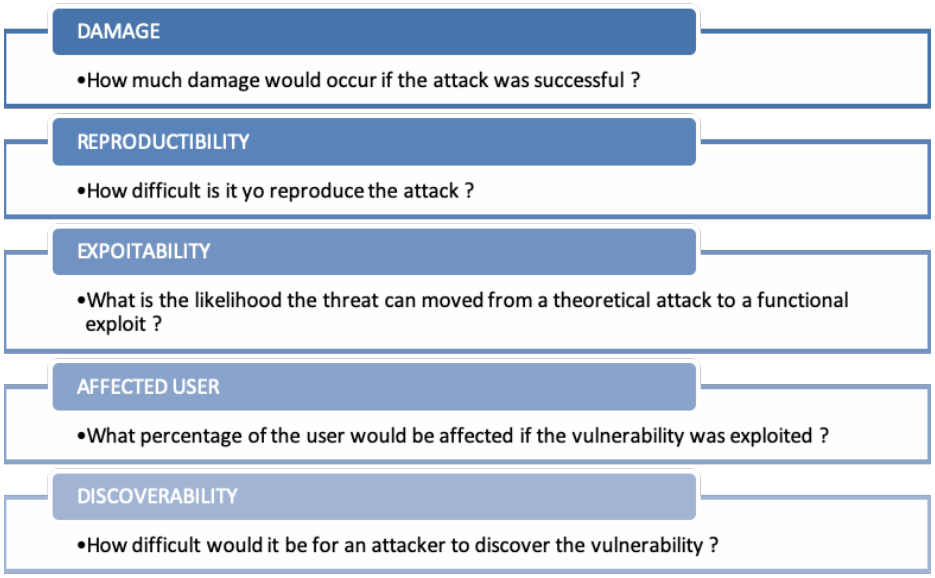


FIGURE 3.10 – *DREAD (modèle d'évaluation des risques)*

3.7.2 Confiance

La confiance est liée à tous les défis auxquels fait face l'adoption du cloud computing. Elle est grandement influencée par la sécurité de l'information et systèmes. La complexité du cloud computing rend la problématique de sécurité d'une importance primordiale pour les consommateurs potentiels et les fournisseurs de services. Ces différents points soulèvent la problématique de confiance dans l'utilisation des services de cloud computing [Filali, 2015].

La notion de confiance dans le cloud peut être définie comme étant la croyance du CSU (Cloud Service User) dans le fait que le CSP (Cloud Service Provider) est capable de fournir les services requis de façon précise et infaillible grâce à l'efficacité de ses mécanismes de sécurité et le respect de tous les règlements. De plus, la confiance dans un environnement de cloud dépend fortement du modèle de déploiement choisi. Dans le cas d'un cloud privé, le contrôle est réalisé par l'organisation propriétaire de l'infrastructure et la confiance reste alors à assurer à l'intérieur d'une même organisation. Cependant, lors du déploiement sur un cloud public, le contrôle est délégué au CSP pour appliquer une politique de sécurité adéquate afin de garantir que les mécanismes de sécurité appropriés soient mis en place. La confiance du CSU dépendra de l'efficacité de cette politique de sécurité qu'il ne contrôle pas dans un environnement de cloud public [Hamze, 2015].

La confiance est liée principalement aux processus de sécurité mis en place par le CSP et le modèle de sécurité du cloud doit être basé sur l'hypothèse que le consommateur devrait faire confiance au provider. Cette sécurité relative à l'offre de service du cloud peut faire l'objet d'un accord de niveau de service (SLA) qui définit les attentes des CSU et les obligations des CSP pour le provisionnement des services de Cloud [Demchenko et al., 2011].

3.7.3 Service Level Agreement de sécurité

La sécurité dans le cloud peut être définie dans le Service Level Agreement (SLA), afin de prévenir et garantir les niveaux de sécurité pour chaque service. Le SLA définit la sécurité mise en place contre les attaques malveillantes et les pannes éventuelles entrainant des problèmes de sécurité. Cet accord de niveau de service peut être négocié et établi entre le provider et le consommateur ou entre les providers [Hamze, 2015].

De plus, la spécification d'un niveau de sécurité mesurable dans le SLA est utile pour améliorer la transparence et la confiance dans la relation entre le consommateur et le provider. Cette spécification d'un niveau de sécurité permet d'établir une sémantique commune afin de gérer la sécurité du cloud à partir de deux perceptions différentes, à savoir le niveau de sécurité tel qu'il est offert par un provider et le niveau de sécurité tel qu'il est demandé par le consommateur [Hamze, 2015].

3.7.4 Challenges

Dans le cloud, les services sont fournis via Internet à des clients à la demande selon leurs besoins. Les ressources sont disponibles dans des data centers accessibles partout sur Internet. La sécurité est l'un des défis à relever les plus importants pour l'adoption du Cloud. L'hébergement et le traitement ont amené à des préoccupations portant sur la confiance et la sécurité sur cloud. En effet, l'externalisation du traitement ou encore du stockage des données dans un environnement de cloud computing s'accompagne d'un risque de sécurité puisque les données peuvent être compromises à différentes étapes comme le transfert de données du réseau interne de l'entreprise vers le Cloud ou encore lors du processus de restauration des données. Par conséquent, nombreuses organisations ont hésité à externaliser leur SI vers le cloud en raison de restrictions réglementaires ainsi que des préoccupations quant à la confiance et la garantie de sécurité [Hamze, 2015].

Le modèle de cloud présente un certain nombre de menaces cela est dû entre autres à la délégation du contrôle des données, les données deviennent ainsi accessibles à un nombre important de partenaires [Hamze, 2015].

3.7.5 Travaux de standardisation portant sur la sécurité dans le cloud

Dans cette section, nous présentons des organismes de standardisation qui étudient la sécurité dans le cloud [Hamze, 2015]. Nous remarquons que plusieurs organismes contribuent aux efforts de standardisation portant sur la sécurité, cependant, il n'y a pas encore des standards (Table 3.5) :

Nom	**But**
OMG Cloud Working Group [Object Management Group, 2018]	Accélérer l'adoption du Cloud en proposant des standards de sécurité et d'interopérabilité liés à la transition vers le Cloud.

DMTF Cloud Management Standards [Distributed Management Task Force, 2016]	Présenter des métriques pour le SLA, y compris les attributs de sécurité pour l'environnement Inter-Cloud.
ENISA (European Network and Information Security Agency) [European Union Agency for Cybersecurity, 2015]	Présenter une liste hiérarchisée des risques organisationnels, techniques et juridiques, avec une comparaison des différents CSP selon leurs pratiques de sécurité. De plus, cet organisme a pour but de présenter les avantages et les inconvénients de sécurité des Clouds communautés, privés et publics.
CSA (Cloud Security Alliance) [Cloud Security Alliance (CSA), 2020]	Proposer plusieurs documents de référence et des guides portant sur la sécurité du Cloud pour favoriser un niveau commun de compréhension entre le CSU et le CSP en ce qui concerne les exigences de sécurité. De plus, cet organisme a pour objectif de créer des listes de questions réponses avec des conseils pour la garantie de la sécurité du Cloud grâce à des programmes éducatifs portant sur les utilisations appropriées du Cloud et des solutions de sécurité.
ITU-T [Sector, 2011]	Publier des rapports et des guides portant sur la sécurité du Cloud Computing [Sector, 2011], tels que : Security guidelines for Cloud Computing in the telecommunication area (X.ccsec), Security requirements and framework of the Cloud-based telecommunication service environment (X.srfcts), Security functional requirements for SaaS application environment (X.sfcse), Requirement of IdM in Cloud Computing (X.idmcc), X.gpim, Guidelines on information security management for telecommunications (ITU-T X.1051, ITU-T X.1055), Cybersecurity Information Exchange (CYBEX), (ITU-T X.1500 (Overview), ITU-T X.1520 (CVE) et ITU-T X.1521 (CVSS)).
NIST [Mell et Grance, 2011]	Réaliser un projet d'évaluation et d'autorisation de sécurité dans le Cloud et étudier les exigences et les défis de sécurité du Cloud pour le gouvernement américain.
ISO/IEC JTC1/SC27 [for Standardization, 2014]	Étudier la sécurité et la vie privée dans le Cloud : ce travail est réalisé au sein des groupes de travail WG1/WG4/WG5.

OASIS [for the Advancement of Structured Information Standards, 2016]	Développer des guidelines pour l'atténuation des vulnérabilités et l'analyse des risques et des menaces concernant certains cas d'utilisation dans le Cloud.
SNIA Cloud Data Management Interface (CDMI) [Organization, 2015]	Développer une interface standardisée portant sur la sécurité dans le Cloud.

TABLE 3.5 – *Exemple d'organisations de standardisation de la sécurité dans le Cloud [Hamze, 2015]*

3.8 Conclusion

Dans ce troisième chapitre, nous avons présenté les concepts liés à la sécurité. Nous avons introduit aussi la gestion la sécurité qui est fortement dépendante des besoins et objectifs métier qu'il faut bien identifier pour pouvoir mettre en place les mesures de sécurité adaptées au contexte de l'entreprise en se basant sur des normes et des guides.

Ensuite, nous avons abordé la modélisation des menaces ainsi les défis de la sécurité dans le cloud. Nous avons noté la particularité de cette architecture concernant l'étendue du périmètre et la nécessité d'aborder les problématiques de la sécurité du cloud computing pour donner confiance aux entreprises.

Etat de l'art

4

4.1 Introduction

Dans ce chapitre, nous nous intéressons d'abord aux travaux qui traitent la problématique d'extension du BPMN d'une manière générale, après nous passerons en revue les différentes approches d'annotations de sécurité dans les processus métiers qui sont basé sur le BPMN Chergui et Benslimane [2018].

Par la suite, nous abordons les approches qui traitent le sujet de sécurité dans le cloud. Cette revue de littérature est importante, parce qu'elle nous permettra de dégager les limites des approches existantes pour pouvoir nous positionner.

4.2 Extension du BPMN

Le BPMN (Business Process Model and Notation) est une norme ISO pour la modélisation des processus métiers. BPMN fournit un ensemble d'éléments de processus métier génériques et indépendants. Cependant, il est souvent nécessaire d'étendre le BPMN avec de nouveaux éléments afin de représenter les concepts d'un domaine particulier (par exemple, la santé ou la gestion de la sécurité). Le BPMN 2.0 supporte nativement les extensions afin de facilter l'intégration et l'échange entre les différents outils de modélisation.

Une extension BPMN est défini comme une amélioration des fonctionnalités de base de BPMN. BPMN est l'un des très rares langages de modélisation à fournir un mécanisme d'extension génériques au niveau du méta-modèle par addition qui garantit la validité des éléments de base du BPMN.

Dans cette première section, nous allons examiner le mécanisme d'extension et étudier quelques travaux pour tirer des conclusions sur les meilleurs pratiques de développement des extensions et les limites.

Le métamodèle BPMN peut être étendu avec l'ajout de nouveaux attributs (ou éléments) à ses éléments de base prédéfinis. Ceci est possible grâce au mécanisme d'extension qui offre quatre éléments [Stroppi et al., 2011] :

— **Extension Definition** : regroupe les nouveaux attributs à ajouter aux éléments BPMN de base sous un nouveau nom de concept.

— **Extension-Attribute Definition** : représente un attribut défini pour un élément « Extension Definition »

— **Extension Attribute Value** : stocke la valeur d'un attribut d'extension.

— **Extension** : importe l'élément « Extension Definition » à l'élément BPMN « Definition ».

Le mécanisme d'extension BPMN est prévu directement dans le métamodèle. Le mécanisme permet la définition des groupes d'attributs et d'éléments qui sont attachés aux éléments standard du BPMN. Les modèles BPMN utilisant des extensions restent interchangeables car la structure des éléments d'origine n'est pas modifiée. La spécification BPMN fournit deux représentations (La figure 4.1). Un métamodèle MOF décrivant les concepts du langage. Le second est un ensemble de documents XML Schema spécifiant le format d'échange pour les modèles BPMN. Comme MOF a son propre format d'échange appelé XML Metadata Interchange (XMI), OMG fournit également un ensemble de transformations XSL visant à convertir les modèles BPMN en formats XML Schema ou XMI [Stroppi et al., 2011].

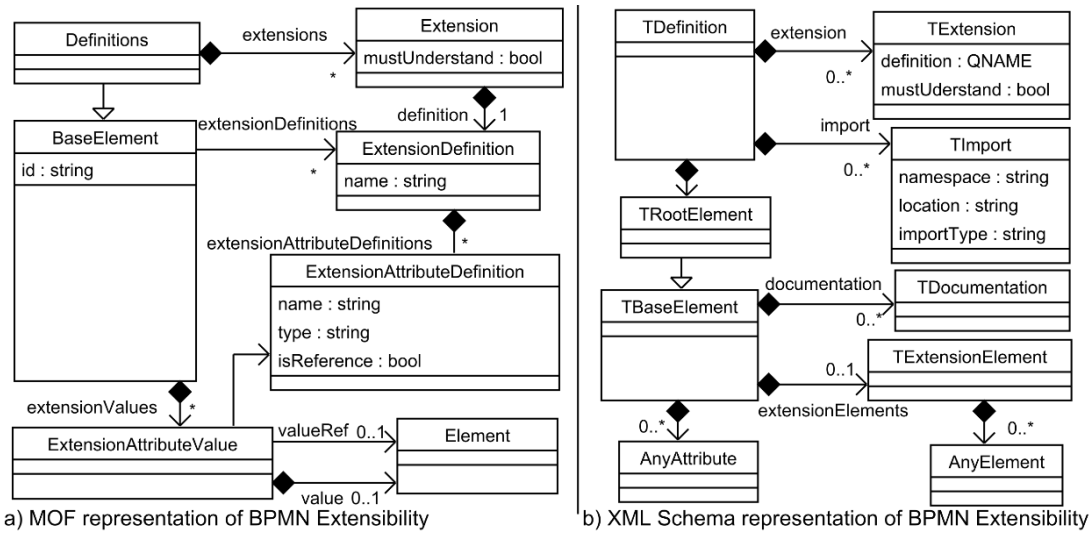


FIGURE 4.1 – *Représentations des schémas MOF et XML du mécanisme d'extension BPMN [Stroppi et al., 2011]*

Dans [Braun et Esswein, 2014], les auteurs ont abordé le développement des extensions BPMN avec l'analyse descriptive et la classification de 30 extensions BPMN. Pour notre état de l'art, nous avons utilisé le critère de conformité par rapport au standard BPMN 2.0 défini dans [Braun et Esswein, 2014]. Le critère décrit la manière dont l'extension est définie et expliquée. « Extension valide » représente la définition en tant que modèle d'extension BPMN. « Extension non valide » dans le cas d'une définition dédiée (par exemple, modèle UML) - Tableau 4.1

Critère	Description	Valeurs
Définition	Type de définition d'extension	Extension valide ; Extension non valide ; Nouvelle notation graphique ; aucune
Syntaxe abstraite	Définition du méta-modèle	Par exemple UML
Syntaxe concrète	Définition de nouvelles notations	Explicite ; implicite ; aucune
Modèle de processus / MDA	Une approche méthodologique est-elle appliquée (si oui, laquelle) ?	Par exemple Stroppi et al

TABLE 4.1 – *Conformité du standard [Braun et Esswein, 2014]*

Nous dressons dans ce qui suit, quelques travaux pertinents pour notre problématique d'extension du BPMN :

[Chaâbane et al., 2010] ont introduit une nouvelle extension du langage BPMN afin de d'automatiser la composition des services dans l'architecture SOA. L'extension BPMN4SOA permet de passer du langage BPMN vers le BPEL d'une façon automatique et minimise les modifications manuelles. Les auteurs ils ont proposé une extension du méta modèle illustré dans la figure 4.2.

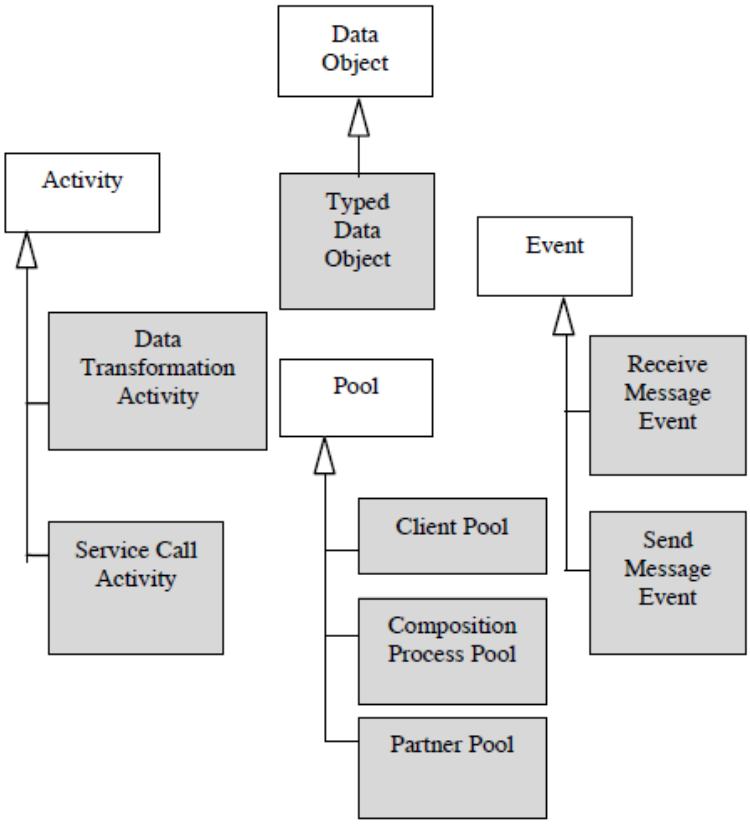


FIGURE 4.2 – *Méta modèle du BPMN4SOA [Chaâbane et al., 2010]*

Pour l'implémentation, les auteurs ont utilisé la plateforme open Architecture Ware

qui est maintenant intégré dans Eclipse Galileo sous le nom Modeling Workflow Engine et le langage Xpand (un langage dédie à la génération à partir du modèle EMF) vers le Java. Ils ont développé deux plugins pour Eclipse et pour les annotations ils ont utilisé STP BPMN editor.

[Saeedi et al., 2010] ont proposé une extension du langage BPMN pour évaluer le temps, le coût et la fiabilité. Les auteurs ils ont développé une extension du méta-modèle en intégrant le concept de la qualité de service figures (4.3, 4.4). C'est parmi les premières extensions à exploiter le mécanisme d'extension en se basant sur la version beta du BPMN 2.0.

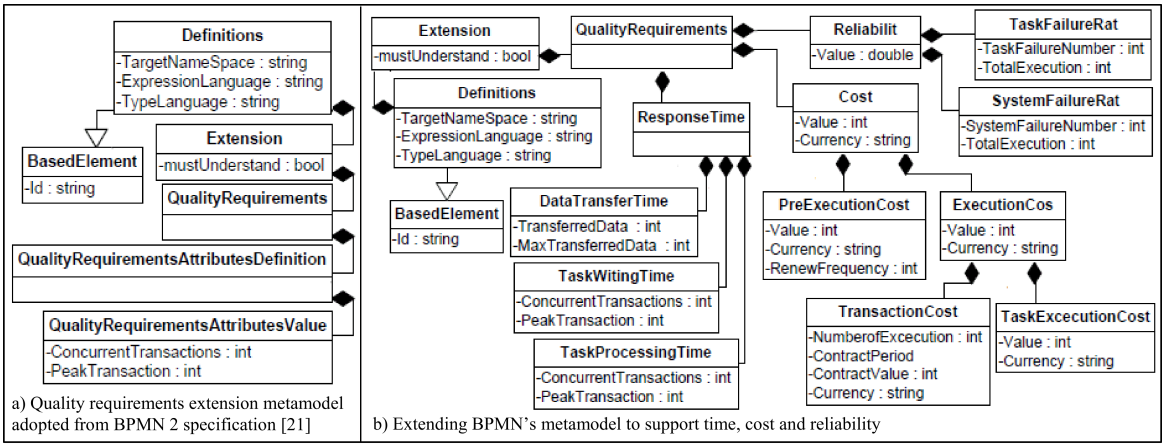


FIGURE 4.3 – *Extension du méta model BPMN [Saeedi et al., 2010]*

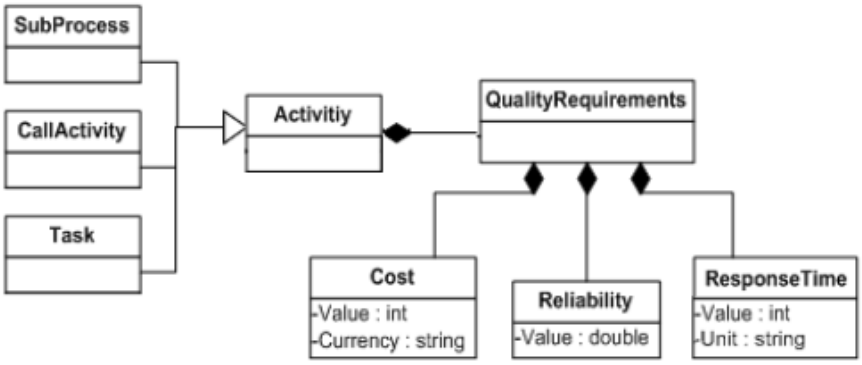


FIGURE 4.4 – *La liaison de l'élément Activity avec l'élément QualityRequirements [Saeedi et al., 2010]*

[Bocciarelli et D'Ambrogio, 2011] ont introduit l'extension PyBPMN (Performability-enabled BPMN) pour le langage BPMN. L'extension permet la spécification des exigences non fonctionnelles telles que la performance et la fiabilité. L'approche proposée se base sur l'architecture MDA (Figure 4.5)

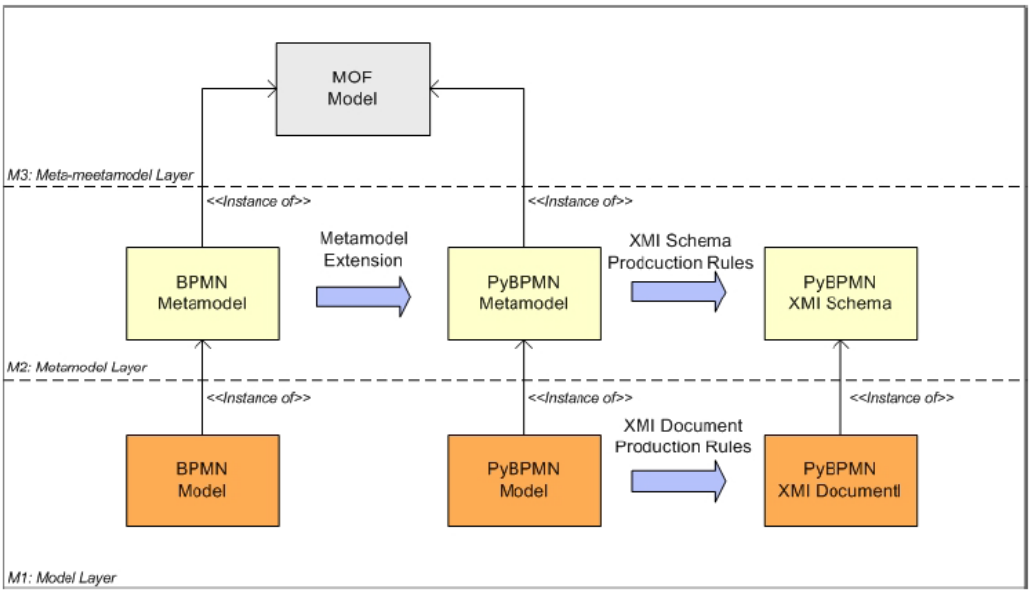


FIGURE 4.5 – *Processus extension PyBPMN [Bocciarelli et D'Ambrogio, 2011]*

Les auteurs de [Bocciarelli et D'Ambrogio, 2011] ont modifié le méta modèle du BPMN en ajoutant des méta-classes afin d'intégrer les notions de performances, de chargement et de fiabilité (Figure 4.6)

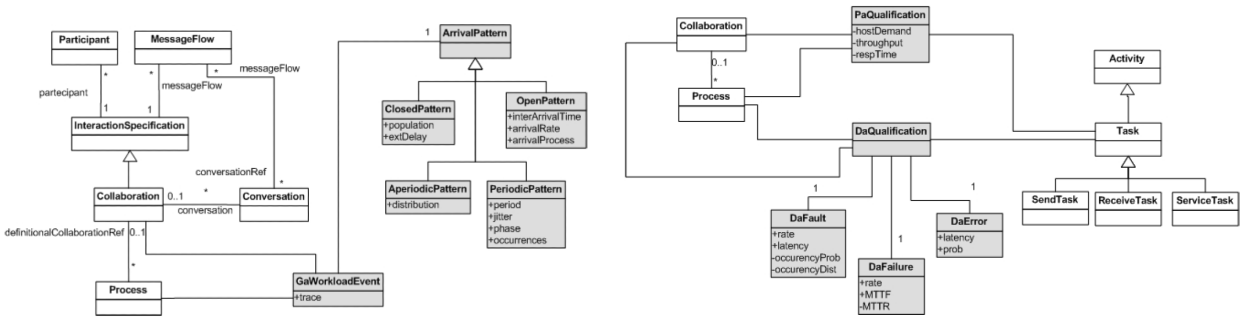


FIGURE 4.6 – *Méta modèle d'extension PyBPMN [Bocciarelli et D'Ambrogio, 2011]*

Les auteurs ont proposé une méthode complète afin d'exécuter les processus métiers en transformant le modèle vers le BPEL et une autre transformation vers UML (Figure 4.7).

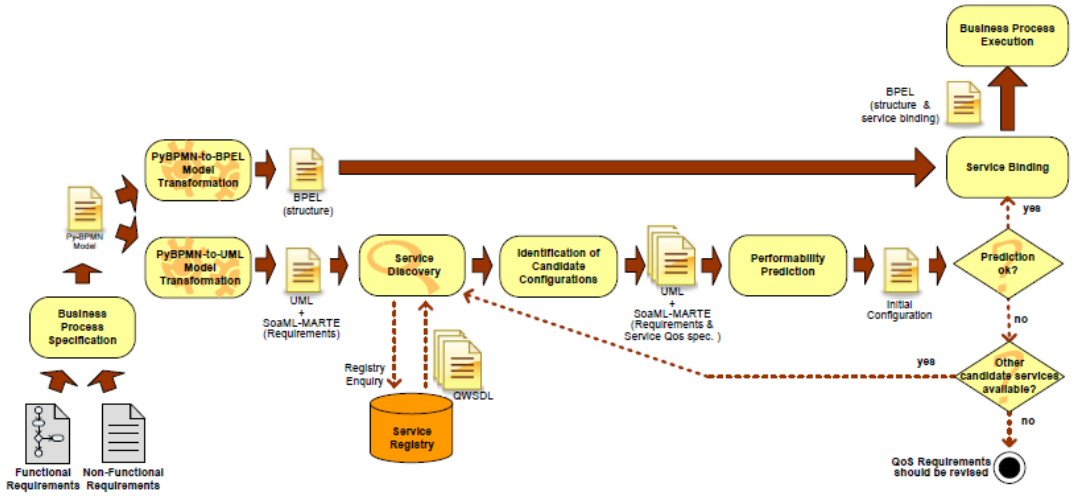


FIGURE 4.7 – *Méthode pour prédilection des performances [Bocciarelli et D'Ambrogio, 2011]*

[Cheikhrouhou et al., 2013] ont présenté une nouvelle approche afin de prendre en compte les contraintes de temps dans la modélisation des processus métiers BPMN (Figure 4.8). Ils ont développé une extension BPMN en se basant sur la plateforme Activiti (Figure 4.9). Il faut noter que nous n'avons pas trouvé le méta modèle qui décrit l'extension.

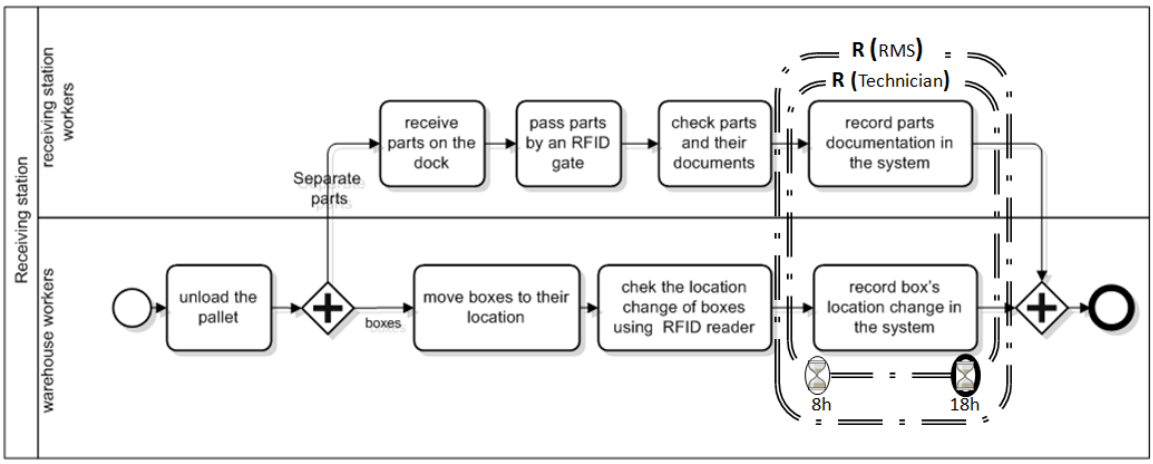


FIGURE 4.8 – *Exemple de contraintes de temps intégrées dans le BPMN [Cheikhrouhou et al., 2013]*

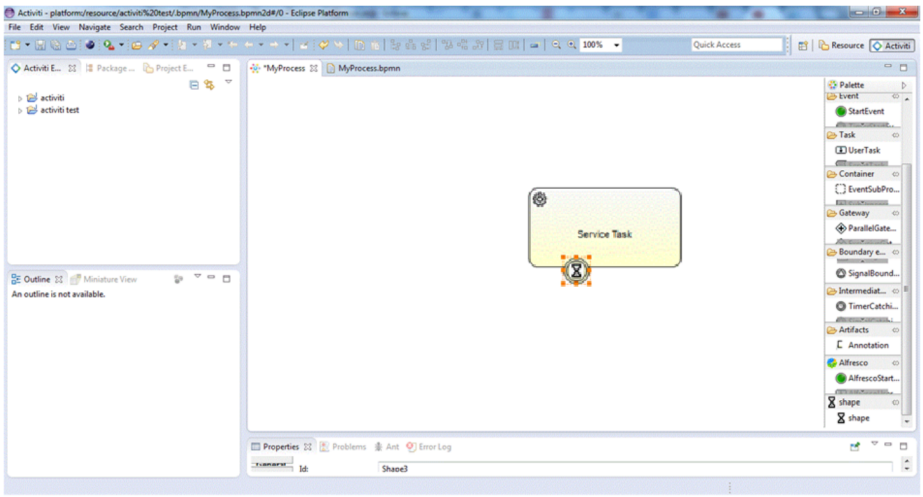


FIGURE 4.9 – *Modélisation de la contrainte de temps dans l'outil Activiti eclipse designer [Cheikhrouhou et al., 2013]*

Dans l'approche proposée par [Cheikhrouhou et al., 2013], nous n'avons pas trouvé la définition formelle de l'extension avec un méta-modèle.

[Pillat et al., 2015] ont proposé une extension au BPMN afin d'intégrer la notion d'adaptabilité (tailoring) du SPEM [OMG, 2008]. Le SPEM Software Process Engineering Metamodel - que l'on peut traduire par méta-modèle d'ingénierie des procédés logiciels - est un métamodèle (ou modèle décrivant les concepts) visant à décrire le processus de production de logiciels pour répondre à ces problématiques.

Leur approche consiste à enrichir le méta model du BPMN avec une partie de celui du SPEM (partie structure de processus).

Dans leurs travaux, [Braun et Esswein, 2015] introduisent une nouvelle approche pour supporter le concept de perspective (des vues sur le processus métier) (Figure 4.10) dans la modélisation des processus métiers en proposant aussi une extension du méta model du BPMN (Figure 4.11).

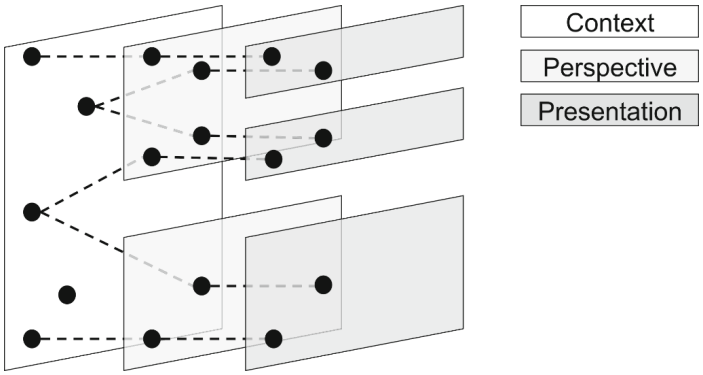


FIGURE 4.10 – *Les perspectives dans l'aspect contextuel [Braun et Esswein, 2015]*

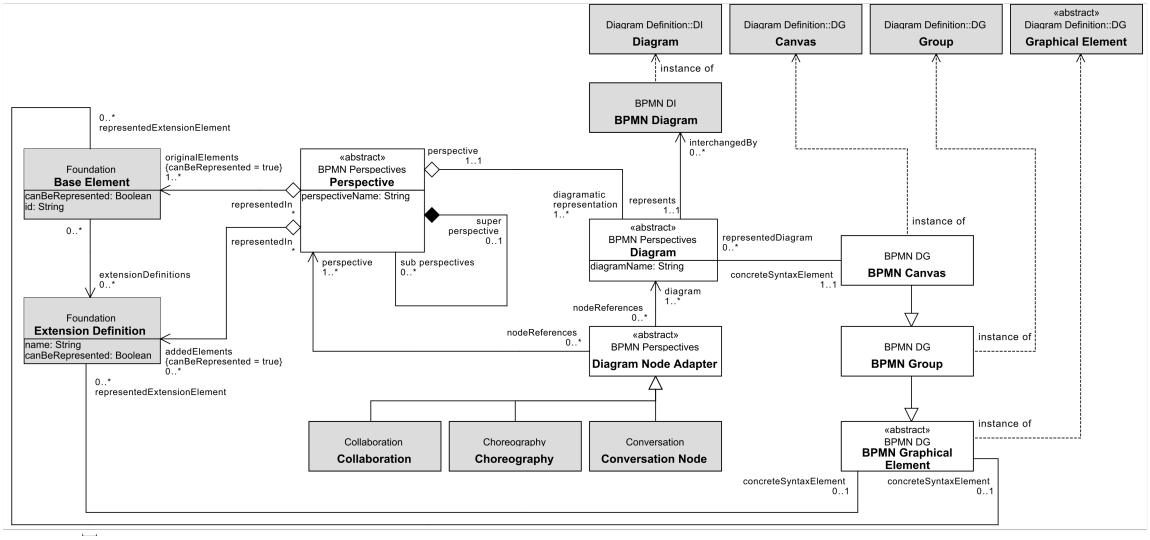


FIGURE 4.11 – *L'extension du métal model [Braun et Esswein, 2015]*

Les auteurs ont développé une extension qui se base sur les travaux de [Stroppi et al., 2011]. La Figure 4.12, représente une démonstration d'un un cas réel de la modélisation des ressources dans le secteur médical.

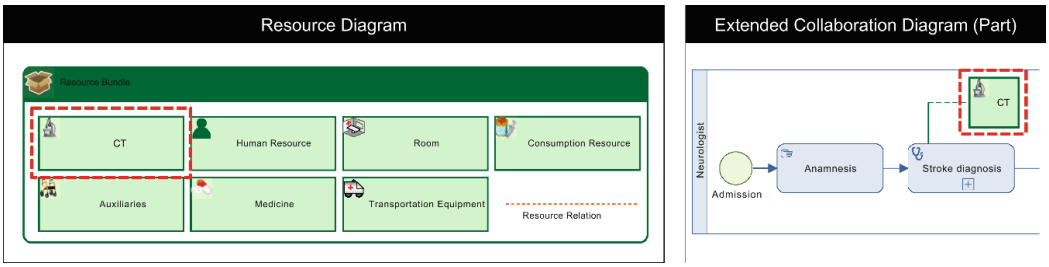


FIGURE 4.12 – *Démonstration de l'extension proposée [Braun et Esswein, 2015]*

Les auteurs de [Braun et al., 2015] ont proposé une l'approche BPMN4CP pour modéliser le parcours clinique dans le secteur de la santé. Ils se basent aussi sur la méthode de [Stroppi et al., 2011] mais avec une amélioration de la méthode Figure 4.13. Les auteurs ont proposé une extension du méta model Figure 4.14 en utilisant le mécanisme d'extension du BPMN 2.0. La figure 4.15, représente un cas d'utilisation d'un parcours clinique avec extension.

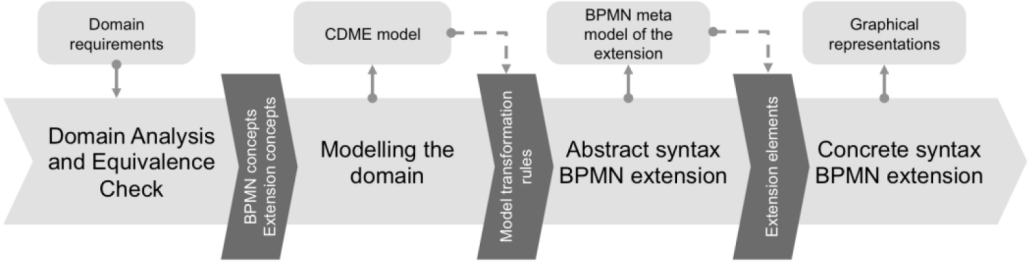


FIGURE 4.13 – *Procédure d'intégration des modèles pour le développement des extensions du BPMN [Braun et al., 2015]*

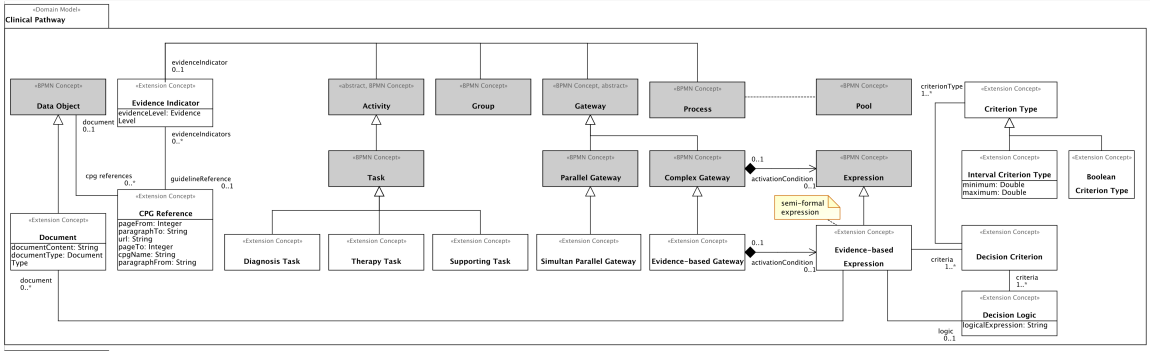


FIGURE 4.14 – *Le méta model d'extension BPMN4CP [Braun et al., 2015]*

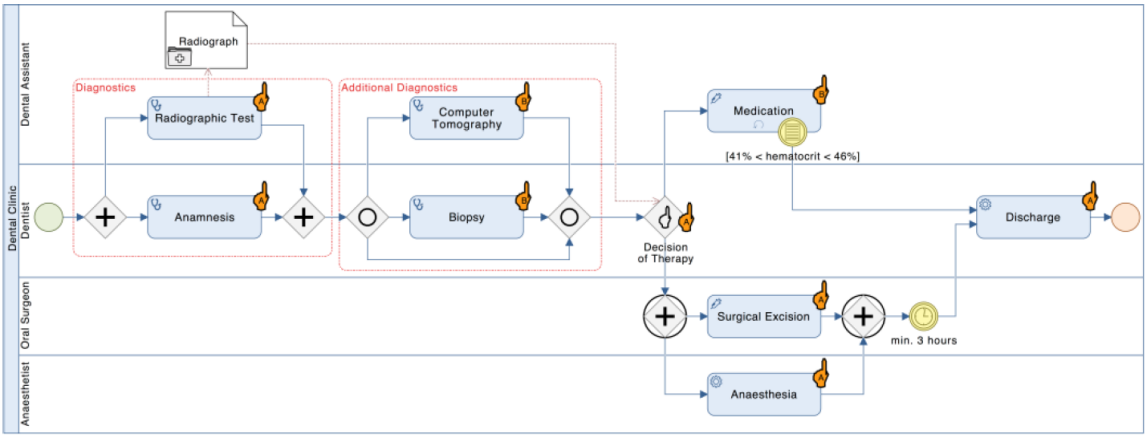


FIGURE 4.15 – *Démonstration d'un cas d'utilisation de l'extension BPMN4CP [Braun et al., 2015]*

[Polančič, 2020], a introduit une nouvelle extension BPMN-L pour modéliser le paysage des processus métiers pour avoir un aperçu de tous les processus métier et de leurs interactions (Figure 4.16). Il faut noter que l'auteur ne propose pas un outil pour faciliter l'utilisation de l'extension.

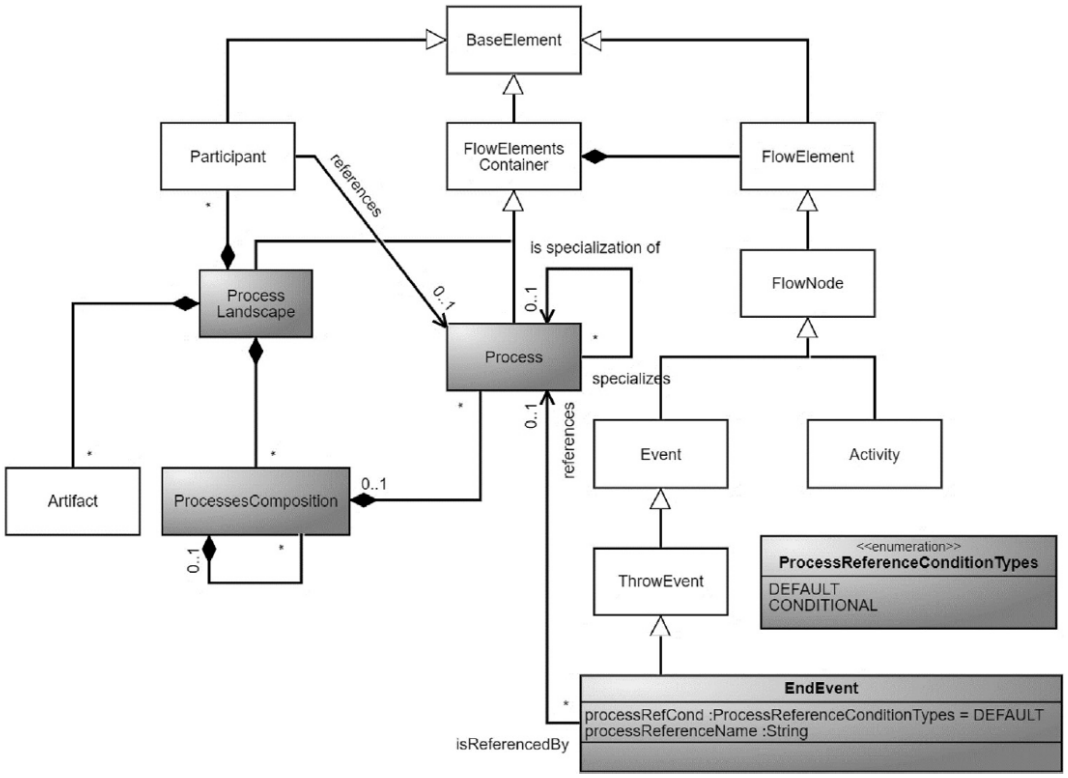


FIGURE 4.16 – *Le méta model d'extension BPMN-L [Polančič, 2020]*

Auteurs	**Année**	**Définition**	**Syntaxe abstraite**	**Syntaxe concrète**	**Modèle de processus / MDA**
Chaâbane et al	2010	Non valide	UML	Implicite	Non
Saeedi et al	2010	Valide	UML	Implicite	Non
Bocciarelli et al	2011	Non valide	UML	Aucune	Oui
Cheikhrouhou et al	2013	Non valide	Aucune	Implicite	Non
Pillat et al	2015	Valide	UML	Implicite	Non
Braun et al	2015	Valide	UML	Explicite	Oui
Gregor	2020	Valide	UML	Implicite	Oui

TABLE 4.2 – *Tableau comparatif des extensions pour le BPMN*

Le tableau 4.2 résume les principaux aspects des extensions BPMN sélectionnées dans cette partie. Nous remarquons, que plusieurs extensions BPMN n'exploitent pas le mécanisme d'extension du BPMN et ne sont pas compatible avec l'approche MDA. La plupart des approches ne proposent pas aussi une syntaxe concrète explicite.

Il faut noter que les approches étudiées dans cette section c'est un échantillon parmi les travaux important dans le domaine extension du BPMN. Dans la littérature la plupart des extensions ne sont pas valides [Braun et Esswein, 2014].

Le développement méthodologique des extensions BPMN est primordial pour le respect de la conformité du standard BPMN. Pour garantir cette conformité, il faut une utilisation stricte du mécanisme d'extension BPMN.

4.3 L'intégration des exigences de sécurité dans le processus métier

Outre les caractéristiques fonctionnelles d'un processus métier, il existe également un certain nombre d'aspects non fonctionnels qui doivent être pris en considération comme la sécurité. Les exigences de sécurité et les réglementations de conformité sont une préoccupation majeure pour la conception et l'exécution de systèmes pilotés par les processus métier en raison de l'impact potentiel sur les organisations en termes de réputation, de finances et de conformité légale [Argyropoulos et al., 2019].

Les exigences de sécurité ont été reconnues comme une préoccupation importante. L'association entre les processus métier et la sécurité est inévitable. Des études empiriques montrent que ceux qui modélisent le processus métier, c'est-à-dire l'expert du domaine métier, sont capables de spécifier les exigences de sécurité [RODRIGUEZ et al., 2007]. Étant donné que la prise en compte de la sécurité dès l'étapes de conception est considérée comme très bénéfique [Leitner et al., 2013]. La modélisation des processus métier est la couche la plus appropriée pour décrire les exigences de sécurité [Menzel et al., 2009]. Cependant, dans la pratique, l'expert du domaine métier se concentre principalement sur la fonctionnalité car l'expert du domaine métier n'est pas un expert en sécurité [RODRIGUEZ et al., 2007]. Les méthodes de développement traitent souvent la sécurité, séparément à un stade ultérieur. Dans cette partie, nous allons voir les travaux qui ont traité la problématique de l'annotation des diagrammes BPMN avec les exigences de sécurité.

[RODRIGUEZ et al., 2007] ont présenté un métamodèle BPMN avec l'extension des éléments de base pour permettre l'intégration des exigences de sécurité dans les diagrammes de processus métiers, afin d'enrichir le langage avec les concepts de sécurités. Ils ont utilisé des concepts tels que la non-répudiation, la détection des attaques / préjudices, l'intégrité, la confidentialité, le contrôle d'accès, le rôle de sécurité et les autorisations de sécurité (Figure 4.17). Nous notons le manque de concept tel que la disponibilité, c'est une exigence nécessaire qui aurait dû être incluse.

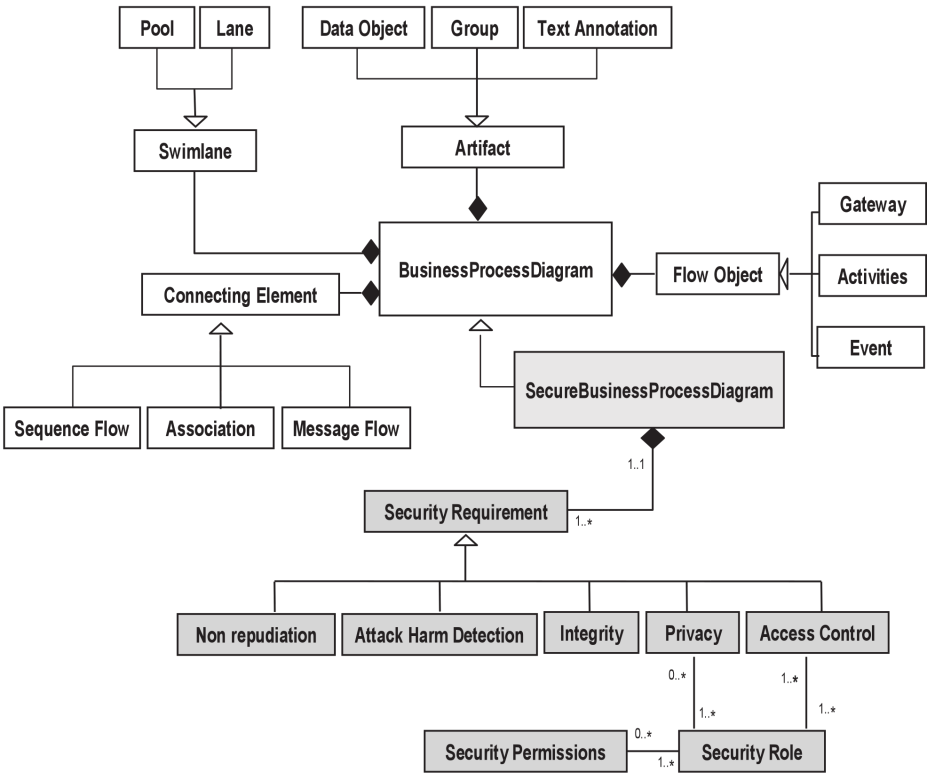


FIGURE 4.17 – *Le méta-modèle BPMN avec les exigences de sécurité [RODRIGUEZ et al., 2007]*

[Souza et al., 2009], ont proposé une approche afin d'identifier les exigences de sécurité pour la composition de services. Ils ont défini une notation pour exprimer les différents niveaux d'abstraction. Leur approche Sec-MoSC permet d'intégrer les exigences de sécurité dans la composition de services, pour s'assurer le respect des exigences durant la phase d'exécution. Ils ont proposé une extension BPMN et le moteur d'exécution BPEL.

Les auteurs ont défini dix exigences non-fonctionnelles pour présenter les besoins de sécurité :

— NFR 01 : Confidentialité
— NFR 02 : Conservation des données
— NFR 03 : Contrôle d'accès
— NFR 04 : Authentification
— NFR 05 : Accès restreint
— NFR 06 : L'intégrité des données
— NFR 07 : Le partage des données
— NFR 08 : Certification de service
— NFR 09 : Audit
— NFR 10 : Surveillance

Les différentes étapes de leur approche sont illustrées dans la Figure 4.18.

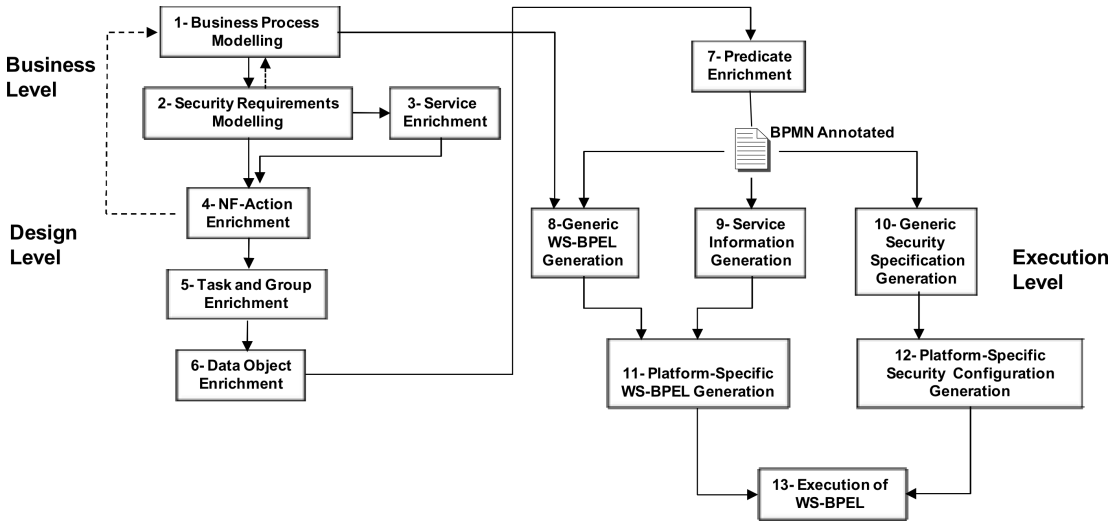


FIGURE 4.18 – *Méthodologie Sec-MoSC [Souza et al., 2009]*

1. Modélisation du processus métier : la première étape consiste à modéliser le processus métier en utilisant le BPMN.
2. Modélisation des exigences de sécurité : dans cette étape les auteurs préconisent de lister les exigences de sécurité afin de les liées aux éléments du model BPMN. Ils ont développé une extension du model BPMN pour inclure NF-Attribute, NF-Statement et NF-Action.
3. Enrichissement des services : durant cette étape des annotations supplémentaires sont ajouté pour faciliter après la génération du code BPEL.
4. La génération d'un BPEL générique : la génération est faite d'un fichier BPEL et d'un fichier de sécurité générique.
5. BPEL spécifique : dans cette étape il y a la génération d'un BPEL spécifique pour l'exécution dans un environnement particulier, par exemple Apache ODE.
6. Exécution du WS-BPEL : utilisation d'un moteur d'exécution auxiliaire pour satisfaire les exigences de sécurité.

La Figure 4.19, représente l'architecture proposée par les auteurs.

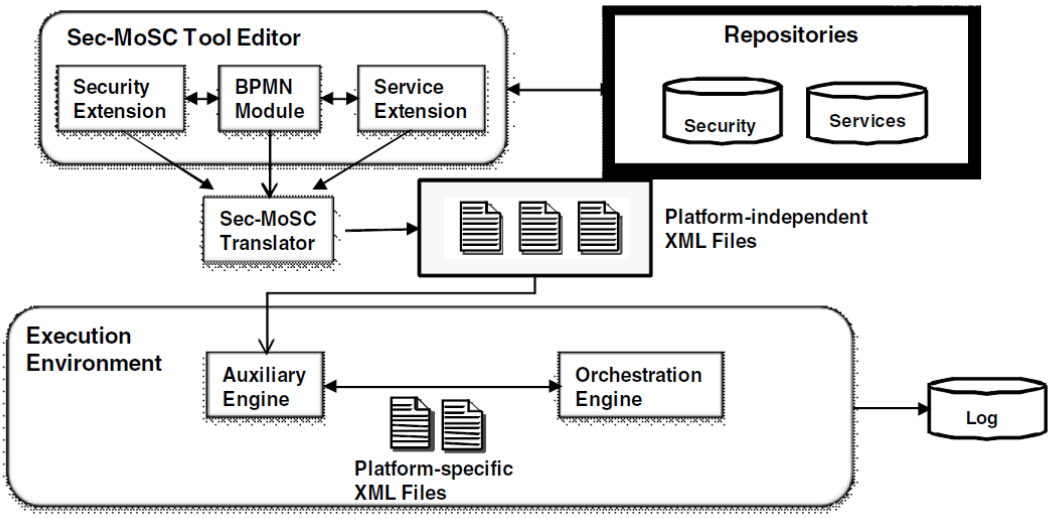


FIGURE 4.19 – *L'architecture de Sec-MoSC [Souza et al., 2009]*

Les auteurs ont développé un plugin sous éclipse qui permet de modéliser un BPMN avec des annotations de sécurité.

Les principales contributions de l'approche proposée comprennent la définition d'un ensemble d'abstractions non-fonctionnel pour exprimer les exigences de sécurité à différents niveaux d'abstraction, une méthodologie pour intégrer les exigences de sécurité et les informations de service en BPMN, mappage des informations et de la sécurité du service en éléments exécutables, et fournir un support d'exécution pour les exigences de sécurités.

[Wolter et al., 2009] proposent une approche pour décrire les exigences de sécurité dans la couche du processus métier et la transformation en configuration de sécurité concrète pour les systèmes basés sur les services. Ils ont introduit des éléments de sécurité pour la modélisation des processus métiers qui permettent d'évaluer la fiabilité des participants basées sur une estimation des actifs de l'entreprise et d'exprimer les intentions de sécurité telles que la confidentialité ou l'intégrité à un niveau abstrait.

Dans leur approche, ils ont pris en compte l'utilisation des informations d'identité et les droits associés (authentification, l'autorisation, la confiance), les informations stockées ou échangées (confidentialité, intégrité). Le fonctionnement du service (l'intégrité et la disponibilité du système).

Ils ont proposé différents niveaux de risque (d'extrême à négligeable) et des niveaux aussi pour la confiance. Concernant l'intention comme l'intégrité et la confidentialité, sont définies au niveau du pool parce que souvent leur vérification implique plusieurs éléments et des échanges complexes.

[Menzel et al., 2009] ont défini un modèle de politique de sécurité (Figure 4.20) indépendant afin de générer des configurations de sécurité spécifiques pour les plate-formes en différentes langues.

L'approche proposée repose uniquement sur des transformations de modèles ce qui permet une description abstraite des exigences et une indépendance vis-à-vis les environnements techniques.

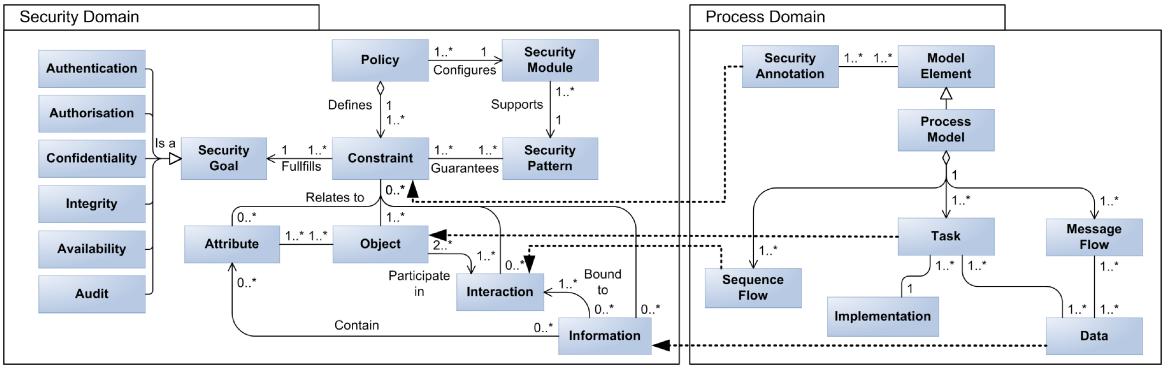


FIGURE 4.20 – *Modèle de la politique de sécurité [Menzel et al., 2009]*

Pour la génération des politiques de sécurités, ils ont présenté aussi un autre modèle pour faire le mappage avec l'outil Apache Axis 2 Web Service Stack – Figure 4.21.

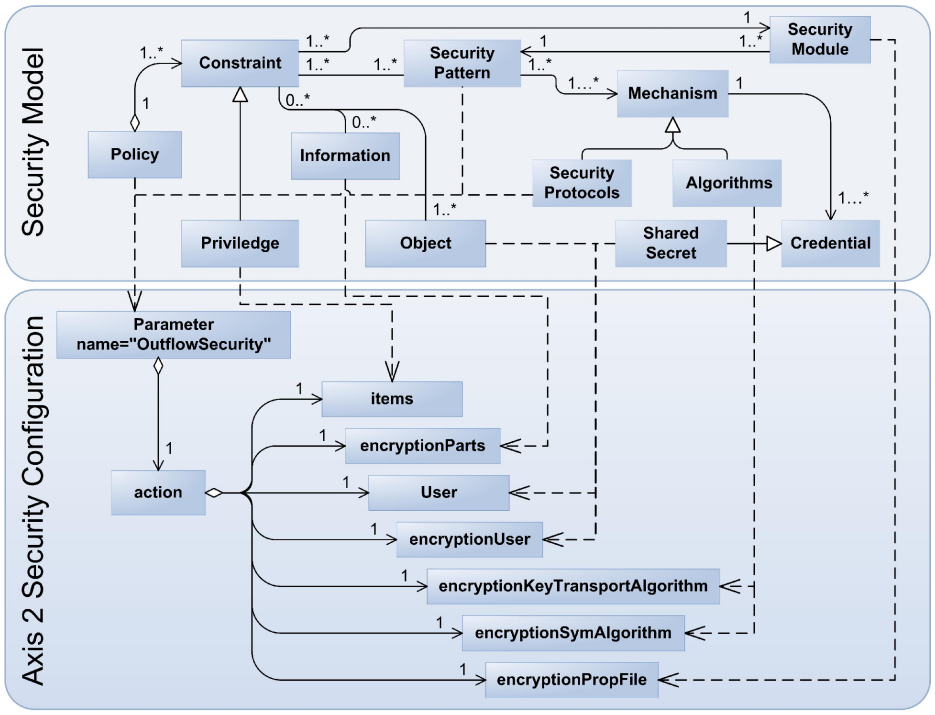


FIGURE 4.21 – *Liaison avec Apache Rampart Security Configuration [Menzel et al., 2009]*

[Mülle et al., 2011] ont proposé un langage riche pour représenter les contraintes de sécurité des processus métier de la modélisation à la phase d'exécution (Figure 4.22). Ils ont introduit plusieurs concepts comme confidentialité, intégrité, autorisation, authentification et audit. L'approche se base sur des annotations textuelles.

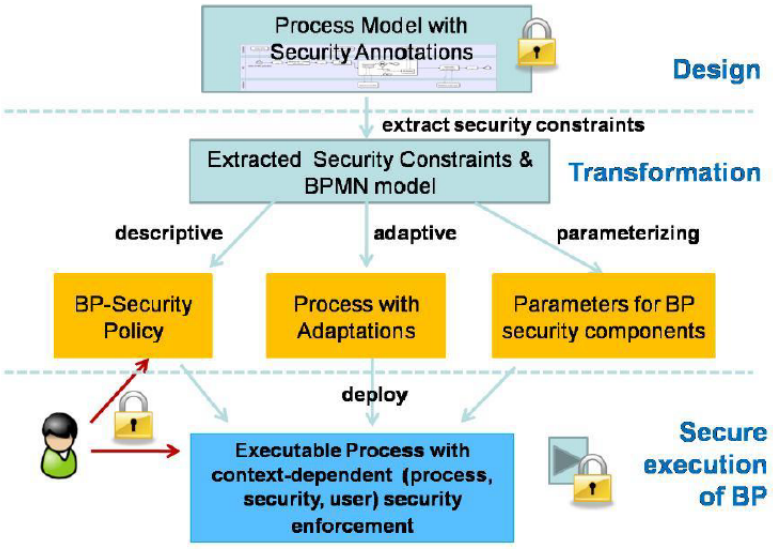


FIGURE 4.22 – *Les trois phases de l'approche de [Mülle et al., 2011]*

[Basin et al., 2011] ont introduit une nouvelle approche pour aligner la sécurité et les objectifs métiers pour les systèmes d'information. À l'aide de CSP, ils ont modélisé un système à deux niveaux d'abstraction : le niveau de flux de contrôle pour la modélisation des objectifs métiers d'un système et le niveau d'exécution de la tâche, la modélisation de qui exécute quoi. En outre, ils ont présenté une nouvelle approche pour déterminer les contraintes de SoD et de BoD sur des sous-ensembles d'instances de tâches utilisant des points de sortie – Figure 4.23.

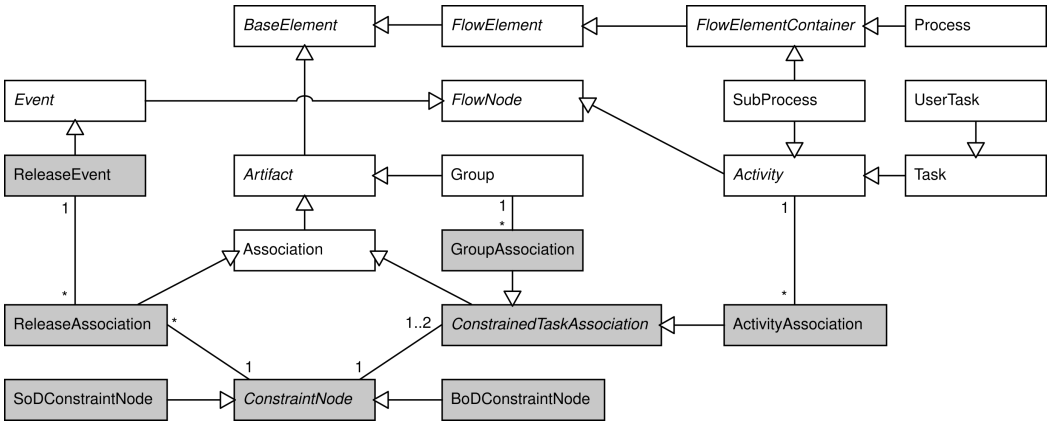


FIGURE 4.23 – *L'extension en gris proposée par [Basin et al., 2011]*

[Brucker, 2013] ont présenté SecureBPMN une approche basée sur des modèles pour la conception et l'exploitation de systèmes pilotés par des processus métier, intégrant les exigences de sécurité et de conformité durant la phase de modélisation et aussi à la phase d'exécution. Les auteurs se sont basés principalement sur le contrôle d'accès, mais ils ont introduit d'autres concepts tel que : séparation des tâches, obligation de devoir et besoin de savoir – Figure 4.24.

[Saleem et al., 2012] ont présenté une DSL, pour modéliser les exigences de sécurité

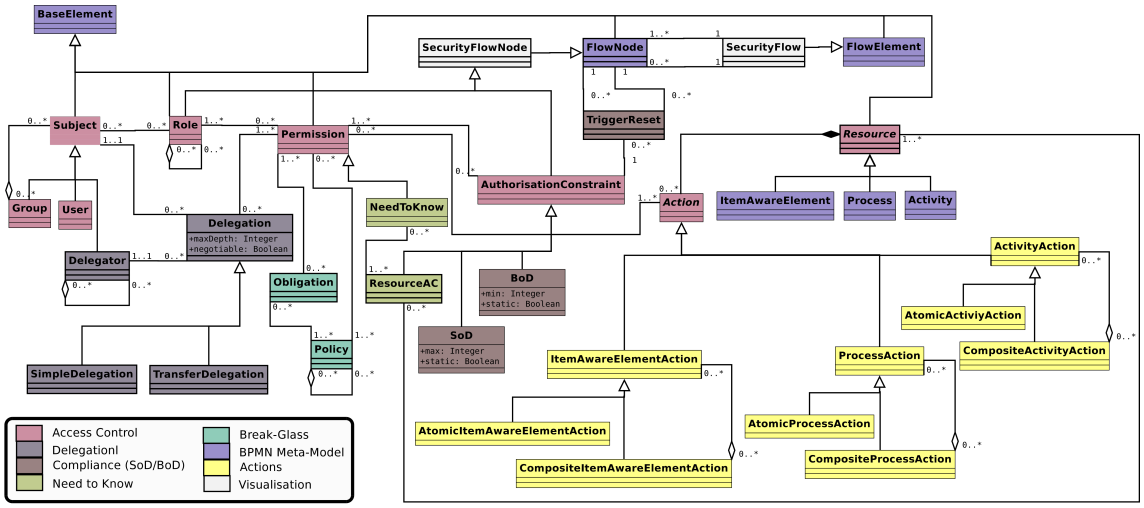


FIGURE 4.24 – *Le métamodèle de SecureBPMN [Brucker, 2013]*

directement dans le processus métier. Ils soulignent la nécessité de spécifier les exigences de sécurité au moment de la conception. Dans leur approche, seuls les concepts de base (confidentialité, intégrité et disponibilité) sont utilisés – Figure 4.25.

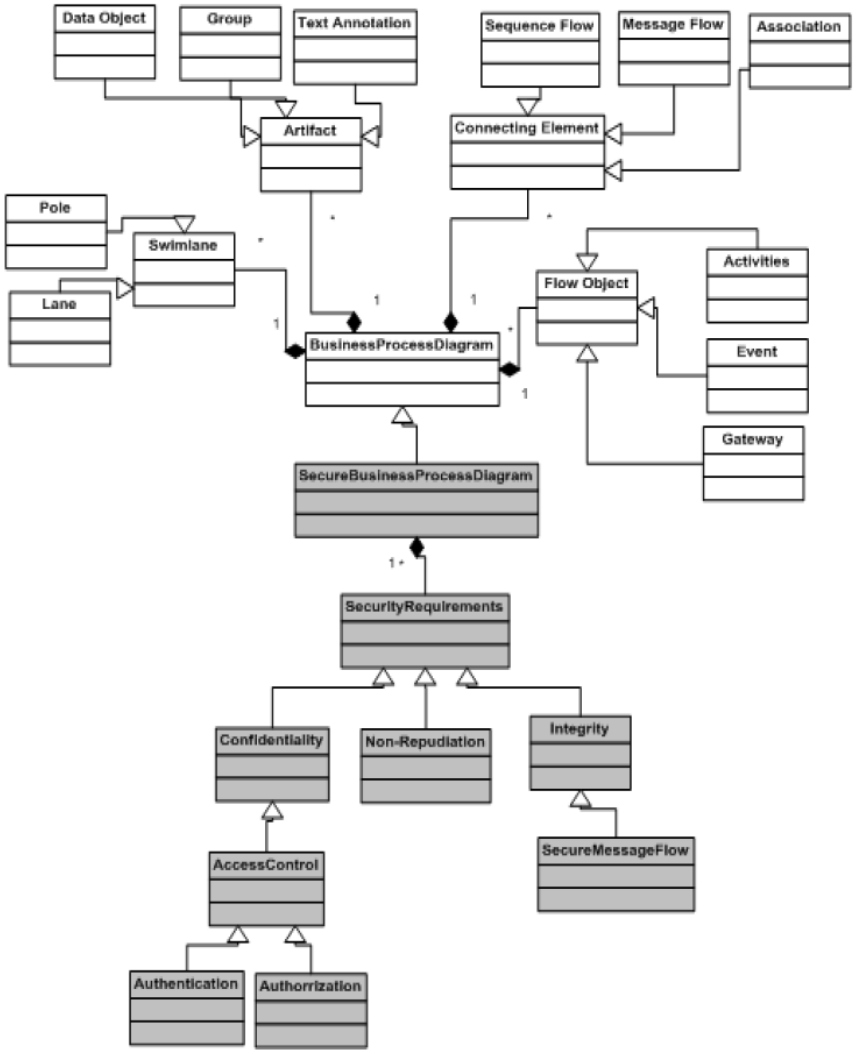


FIGURE 4.25 – *Le métamodèle de l'extension de [Saleem et al., 2012]*

[Ahmed et Matulevicius, 2013] proposent une taxonomie avec trois dimensions du processus métier et la sécurité (Figure 4.26).

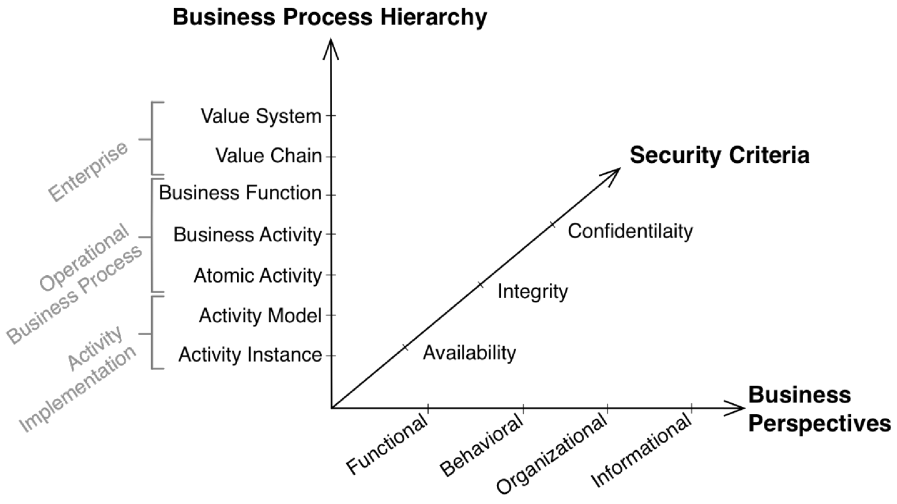


FIGURE 4.26 – *Taxonomie en trois dimensions [Ahmed et Matulevicius, 2013]*

— Les niveaux hiérarchiques représentent les niveaux dans le processus métiers
— La deuxième dimension représente les perspectives de modélisation (fonctionnelle, du comportement, organisationnelle et informationnelle)
— La dernière dimension concerne les objectives de sécurité (la confidentialité, l'intégrité et la disponibilité)

Les auteurs ont par la suite appliqué la taxonomie au cas du BPMN Figure 4.27.

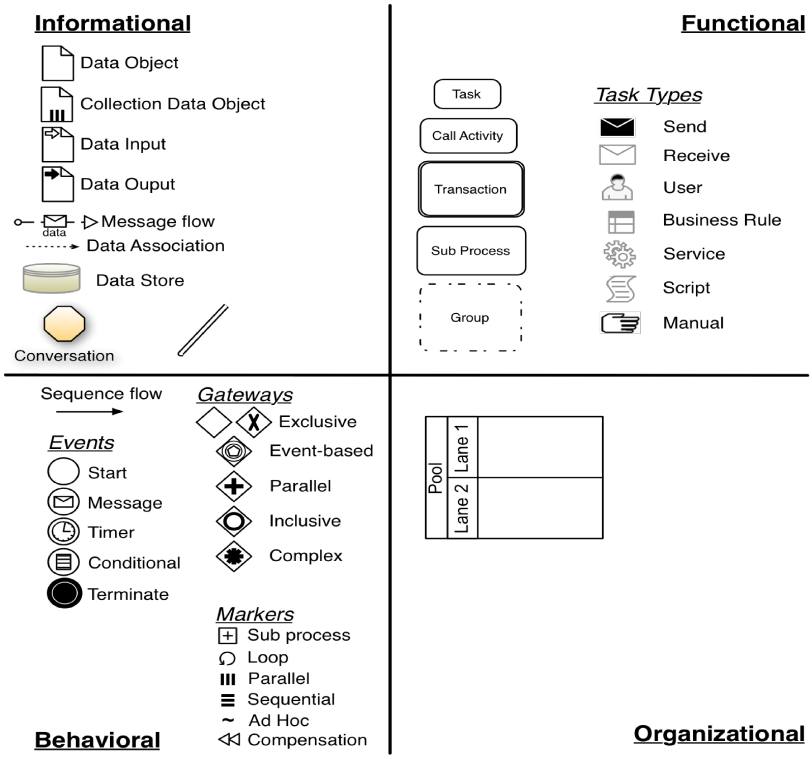


FIGURE 4.27 – *Classement des éléments du BPMN [Ahmed et Matulevicius, 2013]*

[Leitner et al., 2013] proposent une étude bien intéressante des extensions actuelles du BPMN qui ajoutent les concepts de sécurités. Les auteurs ont évalué plusieurs approches (Figure 4.28) selon plusieurs critères avec un questionnaire. Ils ont regroupé les différents symboles des approches d'extensions dans une table.

#	Symbol(s)	Title (Meaning)	Ref.	Position					
				Pool	Lane	Group	Activity	Message Flow	Data Object
A		Access Control	[3]						
B		Privacy	[3]						
C		Non-repudiation	[3]						
D		Attack Harm Detection	[3]						
E		Integrity	[3]						
F	none	Security Role	[3]						
G	none	Security Permission	[3]						
H		Manual Task	[6]						
I		Automatic Task	[6]						
J		Separation of Duty (2007)	[6]						
K		Binding of Duty (2007)	[6]						
L		Separation of Duty (2008)	[16]						
M		Binding of Duty (2008)	[16]						
N		Separation of Duty (2008)	[4]						
O		Binding of Duty (2008)	[4]						
P		Manual Task (2008)	[4]						
Q		Automatic Task (2008)	[4]						
R		Overall Asset Value Scale	[17]						
S		Organizational Trust	[17]						
T		Security Group	[17]						

FIGURE 4.28 – *Vue d'ensemble des extensions BPMN liés à la sécurité [Leitner et al., 2013]*

Parmi les approches citées dans cette table, on peut noter ci-dessus celle de [Souza et al., 2009] et [Menzel et al., 2009]. [Compagna et al., 2013] Proposent un service (Security Validation as a Service) pour la validation de la conformité des processus métiers. Ils ont défini le concept de BPCP (Business Process Compliance Problem), c'est un fichier XML qui décrit le processus métier en BPMN et les besoins de sécurités en BPMN Sec Figure 4.29, une extension qu'ils ont développé afin de spécifier les besoins de sécurités. Cette extension se base sur RBAC pour définir les rôles de chacun.

Ils ont proposé une architecture client/ serveur complète - Figure 4.29, afin de faire la validation dans le Cloud et fournir les ressources (BPCP) avec une API Rest.

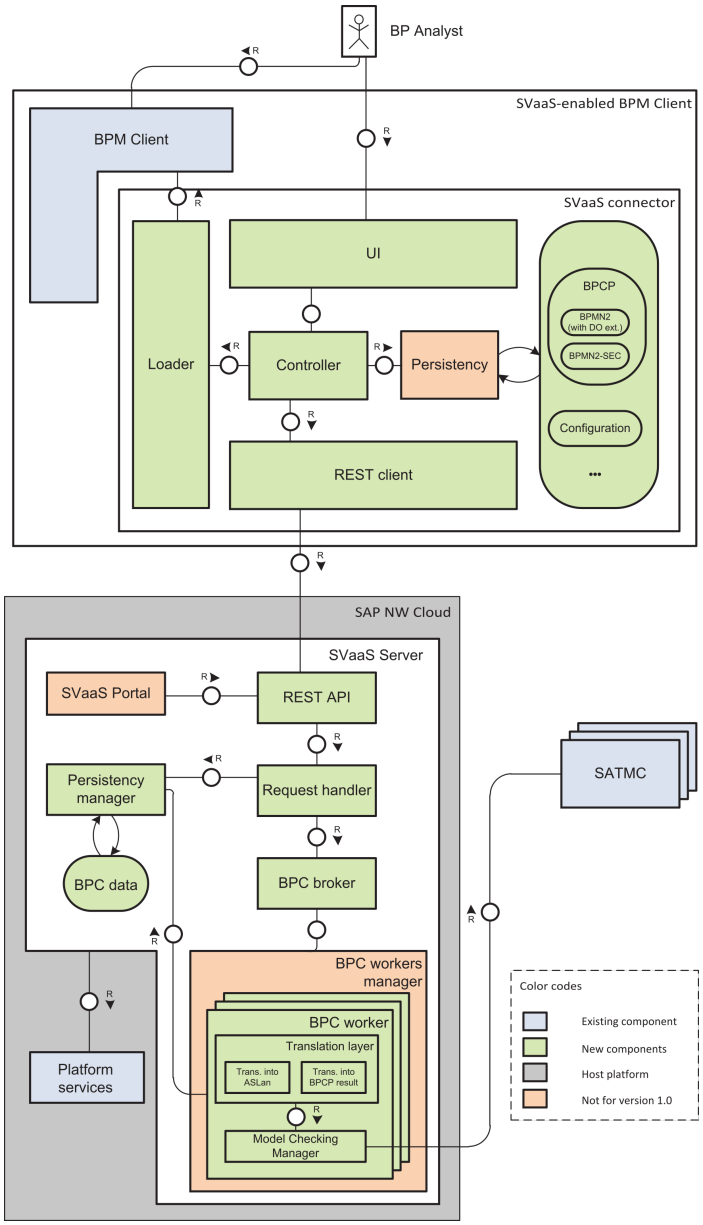


FIGURE 4.29 – *L'architecture détaillée de BPMN sec [Compagna et al., 2013]*

[Lins et al., 2013] ont fait une étude comparative entre les différentes approches qui supportent les annotations de sécurités dans le BPMN avec le passage vers BPEL. Ils ont défini plusieurs métriques quantitatives afin d'évaluer cinq outils (BPMN2BPEL, SSC4Cloud, Eclarus, Intalio, BPI). Un exemple de comparaison de la complexité du code BPEL généré. Figure 4.30

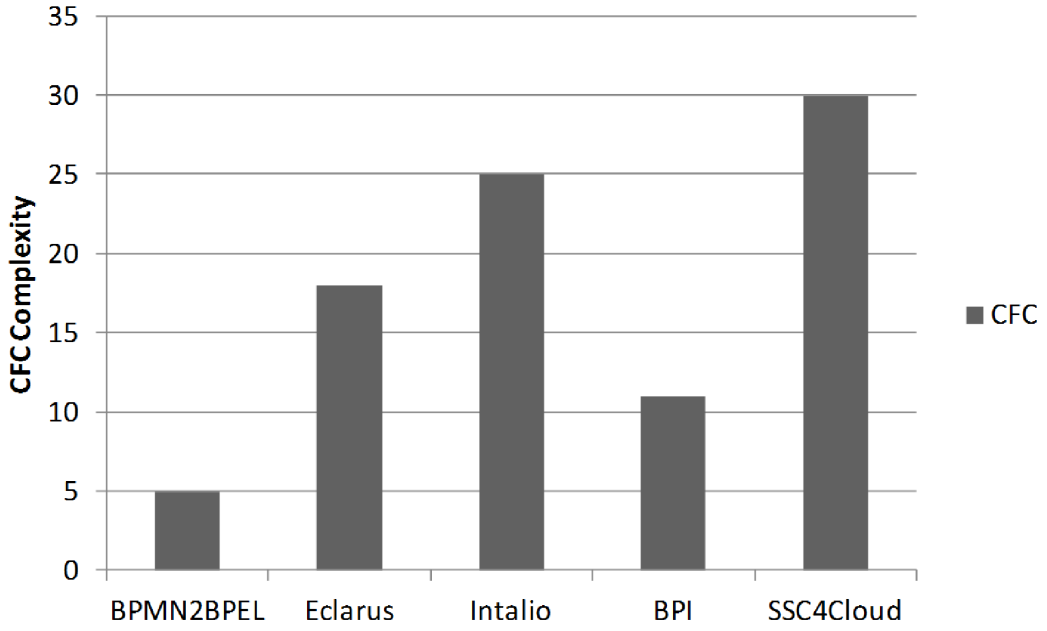


FIGURE 4.30 – *La complexité des flux de contrôle du code source WS-BPEL généré [Lins et al., 2013]*

[Altuhhov et al., 2013] proposent une approche structurée qui étend BPMN pour représenter les risques de sécurité basé sur ISSRM (model of the IS security risk management). Ils spécifient différentes couleurs pour représenter différentes ressources. En outre, les éléments de tâches sont utilisés pour modéliser les activités de sécurité, par exemple pour authentifier les utilisateurs. Cependant, leur approche manque de nombreux concepts de sécurité importants – Figure 4.31.

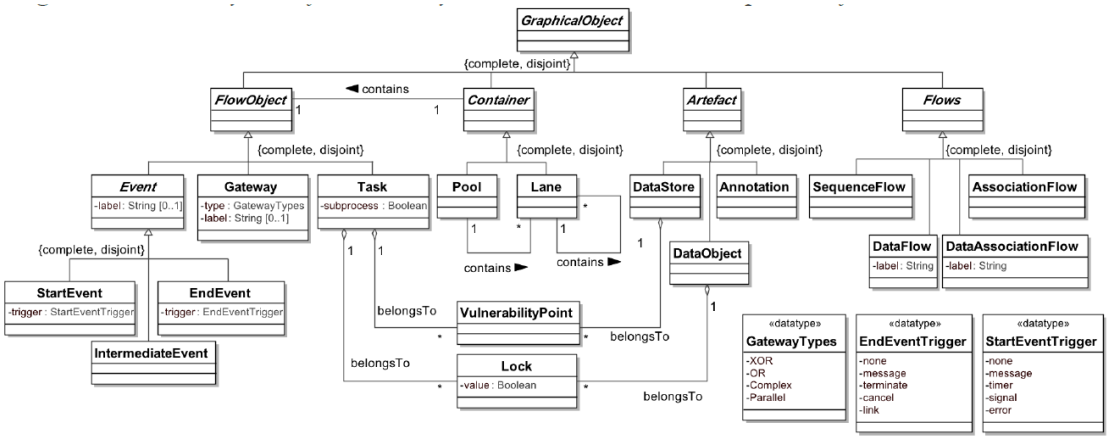


FIGURE 4.31 – *Métamodèle de l'extension de [Altuhhov et al., 2013]*

[Salnitri et al., 2014] ont introduit un framework permettant de spécifier des systèmes d'information dans SecBPMN, une extension de BPMN axée sur la sécurité. Plusieurs concepts sont utilisés dans leur framework : la responsabilité, l'auditabilité, l'authenticité, la disponibilité, la confidentialité, l'intégrité, la non-répudiation et la confidentialité. Ces concepts découlent du modèle de référence de l'assurance et de la sécurité de l'information (RMIAS). L'approche se base sur BPMN-Q pour exécuter les requêtes sur les processus métier – 4.32.

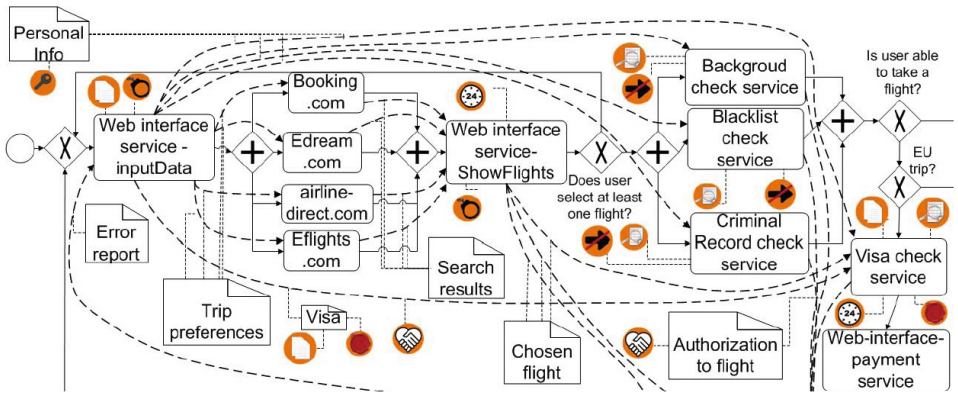


FIGURE 4.32 – *Exemple de modèle de processus métier SecBPMN [Salnitri et al., 2014]*

[Labda et al., 2014] ont proposé une nouvelle extension à la notation visuelle du BPMN en vue de supporter les préoccupations vie privée. L'extension se concentre sur la représentation des exigences de confidentialité des données personnelles. Leur extension traite principalement le problème de la protection de la vie privée. Une partie seulement des concepts de la cybersécurité sont inclus dans l'approche : séparation des tâches, contrôle d'accès, liaison des tâches, nécessité de connaître et consentement de l'utilisateur (Figure 4.33).

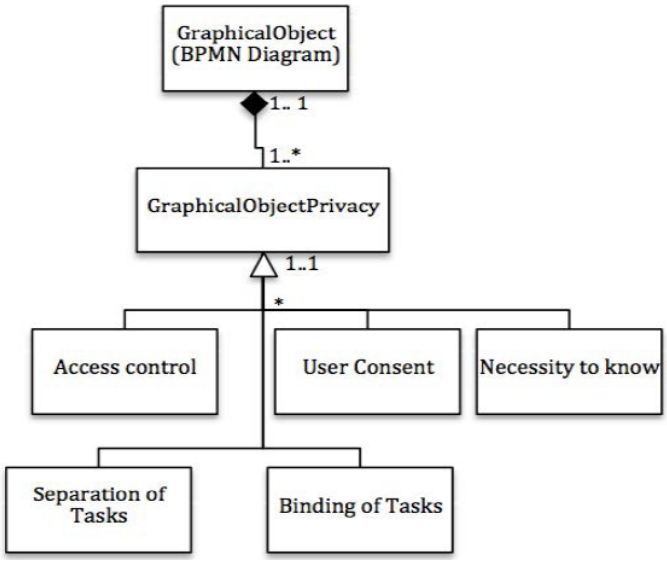


FIGURE 4.33 – *Le métamodèle de l'extension [Labda et al., 2014]*

[Sang et Zhou, 2015] ont proposé une extension dédiée pour la santé avec plusieurs concepts de sécurités avec les évènements ainsi que des niveaux de sécurité. Mais ils n'ont pas utilisé le mécanisme d'extension du BPMN - Figure 4.34.

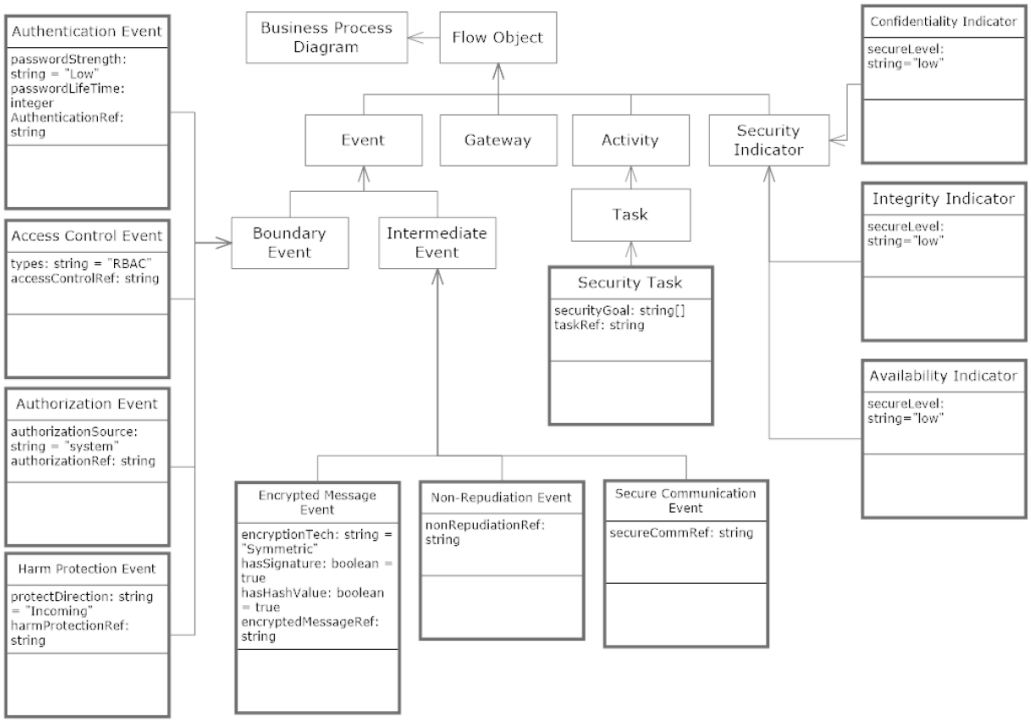


FIGURE 4.34 – *Le métamodèle de l'extension [Sang et Zhou, 2015]*

[Maines et al., 2016] ont introduit une nouvelle ontologie complète comprenant tous les concepts potentiellement modélisables dans BPMN liés à la cybersécurité. Ils ont proposé l'utilisation d'une troisième dimension pour modéliser les concepts de sécurité. Cependant, l'approche reste théorique. Les auteurs ont inclut un exemple de l'utilisation de l'approche - Figure 4.35.

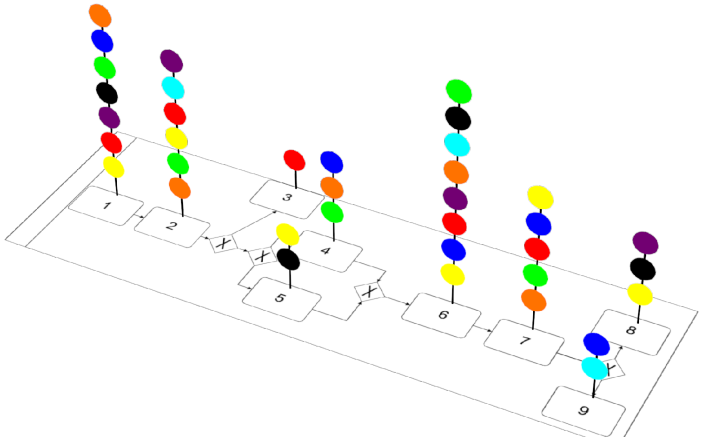


FIGURE 4.35 – *Un exemple d'illustration de l'approche [Maines et al., 2016]*

[Argyropoulos et al., 2017] ont ajouté une série d'attributs de sécurité aux concepts existant de BPMN (Figure 4.36) et ils ont proposé un algorithme pour vérifier la conformité d'un modèle par rapport aux exigences de sécurité.

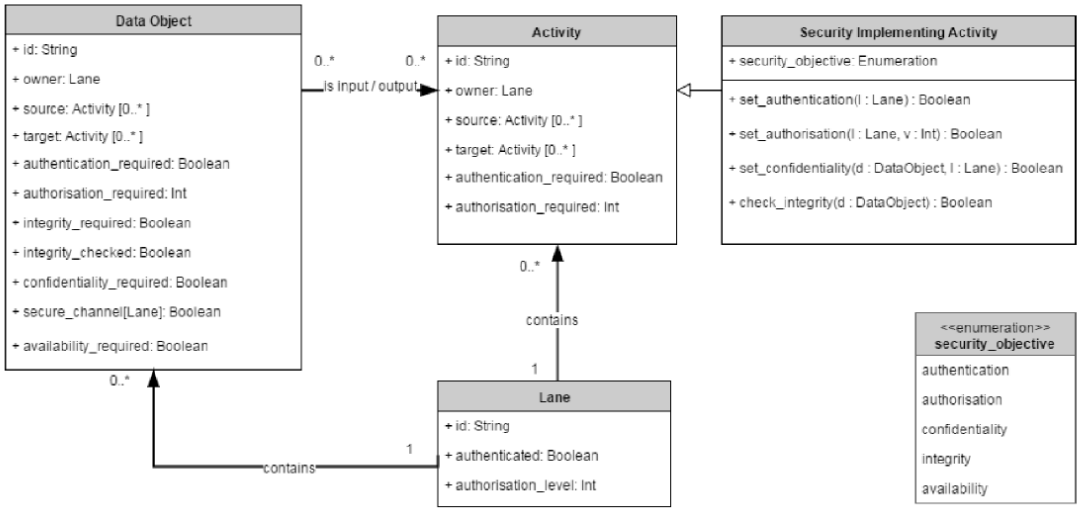


FIGURE 4.36 – *Le métamodèle de l'extension [Argyropoulos et al., 2017]*

[Zhou et al., 2018] proposent un nouveau framework qui permet l'extension, visualisation et vérification des exigences de cybersécurité non seulement pour le BPMN, mais pour d'autres langages de modélisation existants. Le framework permet de représenter tous les concepts potentiellement modélisables dans BPMN liés à la cybersécurité en ajoutant une troisième dimension (illustré par un exemple dans la figure 4.37). L'approche est intéressante mais il est difficile de visualiser tous les concepts sur plusieurs niveaux et les outils BPMN existants ne sont pas compatibles avec la représentation 3D. L'approche manque d'une définition abstraite du méta model.

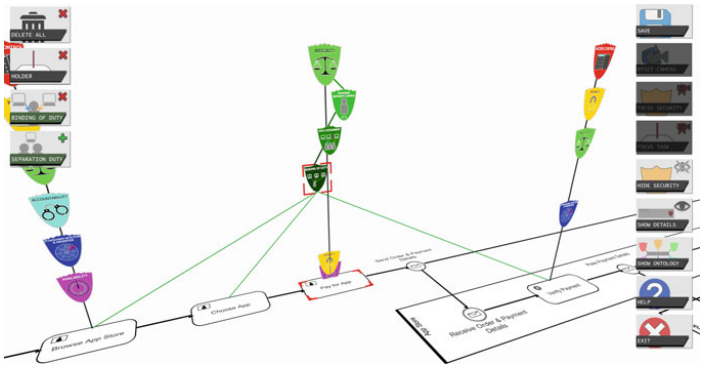


FIGURE 4.37 – *Exemple de modélisation des concepts de cybersécurité en 3D [Zhou et al., 2018]*

[Argyropoulos et al., 2019] proposent une approche basée sur des modèles pour supporter la conception et l'analyse des processus métier sécurisés. Ils ont utilisé les mêmes concepts de sécurité que dans les travaux précédents [Argyropoulos et al., 2017]. Il faut noter l'absence de concepts importants comme la non-répudiation et l'audit. De plus, l'extension n'exploite pas le mécanisme d'extension BPMN 2.0 (figure 4.38).

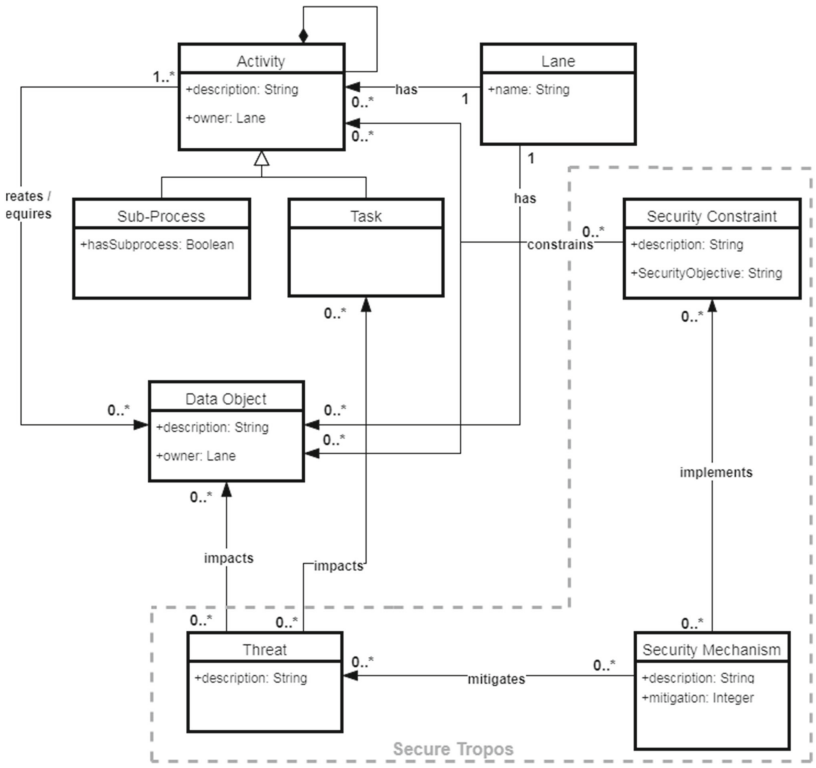


FIGURE 4.38 – *Métamodèle du modèle de processus de référence hybride [Argyropoulos et al., 2019]*

[Pullonen et al., 2019] présentent PE-BPMN, une extension BPMN pour la prise en charge de la confidentialité. Ils illustrent l'usage de l'extension avec un scénario d'une application mobile pour trouver et analyser des fuites de données tout au long du processus métier. Les auteurs ils ont choisi de traiter que les exigences de confidentialité (intégrité et confidentialité) donc l'extension manque de nombreux concepts de sécurité importants (Métamodèle de PE-BPMN - Figure 4.39). La solution se base sur bpmn.js comme notre approche pour modéliser les processus métier.

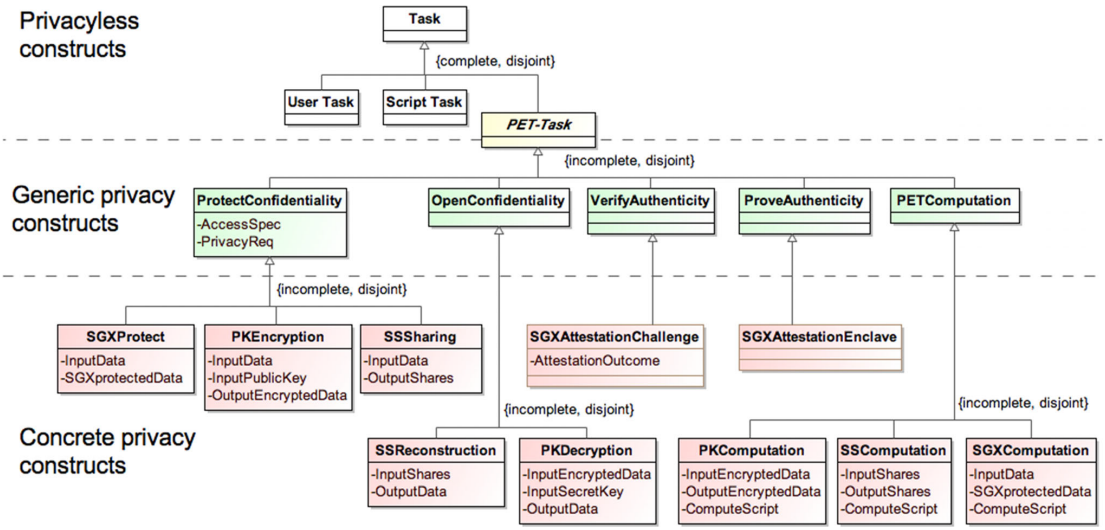


FIGURE 4.39 – *Métamodèle PE-BPMN [Pullonen et al., 2019]*

Dans le tableau 4.3, nous avons listé les extensions de sécurité BPMN trouvées dans la littérature. Chaque extension a été analysée par rapport aux concepts de cybersécurité et au critère de conformité du standard d'extension BPMN défini par [Braun et Esswein, 2014]. Nous avons analysé l'exactitude syntaxique et sémantique des extensions par rapport norme BPMN. Il n'y a pas une seule extension intégrant tous les concepts de sécurité importants. Il est remarquable que aussi les extensions répertoriées ne soient pas conformes à la norme BPMN concernant l'utilisation du mécanisme d'extension BPMN et ces approches sont restent souvent théoriques.

		Rodriguez et al	Brucker et al	Saleem et al	Salnitri et al	Wolter et al	Labda et al	Mulle et al	Sang et al	Altuhhova et al	Basin et al	Maines et al	Argyropoulos et al	Zhou et al	Pullonen et al	Notre approche
Conformité du standard	Année	2007	2013	2012	2014	2009	2014	2011	2015	2013	2011	2016	2019	2018	2019	2019
	Définition	Non Valide	Non Valide	Non Valide	Aucune	Non Valide	Non Valide	Aucune	Non Valide	Non Valide	Non Valide	Aucune	Non Valide	Aucune	Non Valide	Ext Valide
	Syntaxe abstraite	UML, OCL	UML	UML	Aucune	UML	UML	Aucune	UML	UML	UML	Aucune	UML	Aucune	UML	UML
	Syntaxe concrète	Explicite	Aucune	Explicite	Explicite	Implicite	Explicit	Implicite	Explicite	Explicite	Explicite	Implicite	Explicite	Explicite	Implicite	Explicite
	Process Model / MDA	Non	Non	Non	Non	Oui	Non	Non	Non	Non	Non	Non	Oui	Non	Oui	Oui
Les concepts de sécurités																
Control d'accès	Control d'accès / Authenticité	✓	✓		✓		✓		✓		✓	✓		✓		✓
	Authentification					✓		✓	✓				✓			✓
	Autorisation					✓		✓	✓				✓		✓	✓
	Politique de confiance							✓								
	Autorisations de sécurité	✓														
	Mécanisme d'affectation							✓								
Responsabilité	Responsabilité				✓							✓		✓		✓
	Non-répudiation	✓			✓									✓		✓
	Auditabilité / Traçabilité				✓	✓		✓						✓		✓
	Disponibilité			✓	✓	✓			✓	✓		✓	✓	✓		✓
Vie privée	Vié privée	✓			✓							✓		✓	✓	✓
	Confidentialité			✓	✓	✓		✓	✓	✓			✓		✓	✓
	Nécessité / Besoin de savoir		✓				✓									
	Consentement de l'utilisateur						✓	✓						✓		✓
Intégrité	Intégrité	✓		✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓
	Rôle de sécurité	✓														
	Délégation							✓								
	Séparation des tâches		✓				✓	✓			✓					
	Obligation de devoir		✓				✓	✓			✓					
	La séparation des taches								✓							
	Détection d'attaques / dommages	✓										✓		✓		✓

TABLE 4.3 – *Tableau comparatif des extensions de sécurité pour le BPMN*

4.4 Extensions BPMN pour supporter la sécurité dans le Cloud

Le déploiement de processus métier (BP) dans un environnement cloud doit aller au-delà des configurations de machines virtuelles pour prendre en charge l'exécution des processus métier. Il faut une approche efficace pour identifier, modéliser et spécifier les exigences de sécurité telles que la confidentialité, le contrôle d'accès, la non-répudiation et l'intégrité, etc. Les exigences doivent être prises en compte durant la phase de conception du processus métier. La prise en compte des exigences de sécurité dans la phase d'intégration d'une application peut avoir des conséquences sur les aspects sécuritaires. Durant cette section, nous allons lister les travaux qui ont traité la problématique de sécurité pour le contexte particulier du Cloud Computing.

Dans [Damasceno et al., 2011], les auteurs qui ont proposé méthodologie Sec-MoSC [Souza et al., 2009], proposent une extension de leur méthode pour le Cloud. Dans cette nouvelle approche ils proposent un outil pour modéliser et exécuter les processus métiers dans l'environnement Cloud en se basant sur la méthodologie Sec-MoSC (Figure 4.40).

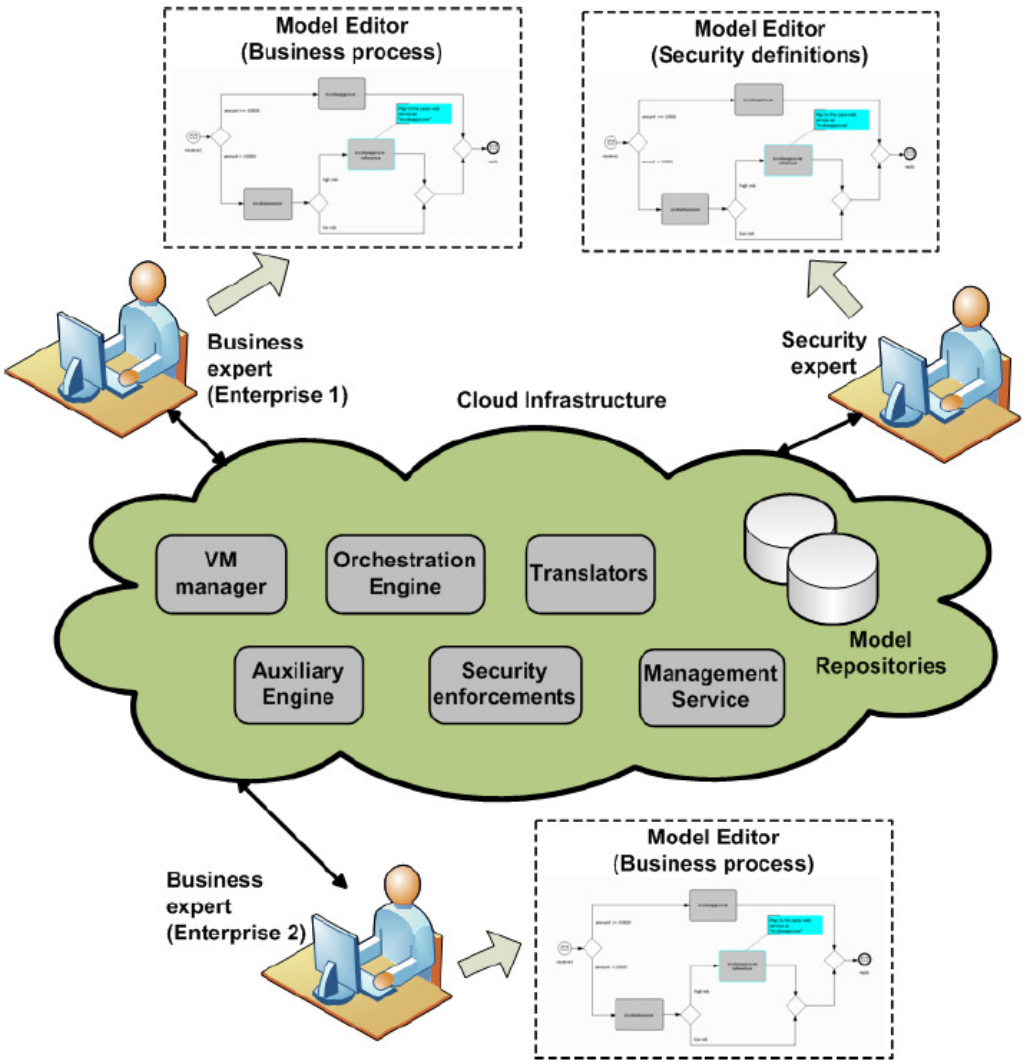


Figure 4.40 – *Modélisation, partage, déploiement et exécution d'un processus métier avec exigences de sécurité dans le Cloud [Damasceno et al., 2011]*

SSC4Cloud permet aux différents acteurs de partager les processus métiers et de gérer l'exécution à l'aide de machines virtuelles. Les experts de sécurité définissent un profile pour un type d'application exportable en format XML. Le processus métier est traduit en WS-BPEL. L'environnement d'exécution prend en charge à la fois l'exécution des processus métier et la vérification des exigences de sécurités au moment de l'exécution - Figure 4.41. Il faut noter que dans l'approche il n y pas un métamodèle qui défini l'extension et que les auteurs ne prennent pas vraiment en compte les aspects sécuritaires du contexte du Cloud Computing.

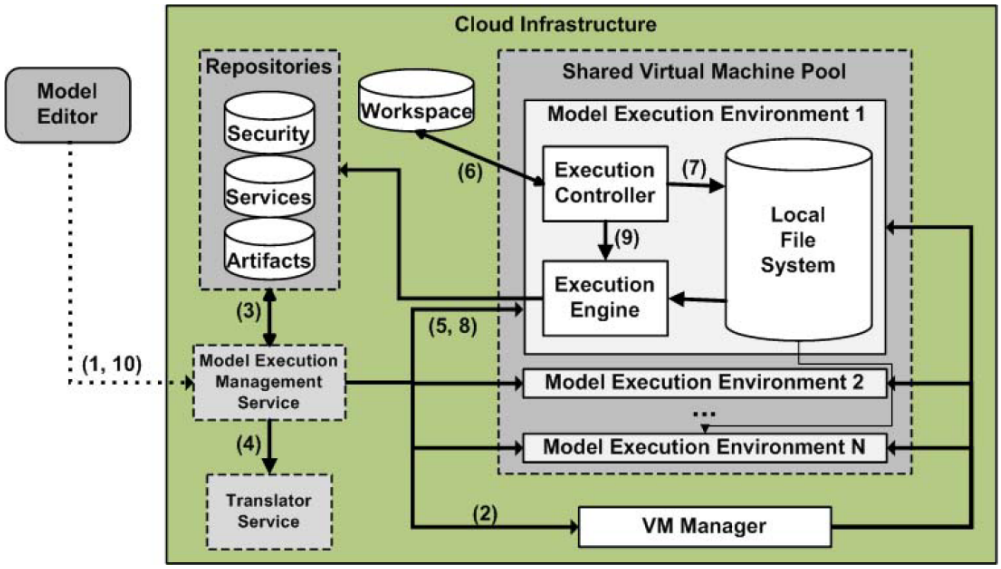


FIGURE 4.41 – *Architecture du model d'exécution du SSC4Cloud [Damasceno et al., 2011]*

[Rekik et al., 2012] ont proposé l'extension BPMN-SEC pour modéliser les objectifs de sécurité pour le contexte d'externalisation des processus métier dans l'environnement de cloud computing. Ils ont proposé l'utilisation de plusieurs concepts de sécurité (métamodèle Figure 4.42) et ils ont défini aussi un profil UML. Ils ont inclus dans le profil les exigences de sécurité tel que « Intégrité », « Non répudiation », « Confidentialité » et « Contrôle d'accès ». Mais l'approche reste théorique, puisqu'ils n'ont pas proposé un outil pour modéliser les concepts et en plus BPMN-SEC n'exploite pas aussi le mécanisme d'extension du BPMN 2.0.

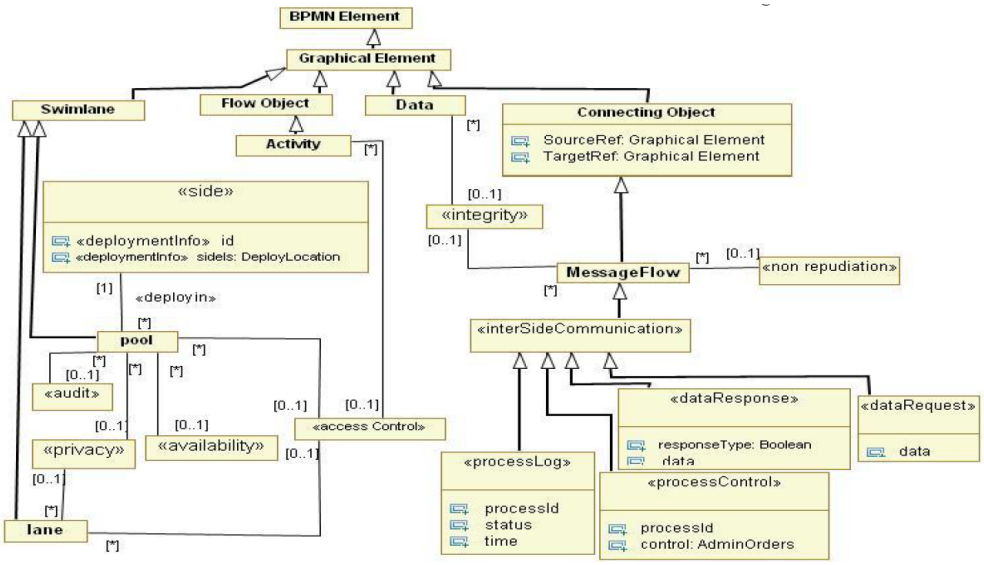


FIGURE 4.42 – *Le métamodèle de l'extension BPMN-SEC [Rekik et al., 2012]*

[Somayeh Sobati Moghadam, 2018] a présenté SeCloudBPMN, une extension BPMN pour prendre en charge les menaces de sécurité dans le cadre d'externalisation des processus métiers dans le cloud. D'après l'auteur, SeCloudBPMN aide les experts en sécurité de l'entreprise à externaliser les processus métier vers le cloud en tenant compte des différentes menaces de l'intérieur et de l'extérieur du cloud. Il a proposé une nouvelle représentation graphique des menaces de sécurité pour le contexte du Cloud. L'extension propose un nombre limité de menaces et l'auteur n'a pas justifié le choix de la sélection des 4 menaces :

— Exploitation malveillante : Lorsque des données privées sont exploités sans autorisation à des fins malveillantes.
— Corruption des données : Lorsque les données stockées sont modifiées ou supprimées par des codes malveillants.
— Violation de la vie privée : lorsque les données sont accédées par des tiers non autorisés.
— Détournement de session : Une session établie est exploitée par un attaquant.

L'auteur n'a présenté aucun métamodèle qui décrit d'une façon formelle l'extension. L'auteur n'a pas proposé aussi un outil pour modéliser facilement les menaces mais il a introduit un exemple illustré par la figure 4.43

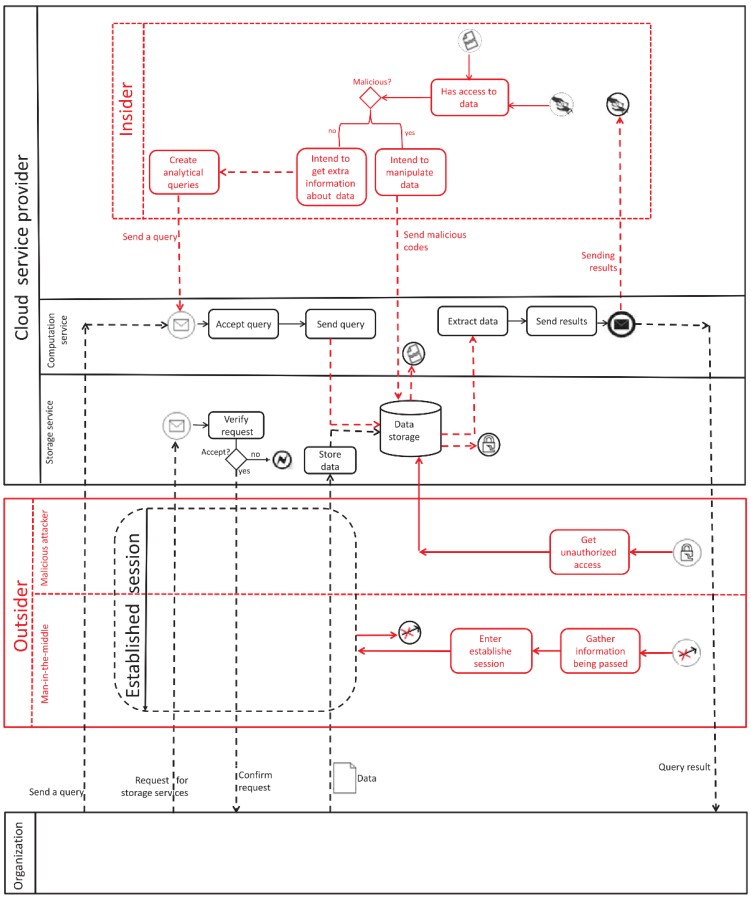


FIGURE 4.43 – *Modélisations des menaces de sécurité avec SeCloudBPMN [Somayeh Sobati Moghadam, 2018]*

[Zarour et al., 2019] ont proposé une extension BPMN (appelée BPOMN) qui permet de spécifier les exigences en termes de sécurité, de conformité, de coût et de performance dans le contexte aussi de l'externalisation des processus métier dans le cloud. Les auteurs ont proposé une extension valide qui exploite le mécanisme d'extension (Figure 4.44) et une intégration dans l'outil MS Visio. L'extension traite la sécurité avec un seul élément « sécurité » ce qui limite vraiment l'usage pour les non experts et aussi les vérifications durant la phase d'exécution.

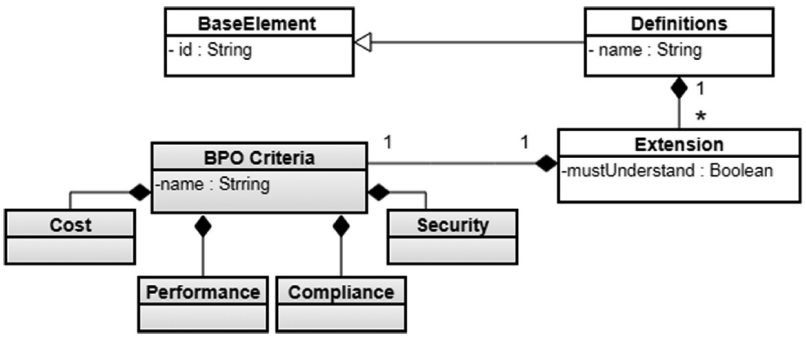


FIGURE 4.44 – *Métamodèle d'extension BPOMN [Zarour et al., 2019]*

Dans cette section, nous avons listé les travaux qui ont proposé des extensions spécifiques au contexte de la sécurité dans le cloud. Il y a très peu de travaux qui traitent le sujet. Les approches proposées ne couvrent pas toutes les menaces et les objectifs de sécurité associés. Comme déjà constaté pour les extensions de sécurité généralistes, la plupart des approches proposées ne sont pas conformes au mécanisme d'extension du BPMN 2.0.

4.5 Conclusion

Plusieurs approches existent dans domaine de la modélisation en prenant en compte l'aspect de la sécurité dès les premières étapes du projet. Pour la modélisation des processus métiers, c'est souvent le langage du BPMN qui est utilisé avec des extensions pour permettre l'ajout d'annotations de sécurités. Ce langage peut être transformé directement vers du BPEL pour permettre l'exécution dans les moteurs spécifiques. La majorité des approches ne couvrent pas la totalité des concepts de sécurité et n'exploitent pas le mécanisme d'extension du BPMN.

Concernant l'environnement du Cloud, il faut noter que plusieurs approches qui traitent la sécurité dans le contexte spécifique du Cloud. Nous avons trouvé très peu de travaux qui exploitent le langage BPMN pour proposer des annotations des exigences de sécurité dans l'environnement Cloud. Souvent les extensions ne sont pas conformes au mécanisme d'extension et n'incluent pas les menaces répondus le Cloud Computing.

5 L'intégration des exigences de sécurité dans le BPMN

5.1 Introduction

L'intégration des exigences de sécurité durant les premières étapes de conception des systèmes est très bénéfique [Leitner et al., 2013]. La modélisation des processus métier est la couche appropriée pour décrire les exigences de sécurité [Menzel et al., 2009]. Cependant, dans la pratique, l'expert du domaine métier se concentre principalement sur les fonctionnalités, car il n'est pas un expert en sécurité [RODRIGUEZ et al., 2007]. La plupart des méthodes de développement logiciel, traitent souvent la sécurité, séparément vers la fin. En outre, la principale préoccupation des développeurs est la fonctionnalité, l'aspect sécuritaire n'est pas prioritaire durant la phase de développement.

La nécessité d'une approche pour annoter les processus métier avec les exigences de sécurité est reconnue par plusieurs auteurs. Plusieurs extensions de sécurité BPMN ont été proposées pour modéliser les exigences de sécurité comme vu précédemment dans le chapitre état de l'art. Cependant, la plupart des approches restent théoriques et ne couvrent pas tous les concepts de sécurité importants Chergui et Benslimane [2018]. Les approches sont construites de manière non systématique, sans aucune preuve empirique pour étayer le choix des concepts de sécurité [Leitner et al., 2013]. La plupart des extensions de sécurité ne sont pas conformes à la norme BPMN 2.0.

Nous proposons dans un premier temps une nouvelle extension BPMN pour annoter les exigences de sécurité. Contrairement aux approches actuelles, notre extension est construite en se basant sur la littérature existante et sur des preuves empiriques. Suite à l'évaluation des approches existantes, nous avons identifié les lacunes de chaque approche afin de proposer un nouvel ensemble d'exigences de sécurité. Dans notre approche nous proposons un ensemble complet de concepts de sécurité dérivé de l'ontologie de la cybersécurité [Maines et al., 2015] avec leur représentation graphique.

Les concepts de sécurité sont intégrés dans des modèles de processus métier pour annoter différents types d'exigences de sécurité (par exemple, disponibilité, confidentialité, intégrité) et sont exprimés à un niveau d'abstraction suffisamment générique pour pouvoir être implémenté par différents types de technologies de mise en œuvre de la sécurité. Nous avons appliqué la méthode Stroppi [Stroppi et al., 2011], pour le développement d'extensions afin d'avoir une extension BPMN 2.0 valide. Nous avons implémenté notre approche en tant qu'application web pour faciliter la collaboration entre les acteurs (ex-

pert du domaine métier, expert en sécurité et développeur). De plus, nous avons défini l'extension en tant que schéma XML pour pouvoir l'intégrer aux outils BPMN existants Chergui et Benslimane [2020].

L'extension est appliquée à un cas d'utilisation réel (processus typique d'admission d'un patient) pour illustrer l'usage de l'extension. Nous avons choisi ce cas d'utilisation car le secteur de la santé s'appuie de plus en plus sur la technologie. Par conséquent, le problème de sécurité peut avoir un impact profond sur les soins aux patients et la confidentialité.

Par la suite, nous adaptons notre nouvelle extension au contexte spécifique du Cloud Computing afin de prendre en considération les menaces du Cloud Computing.

5.2 Extension BPMN basée sur l'ontologie de la cyber-sécurité

D'après nos recherches, l'approche de Stroppi [Stroppi et al., 2011] est la seule méthode trouvée dans la littérature pour la conception des extensions BPMN valides. Ils ont défini un ensemble d'étapes basé sur la transformation des modèles pour le développement méthodique des extensions BPMN valides. Les auteurs ils ont proposé les étapes suivantes :

1. Conceptualisation du domaine en définissant un modèle de domaine conceptuel de l'extension (CDME) avec le diagramme de classes UML.
2. Transformation du CDME en un modèle d'extension BPMN valide à l'aide de profil UML (BPMN + X)
3. Transformation du modèle BPMN + X en un modèle de définition d'extension de schéma XML
4. Transformation du modèle de définition d'extension de schéma XML en un document de définition d'extension de schéma XML.

La syntaxe concrète de l'extension sera définie dans une dernière étape du processus de développement (Figure 5.1).

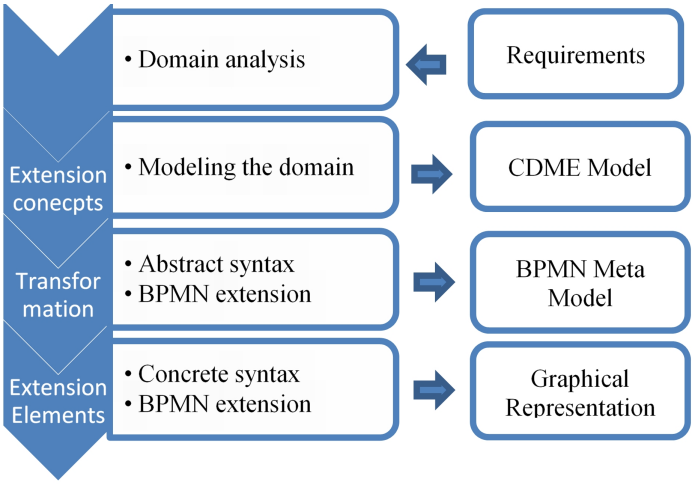


Figure 5.1 – *Processus de développement d'extensions BPMN*

Dans cette section, nous présentons notre extension BPMN avec un ensemble complet de concepts de sécurité dérivés de l'ontologie de la cybersécurité afin de permettre la modélisation des exigences de sécurité Chergui et Benslimane [2020]. En se référant au processus de développement (voir Figure 5.1), la conception de l'extension est présentée progressivement ci-dessous.

5.2.1 Analyse de domaine

Il est nécessaire de spécifier avec précision les exigences de cybersécurité au sein du BPMN. Nous proposons l'utilisation d'une nouvelle ontologie complète, qui inclut tous les concepts potentiellement modélisables dans BPMN liés à la cybersécurité.

Les extensions de sécurité BPMN actuelles sont construites de manière non systématique, sans aucune preuve empirique pour étayer leur choix de concepts [Leitner et al., 2013].

Lors de la création d'une extension de sécurité, il y a la problématique du choix des concepts de sécurité à inclure. Une ontologie de la cybersécurité pour les extensions BPMN a été créée par [Maines et al., 2015]. L'objectif principal étant de fournir un ensemble complet des objectifs de sécurité afin de répondre aux exigences de la cybersécurité (Figure 5.2). Dans notre approche on va se baser sur cette ontologie.

5.2.2 Modèle de domaine conceptuel de l'extension (CDME)

La première étape de la méthode consiste à définir un modèle de domaine conceptuel de l'extension (CDME) décrivant les concepts du domaine à représenter dans les modèles BPMN et leurs relations avec les concepts du métamodèle BPMN. Les figures 5.3 et 5.4 présentent notre modèle de domaine conceptuel proposé en tant que diagramme de classes (UML). Les classes du méta-modèle BPMN 2.0 sont surlignées en gris. Ces classes BPMN sont associées à d'autres classes. Pour des raisons de clarté, ceux-ci sont omis dans notre modèle. Pour la même raison, nous avons divisé le méta-modèle en deux parties. Notre extension se base sur la classe «SecurityRequirement» qui représente toutes les exigences de sécurité telles que représentées dans l'ontologie des exigences de cybersécurité. Nous reprenons les six concepts clés (contrôle d'accès, détection et prévention des attaques / dommages, intégrité, responsabilité, confidentialité et disponibilité) et les sous-classes importantes comme (confidentialité, consentement de l'utilisateur, authentification, autorisation, identification, etc.)

L'extension est uniquement liée (via la composition) aux classes BPMN Activity, Message and Data Object. Selon BPMN 2.0, une activité est effectuée dans un processus métier et peut être atomique ou composée. Grâce à cette composition, une classe BPMN peut hériter des attributs des exigences de sécurité. De plus, les tâches BPMN sont des activités atomiques dans le flux de processus et permettent de spécifier une ressource, une interface ou un ensemble de règles pour l'exécution de la tâche. Comme la classe BPMN Task hérite de l'activité BPMN, elle peut également être étendue avec les attributs des exigences de sécurité. Dans notre extension, les différents types de tâches BPMN sont utilisés pour représenter la nature d'un contrôle pour vérifier les exigences de sécurité.

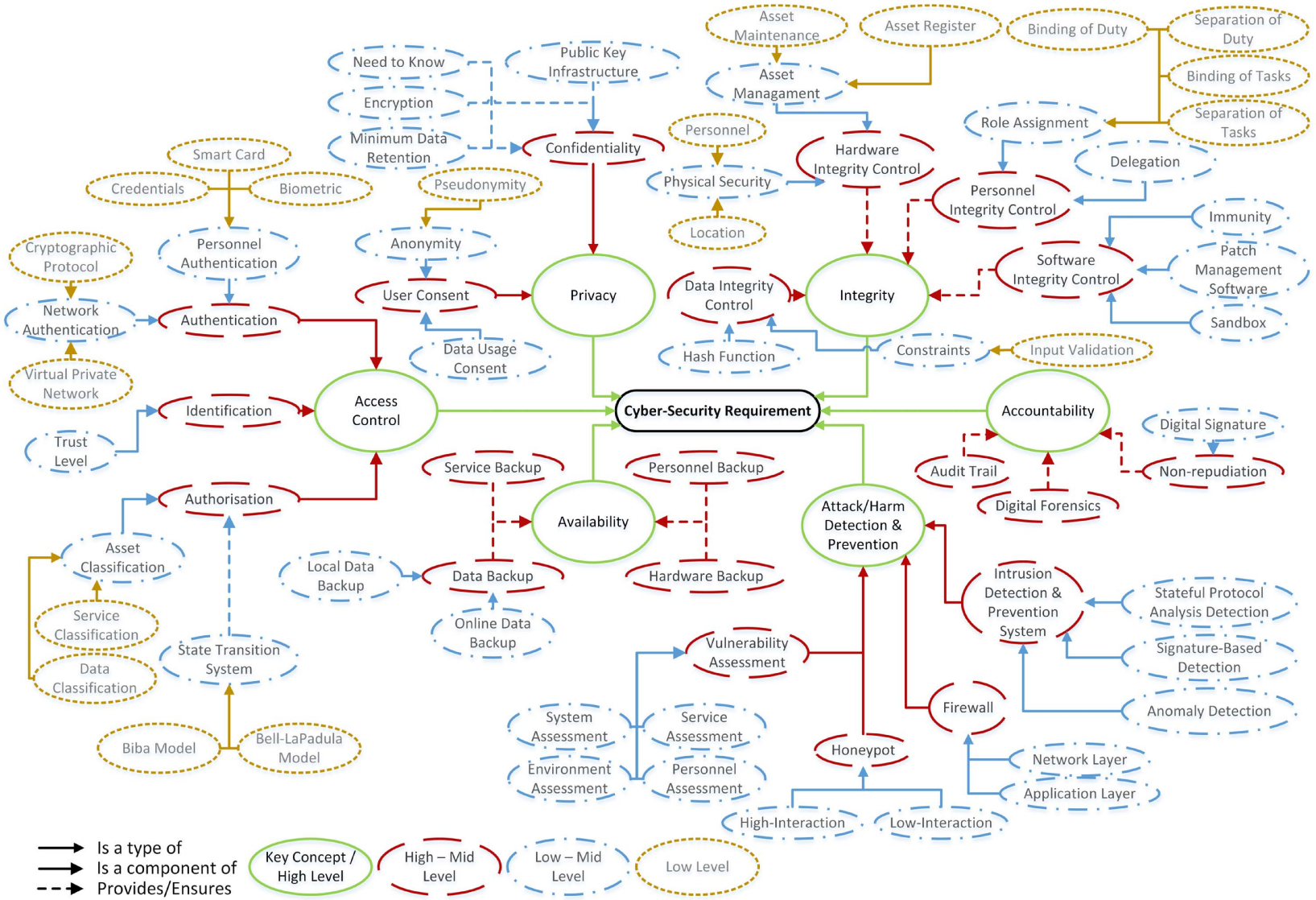


FIGURE 5.2 – *Ontologie des exigences de cybersécurité pour une extension de sécurité BPMN [Maines et al., 2015]*

Concernant le mappage entre les types de tâche et BPMN Task, nous avons le contrôle automatisé représenté par l'utilisation de BPMN ScriptTask ou BusinessRuleTask dans ce cas l'exécution est automatique sans intervention manuelle. Les moyens de contrôle manuel sont représentés par UserTask ou ManualTask car ils impliquent une action humaine.

Le modèle conceptuel décrit les sémantiques souhaitées pour l'extension BPMN. Ce modèle de domaine est la base pour le modèle d'extension. Le mécanisme d'extension du BPMN est définit avec deux représentations : le méta-modèle Meta Object Facility (MOF) et un schéma XML. Les classes BPMN présentées dans le modèle de domaine font partie du méta-modèle MOF.

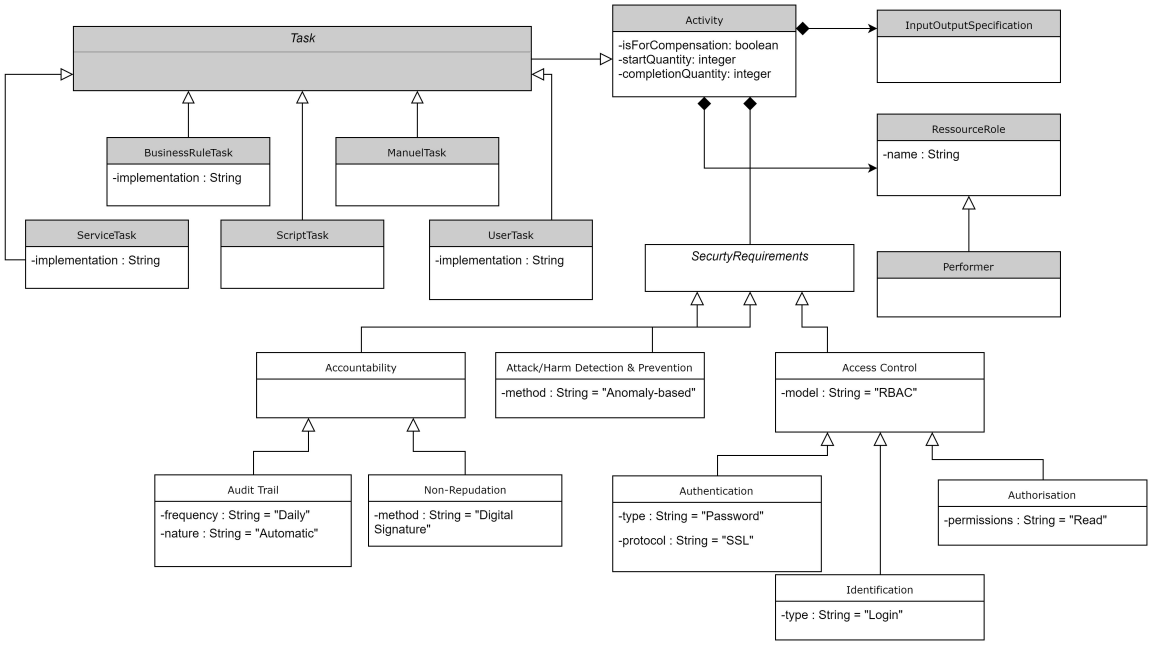


FIGURE 5.3 – *Modèle de domaine pour l'extension BPMN partie 1*

5.2.3 Modèle d'extension BPMN (BPMN + X)

La deuxième étape consiste à faire un modèle BPMN + X basé sur le CDME résultant de la première étape. BPMN + X est un langage développé par [Stroppi et al., 2011] en tant que profil UML. Ainsi, il peut être pris en charge par les outils UML existants. UML est un langage de modélisation populaire, donc c'est un vrai avantage de définir BPMN + X en tant que profil UML. La sémantique et la syntaxe abstraite des éléments BPMN + X sont basées sur la spécification du mécanisme d'extension BPMN (Figure 5.5).

Le modèle BPMN + X est enrichi par des stéréotypes. Le stéréotype ExtensionDefinition décrit un conteneur et correspond à la classe respective dans le mécanisme d'extensibilité MOF. Le stéréotype ExtensionElement est défini dans le profil UML BPMN-X et correspond à la classe ExtensionAttributeValue du mécanisme d'extensibilité MOF. Cela permet de représenter les différents éléments comme des objets de classe pour la prochaine étape de transformation.

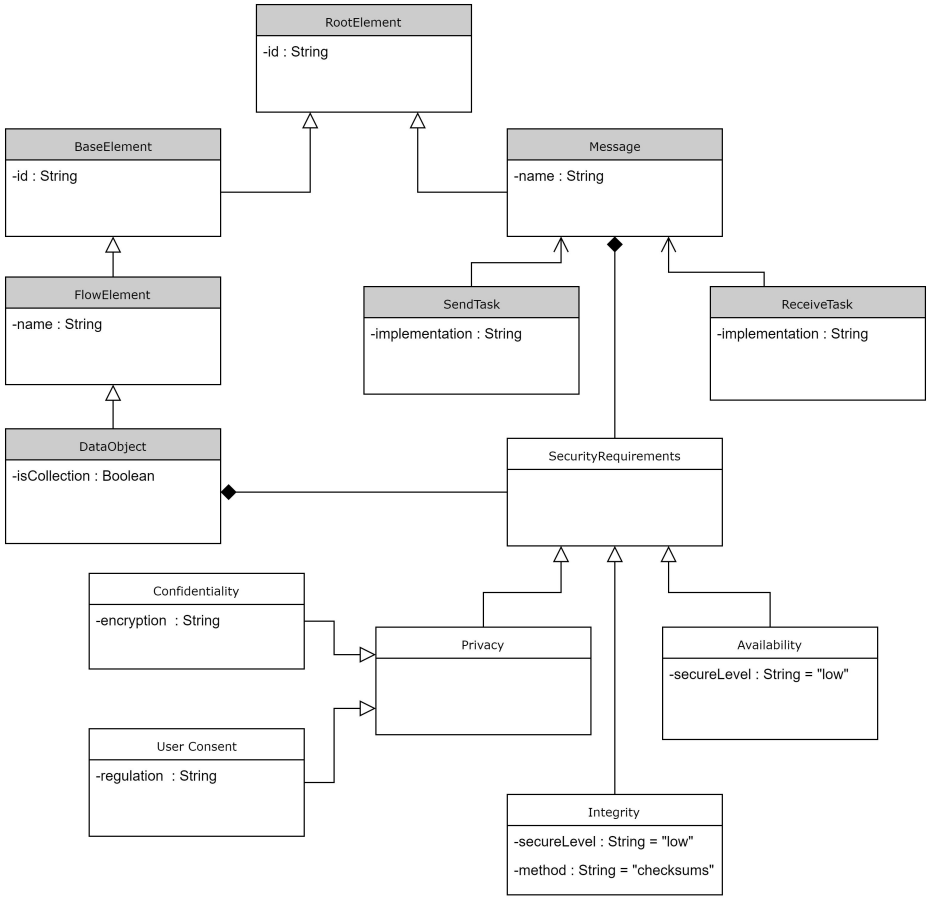


FIGURE 5.4 – *Modèle de domaine pour l'extension BPMN partie 2*

5.2.4 Transformation BPMN du modèle BPMN + X en un modèle de définition d'extension de schéma XML

La troisième étape consiste à transformer le modèle BPMN + X en un modèle de définition d'extension de schéma XML qui est une instance d'un métamodèle MOF représentant les concepts de la spécification de schéma XML.

— L'élément ExtensionElement est transformé en un élément ComplexTypeDenition.

— L'élément ExtensionEnum est transformé en un élément SimpleTypeDenition.

— Les éléments BPMNElement et BPMNEnum ne sont transformés en aucun type d'élément de schéma XML. Cela est dû au fait que le schéma généré importe la spécification BPMN afin que les éléments BPMN puissent être référencés par les autres éléments définis dans ExtensionModel [Stroppi et al., 2011].

La troisième étape de la méthode est prise en charge par une transformation de modèle à l'aide du QVT (Query / View / Transformation). Cette transformation prend en entrée un modèle BPMN + X pour génrer un modèle de définition d'extension de schéma XML qui est une instance d'une représentation Ecore du schéma XML.

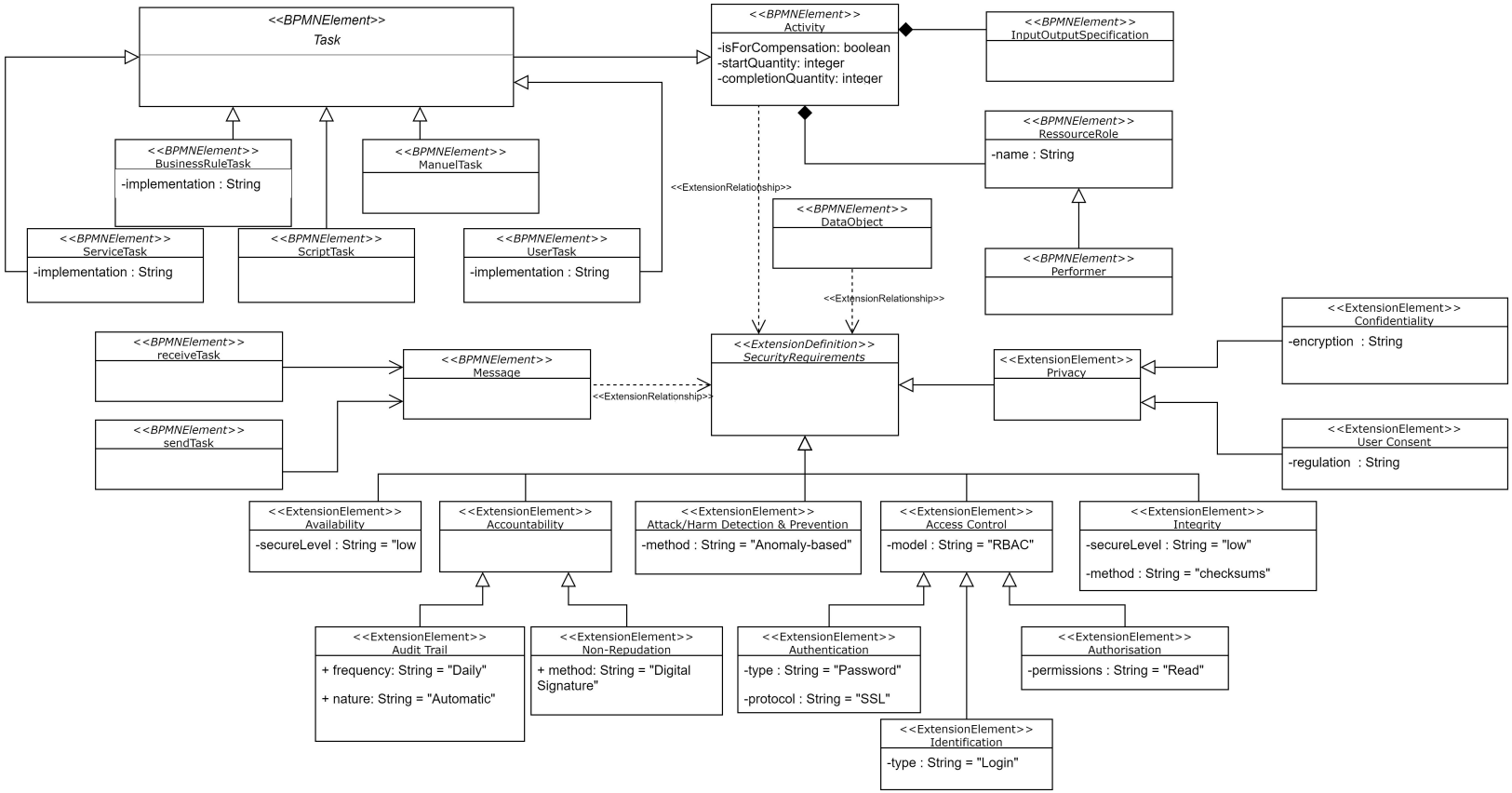


FIGURE 5.5 – *Modèle d'extension BPMN + X*

```
<?xml version="1.0" encoding="UTF-8"?>
<schema:Schema xmi:version="2.0"
    xmlns:xmi="http://www.omg.org/XMI"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:schema="http://xmlschema/1.0" xsi:schemaLocation=
"http://xmlschema/1.0 ../../org.cidisi.bpmn.extension.transformation/model/XMLSchema.ecore" targetNamespace=
"http://www.cidisi.org/bpmn/extensions/samples/workdistribution">
    <definitions xsi:type="schema:SimpleTypeDefinition" name="xsd:boolean"/>
    <definitions xsi:type="schema:SimpleTypeDefinition" name="xsd:QName"/>
    <definitions xsi:type="schema:SimpleTypeDefinition" name="xsd:string"/>
    <definitions xsi:type="schema:EnumerationTypeDefinition" name="AgentType">
        <values value="SYSTEM"/>
        <values value="ADMINISTRATOR"/>
    </definitions>
    <definitions xsi:type="schema:ComplexTypeDefinition" name="Integrity">
        <attributeUses required="true">
            <attributeDeclaration name="name" typeDefinition="//@definitions.2"/>
        </attributeUses>
        <attributeUses required="true">
            <attributeDeclaration name="" typeDefinition="//@definitions.1"/>
        </attributeUses>
    </definitions>
    <definitions xsi:type="schema:ComplexTypeDefinition" name="Audit Trail" baseTypeDefinition=
"//@definitions.8">
        <attributeUses required="true">
            <attributeDeclaration name="name" typeDefinition="//@definitions.2"/>
        </attributeUses>

...
```

FIGURE 5.6 – *Modèle de définition d'extension de schéma XML*

5.2.5 Transformation du modèle de définition d'extension de schéma XML en un document de schéma XML

La dernière étape de la méthode consiste à générer un document de schéma XML représentant les éléments du modèle de définition d'extension de schéma XML résultant de la troisième étape. Ce document est généré avec une transformation simple de modèle en code. Cette étape est prise en charge par une transformation de modèle en code avec JET.

5.2.6 Notation graphique

Pour visualiser les nouveaux éléments dans le processus métier, nous proposons une notation graphique correspondante. Pour décrire les modèles de processus sous forme de diagrammes, BPMN fournit un schéma pour l'échange de diagrammes (BPMN : DI) qui est destiné à faciliter les échanges entre les outils de modélisation. Ce schéma permet de spécifier les attributs visuels d'un modèle de processus dans sa représentation XML [Schultz et Radloff, 2014].

À cet égard, la spécification BPMN ne fournit ni directives pour la représentation graphique des éléments d'extension ni mécanisme d'extensibilité pour les nouveaux éléments de notation. La notation doit être mise en œuvre séparément de la sémantique dans un outil de modélisation [Stroppi et al., 2011]. En général, la notation d'une extension ne doit pas altérer la notation BPMN et doit être aussi proche que possible de celle-ci.

```
<xsd:schema elementFormDefault="qualified" attributeFormDefault="unqualified"
    xmlns="http://www.cidisi.org/bpmn/extensions/samples/workdistribution"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:bpmn="http://www.omg.org/spec/BPMN/20100524/MODEL" targetNamespace=
"http://www.cidisi.org/bpmn/extensions/samples/workdistribution">
    <xsd:import namespace="http://www.omg.org/spec/BPMN/20100524/MODEL" schemaLocation="BPMN20.xsd"/>
    <xsd:complexType name="Authorisation" abstract="false">
        <xsd:complexContent>
            <xsd:extension base="Access Control">
                <xsd:attribute name="name" type="xsd:string" />
            </xsd:extension>
        </xsd:complexContent>
    </xsd:complexType>
    <xsd:complexType name="Privacy" abstract="false">
        <xsd:attribute name="name" type="xsd:string" />
        <xsd:attribute name="granted" type="xsd:boolean" />
    </xsd:complexType>
    ../..
    <xsd:group id="SecurityRequirements" name="SecurityRequirements">
        <xsd:sequence>
            <xsd:element name="distributionAgent" type="AgentType" minOccurs="1" maxOccurs="1"/>
            <xsd:element name="attackHarm" type="Attack/Harm Detection & Prevention" minOccurs="1"/>
            <xsd:element name="privacy" type="Privacy" minOccurs="1" maxOccurs="unbounded"/>
            <xsd:element name="accessControl" type="Access Control" minOccurs="1" maxOccurs="unbounded"/>
            <xsd:element name="integriy" type="Integrity" minOccurs="1" maxOccurs="1"/>
            <xsd:element name="avaibility" type="Availability" minOccurs="1" maxOccurs="unbounded"/>
            <xsd:element name="accountability" type="Accountability" minOccurs="1" maxOccurs="unbounded"/>
            <xsd:element name="distributionTrigger" type="xsd:QName" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:group>
</xsd:schema>
```

FIGURE 5.7 – *Document de définition d'extension de schéma XML*

Notre notation étend les formes de tâche BPMN, du message et de l'objet de données - le tableau 5.1.

Concept	Representation	Concept	Representation
Attack/harm detection and prevention		Authorization	
Audit Trail		Integrity	
Non-Repudiation		User-Consent	
Confidentiality		Authentication	
Availability		Identification	

TABLE 5.1 – *Notation pour notre extension de sécurité*

5.2.7 Démonstration

Nous avons développé un nouvel outil basé sur le framework bpmn-js afin d'intégrer les objectifs de sécurité définis précédemment directement dans la palette des éléments BPMN. Pour illustrer l'utilisation de notre approche, nous avons annoté un processus métier typique d'admission d'un patient à l'hôpital issue des travaux de [RODRIGUEZ et al., 2007]. Trois pistes décrivent le processus métier (voir Figure 5.8) :

— La piste du patient représente la personne qui reçois des soins médicaux
— La piste d'administration est divisée en deux couloirs, une partie pour l'admission et une autre partie pour le traitement des factures et des assurances.
— La piste médicale est divisée en deux couloirs (évaluation médicale et examens) où sont effectués des tests de préadmission, des examens, des évaluations et une collecte complète de données cliniques.

Nous avons annoté ce processus métier avec les exigences de sécurité.

— Nous avons examiné plusieurs aspects de la sécurité. Nous avons ajouté la confidentialité à la demande d'admission, dans le but d'empêcher la divulgation d'informations sensibles sur les patients.
— La non-répudiation a été définie sur le flux de messages qui va de la piste « patient » vers la piste « administration » dans le but d'éviter être remis en cause de la « demande d'admission ».
— L'authentification a été définie pour l'activité « examen de la demande d'admission ».
— L'objectif d'audit a été ajouté à l'activité « calcul du coût ». Ce qui implique l'enregistrement du nom, du rôle, la date et l'heure de tous les événements liés à la mise à jour des coûts.
— Une exigence d'intégrité a été spécifiée aussi pour protéger les l'objet de données « informations cliniques » et « données comptables ».
— Enfin, nous avons annoté « évaluation médicale » par la détection des dommages d'attaque avec aussi de l'audit. Tous les événements liés aux tentatives d'attaques doivent être enregistrés.

Comme illustré, l'exemple montre comment notre extension de sécurité améliore la norme BPMN actuelle afin de prendre en charge la spécification des exigences de sécurité dans le processus de métier.

Compte tenu des approches actuelles des extensions de sécurité et des langages de modélisation en général, notre solution offre un ensemble complet de concepts de sécurité avec leur présentation graphique pour simplifier la modélisation des exigences de sécurité.

5.2.8 Evaluation

Dans un projet de recherche de conception, l'étape d'évaluation tente d'observer et de mesurer dans quelle mesure l'artefact conçu résout le problème traité [Schultz et Radloff, 2014].

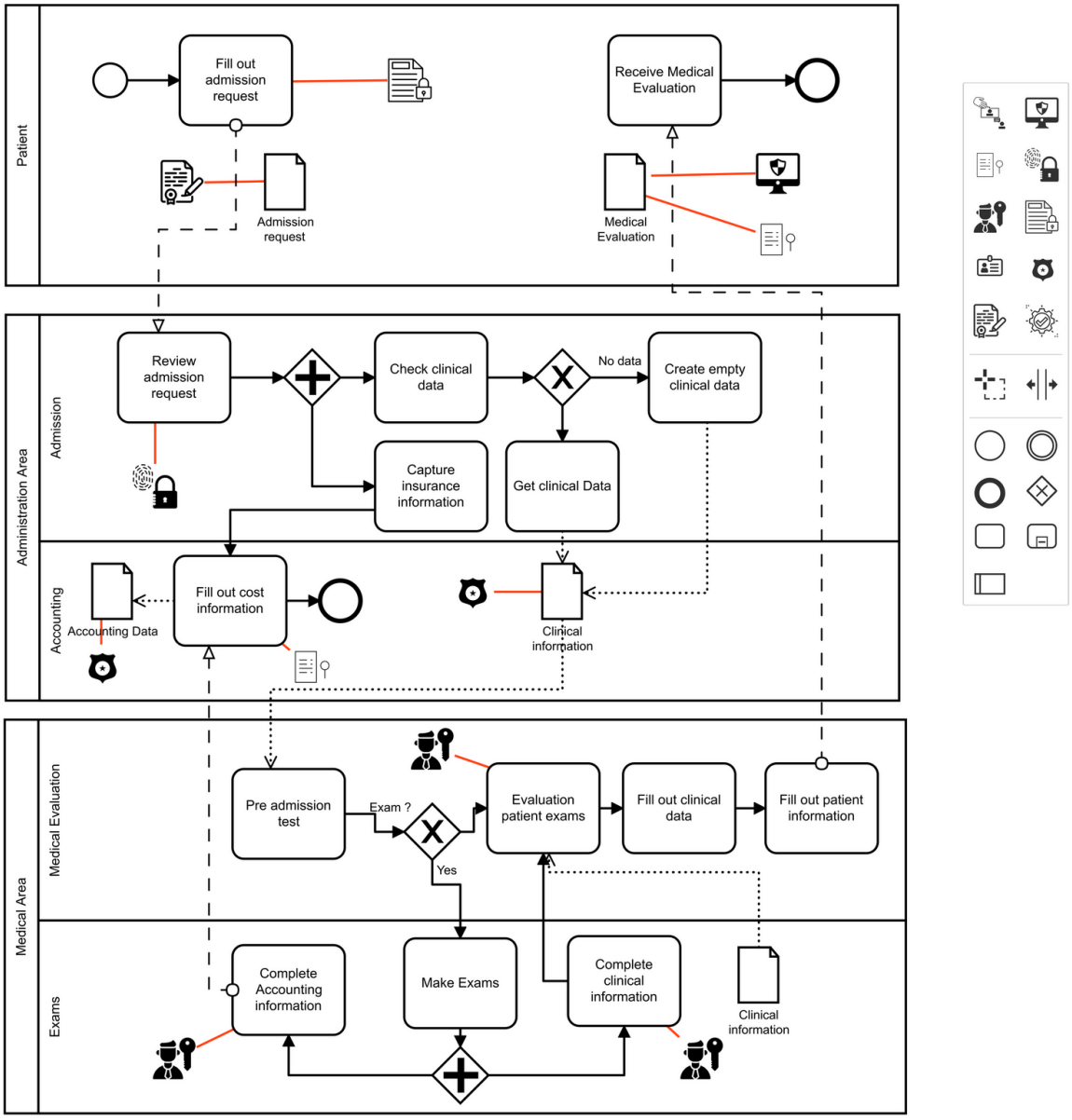


FIGURE 5.8 – *Processus métier d'admission d'un patient dans un hôpital*

Afin d'évaluer notre extension de sécurité BPMN, nous avons effectué une expérimentation afin de mesurer la compréhension de notre nouvelle extension. Nous avons montré un diagramme BPMN aux participants et par la suite nous avons posé 10 questions pour tester leur compréhension de la sémantique de certains concepts de sécurité.

Nous avons posé les questions suivantes :

— Est-ce qu'il y a un objectif de sécurité lié au message « Admission request » ?
— Y'a-t-il trois taches qui ont un objectif de « Authorization » ?
— Y'a-t-il un objectif de « Non-Repudiation » sur l'objet « Accounting Data » ?
— La piste "Patient" contient-elle trois objectifs ?
— Y'a-t-il un objectif de « Integrity » lié à la tâche « Complete Accounting information » ?

— La piste de « administration area » contient-elle plusieurs objectifs ?
— Est-ce qu'il y a un objectifs de « Integrity » lié à l'objet « Clinical information » ?
— Y'a-t-il un objectif « User-Consent » au niveau du processus d'admission ?
— L'objet « Medical Evaluation » est-il lié aux objectifs « Audit Trail» et « Attack/harm detection and prevention» ?
— Est-ce qu'il y a un objectif de « Authorization » liée à la tâche « Complete Accounting information » ?

Une expérimentation entre groupes 1x2 est proposée. Trois mesures dépendantes ont été utilisées comme dans [Bodart et al., 2001] :

— Précision : 10 questions ont été posées aux participants sur la sémantique sous-jacente des concepts de sécurité. Nous avons évalué leur réponse comme correcte ou incorrecte. Le score d'exactitude représente le nombre total de réponses correctes divisé par le nombre de participants.
— Temps : Nous avons enregistré le temps pris (en secondes) pour chaque participant à répondre. Le score en temps correspond au temps total nécessaire pour répondre aux 10 questions.
— Précision normalisée : la précision et le temps sont des mesures de performance, il est bien connu que les participants peuvent faire des compromis - par exemple, ils peuvent compromettre la précision de leurs réponses pour augmenter la vitesse de réponse. En conséquence, un score de précision normalisé a été calculé, qui est le score de précision d'un participant divisé par son score de temps. Le score de précision normalisé d'un participant à chaque essai correspond au nombre de réponses correctes qu'il a fournies par seconde écoulée.

L'expérimentation se base sur un processus d'admission d'un patient dans un hôpital. Deux diagrammes de processus métier ont été créés. Le premier un diagramme annoté avec des informations relatives à la sécurité basées avec l'extension BPMN précédemment présentée (groupe BPMN avec extension). Le second un diagramme BPMN traditionnel avec des concepts de sécurité dans une matrice(séparément des modèles de processus). Les ligne de la matrice de sécurité représente les concepts de sécurité et les colonnes les éléments BPMN, si un concept est lié à un élément, nous l'indiquons dans la cellule.

Les participants doivent répondre à des questions se référant aux concepts de sécurité liés au processus métier d'admission d'un patient dans un hôpital. Nous avons posé des questions pour identifier quel élément est concerné par un concept de sécurité particulier. Etant donné un élément, quels concepts sont appliqués.

Pour l'expérimentation, nous avons invité 30 ingénieurs en informatique qui travaillent dans des sociétés d'ingénierie logicielle à répondre en ligne à notre questionnaire.

Nous avons présenté le même processus d'admission d'un patient dans l'hôpital avec les concepts de sécurité associés. Nous avons fourni au premier groupe une matrice avec les concepts de sécurité séparées (groupe BPMN). L'autre groupe a accès aux modèles de processus qui sont annotés directement avec les concepts de sécurité. L'objectif était d'évaluer l'interprétation et la compréhension des modèles. Pour évaluer la qualité de l'interprétation du modèle, deux perspectives sont discutées : la précision (dans quelle

mesure l'interprétation du modèle aide-t-elle le participant à comprendre la sémantique du domaine incluse dans le modèle ?) Et la précision normalisée (efficacité de la tâche de compréhension) [Burton-Jones et al., 2009].

Dans notre expérimentation, les hypothèses suivantes sont testées :

— H1 : la précision est positivement affectée par l'utilisation de l'extension BPMN pour représenter les concepts de sécurité dans les modèles de processus.
— H2 : la précision normalisée est positivement affectée par l'utilisation de l'extension BPMN pour représenter les concepts de sécurité dans les modèles de processus.

L'expérimentation s'est déroulée entièrement en ligne à l'aide de la suite de recherche Qualtrics [1].

Les participants arrivent sur une landing page qui explique la nature de l'expérimentation. Après un bref aperçu des éléments BPMN pertinents (types de tâches, passerelles) est fourni avant d'enchainer avec les questions. Par la suite, le participant il est affecté à l'un des deux groupes afin de répondre aux 10 questions (des questions simples oui/non). Le processus annoté il est affiché seulement pour le groupe BPMN avec extension. Le but principal de l'utilisation de plusieurs essais est de déterminer si l'évolution de la précision normalisée est différente à cause de l'apprentisage entre les deux groupes.

Le tableau 5.2 présente les résultats des trois mesures de performance.

Le groupe avec qui a eu les diagrammes annotés avec les concepts de sécurité à eu de meilleurs résultats de précision. Les deux groupes ne différaient pas beaucoup en termes de temps. Nous remarquons que le temps se réduits avec les essais et la précision augmente. Les résultats expérimentaux indiquent que l'extension BPMN a eu un effet positif sur la compréhension et l'interprétation des concepts de sécurité du processus d'admission. Les concepts de sécurité intégrés réduisent la charge cognitive pour l'interprétation du modèle avec les concepts de sécurité.

5.3 La modélisation des menaces de sécurité du cloud

Le cloud computing transforme la façon dont les technologies de l'information sont consommées et gérées, avec une promesse d'une meilleure rentabilité, une mise sur le marché plus rapide, une innovation accélérée et plus de flexibilité. Mais cela soulève également de nombreuses préoccupations concernant les menaces à la sécurité. Le cloud computing est un modèle dans lequel les ressources informatiques sont proposées à l'utilisateur en tant que service. Dans ce contexte, l'importance de la sécurité est évidente, car les données sensibles envoyées sur Internet peuvent être consultées par des tiers non autorisés. Dans cette section on va proposer une approche d'annotation des processus métier avec les menaces les plus courantes dans cloud computing.

L'émergence du cloud computing à induit l'apparition de nouvelles vulnérabilités de sécurité et l'amplification des vulnérabilités existantes. Parmi les risques de sécurité les

1. https://www.qualtrics.com/fr/

	Nombre de participants	Réponses correctes	Précision	Temps	Précision normalisée
	Essai 1				
Groupe avec extension de sécurité BPMN	15	95	6.33	82.38 sec	0.077
Groupe BPMN	15	69	4.60	90.14 sec	0.051
	Essai 2				
Groupe avec extension de sécurité BPMN	15	106	7.06	67.16 sec	0.105
Groupe BPMN	15	80	5.33	78.65 sec	0.068
	Essai 3				
Groupe avec extension de sécurité BPMN	15	121	8.06	56.54 sec	0.143
Groupe BPMN	15	102	6.80	63.49 sec	0.107
	Moyenne				
Groupe avec extension de sécurité BPMN	15	107.33	7.15	68.70 sec	0.108
Groupe BPMN	15	83.66	5.58	77.43 sec	0.075

TABLE 5.2 – *Statistiques de performance*

plus importants associés au cloud computing, il y a la tendance à contourner les départements informatique (IT) et les responsables de l'information. Bien que le passage exclusif aux technologies cloud puisse générer des gains de coût et d'efficacité, il faut mettre en place des politiques de sécurité, des processus et l'application des meilleures pratiques.

5.3.1 Analyse de domaine

La Cloud Security Alliance (CSA) a créé des normes de référence pour la sécurité dans le cloud. Ces dernières années, la CSA a publié le « Guide de sécurité pour les zones critiques du cloud computing » et le « Guide de mise en œuvre de la sécurité en tant que service ».

Pour notre extension BPMN dédiée à la sécurité dans le cloud computing, nous allons nous baser sur le document de référence « principales menaces pour cloud computing » [Cloud Security Alliance (CSA), 2019] afin d'inclure dans l'extension les principales menaces pour le cloud. Pour les objectifs de sécurité, nous reprenons les objectifs dérivés

de l'ontologie de la cybersécurité. Notre extension de sécurité pour le cloud inclut les menaces du cloud computing ainsi que les objectifs de sécurité.

5.3.2 Modèle de domaine conceptuel de l'extension (CDME)

Les figures 5.9, 5.10 et 5.11 représentent notre modèle de domaine conceptuel pour modéliser les menaces du cloud computing. Nous proposons une extension du modèle CDME précédent avec les 11 menaces dérivées du document CSA afin de pouvoir représenter toutes les menaces possibles qui existent dans le cloud computing. Il faut noter que sur ce nouveau modèle n'inclut pas les anciens éléments (les objectifs de sécurité) pour des raisons de clarté.

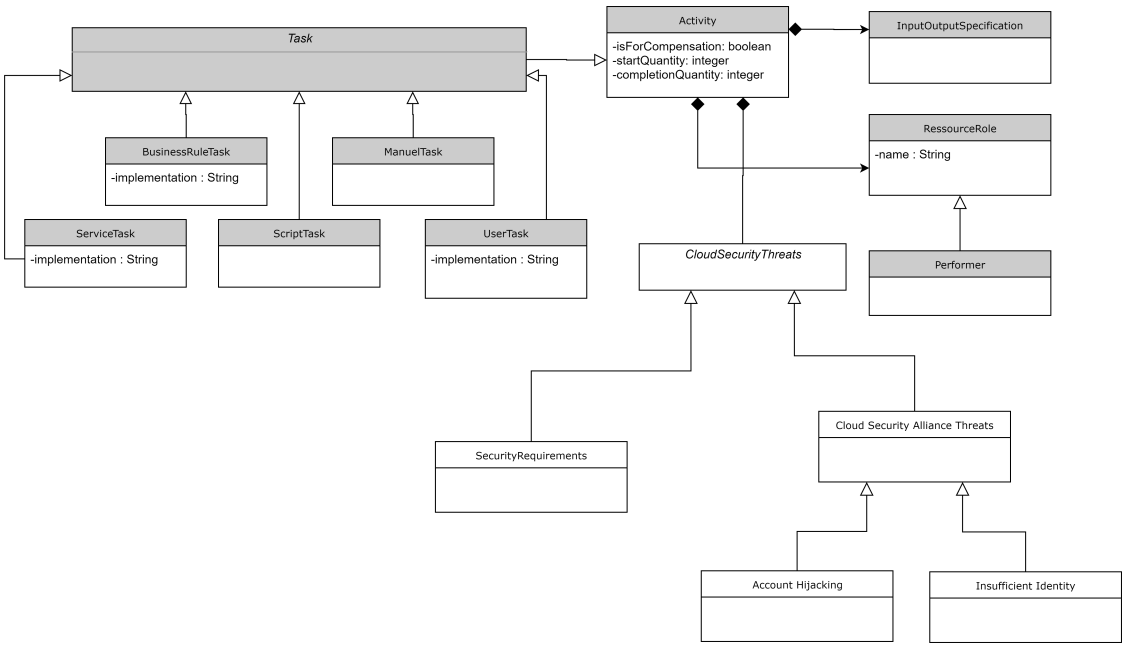


FIGURE 5.9 – *Modèle de domaine des menaces du cloud computing pour l'élément activité*

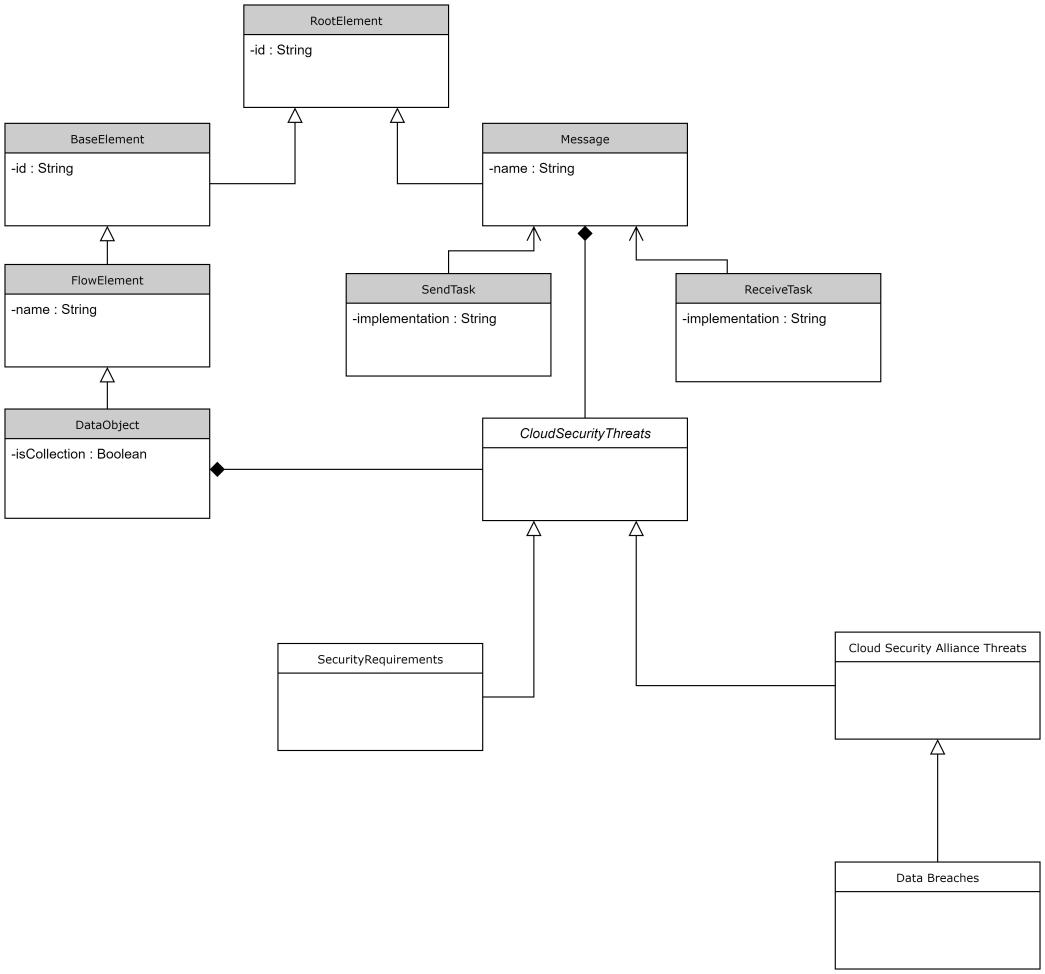


FIGURE 5.10 – *Modèle de domaine des menaces du cloud computing pour les éléments objet de donnée et message*

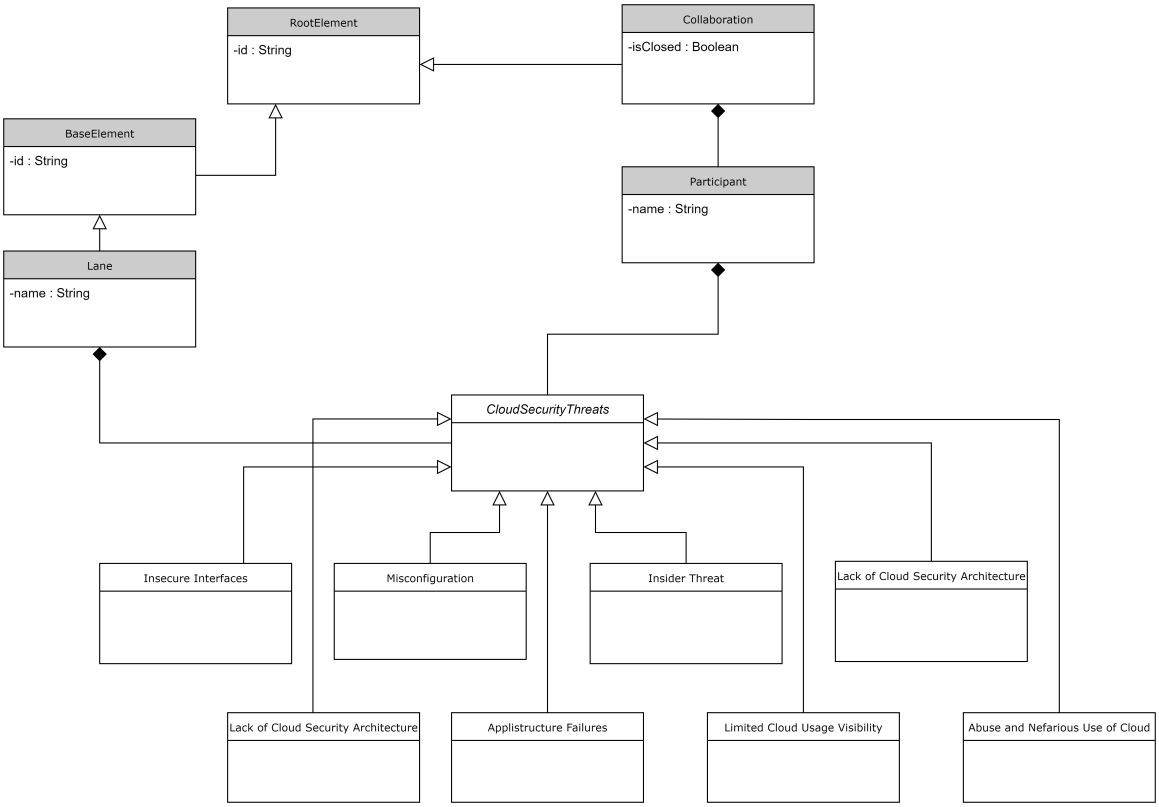


FIGURE 5.11 – *Modèle de domaine des menaces du cloud computing pour les éléments « participant et piste »*

5.3.3 Modèle d'extension BPMN (BPMN + X)

La figure 5.12 représente le modèle d'extension BPMN + X qui inclut les menaces du cloud computing Chergui et Benslimane [2020]. Dans le but de simplifier le méta modèle, nous avons omis les objectifs de sécurité défini précédemment. Nous avons par la suite généré le modèle de définition d'extension de schéma XML et document de définition d'extension de schéma XML.

5.3.4 Notation graphique

Pour la notation graphique, nous avons étendu la notation graphique précédente des objectifs de sécurité de la table 5.1 avec les menaces du cloud computing de la table 5.3.

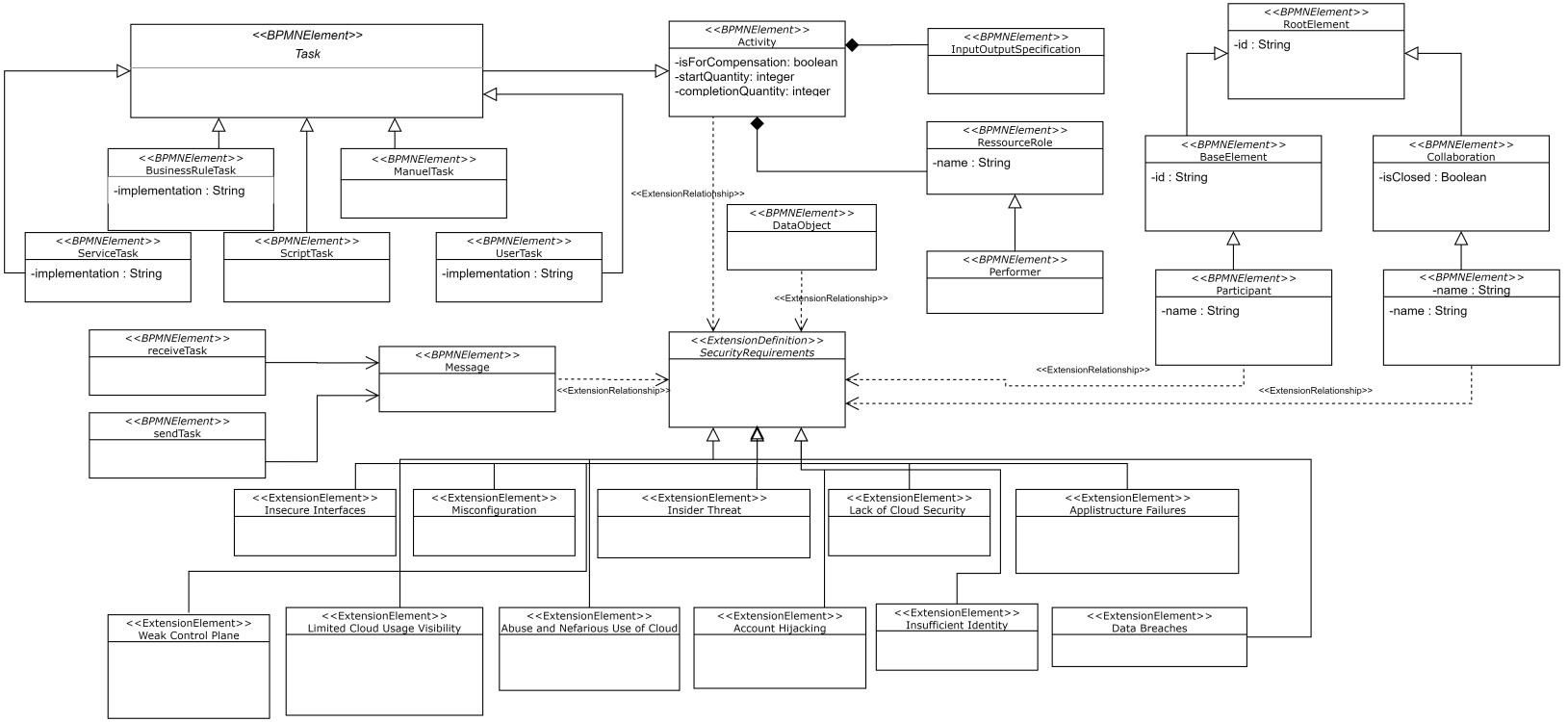


FIGURE 5.12 – *Modèle d'extension BPMN + X des menaces dans le cloud computing*

Concept	Representation	Concept	Representation
Data Breaches		Misconfiguration and Inadequate Change	
Lack of Cloud Security Architecture		Insufficient Identity	
Account Hijacking		Insider Threat	
Insecure Interfaces		Weak Control Plane	
Applistructure Failures		Limited Cloud Usage Visibility	
Abuse and Nefarious Use of Cloud Services			

TABLE 5.3 – *Extension de notation graphique avec les menaces du cloud computing*

5.3.5 Démonstration

L'outil développé précédemment à était modifié aussi afin d'inclure la palette des menaces du cloud computing avec la possibilité aussi d'annoter les processus métier avec les objectifs de sécurité. Pour illustrer la modélisation des menaces du cloud computing. Nous reprenons le même processus d'admission du patient mais nous supposons maintenant que l'exécution ça se passe dans le cloud - Figure 5.13.

Par exemple, nous avons :

- Ajouté la menace « détournement de compte (account hijacking) » à la tâche « examiner la demande d'admission » puisqu'il y a une authentification avant la validation de l'admission qui est assurée dans ce cas-là avec l'objectif « authentification ».

- Ajouté la menace « violation de données (data breaches) » aux objets « données de comptabilité » et « informations cliniques » pour signaler un risque de fuite de données sensibles.

- Appliqué la menace « identité insuffisante (Insufficient Identity) » à la tâche « enrichir la facturation » dans le service médical.

Les autres menaces, sont définies au niveau des piste comme « mauvaise configuration (Misconfiguration) », « interfaces non sécurisées (Insecure Interfaces) » et « absence d'architecture de sécurité cloud (Lack of Cloud Security Architecture) » pour signaler différentes menaces possibles au niveau des pistes.

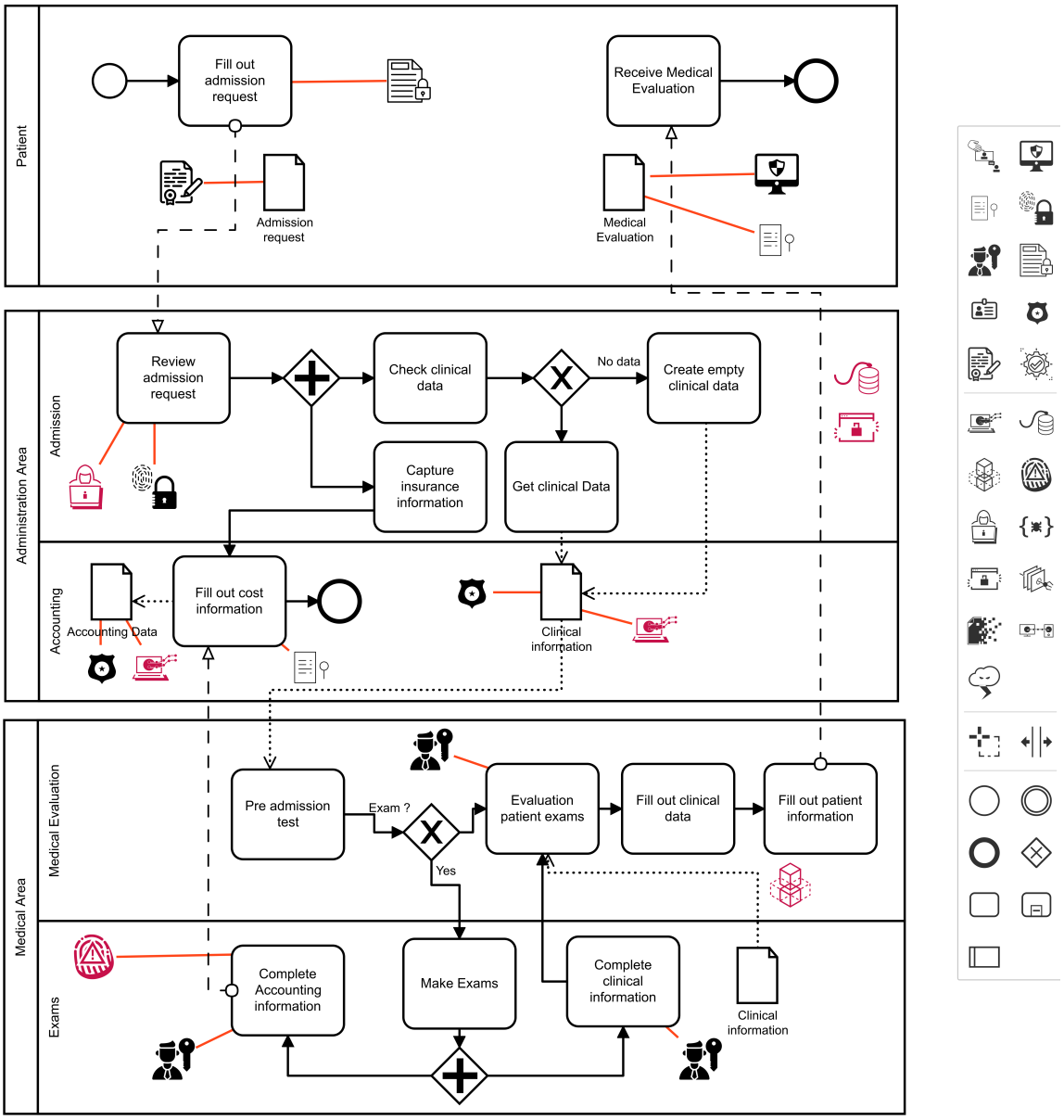


FIGURE 5.13 – *Annotation du processus métier d'admission d'un patient avec les menaces du cloud computing*

5.3.6 Evaluation

Nous avons reconduit la même expérimentation définie précédemment, nous avons présenté le processus d'admission d'un patient dans l'hôpital annoté avec les menaces de Cloud Computing. Nous avons fourni au premier groupe une matrice avec les menaces de sécurité séparées (groupe BPMN) et pour le deuxième groupe un processus métier annoté avec les menaces de sécurité. L'objectif était d'évaluer l'interprétation et la compréhension des menaces de sécurité intégré dans le processus métier.

Pour l'expérimentation nous avons demandé au même groupe d'ingénieur qui répondu précédemment de participer une nouvelle fois à l'expérimentation sur les menaces cloud computing. Nous avons posé 10 questions pour tester leur compréhension de la représentation des menaces.

Nous avons posé les questions suivantes :

— Est-ce qu'il y a une menace liée à la tâche « review admission request » ?
— Y'a-t-il un risque de « Data Breaches » sur l'objet « Accounting Data » ?
— Est-ce qu'il y a une menace de « Data Breaches » liée à la tâche « Complete Accounting information » ?
— La piste "Medical Area" contient-elle trois menaces ?
— Y'a-t-il un risque de « Insufficient Identity » sur la tâche « Complete Accounting information » ?
— La piste du patient contient-elle plusieurs menaces ?
— Est-ce qu'il y a un risque de « Data Breaches » lié à l'objet « Clinical information » ?
— Quelle sont les taches qui ont un risque de « Data Breaches » ?
— Y'a-t-il une menace de « Insider Threat » au niveau du processus d'admission ?
— Quelle sont les taches qui ont un risque de « Insufficient Identity » ?

Pour rappel, nous avons utilisé les mêmes mesures que l'expérience précédente :

— Précision : 10 questions ont été posées aux participants sur la sémantique des menaces de sécurité. Nous avons évalué leur réponse comme correcte ou incorrecte. Le score d'exactitude représente le nombre total de réponses correctes divisé par le nombre de participants.
— Temps : Nous avons enregistré le temps pris (en secondes) pour chaque participant à répondre. Le score en temps correspond au temps total nécessaire pour répondre aux 10 questions.
— Précision normalisée : Un score de précision normalisé a été calculé, qui est le score de précision d'un participant divisé par son score de temps. Le score de précision normalisé d'un participant à chaque essai correspond au nombre de réponses correctes qu'il a fournies par seconde écoulée.

Le tableau 5.4 présente les résultats de notre expérimentation. Le groupe qui a eu le processus métier annoté avec les menaces de sécurité à eu de meilleurs résultats de précision. Il faut noter que le temps de réponse a augmenté par rapport à l'autre expérience à cause de la nature des questions (nous avons inclut deux questions à choix multiples).

Comme la première expérimentation, les résultats expérimentaux indiquent que la nouvelle l'extension BPMN a eu un effet positif sur la compréhension et l'interprétation des menaces de sécurité en réduisant la charge cognitive.

	Nombre de participants	Réponses correctes	Précision	Temps	Précision normalisée
	Essai 1				
Groupe avec extension	15	93	6.20	120.38 sec	0.051
Groupe BPMN	15	71	4.73	144.14 sec	0.032
	Essai 2				
Groupe avec extension	15	99	6.60	102.57 sec	0.064
Groupe BPMN	15	83	5.53	115.31 sec	0.048
	Essai 3				
Groupe avec extension	15	117	7.80	80.81 sec	0.097
Groupe BPMN	15	106	7.07	93.88 sec	0.075
	Moyenne				
Groupe avec extension	15	103	6.87	101.25 sec	0.071
Groupe BPMN	15	86.66	5.78	117.78 sec	0.051

TABLE 5.4 – *Statistiques de performance de l'extension Cloud*

5.4 CONCLUSION

Dans ce chapitre nous avons proposé d'abord une nouvelle extension BPMN afin de permettre l'annotation des exigences de sécurité. Nous avons appliqué la méthode de [Stroppi et al., 2011] pour concevoir une extension valide qui exploite le mécanisme d'extension du BPMN 2.0 pour avoir l'interopérabilité. Dans notre approche nous avons un ensemble complet de concepts de sécurité dérivés de l'ontologie de la cybersécurité pour permettre la modélisation des exigences de sécurité.

Par la suite, nous avons adapté note extension BPMN pour répondre au besoin spéficique de la sécurité dans le cloud computing. Nous avons ajouté les menaces du cloud computing dérivées du top 11 de la CSA [Cloud Security Alliance (CSA), 2020].

Les expérimentations ont montré que notre extension augmente la compréhension des concepts de sécurité intégrés par rapport au BPMN standard avec une matrice de concepts de sécurité séparée. Les participants à cette expérimentation ont également indiqué que la conception de processus sécurisés via notre extension était préférable aux approches ad hoc.

Nous avons développé une application web qui facilite l'annotation des concepts de sécurités et des menaces du cloud computing. Nous avons illustré l'usage de l'application avec le scénario simple (admission de patients à l'hôpital). Avec notre approche, les experts de sécurité seront en mesure d'exprimer les exigences de sécurité ou les menaces directement au niveau des processus métier BPMN ce qui améliora la prise en considération des objectifs de sécurité dès la phase de modélisation.

Conclusion générale

Les sociétés adoptent de plus en plus la modélisation de processus métier pour exprimer et concevoir les exigences fonctionnelles de leur activité. La modélisation des processus métier est normalement effectuée dans un langage de modélisation tel que le langage de modélisation unifié (UML) ou le modèle de processus métier et la notation (BPMN). Ces langages de modélisation ne prennent pas en charge de manière native la sécurité des annotations, ce qui peut entraîner des problèmes importants concernant la compréhensibilité et la maintenabilité de ces modèles ad hoc. Le BPMN a été initialement développé pour fournir une notation facilement compréhensible par tous les utilisateurs métier. Nous avons utilisé BPMN comme langage de modélisation pour notre travail, parce que c'est un standard de la modélisation des entreprises et répond à l'exigence de représentation visuelle. De plus, le BPMN fournit un mécanisme d'extension qui est supporté par un large éventail d'outils de modélisation.

Les entreprises migrent leurs applications vers le cloud pour devenir plus agile, réduire les délais de mise sur le marché et réduire les coûts. Le logiciel est hébergé sur un serveur et les clients peuvent se connecter au logiciel via Internet, principalement à l'aide d'un navigateur. L'un des grands avantages ici est que les entreprises peuvent modifier leur produit relativement facilement sans avoir à distribuer les mises à jour à tous leurs clients. Au lieu de cela, ils n'ont qu'à mettre à jour le logiciel qui s'exécute sur leurs propres serveurs. Offrir un logiciel en tant que service offre également aux fournisseurs de nouveaux défis.

Le cloud computing est un exemple de modèle dans lequel les ressources informatiques sont proposées à l'utilisateur en tant que service. Dans ce contexte, l'importance de la sécurité est évidente, car les données sensibles envoyées sur Internet peuvent être consultées par des tiers non autorisés. Pour éviter les problèmes de sécurité, les utilisateurs peuvent associer des exigences de sécurité qui doivent être appliquées dans les tâches essentielles du processus métier. L'intégration d'exigences de sécurité et de conformité de haut niveau dans les processus métier est une préoccupation majeure pour la conception et l'exécution de systèmes pilotés par les processus métier. De plus, les exigences de sécurité ont été reconnues comme une préoccupation importante parmi les développeurs et les utilisateurs ce qui implique que l'association entre les processus métier et la sécurité est inévitable. De nombreuses méthodes de développement de logiciels traitent souvent la sécurité, séparément à la fin du cycle de développement. Pour nous, la modélisation des processus métier est la couche idéale pour pour décrire les exigences de sécurité.

Plusieurs approches ont été proposées pour modéliser les exigences de sécurité au niveau du processus métier. Cependant, la plupart de ces approches restent théoriques et manquent de nombreux concepts de sécurité importants. Les extensions de sécurité BPMN actuelles sont construites de manière non systématique, sans aucune preuve empi-

rique pour étayer leur choix de concepts et la plupart des extensions ne sont pas conformes à la norme BPMN 2.0. Nous avons évalué les extensions de sécurité BPMN existantes. À partir de cette revue de la littérature, nous avons pu mettre en évidence les principaux problèmes rencontrés par les extensions actuelles que notre approche vise à résoudre. Nous avons proposé des extensions de la norme BPMN pour répondre aux exigences de sécurité en premier lieu en appliquant la méthode Stroppi et al. [2011]. L'idée d'utiliser la méthode Stroppi et al. [2011] est née suite à l'examen des différentes extensions de sécurité BPMN existantes qui manquent de définition claire (syntaxe abstraite et concrète) et n'utilisent pas le mécanisme d'extension de BPMN. Nous pensons que la méthode est très utile pour avoir une extension bien définie et valide.

Comme préalable à la création de notre extension, nous avions besoin d'une ontologie des exigences de cybersécurité. Cela permet une analyse ontologique à la fois tout au long de la mise en œuvre de l'extension, garantissant que tous les concepts nécessaires ont été inclus. Heureusement, une telle ontologie a déjà été créée par (Maines et al, 2015). Ils proposent un total de 79 exigences de cybersécurité. Nous avons décidé de sélectionner un sous-ensemble (10) des concepts les plus importants pour ne pas augmenter la complexité au niveau de la modélisation. Par la suite, nous avons présenté une deuxième extension BPMN dédié à la sécurité dans le cloud computing. Nous avons ajouté les menaces du cloud computing dérives du top 11 de la CSA. Nous avons illustré usage de notre approche avec une application web qui permet l'annotation facile de la sécurité avec des concepts de sécurité ou les menaces pour le contexte du cloud computing. Nous avons appliqué notre approche sur le processus métier d'une admission à un hôpital. Notre solution propose un ensemble complet de concepts de sécurité et permet d'introduire les exigences de sécurité à un stade de développement relativement précoce pour concevoir des systèmes d'informations sécurisés. Notre approche aide à identifier et à résoudre les problèmes de sécurité lors de la conception du système, prend en charge la communication et la documentation du contrôle souhaitable pour un système afin de remédier à chaque menace.

Les futurs travaux doivent être orientés pour enrichir l'expérimentation en l'appliquant à différents domaines afin d'évaluer la capacité d'apprentissage et la prise en main de notre approche. Nous envisageons d'approfondir les techniques de modélisation des menaces pour identifier les menaces et les exigences de conformité, et évaluer leur risque. En outre, les prochaines étapes impliqueront le développement d'un framework complet de modélisation et d'exécution des processus métier prenant en charge la sécurité, avec la vérification des contraintes de sécurité pendant l'exécution. Aussi, l'étude de l'intégration de l'approche dans le DevSecOps afin de forcer l'intégration continu des objectifs de sécurité au cycle de vie de développement.

Nos contributions scientifiques

— Chergui, M. E. A., Benslimane, S. M. (2020). Towards a BPMN Security Extension for the Visualization of Cyber Security Requirements. International Journal of Technology Diffusion, 11(2), 1–17. https://doi.org/10.4018/ijtd.2020040101

— Chergui M.E.A., Benslimane S.M. (2018) A Valid BPMN Extension for Supporting Security Requirements Based on Cyber Security Ontology. In : Abdelwahed E., Bellatreche L., Golfarelli M., Méry D., Ordonez C. (eds) Model and Data Engineering. MEDI 2018. Lecture Notes in Computer Science, vol 11163. Springer, Cham. https://doi.org/10.1007/978-3-030-00856-7_14

Bibliographie

ARIS - MÉTHODE Version 9.8. Rapport technique, Software AG, 2016.

J. Galler A. Scheer et C. Kruse. Workflow management within the ARIS framework. Dans *European Workshop on Integrated Manufacturing Systems Engineering*, 1994.

Anis Abdmouleh. *Composants pour la modélisation des processus métier en productique, basés sur CIMOSA*. Theses, Université Paul Verlaine - Metz, Septembre 2004. URL https://hal.univ-lorraine.fr/tel-01750149.

M. H. Said Ahmed, Abu Ali Ibn Sina, Raju Chowdhury, et Mustaq Ahmed. An Advanced Survey on Cloud Computing and State-of-the-art Research Issues. 2012.

Naved Ahmed et Raimundas Matulevicius. A taxonomy for assessing security in business process modelling. Dans *IEEE 7th International Conference on Research Challenges in Information Science (RCIS)*. IEEE, may 2013.

Steven Alter. Information System-The Foundation of E-Business. 01 2002.

Olga Altuhhov, Raimundas Matulevičius, et Naved Ahmed. An Extension of Business Process Model and Notation for Security Risk Management. *International Journal of Information System Modeling and Design*, 4(4) :93–113, oct 2013.

A. Anagnostopoulos. *Hands-On Software Engineering with Golang : Move beyond basic programming to design and build reliable software with clean code*. Packt Publishing, 2020. ISBN 9781838550240. URL https://books.google.fr/books?id=mWbMDwAAQBAJ.

Ross Anderson, Frank Stajano, et Jong-Hyeon Lee. Security policies. *Advances in Computers*, 55 :186–237, 2001.

Nikolaos Argyropoulos, Haralambos Mouratidis, et Andrew Fish. Attribute-Based Security Verification of Business Process Models. Dans *2017 IEEE 19th Conference on Business Informatics (CBI)*. IEEE, jul 2017.

Nikolaos Argyropoulos, Haralambos Mouratidis, et Andrew Fish. Enhancing secure business process design with security process patterns. *Software and Systems Modeling*, 19 (3) :555–577, jul 2019.

Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et Matei Zaharia. A view of cloud computing. *Communications of the ACM*, 53(4) :50–58, apr 2010.

Aukfood. La methode devops. Online at https ://www.aukfood.fr/devops/, 2020.

David Basin, Samuel J. Burri, et Gunter Karjoth. Obstruction-Free Authorization Enforcement : Aligning Security with Business Objectives. Dans *2011 IEEE 24th Computer Security Foundations Symposium*. IEEE, jun 2011.

Imen Ben Said. *BPMN4V pour la modélisation de versions de processus intra- et inter-organisationnels*. PhD thesis, 2017. URL http://www.theses.fr/2017TOU10004. Thèse de doctorat dirigée par Hanachi, Chihab et Bouaziz, Rafik Informatique Toulouse 1 2017.

Hajar Benabdejlil. *Modélisation des processus de soins : vers une implantation de nouveaux services à valeur ajoutée*. Theses, Université de Bordeaux, Décembre 2016. URL https://tel.archives-ouvertes.fr/tel-01466758.

Paolo Bocciarelli et Andrea D'Ambrogio. A BPMN Extension for Modeling Non Functional Properties of Business Processes. Dans *Proceedings of the 2011 Symposium on Theory of Modeling & Simulation : DEVS Integrative M&S Symposium*, TMS-DEVS '11, page 160–168, San Diego, CA, USA, 2011. Society for Computer Simulation International.

François Bodart, Arvind Patel, Marc Sim, et Ron Weber. Should optional properties be used in conceptual modelling ? A theory and three empirical tests. *Information Systems Research*, 12(4) :384–405, 2001.

Pascal Bou Nassar. *Security management in a dynamic services' infrastructure : A risk management approach*. Theses, L'institut national des sciences appliquées de Lyon – France, Décembre 2012. URL https://tel.archives-ouvertes.fr/tel-00828598.

Abdellatif Bourjij. *Contribution à la sûreté de fonctionnement des processus industriels par les réseaux de Pétri*. PhD thesis, 12 1994.

H. Brandenburg et J.P. Wojtyna. *L'approche processus, mode d'emploi*. Ed. d'Organisation, 2006. ISBN 9782708134829. URL https://books.google.fr/books?id=lC0g2_uJFm4C.

Richard Braun et Werner Esswein. Classification of Domain-Specific BPMN Extensions. Dans *Lecture Notes in Business Information Processing*, pages 42–57. Springer Berlin Heidelberg, 2014.

Richard Braun et Werner Esswein. Towards Multi-perspective Modeling with BPMN. Dans *Lecture Notes in Business Information Processing*, pages 67–81. Springer International Publishing, 2015.

Richard Braun, Hannes Schlieter, Martin Burwitz, et Werner Esswein. Extending a Business Process Modeling Language for Domain-Specific Adaptation in Healthcare. Dans *Wirtschaftsinformatik*, 2015.

P. Briol. *Ingenierie Des Processus Metiers, de L'Elaboration A L'Exploitation*. Lulu Press, Incorporated, 2008. ISBN 9781409200406. URL https://books.google.fr/books?id=BdF6Z4vh414C.

Achim D. Brucker. Integrating Security Aspects into Business Process Models. *it – Information Technology*, 55(6), jan 2013.

Andrew Burton-Jones, Yair Wand, et Ron Weber. Guidelines for Empirical Evaluations of Conceptual Modeling Grammars. *Journal of the Association for Information Systems*, 10(6) : 495–532, jun 2009.

Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, et Ivona Brandic. Cloud computing and emerging IT platforms : Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6) :599–616, jun 2009.

Michel Cattan. *Management des processus - Une approche innovante*. AFNOR, 2000.

Centers for Medicare & Medicaid Services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Online at http ://www.cms.hhs.gov/hipaa/, 1996.

Ayman Chaâbane, Sameh Hbaieb Turki, Anis Charfi, et Rafik Bouaziz. From platform independent service composition model in BPMN 4SOA to executable service compositions. Dans *Proceedings of the 12th International Conference on Information Integration and Web-based Applications Services - iiWAS 10*. ACM Press, 2010.

David Yu Chang, Messaoud Benantar, John Yow-Chun Chang, et Vishwanath Venkataramappa. Authentication and authorization methods for cloud computing security, 2014. US Patent 8,769,622.

Saoussen Cheikhrouhou, Slim Kallel, Nawal Guermouche, et Mohamed Jmaiel. Toward a Time-centric modeling of Business Processes in BPMN 2.0. Dans *Proceedings of International Conference on Information Integration and Web-based Applications & Services - IIWAS 13*. ACM Press, 2013.

Mohamed El-Amine Chergui et Sidi Mohamed Benslimane. A valid BPMN extension for supporting security requirements based on cyber security ontology. Dans El Hassan Abdelwahed, Ladjel Bellatreche, Matteo Golfarelli, Dominique Méry, et Carlos Ordonez, éditeurs, *Model and Data Engineering - 8th International Conference, MEDI 2018, Marrakesh, Morocco, October 24-26, 2018, Proceedings*, volume 11163 de *Lecture Notes in Computer Science*, pages 219–232. Springer, 2018. URL https://doi.org/10.1007/978-3-030-00856-7_14.

Mohamed El-Amine Chergui et Sidi Mohamed Benslimane. Towards a BPMN security extension for the visualization of cyber security requirements. *Int. J. Technol. Diffusion*, 11(2) :1–17, 2020. URL https://doi.org/10.4018/IJTD.2020040101.

Audrey Dorofee Christopher Alberts. *Managing Information Security Risks*. Pearson Education (US), 2002. ISBN 0321118863. URL https://www.ebook.de/de/product/3252338/christopher_alberts_audrey_dorofee_managing_information_security_risks.html.

Cloud Security Alliance (CSA). Top threats to cloud computing : Egregious eleven. Online at https ://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/, 2019.

Cloud Security Alliance (CSA). Cloud security alliance. Online at https ://cloudsecurityalliance.org/, 2020.

Luca Compagna, Pierre Guilleminot, et Achim D. Brucker. Business process compliance via security validation as a service. Dans *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation*. IEEE, mar 2013.

Microsoft Community Contributor. Comprendre le modèle "STRIDE". Online at https ://social.technet.microsoft.com/wiki/contents/articles/51078.comprendre-le-modele-stride-fr-fr.aspx, 2018.

PCI Security Standards Council. Norme de sécurité des données. 2018.

J. Damasceno, F. Lins, R. Medeiros, B. Silva, A. Souza, D. Aragão, P. Maciel, N. Rosa, B. Stephenson, et J. Li. Modeling and Executing Business Processes with Annotated Security Requirements in the Cloud. Dans *2011 IEEE International Conference on Web Services*. IEEE, jul 2011.

Secrétariat Général De la Défense Nationale. EBIOS-Expression des Besoins et Identification des Objectifs de Sécurité. 2004.

Bernard Debauche et Patrick Mégard. *BPM - Business Process Management : Pilotage métier de l'entreprise*. Hermès - Lavoisier, 2004.

Yuri Demchenko, Canh Ngo, Cees de Laat, Tomasz Wiktor Wlodarczyk, Chunming Rong, et Wolfgang Ziegler. Security infrastructure for on-demand provisioned cloud infrastructure services. Dans *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, pages 255–263. IEEE, 2011.

Hedi Dhouibi. *UTILISATION DES RESEAUX DE PETRI A INTERVALLES POUR LA REGULATION D'UNE QUALITE : APPLICATION A UNE MANUFACTURE DE TABAC*. Theses, Ecole Centrale de Lille ; Université des Sciences et Technologie de Lille - Lille I, Décembre 2005. URL https://tel.archives-ouvertes.fr/tel-00394199.

Distributed Management Task Force. Dmtf cloud management standards. Online at https ://www.dmtf.org/standards/cloud, 2016.

Sébastien Déon. *OpenStack Cloud-computing d'entreprise, Infrastructure as a Service (IaaS)*. Eni, 2015.

Thomas Dufresne et James Martin. Methods for Information Systems Engineering : Knowledge Management and E-Business. *Process Modeling for E-Business*, 2003.

Aymeric Dussart, Benoit Aubert, et Michel Patry. An evaluation of inter-organizational workflow modeling formalisms. *J. Database Manag.*, 15 :74–104, 04 2004.

European Union Agency for Cybersecurity. Cloud security guide for smes. Online at https ://www.enisa.europa.eu/, 2015.

David Ferraiolo, Janet Cugini, et D. Richard Kuhn. Role-based access control (RBAC) : Features and motivations. Dans *Proceedings of 11th annual computer security application conference*, pages 241–48, 1995.

Fatima Zohra Filali. *Gestion de Confiance dans le Cloud Computing*. Theses, Université d'Oran 1 - Algérie, 2015.

International Organization for Standardization. Iso/iec jtc 1 information technology. Online at https ://www.iso.org/isoiec-jtc-1.html, 2014.

Organization for the Advancement of Structured Information Standards. Oasis technical committees. Online at https ://www.oasis-open.org/committees/, 2016.

Ian Foster, Yong Zhao, Ioan Raicu, et Shiyong Lu. Cloud Computing and Grid Computing 360-Degree Compared. Dans *2008 Grid Computing Environments Workshop*. IEEE, nov 2008.

Manon Froger. *Une approche d'accompagnement de la maturation BPM d'une entreprise et de la formalisation de ses processus métiers*. Theses, Ecole des Mines d'Albi-Carmaux, Février 2020. URL https://tel.archives-ouvertes.fr/tel-02903019.

Keke Gai et Saier Li. Towards Cloud Computing : A Literature Review on Cloud Computing and Its Development Trends. Dans *2012 Fourth International Conference on Multimedia Information Networking and Security*. IEEE, nov 2012.

Santorum Gaibor et Marco Oswaldo. *Isea : a Ludic Collaborative Business Process Modelling and Improvement Method*. Theses, Université Grenoble Alpes, Novembre 2011. URL https://tel.archives-ouvertes.fr/tel-00647688.

Christine Gaubert-Macon. Approche des processus organisationnels et modélisation. Rapport technique, CERTA, 2006.

Jean-Noel Gillot. *The Complete Guide to Business Process Management : Business process transformation or a way of aligning the strategic objectives of the company and the information system through the processes*. Lulu.com, 2008.

Mohamad Hamze. *Security, QoS and self-management within an end-to-end Cloud Computing environment*. Theses, Université de Bourgogne, Décembre 2015. URL https://tel.archives-ouvertes.fr/tel-01257829.

Xabier Heguy. *Extensions de BPMN 2.0 et méthode de gestion de la qualité pour l'interopérabilité des données*. PhD thesis, 2018. URL http://www.theses.fr/2018BORD0375. Thèse de doctorat dirigée par Ducq, YvesZacharewicz, Grégory et Tazi, Saïd Automatique, Productique, Signal et Image, Ingénierie cognitique Bordeaux 2018.

C. N. Höfer et G. Karagiannis. Cloud computing services : taxonomy and comparison. *Journal of Internet Services and Applications*, 2(2) :81–94, jun 2011.

ISO. Quality management standard (iso27034 :2011). Rapport technique, International Organization for Standardization, 2011.

ISO. Quality management standard (iso9001 :2015). Rapport technique, International Organization for Standardization, 2015.

ISO. Quality management standard (iso27000 :2018). Rapport technique, International Organization for Standardization, 2018a.

ISO. Quality management standard (iso27001 :2018). Rapport technique, International Organization for Standardization, 2018b.

Anya Kim, Jim Luo, et Myong Kang. Security ontology for annotating resources. Dans *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 1483–1499. Springer, 2005.

Wadha Labda, Nikolay Mehandjiev, et Pedro Sampaio. Modeling of privacy-aware business processes in bpmn to protect personal data. Dans *Proceedings of the 29th Annual ACM Symposium on Applied Computing - SAC 14*. ACM Press, 2014.

Maria Leitner, Michelle Miller, et Stefanie Rinderle-Ma. An Analysis and Evaluation of Security Aspects in the Business Process Model and Notation. Dans *2013 International Conference on Availability, Reliability and Security*. IEEE, sep 2013.

Fernando Lins, Julio Damasceno, Robson Medeiros, Erica Sousa, et Nelson Rosa. Comparative Study of Service-Based Security-Aware Business Processes Automation Tools. Dans *2013 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, oct 2013.

Curtis L. Maines, David Llewellyn-Jones, Stephen Tang, et Bo Zhou. A cyber security ontology for BPMN-security extensions. Dans *2015 IEEE International Conference on Computer and Information Technology Ubiquitous Computing and Communications Dependable, Autonomic and Secure Computing Pervasive Intelligence and Computing*. IEEE, oct 2015.

Curtis L. Maines, Bo Zhou, Stephen Tang, et Qi Shi. Adding a Third Dimension to BPMN as a Means of Representing Cyber Security Requirements. Dans *2016 9th International Conference on Developments in eSystems Engineering (DeSE)*. IEEE, aug 2016.

Raida EL MANSOURI. *Modélisation et Vérification des processus métiers dans les entreprises virtuelles : Une approche basée sur la transformation de graphes*. PhD thesis, Université Mentouri Constantine, 2009.

Houssem Medhioub. *Architectures and federation mechanisms in cloud computing and cloud networking environments*. Theses, Institut National des Télécommunications, Avril 2015. URL https://tel.archives-ouvertes.fr/tel-01217187.

Riad MEGARTSI. Etude comparative des méthodes d'analyse des systèmes de production. Master's thesis, Aix-Marseille III, 1997.

P. M. Mell et T. Grance. The NIST definition of cloud computing. Rapport technique, NIST, 2011.

Michael Menzel, Ivonne Thomas, et Christoph Meinel. Security requirements specification in service-oriented business process management. Dans *2009 International Conference on Availability, Reliability and Security*. IEEE, 2009.

Randy H. Katz Michael Armbrust, Anthony D Joseph et David A. Patterson. Above the Clouds : A Berkeley View of Cloud Computing. Rapport technique, EECS Department, University of California, Berkeley, 2009.

Microsoft. Security development lifecycle. Online at https ://www.microsoft.com/en-us/securityengineering/sdl, 2012.

Shivaji P. Mirashe et N. V. Kalyankar. Cloud Computing. *CoRR*, abs/1003.4074, 2010. URL http://arxiv.org/abs/1003.4074.

Jutta Mülle, Silvia von Stackelberg, et Klemens Böhm. A Security Language for BPMN Process Models. Rapport Technique 9, Karlsruher Institut für Technologie (KIT), 2011.

Jean-Louis Le Moigne. *La modélisation des systèmes complexes*. Dunod, 1999.

C. Morley, M.B. Figueiredo, et Y. Gillette. *Processus métiers et SI : Gouvernance, management, modélisation*. InfoPro. Management des systèmes d'information. Dunod, 2011. ISBN 9782100557059. URL https://books.google.fr/books?id=_7w-YgEACAAJ.

C Morley, J Hugues, B Leblanc, et O Hugues. *Processus métiers et SI : évaluation, modélisation, mise en oeuvre*. DUNOD, 2005.

Fadi Obeid. *Formal validation of security patterns implementation*. Theses, ENSTA Bretagne - École nationale supérieure de techniques avancées Bretagne, Mai 2018. URL https://tel.archives-ouvertes.fr/tel-02319224.

Object Management Group. Omg cloud working group. Online at https ://www.omg.org/cloud/, 2018.

OMG. Software Process Engineering Metamodel (SPEM) 2.0 Specification. Online at http ://www.omg.org/spec/SPEM/2.0/PDF/, 2008.

Open Web Application Security Project. OWASP Top Ten 2017. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017, 2017.

SNIA Organization. Cloud data management interface (cdmi). Online at https ://www.snia.org/cdmi, 2015.

Raquel M. Pillat, Toacy C. Oliveira, Paulo S. C. Alencar, et Donald D. Cowan. BPMNt : A BPMN extension for specifying software process tailoring. *Information and Software Technology*, 57 :95–115, jan 2015.

PivotalTracker. What is agile project management". Online at https ://www.pivotaltracker.com/agile/what-is-agile-project-management, 2020.

G. Plouin. *Cloud et transformation digitale - 5e éd : SI hybride, protection des données, anatomie des grandes plateformes*. Dunod, 2019. ISBN 9782100792696. URL https://books.google.fr/books?id=0vWFDwAAQBAJ.

Guillaume Plouin. *Cloud et transformation digitale 4e édition SI hybride, protection des données, anatomie des grandes plateformes*. Dunod, 2016.

Gregor Polančič. BPMN-L : A BPMN extension for modeling of process landscapes. *Computers in Industry*, 121 :103276, oct 2020.

Andrew Powell-Morse. Waterfall Model : What Is It and When Should You Use It ? Online at https ://airbrake.io/blog/sdlc/waterfall-model, 2016.

F. I. P. S. Pub. Standards for security categorization of federal information and information systems. *NIST FIPS*, 199, 2004.

Pille Pullonen, Jake Tom, Raimundas Matulevičius, et Aivo Toots. Privacy-enhanced BPMN : enabling data privacy analysis in business processes models. *Software and Systems Modeling*, 18(6) :3235–3264, jan 2019.

Sameer Rajan et Apurva Jairath. Cloud Computing : The Fifth Generation of Computing. Dans *2011 International Conference on Communication Systems and Network Technologies*. IEEE, jun 2011.

Mouna Rekik, Khouloud Boukadi, H. A. N. A. N. E. Ben-Abdallah, Rekik. Mona, et Hanêne Ben-Abdallah. Bpmn meta-model extension with deployment and security information. 2012.

A. RODRIGUEZ, E. FERNANDEZ-MEDINA, et M. PIATTINI. A BPMN extension for the modeling of security requirements in business processes. *IEICE Transactions on Information and Systems*, E90-D(4) :745–752, mar 2007.

Kawther Saeedi, Liping Zhao, et Pedro R. Falcone Sampaio. Extending BPMN for Supporting Customer-Facing Service Quality Requirements. Dans *2010 IEEE International Conference on Web Services*. IEEE, jul 2010.

Muhammad Qaiser Saleem, Jafreezal B. Jaafar, et Mohd Fadzil Hassan. A domain-specific language for modelling security objectives in a business process models of SOA applications. *INTERNATIONAL JOURNAL ON Advances in Information Sciences and Service Sciences*, 4(1) :353–362, jan 2012.

Mattia Salnitri, Fabiano Dalpiaz, et Paolo Giorgini. Modeling and Verifying Security Policies in Business Processes. Dans *Enterprise, Business-Process and Information Systems Modeling*, pages 200–214. Springer Berlin Heidelberg, 2014.

Pierangela Samarati et Sabrina Capitani de Vimercati. Access control : Policies, models, and mechanisms. Dans *International School on Foundations of Security Analysis and Design*, pages 137–196. Springer, 2000.

Koh Song Sang et Bo Zhou. BPMN security extensions for healthcare process. Dans *2015 IEEE International Conference on Computer and Information Technology Ubiquitous Computing and Communications Dependable, Autonomic and Secure Computing Pervasive Intelligence and Computing*. IEEE, oct 2015.

Lutz Schubert et Keith Jeffery. Advances in Clouds - Research in Future Cloud Computing. 2012.

Lutz Schubert, Keith Jeffery, et Burkhard Neidecker-Lutz. The Future of Cloud Computing. Rapport technique, European Commission, 2010.

Martin Schultz et Michael Radloff. Modeling concepts for internal controls in business processes – an empirically grounded extension of BPMN. Dans *Lecture Notes in Computer Science*, pages 184–199. Springer International Publishing, 2014.

International Telecommunication Union Telecommunication Standardization Sector. Focus group on cloud computing. Online at https ://www.itu.int/en/ITU-T/focusgroups/cloud/Pages/default.aspx, 2011.

Somayeh Sobati Moghadam. Secloudbpmn : A Lightweight Extension For Bpmn Considering Security Threats In The Cloud. 2018.

Andre R. R. Souza, Bruno L. B. Silva, Fernando A. A. Lins, Julio C. Damasceno, Nelson S. Rosa, Paulo R. M. Maciel, Robson W. A. Medeiros, Bryan Stephenson, Hamid R. Motahari-Nezhad, Jun Li, et Caio Northfleet. Incorporating security requirements into service composition : From modelling to execution. Dans *Service-Oriented Computing – ICSOC 2007*, pages 373–388. Springer Berlin Heidelberg, 2009.

Luis Jesús Ramón Stroppi, Omar Chiotti, et Pablo David Villarreal. Extending BPMN 2.0 : Method and Tool Support. Dans *Lecture Notes in Business Information Processing*, pages 59–73. Springer Berlin Heidelberg, 2011.

F. Swiderski et W. Snyder. *Threat Modeling*. O'Reilly Media, 2004. ISBN 9780735637696.

Synopsys. Bsimm7 presentation. Rapport technique, 2018.

Jean Talbot. Les t.i. et la réingénierie des processus. Rapport technique, HEC Montréal-MBA, 2003.

J. Thémée et J. Hennecart. *Sécurité informatique sur le Web : Apprenez à sécuriser vos applications (management, cybersécurité, développement et opérationnel)*. Epsilon (Saint-Herblain). Editions ENI, 2017. ISBN 9782409006340. URL https://books.google.fr/books?id=oGDEswEACAAJ.

Jihed Touzi. *Aide à la conception de Système d'Information Collaboratif , support de l'interopérabilité des entreprises.* PhD thesis, Institut National Polytechnique de Toulouse, 2007.

F. Vernadat. *Enterprise Modeling and Integration*. Springer Netherlands, 1996. ISBN 0412605503. URL https://www.ebook.de/de/product/6386664/f_vernadat_enterprise_modeling_and_integration.html.

Paul Voigt et Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham : Springer International Publishing*, 2017.

Christian Wolter, Michael Menzel, Andreas Schaad, Philip Miseldine, et Christoph Meinel. Model-driven business process security requirement specification. *Journal of Systems Architecture*, 55(4) :211–223, apr 2009.

Yacine Challal and Hatem Bettahar. Introduction à la sécurité informatique - non-répudiation de l'origine, 2008. URL https://moodle.utc.fr/pluginfile.php/16777/mod_resource/content/0/SupportIntroSecu/co/CoursSecurite_15.html. [En ligne ; Page disponible le 11-juillet-2020].

Sonia Yassa. *Multi-constrained optimal allocation of workflows to Cloud Computing resources*. Theses, Université de Cergy Pontoise, Juillet 2014. URL https://tel.archives-ouvertes.fr/tel-01167131.

Ali Zaidat. *Spécification d'un cadre d'ingénierie pour les réseaux d'organisations*. PhD thesis, Ecole Nationale Supérieure des Mines de Saint-Etienne, 2005.

Karim Zarour, Djamel Benmerzoug, Nawal Guermouche, et Khalil Drira. A BPMN Extension for Business Process Outsourcing to the Cloud. Dans *Advances in Intelligent Systems and Computing*, pages 833–843. Springer International Publishing, 2019.

Bo Zhou, Curtis Maines, Stephen Tang, et Qi Shi. A Framework for the Visualisation of Cyber Security Requirements and Its Application in BPMN. Dans *Computer Communications and Networks*, pages 339–366. Springer International Publishing, 2018.

Dimitrios Zissis et Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3) :583–592, mar 2012.