MoRiA Une méthode basée sur les modèles pour l'analyse des risques de cybersécurité : application à un système complexe de défense navale

Douraïd Naouar

DOCTORAT BRETAGNE LOIRE / MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

THESE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPERIEURE MINES-TELECOM ATLANTIQUE
BRETAGNE PAYS DE LA LOIRE - IMT ATLANTIQUE

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : Informatique

Par

Douraïd NAOUAR

MoRiA : Une méthode basée sur les modèles pour l'analyse des risques de cybersécurité. Application à un système complexe de défense navale

Thèse présentée et soutenue à Brest, le 30 Aout 2022
Unité de recherche : Chaire de cyberdéfense des systèmes navals, École navale, ENSTA Bretagne, IMT Atlantique, Naval Group, THALES
Thèse N° : 2022IMTA0307

Rapporteurs avant soutenance :

Nora CUPPENS	Professeur, Polytechnique Montréal
Ana CAVALLI	Professeur émérite, Télécom Sud Paris

Composition du Jury :

Président :	Kavé SALAMATIAN	Professeur, Université de Savoie Mont Blanc
Examinateurs :	Laurent NANA	Professeur, Université Bretagne Occidentale
	Nora CUPPENS	Professeur – HDR, Polytechnique Montréal
	Ana CAVALLI	Professeur émérite, Télécom Sud Paris
	Olivier ASSEU	Professeur, INPHB et ESATIC
	Slim REKHIS	Maître de conférences, Ecole Supérieur des communications de Tunis
Dir. de thèse :	Yvon KERMARREC	Professeur, IMT Atlantique
Encadrante de thèse :	Jamal EL-HACHEM	Maître de conférences, Université Bretagne Sud

Invité(s)

Julien FRANCQ	Responsable recherche & innovation cybersécurité, Naval Group
Marc PENNAMEN	Responsable développement des offres et projets cybersécurité, Thales SIX

Table des matières

Table des figures

Liste des tableaux

Introduction

Sommaire

Pour comprendre l'état futur souhaité de l'ingénierie des systèmes, il est essentiel de comprendre son passé, son évolution et son état actuel. Dans cette introduction, nous mettons en évidence les aspects clés de l'état actuel de la pratique afin d'introduire nos contributions pour ainsi aider et guider ses orientations futures. Certains considèrent l'ingénierie des systèmes comme une jeune discipline, tandis que d'autres la considèrent comme assez ancienne [BOF+14]. Quel que soit notre point de vue, les systèmes et la pratique pour les développer existent depuis longtemps. La constante de cette évolution des systèmes est une complexité toujours croissante qui peut être observée sur le plan du nombre de fonctions,

de composants et d'interfaces du système, ainsi que de leurs interactions non-linéaires et de leurs propriétés émergentes [BOF+14] (Figure 1).

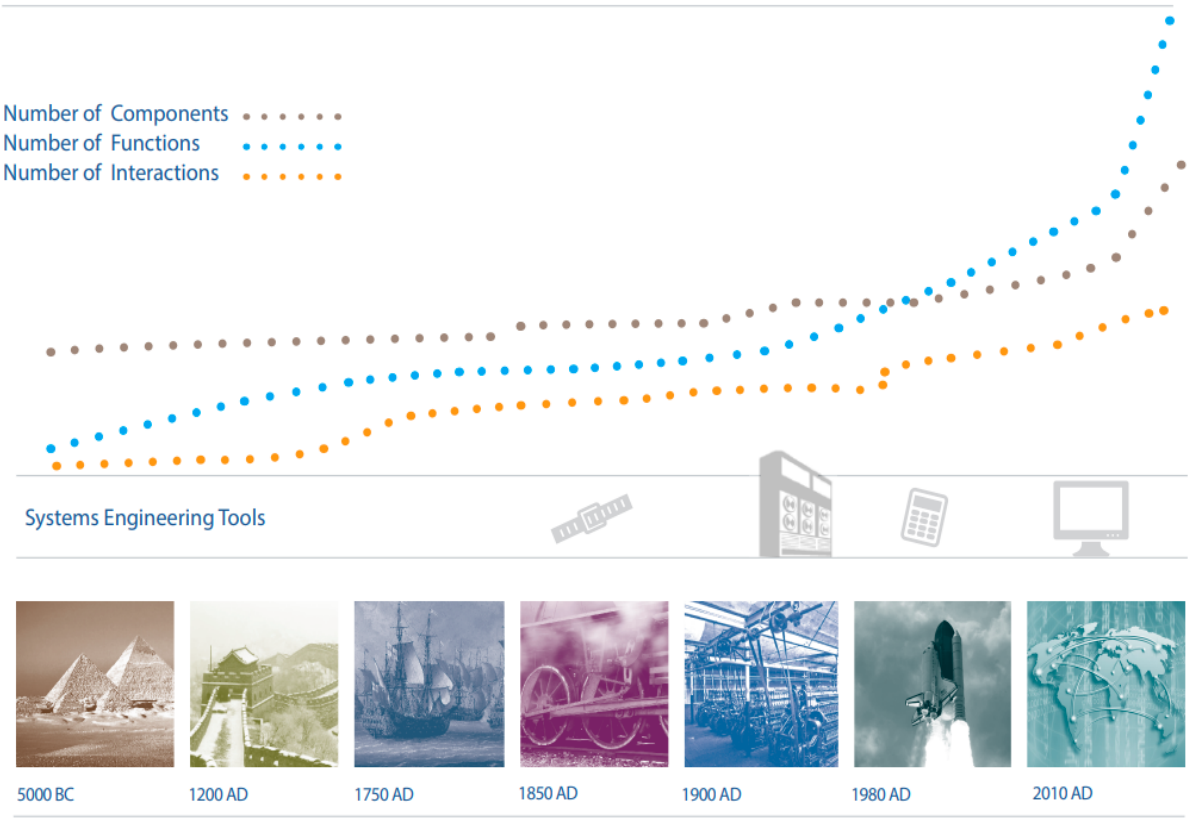


FIGURE 1: Complexification des systèmes à travers le temps [BOF+14].

Chacun de ces indicateurs de complexité a augmenté de façon spectaculaire au cours des cinquante dernières années, et continuera à augmenter en raison des fonctionnalités et services que les parties prenantes (clients, prestataires, gouvernements et organismes de réglementation...) exigent ainsi que des progrès effectués et attendus sur les technologies nécessaires à leur réalisation. C'est pour cela que les pratiques d'ingénierie des systèmes continueront d'évoluer par rapport aux pratiques actuelles pour répondre aux exigences des systèmes complexes et des environnements de travail du XXIe siècle. L'exploitation des technologies de l'information et l'établissement des fondements théoriques des pratiques d'ingénierie des systèmes axées sur la "valeur" [Fon14][BBI18][CH11] ouvriront la voie afin d'optimiser le calendrier, le coût et le risque technique des projets. Pour répondre à ces demandes de compétitivité, de complexité et de satisfaction des besoins en constante évolution des parties prenantes, les méthodes d'ingénierie des systèmes devront s'adapter au domaine et être extensibles à la taille et à la complexité des projets et des systèmes. La pratique

de l'ingénierie des systèmes traitera les systèmes dans un contexte de systèmes à grande échelle, en évolution dynamique et fortement interconnectée. Les pratiques de conception et d'analyse de l'architecture permettront d'intégrer les différents points de vue des parties prenantes afin de créer des systèmes plus conformes aux exigences et efficaces. Les éléments moteurs de la conception, tels que les considérations de cybersécurité et la résilience, devront être identifiés, analysés et préparés à être intégrés à la solution dès les premières phases de l'ingénierie. Comme l'illustre la figure 2, les recherches montrent que 80% des efforts et les décisions prises qui affectent la sécurité au début du cycle de vie notamment avant la génération des exigences d'un système permettent à la fois de réduire les coûts dus aux changements de conception et d'accroître la capacité à influer sur les performances d'un système [CAB+19][FM84][SNMG08]. Il est logique que les efforts en matière de cybersécurité suivent un schéma similaire et il devient donc avantageux d'aborder la sécurité dès le début du cycle de développement en particulier lors des phases d'analyse de besoin et de conception de système.

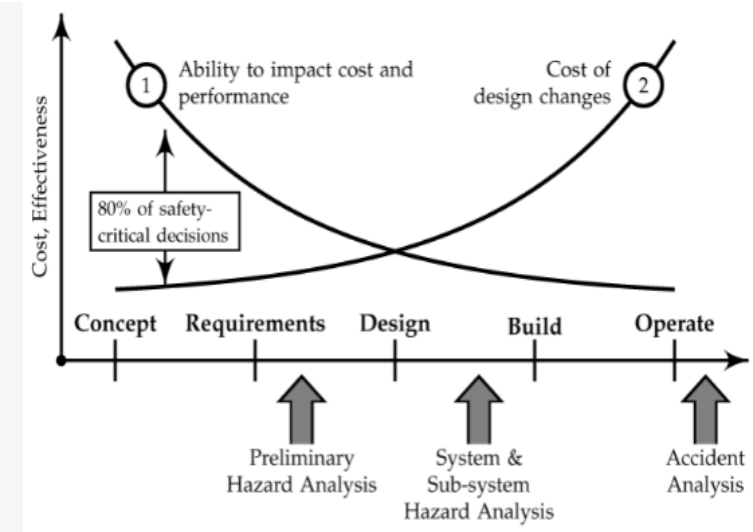


FIGURE 2: Coûts et efficacités des modifications en fonction des étapes du cycle de vie d'un système [CAB+19].

Contexte et Identification des problématiques

.1 L'Ingénierie des Systèmes Basée sur les Modèles - ISBM

Dans le langage courant, nous qualifions souvent une chose de complexe lorsque nous ne pouvons pas comprendre entièrement sa structure ou son comportement : elle est incertaine, imprévisible, compliquée ou tout simplement difficile. Sillitto [Sil09] décrit l'incapacité d'un esprit humain à saisir l'ensemble d'un problème complexe et à en prévoir le résultat comme une complexité subjective. La complexité objective de Sillitto décrit les caractéristiques techniques ou systémiques qui conduisent à la complexité ou à la difficulté subjective. En tant qu'ingénieurs système, nous avons la possibilité de modifier ces caractéristiques ; ce sont également celles qui sont le plus souvent abordées par la science des systèmes complexes. Le processus standard d'ingénierie des systèmes décompose un problème en partie, de manière récursive, jusqu'à ce que les parties soient suffisamment simples pour que nous les comprenions et puissions concevoir des solutions ; nous réassemblons ensuite les parties pour former la solution globale. Cette approche fonctionne bien pour les systèmes dont les parties interagissent de manière fixe (également connus sous le nom de systèmes "compliqués" - un exemple pourrait être une voiture), même s'il y a de nombreuses parties en interaction et que les systèmes peuvent avoir un comportement imprévisible. D'autres systèmes, en revanche, présentent des problèmes importants lorsqu'ils sont analysés de manière fragmentaire. Des systèmes tels que les réseaux de transport comportent des parties autonomes dont les interactions conduisent à des modèles de comportement auto-organisés émergents ou les systèmes navals [GER12] qui comportent les cinq aspects (structurel, comportemental, contextuel, temporel et perceptuel) d'un système complexe comme défini par Rhodes et Ross [RR10a][RR10b]. Dans ces systèmes, définis ici comme des systèmes "complexes", les propriétés émergentes qui nous intéressent vraiment ne sont pas compréhensibles du point de vue des parties prises isolément. C'est surtout sur ces systèmes que nous nous concentrerons dans ce mémoire.

Comme évoqué précédemment, les nouveaux systèmes développés par les industriels ne cessent de se complexifier et nécessitent de prendre en compte des besoins et des contraintes de plus en plus considérables concernant les comportements, les services, ainsi que les nouvelles interdépendances nécessaires ou attendues [BOF+14][Sch17][Pat19]. Ces exigences

clients et/ou utilisateurs sont principalement formulés sous forme d'exigences textuelles, puis analysées et traduites en exigences système par les équipes d'ingénierie [Voi17]. Elles sont ensuite introduites dans les projets d'ingénierie système et logiciels en tant que propriétés fonctionnelles et non fonctionnelles, en particulier la sécurité, qui doivent être satisfaites par le système conçu (figure 3)[Voi17][BCV11][PRRT14].

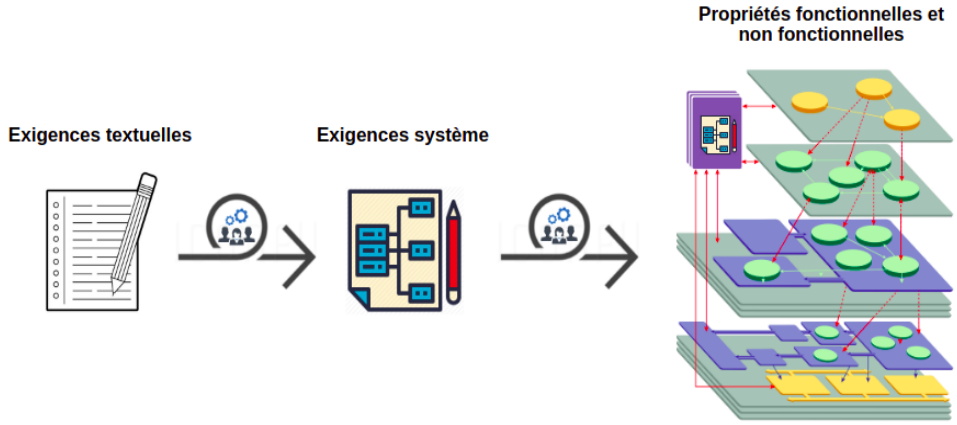


FIGURE 3: Représentation schématique de l'analyse et transformation des exigences textuelles en propriétés que le système va devoir satisfaire.

La satisfaction de ces propriétés implique des processus rigoureux qui pilotent le projet, depuis l'identification et la définition des exigences jusqu'au déploiement et à la maintenance du système [MBC+20]. Pour cela, un certain nombre de normes portant sur l'ingénierie système et son cycle de vie ont été élaborées et utilisées au cours de ces dernières années.

.1.1 Les normes de l'ingénierie système

L'ingénierie des systèmes utilise des normes qui décrivent les activités menées au cours des phases du cycle de vie d'un système. Les normes fournissent les références communes nécessaires pour structurer et institutionnaliser les pratiques d'ingénierie système tout au long du cycle de vie du système (figure 4). Elles proposent des moyens de communication et de coopération entre les utilisateurs et les organisations du domaine. De plus, la présence de normes est un indicateur de maturité, de développement et d'acceptation du domaine considéré [RFB10]. Dans notre travail, nous nous concentrons en particulier sur la norme **ISO 15288 :2015 «Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système»[ISO15]** qui formalise l'ensemble des processus de l'ingénierie système. Elle

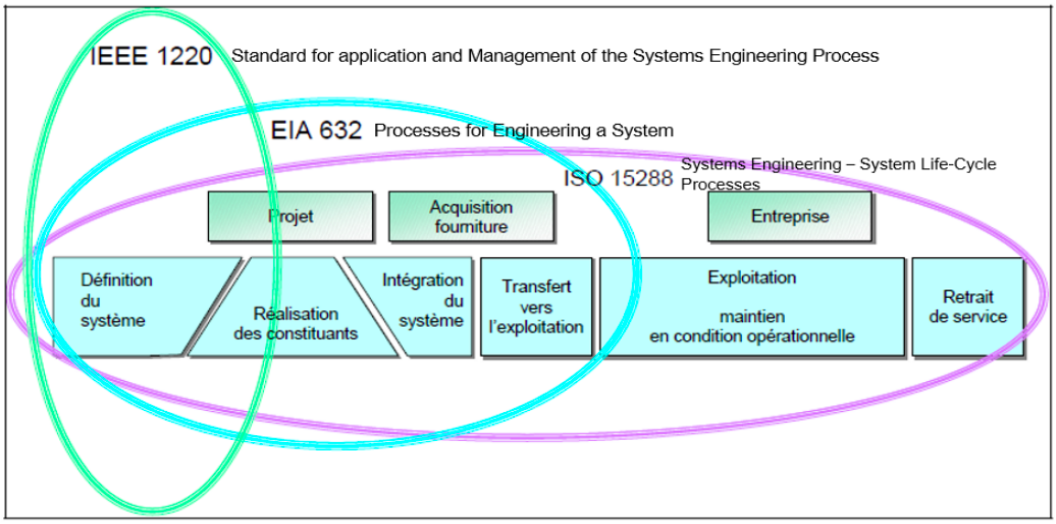


FIGURE 4: Couverture des normes au cours du cycle de vie du projet

les organise autour de quatre thèmes : processus techniques, processus de gestion de projet, processus relatifs aux accords et processus d'entreprise. De plus, elle propose une définition de cycle de vie générique d'un système. Pour gérer les contraintes et le contexte opérationnel, un certain nombre de modèles ou de méthodologies SDLC (System Development Life Cycle) implémentant et s'appuyant sur ces normes ont été créés.

.1.2 Cycle de vie du développement des systèmes

Le cycle de vie du développement de systèmes (SDLC) est le processus global de développement, de mise en œuvre et de retrait des systèmes d'information par le biais d'un processus en plusieurs étapes allant de l'étude de faisabilité initiale, l'analyse, la conception, la mise en œuvre et la maintenance jusqu'à l'élimination. Le SDLC est utilisé pour définir les phases et les étapes de la conception d'un système en donnant une structure et un cadre rigides. Il existe de nombreux modèles et méthodologies SDLC différents, mais chacun d'entre eux consiste généralement en cinq phases (exigences, conception, développement, test et déploiement).

10. Figure modifiée à partir de : https ://www.checkmarx.com/glossary/a-secure-sdlc-with-static-source-code-analysis-tools/

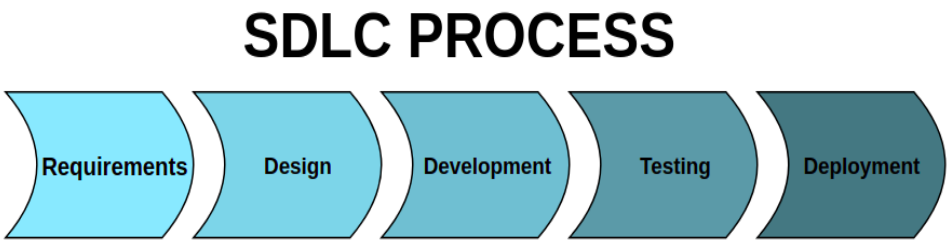


FIGURE 5: Processus de cycle de vie du développement des systèmes [10]

1. **Exigences :** Au cours de cette phase, toutes les informations pertinentes sont recueillies auprès du client afin de développer un produit conforme à ses attentes. Avant de construire un produit, il est très important d'avoir une compréhension ou une connaissance du contexte du produit.
2. **Conception :** Dans cette phase, les exigences recueillies dans le document de spécification sont utilisées comme données d'entrée afin de dériver l'architecture logique et physique qui sera utilisée pour la mise en œuvre du développement du système.
3. **Développement :** La mise en œuvre commence dès que le développeur reçoit le document de conception. La conception du logiciel est traduite en code source et les composants sont mis en œuvre dans cette phase.
4. **Test :** Tous les modules sont rassemblés dans un environnement de test spécial, puis vérifié pour détecter les erreurs, les bogues et l'interopérabilité. Les testeurs se réfèrent au document de spécification des exigences pour s'assurer que le logiciel est conforme à la norme du client.
5. **Déploiement :** Une fois le produit testé, il est déployé dans l'environnement de production ou bien un test d'acceptation par l'utilisateur est effectué en fonction des attentes du client.

.1.2.1 Cycle de vie du développement des systèmes sécurisés

Quel que soit le modèle SDLC utilisé, la sécurité doit être intégrée au SDLC afin de garantir une protection appropriée des informations que le système transmettra, traitera et stockera ainsi que la résilience et protection des services et fonctions que le système doit réaliser. L'application du processus de gestion des risques au développement des systèmes permet aux organisations d'équilibrer les exigences de protection des informations et des actifs de l'agence avec le coût des contrôles de sécurité et des stratégies d'atténuation tout

au long du SDLC. Les processus de gestion des risques identifient les actifs et les opérations critiques, ainsi que les vulnérabilités systémiques dans l'ensemble de l'organisation. Pour réaliser cela, un processus aligné sur le cycle de vie du développement des systèmes a vu le jour (Secure SDLC)[Mat17].

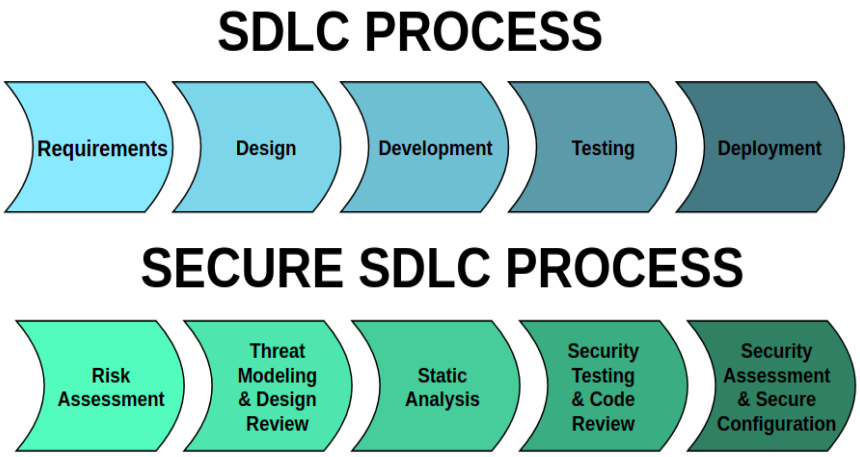


FIGURE 6: Processus de Cycle de vie du développement des systèmes [11]

1. **Exigences et évaluation des risques :** Au cours de la phase d'exigence, les équipes établissent le besoin d'un système et documentent son objectif. La planification de la sécurité doit commencer dès la phase d'exigence et consister en des activités visant à établir les exigences de sécurité et à évaluer les besoins en matière de sécurité. Ici, l'évaluation des risques de sécurité nous aide à définir les caractéristiques fonctionnelles du système nécessitant un besoin de sécurité. Au cours de cette étape, les équipes déterminent également la nécessité d'une modélisation des menaces, de revues, de la conception de la sécurité et de tests de pénétration. Au stade des exigences, on prend en compte les préoccupations en matière de disponibilité et d'intégrité des services du système ainsi que le respect de la vie privée et les mesures relatives à la sensibilité des données.
2. **Conception et modélisation des menaces :** La conception détaillée du système et de l'architecture est soutenue par la modélisation des menaces de sécurité dans le but de réduire la surface d'attaque. Les solutions de conception et d'architecture doivent être revues en permanence en fonction de l'évolution de la menace.

11. Figure modifiée à partir de : https ://www.checkmarx.com/glossary/a-secure-sdlc-with-static-source-code-analysis-tools/

3. **Test de sécurité et analyse de code :** La SSDL met l'accent sur l'application de normes pour éviter les failles de sécurité et pour détecter les risques de sécurité potentiels. Ces activités comprennent l'utilisation d'outils automatisés et la réalisation de revues de code manuelles ou d'architecture pour capturer et corriger les erreurs.
4. **Déploiement et l'évaluation de la sécurité :** Au cours de cette phase, les systèmes et les produits sont en place et fonctionnent, des améliorations et/ou des modifications du système sont développées et testées, et des composants matériels et logiciels sont ajoutés ou remplacés. Les équipes doivent surveiller en permanence les performances du système pour s'assurer qu'elles sont conformes aux exigences préétablies des utilisateurs et de la sécurité, et que les modifications nécessaires sont apportées au système.

Dans cette thèse, les travaux proposés se situent lors des phases 1 et 2 afin d'améliorer les stratégies de prévention des défauts tôt dans le SDLC. Pour cela, nous avons étudié les moyens de compréhension et de représentation utilisés dans l'ISBM lors de ces phases.

.1.3 L'ingénierie des systèmes basée sur le modèle

Les normes de l'ingénierie système prescrivent les processus à mener pour le développement et le pilotage d'un système. Elles se concentrent principalement sur le "quoi ?" et peu sur le "comment ?". La réponse à cette dernière interrogation est destinée aux méthodes d'ingénierie système.

Des revues de la littérature ont été réalisées [CM16][HS21][GBT+20] pour rechercher des études de cas industriel qui pouvant éclairer la décision de soutenir ou non le processus de modification, l'investissement, la formation et les outils nécessaires pour mettre en œuvre une approche ISBM dans toutes les entreprises d'ingénierie système. La question posée était la suivante : comment justifier le passage d'une approche d'ingénierie des systèmes basée sur les documents (ISBD) à une approche d'ingénierie des systèmes basée sur les modèles (ISBM) ? Les études de cas avec des mesures sur les coûts et le calendrier ont principalement attribué le succès à la capacité d'une approche ISBM à améliorer les stratégies de prévention des défauts. La principale conclusion est qu'il y a un avantage significatif à la performance du projet en appliquant une approche ISBM. Une approche ISBM a rendu les processus d'ingénierie plus efficaces en améliorant l'exhaustivité, la cohérence et la communication des exigences à travers une ligne de conduite plus claire grâce à la représentation visuelle qui permet de déceler les erreurs. Le travail devient plus efficace et la collaboration plus

fluide, ce qui permet de booster la productivité de l'entreprise. Elle facilite non seulement la compréhension collective, mais améliore aussi les stratégies de prévention des défauts tôt dans le cycle de vie du développement du système (SDLC). De par ces avantages, nous faisons le choix d'adopter l'approche ISBM pour nos travaux.

L'objectif principal de l'ISBM est de soutenir l'ingénierie des systèmes par la modélisation pour les processus énoncés dans la norme ISO/IEC/IEEE 15288 :2015 et affinés dans les normes EIA/IEEE 632 et 1220. Des travaux [Ala19] ont été menés pour référencer les processus techniques de la norme pour les dériver en un processus générique de phases/perspectives de modélisation d'un système (figure 7) afin de faciliter la modélisation cohérente et, parfois, agile du système.

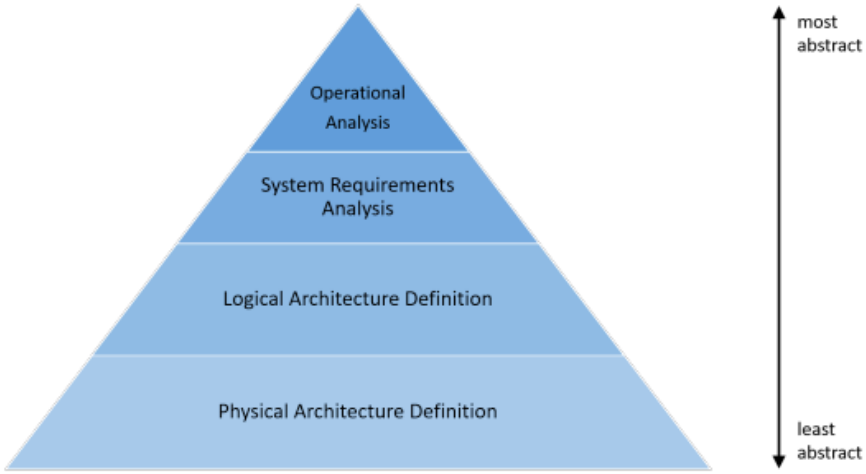


FIGURE 7: Étapes de travail génériques pour le développement de l'architecture, dérivé de la norme ISO 15288 - processus techniques

1. **Analyse opérationnelle** Se concentre sur l'analyse des besoins et des préoccupations des parties prenantes et les traduit en spécifications d'exigences. Sur la base des besoins des parties prenantes, des objectifs commerciaux ou de mission de haut niveau sont identifiés et modélisés à l'aide d'artefacts spécifiques pour créer la formulation la plus abstraite des exigences, appelée cas d'utilisation ;
2. **Analyse des exigences du système** Les exigences des parties prenantes sont utilisées pour dériver les exigences fonctionnelles et non fonctionnelles du système. Elles sont utilisées pour identifier les fonctions internes que le système doit exécuter. L'architecture fonctionnelle du système est ensuite décrite en termes fonctionnels, indépendamment de sa technologie ;

3. **Définition de l'architecture logique :** Une architecture logique est une représentation abstraite des composants du système, indépendamment de leurs solutions techniques, de manière à ce que chaque fonction du système puisse être réalisée par un composant logique correspondant ;
4. **Définition de l'architecture physique :** Ce point de vue définit l'architecture physique du système, qui consiste en un arrangement d'éléments physiques. Le but de cette architecture est de développer une solution technique en support à une architecture logique.

L'utilisation de l'ISBM a prouvé son efficacité pour faire face à la définition fonctionnelle ainsi que de la complexité croissante de ces systèmes [BMP13][SG13] en formalisant le processus de modélisation du développement du système en matière d'exigences, de conception, d'analyse, de vérification et de validation par l'utilisation de modèles. Cependant, la cybersécurité est un domaine assez jeune [EM17] et les experts s'attendent à ce que le nombre et la gravité des cyberattaques augmentent au cours des prochaines années et ont donc exprimé des préoccupations croissantes quant à la protection de ces systèmes [Fis14].

.1.3.1 La sécurité dans le contexte de l'industrie 4.0

La sécurité informatique de ces systèmes ainsi modélisés devient une question majeure pour le monde industriel. Tout particulièrement, dans le contexte actuel appelé l'usine du futur ou Industrie 4.0 [Sch17] caractérisé par des systèmes de plus en plus connectés et par l'intégration de plus en plus forte de technologies numériques dans le processus de définition. L'actualité est riche en cyberattaques, que ce soit afin de voler des identifiants, faire en sorte que certains systèmes ou sites web soient dans l'incapacité de fonctionner, ou encore de bloquer des postes de travail en chiffrant les données. Les techniques d'attaque évoluent et se perfectionnent. De simples virus des années 1990, détectables par leur signature, on est passé à des logiciels malveillants, complexes, capables de communiquer avec l'extérieur, pouvant s'enrichir et se propager ainsi que prendre le contrôle à distance des installations. Pour exemple, nous avons les attaques réalisées sur les systèmes de pilotage d'installation industrielle avec Wanacry [Sym17] [MDCM18] qui par effet collatéral a entraîné des arrêts d'usine et des pertes d'exploitation, l'attaque Stuxnet [FMC11] qui avait pour objectif de détruire les capacités de production d'uranium de l'Iran et enfin de l'attaque Triton [DPDC18] qui visait a rendre inopérant les systèmes de sécurité. Compte tenu de la fréquence et de l'impact de ces attaques, les entreprises sont de plus en plus enclines à initier et intégrer une

démarche de sécurisation de leur système d'information. Pendant longtemps, ces risques ont été négligés : les installations industrielles étaient peu connectées aux réseaux de l'entreprise ou à internet. L'évolution de la technologie, les usages ainsi que les besoins ont conduit à relier ces systèmes aux autres réseaux, que ce soit pour le transfert de données, la maintenance à distance ou encore les mises à jour. Le facteur aggravant de cet état de fait est que, dans le cadre des systèmes complexes existants, les technologies et protocoles ont été conçus à une époque où les cyberattaques n'existaient pas, ils sont donc vulnérables et peu sécurisés. Nous pouvons prendre par exemple les cas des sous-marins, porte-avions et frégates [KK19][Smi17][dSGB17] qui réalisent une refonte à mi-vie entraînant une vingtaine d'années de différence technologique. Le risque est donc bien réel, il convient donc de l'identifier, l'évaluer et le maîtriser d'où la sémantique cybersécurité. Le terme "cyber" est un préfixe provenant du mot grec *Kubernêtikê* signifiant "diriger, gouverner". La cybersécurité concerne la sécurité informatique des systèmes connectés à internet et appartenant au cyberespace qui englobe l'extension de notre espace naturel par internet. Les experts pensent que les nations, les groupes malveillants et les individus mal intentionnés vont intensifier leurs attaques contre les entreprises, les états et les particuliers au cours de la prochaine décennie [RAC14]. Pour établir des contre-mesures efficaces pour maîtriser et limiter ces dégâts, nous avons étudié les processus d'analyse, de modélisation, de gestion et de communication des risques.

.2 L'analyse de risque et sa prise en compte dans la définition des systèmes

Dans la démarche de mise en place de bonnes pratiques de cybersécurité, l'analyse des risques est une étape majeure. Elle permet de positionner le niveau optimal et adéquat de sécurité dans tous les composants d'un Système d'Information, et ceci en fonction des besoins des métiers et des clients. L'analyse des risques est le processus qui consiste à caractériser, gérer et informer les personnes concernées sur l'existence, la nature, l'ampleur, la prévalence, les facteurs contributifs et les incertitudes des pertes potentielles[Mod06]. Dans les systèmes d'ingénierie, la perte peut être externe au système, en étant causée par le système à un ou plusieurs actifs (par exemple, les humains, l'organisation, les actifs économiques et l'environnement). La perte peut également être interne, causant des dommages uniquement au système. Par exemple, dans un bateau, la perte pourrait être une impossibilité de naviguer due à un dysfonctionnement de la boucle d'énergie ou un dommage humain ou matériel dû

à une incapacité de la boucle auxiliaire. Le premier cas est un risque interne au système, et le second représente une perte causée par le système (notre bâtiment naval) aux personnels et matériels à bord. Du point de vue de l'ingénierie, le risque ou la perte potentielle est associé à l'exposition des actifs aux dangers, et est souvent exprimé comme une combinaison de la probabilité ou de la fréquence du danger et de ses conséquences (les blessures ou les pertes de vie, les coûts de reconstruction, la perte d'activité économique, les pertes environnementales, etc.). Dans les systèmes d'ingénierie, l'analyse des risques est effectuée pour quantifier le montant des pertes potentielles et, plus encore, les éléments du système qui contribuent le plus à ces pertes. À travers l'analyse, des objectifs doivent être fixés en termes de niveaux de risque acceptables. Cependant, ce ne sont généralement pas les ingénieurs qui décident de l'acceptation des risques des systèmes. Les décisions sont proposées et prises par les gestionnaires de risques/analystes de sécurité/ingénieurs sécurité et validés/acceptés par les décideurs (client, service juridique et commercial...) qui sont influencés par l'environnement économique, la presse, l'opinion publique, les groupes d'intérêt, etc. Cet aspect souligne également l'importance de la communication des risques entre les différentes parties et acteurs concernés.

.2.1 L'évolution du contexte et paradigme de l'analyse de risque

Une approche traditionnelle de l'analyse des risques a consisté à concevoir ou à réglementer les systèmes d'ingénierie en utilisant une approche forteresse [JT19][Gre98][LO09][BFM13] afin d'éviter les risques. Il s'agit par exemple du paradigme de défense en profondeur dans l'industrie nucléaire, qui comprend de multiples barrières de sécurité, de grandes marges de sécurité, un contrôle de la qualité et des inspections fréquentes.

L'expérience et la recherche ont montré que ce paradigme, était justifié souvent au contexte et moyen de l'époque : système d'information peu ou pas interconnecté, champ de la menace peu développé, réglementation et état de l'art peu mature . . . [Kha20][LO09][And16]. Cette approche conduit cependant à des systèmes, des produits et des technologies coûteux que la société et le marché ne pourraient pas se permettre d'appliquer et d'entretenir. En outre, ces études ont également montré que si certaines conceptions et réglementations basées sur les approches forteresses semblent réduire le risque des systèmes et produits d'ingénierie complexes, cela entraîne un certain coût et n'assure pas le niveau de sécurité attendu.

12. https://www.slideshare.net/Comsoce/prsentation-mthode-ebios-risk-manager

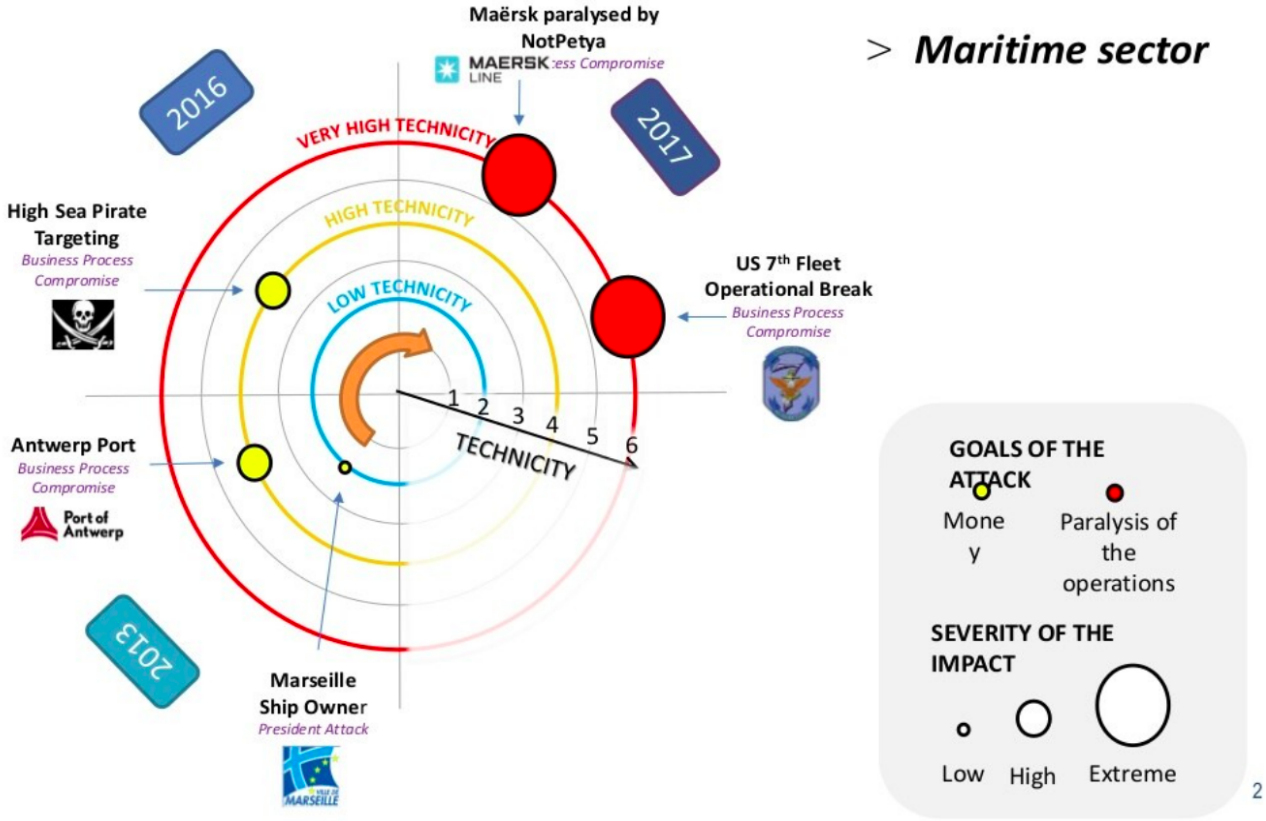


FIGURE 8: Sophistication et objectifs des attaques dans le secteur naval de ces dernières années [12]

Dans le domaine maritime, selon une étude réalisée par l'ANSSI (Figure 8) entre 2013 et 2017, la gravité et la technicité des attaques réalisées ont augmenté de même que les objectifs de celles-ci qui sont passés d'une intention monétaire à une intention de paralyser les opérations de l'organisation.

Conscients de ces problèmes, ainsi que de l'évolution du contexte numérique (prolifération des menaces, attaques de plus en plus sophistiquées, impacts importants et une réglementation plus mature ainsi qu'un état de l'art plus évolué). Les industries et les organismes de réglementation se sont progressivement appuyés sur des techniques d'analyse des risques moins systématiques basés sur la collaboration avec les experts d'autres domaines afin de mieux identifier les besoins et risques encourus. L'analyse des risques peut être utilisée à toutes les étapes de la conception, du développement, de la construction et de l'exploitation des systèmes d'ingénierie.

.2.2 La structure d'une analyse de risque

Le National Research Council [C+83] définit l'analyse des risques comme comportant trois éléments essentiels : l'évaluation des risques, la gestion des risques et la communication des risques. Les interactions et les chevauchements entre ces trois éléments illustrés dans la figure 9 sont présentés et expliqués dans les sous-sections suivantes.

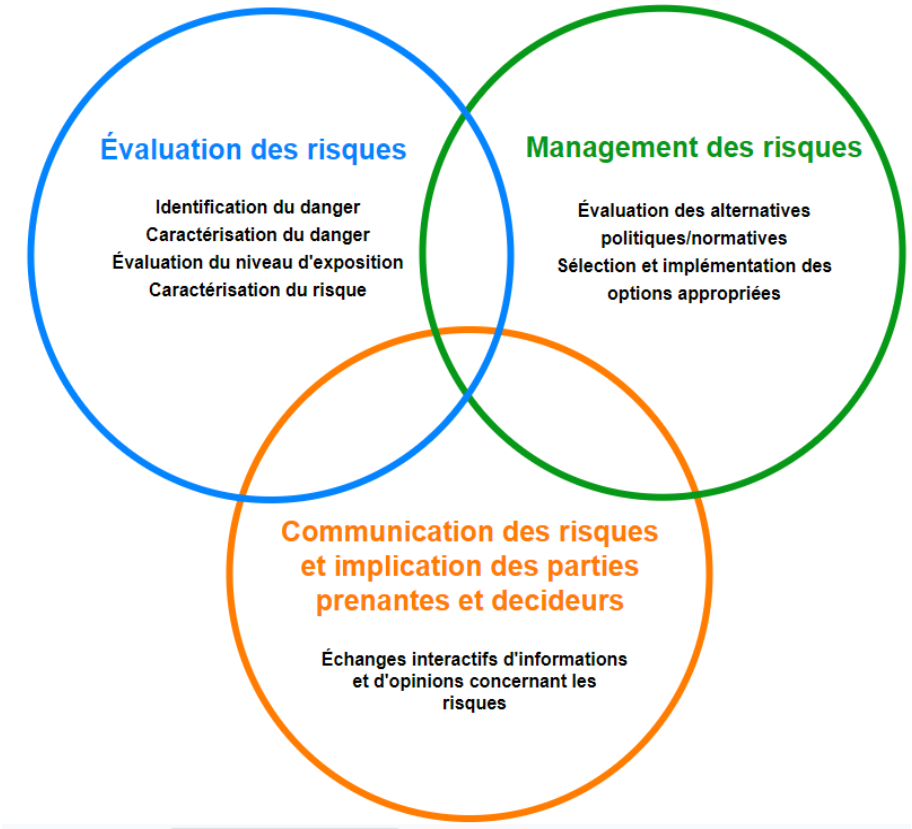


FIGURE 9: Les trois éléments essentiels de l'analyse de risque.

Le premier élément central de l'analyse des risques est l'évaluation des risques, le processus par lequel la probabilité ou la fréquence d'une perte par ou pour un système d'ingénierie est estimée et l'ampleur de la perte (conséquence) est également mesurée ou estimée. La gestion/management des risques est le processus par lequel la probabilité ou la fréquence du risque est estimée, évaluée, minimisée et contrôlée. La communication du risque est le processus par lequel les informations sur la nature du risque (perte attendue) et les conséquences, l'approche d'évaluation du risque et les options de gestion du risque sont échangées, partagées et discutées entre les décideurs et les autres parties prenantes. L'analyse de risques est une étape préalable à toute sécurisation de système d'information, et permet d'évaluer les

éventualités et les conséquences plausibles de multiples risques, avant de décider des actions à mener et de leur ordonnancement. Cela permet de réduire ces risques à un niveau acceptable. Chaque risque est identifié, quantifié, qualifié et priorisé par rapport aux critères de son évaluation et à ses impacts sur l'entreprise. S'il existe des données historiques adéquates sur ces pertes, le risque peut être directement estimé à partir des statistiques de la perte réelle. Cette approche est souvent utilisée dans les cas où les données sur ces pertes sont facilement disponibles. L'autre option concerne les cas où il n'y a pas suffisamment de données sur les pertes réelles. Dans ce cas, la perte est "modélisée" dans l'analyse du risque. La perte potentielle (c'est-à-dire le risque) est donc estimée. Dans la plupart des cas, les données sur les pertes sont faibles ou même indisponibles, en particulier pour les systèmes d'ingénierie complexes. L'analyste doit donc modéliser et estimer le risque. On distingue généralement trois types d'analyse du risque : quantitative, qualitative et un mélange des deux. Tous ces types d'analyse sont largement utilisés, chacune ayant des objectifs, des forces et des faiblesses différents.

.2.2.1 L'évaluation des risques

L'évaluation des risques est une analyse scientifique et systématique visant à identifier ou à quantifier les probabilités et impacts des pertes subies en raison de l'exposition à des dangers provenant de sources de menaces diverses. D'une manière générale, une évaluation des risques revient à répondre à trois questions très fondamentales posées par Kaplan et Garrick [KG81]. 1. Que peut-il se passer (événements redoutés) ? 2. Quelle en est la probabilité ? 3. Quelles sont les pertes (conséquences) ? La réponse à la première question conduit à l'identification de l'ensemble des scénarios indésirables, nos événements redoutés (par exemple, l'accident). La deuxième question nécessite d'estimer les probabilités de ces scénarios, tandis que la troisième estime l'impact des pertes potentielles. Ces questions amènent à l'élaboration de scénarios d'accidents qui sont une partie intégrante de la définition et de l'évaluation du risque. L'élaboration de scénarios de risques commence par un ensemble d'événements initiateurs qui perturbent ou interagissent avec le système. Pour chaque événement initiateur, l'analyse se poursuit en déterminant les événements supplémentaires (par exemple, sous forme d'erreurs matérielles, logicielles ou humaines, de propagation, de latéralisation, ou modification) qui peuvent entraîner des conséquences indésirables. Ensuite, les effets finaux de ces scénarios sont déterminés (par exemple, la nature de l'impact : financier, fonctionnel, l'image, l'environnement, etc., et l'ampleur de toute perte). La probabilité ou la fréquence de chaque scénario est également déterminée à l'aide de méthodes quantitatives ou qualitatives

pour ensuite estimer les conséquences attendues (valeurs des pertes). Enfin, la multitude de ces scénarios est assemblée pour créer un profil de risque complet du système. Le processus d'évaluation des risques consiste donc principalement en l'identification et l'élaboration de tous les scénarios possibles, le calcul de leurs probabilités individuelles et une description cohérente des conséquences qui résultent de chacun.

.2.2.2 La gestion/management des risques

L'évaluation des risques se concentrant sur l'identification, la quantification et la caractérisation des incertitudes liées aux pertes, la gestion des risques devient essentiellement/principalement un effort pour gérer ces incertitudes. La gestion des risques est une pratique impliquant des activités ayant pour objectif de prévenir, contrôler et minimiser les pertes encourues en raison d'une exposition au risque, en pesant les alternatives et en sélectionnant les actions appropriées en tenant compte des valeurs du risque, des contraintes économiques et technologiques ainsi que des questions juridiques, normatives et politiques. L'objectif principal de la gestion des risques tout au long du cycle de vie d'un système consiste à prendre des décisions proactives pour évaluer continuellement le risque, décider quels sont les risques plus importants et qui doivent donc être traités, employer des stratégies pour éviter, contrôler ou minimiser ces risques et évaluer continuellement l'efficacité des stratégies ou les réviser si nécessaire.

La gestion des risques est la partie la plus importante et la plus diversifiée de l'analyse des risques. Elle fait intervenir de nombreuses disciplines, des experts en la matière aux analystes des risques ainsi que les décideurs. Comme l'environnement/contexte interne et externe d'un système change, l'évaluation des risques change également, il s'agit donc d'un effort continu qui doit être maintenu tout au long de la vie du système. Suite au résultat de l'évaluation des risques, la gestion du risque va impliquer l'identification des principaux facteurs de risques lorsque ces derniers sont connus, le processus d'identification et d'analyse des stratégies pour éviter, contrôler et minimiser le risque commence. La première tâche consiste à déterminer si les facteurs de risque sont si importants qu'ils font augmenter le risque total ou entraînent un dépassement des limites d'acceptation du risque. Une fois que la nature et l'impact des facteurs de risque importants sont connus, des stratégies alternatives pour leur gestion doivent être proposées. Généralement, une analyse simple sous la forme d'un jugement subjectif d'experts, d'un brainstorming ou en s'appuyant sur des directives et exigences normatives, législatives ou du client est utilisée pour proposer ces stratégies.

Cette tâche consiste à évaluer et à sélectionner la stratégie la plus prometteuse et la plus efficace pour “éviter le risque” (changement de contexte, modification de la conception, etc.), pour “contrôler le risque” (compartimentation, stratégies de crise, protection, etc.) et pour “minimiser le risque” (ajout de redondances, de diversités, de barrières de réduction de l’exposition dans la conception, l’exploitation et la maintenance du système). Les stratégies se présentent souvent sous la forme d’une attribution de responsabilités, d’une détermination de l’approche appropriée du risque (recherche plus poussée, acceptation, atténuation ou surveillance). Lorsque celle-ci est choisie, il faut la surveiller dans le temps pour mesurer son impact et procéder à des ajustements et à des révisions lorsque cela est jugé nécessaire et afin que la stratégie évolue. L’évaluation et la gestion des risques sont étroitement liées et se renforcent mutuellement (figure 10). L’évaluation des risques est utilisée pour comprendre

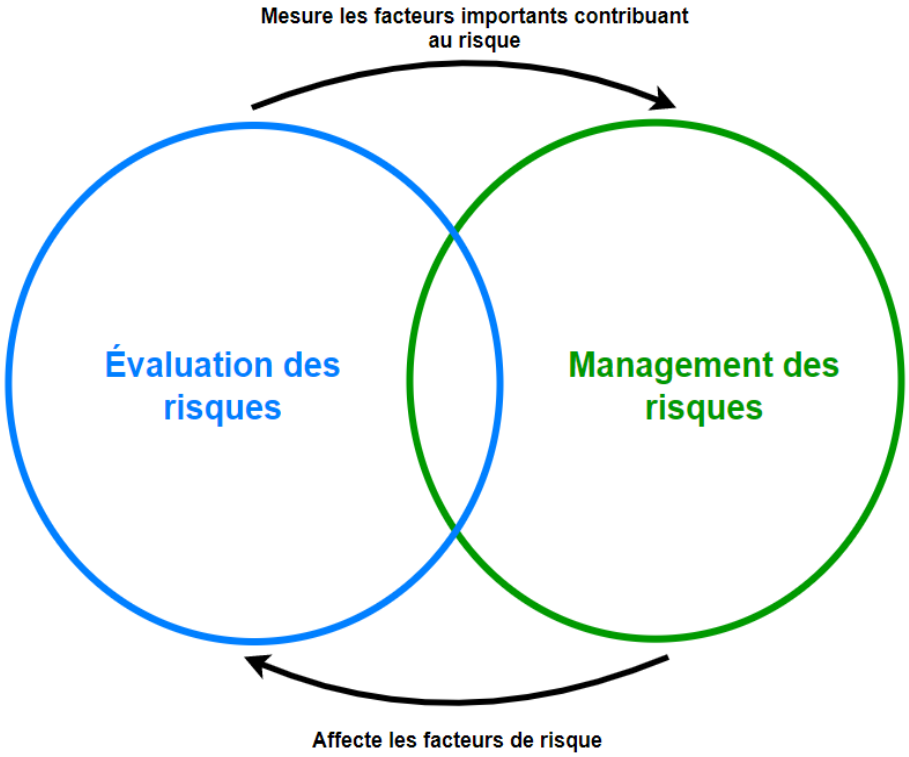


FIGURE 10: Relation entre l’évaluation et la gestion des risques.

les facteurs de risque et mesurer leurs changements au fil du temps. La gestion du risque utilise les valeurs de ces facteurs pour élaborer une stratégie basée sur l’expertise ainsi que les normes pour éviter, contrôler, minimiser et suivre les facteurs de risques importants. Une fois qu’une nouvelle stratégie est adoptée, la valeur du risque change et peut conduire à des facteurs de risque nouveaux et différents. Ceci peut être validé par d’autres efforts d’évaluation du risque, et ainsi le cycle itératif continue.

.2.2.3 Communication des risques

La communication des risques est l'activité consistant à échanger et à partager des données, des informations et des connaissances sur les risques, les résultats de l'évaluation des risques et l'approche de la gestion des risques entre les décideurs, les analystes et les autres parties prenantes. Les informations peuvent porter sur l'existence, la forme, la probabilité, la gravité, l'acceptabilité, la remédiation ou d'autres aspects du risque. Un élément clé de toute communication efficace est une représentation claire de l'élaboration de la nature des options envisagées pour parvenir à une stratégie ou une politique de sécurité et les mesures qui sont ou seront prises pour gérer le risque. La communication doit argumenter la justification du choix d'une option spécifique de gestion des risques et l'efficacité de cette option. De plus, la communication peut servir à l'élaboration de l'analyse et la gestion des risques en servant de supports collaboratifs entre les experts métiers et ceux de la sécurité.

Toute organisation est continuellement exposée à un nombre croissant de menaces et de vulnérabilités, nouvelles ou changeantes, qui peuvent affecter son fonctionnement ou la réalisation de ses objectifs. L'identification, l'analyse et l'évaluation de ces menaces et vulnérabilités sont le seul moyen de comprendre et de mesurer l'impact du risque encouru et donc de décider des mesures et contrôles appropriés pour les gérer. Pour cela, des normes de bonnes pratiques de management des risques appliqué aux systèmes d'information ainsi que leur processus de mise en œuvre ont vu le jour.

.2.3 La sécurité des systèmes d'information

Ces dernières années, de nombreuses normes et guides ont été proposées dans le domaine de la sécurité des systèmes d'information. Une partie de ces normes propose une démarche pour le management des risques dans la lignée de la norme ISO 31000, Management du risque – Lignes directrices, qui fournit des principes, un cadre et des lignes directrices pour gérer toute forme de risque. Notamment, nous retrouvons la famille de normes ISO 2700X (Figure 11).

FIGURE 11: Principales normes de la famille ISO 27000 [Fla19]

La famille de normes ISO 2700X définit les bonnes pratiques pour la gestion de la sécurité des systèmes d'information en décrivant les principes et les lignes directrices du management des risques ainsi que les processus de mise en oeuvre au niveau stratégique et opérationnel. Dans le cadre de cette thèse ; nous nous concentrons sur :

1. **la norme ISO 27000 :** qui donne une vue d'ensemble et définit le vocabulaire du domaine et des concepts utilisés ;
2. **la norme ISO 27001 :** qui propose une démarche permettant à une organisation de mettre en oeuvre et d'améliorer le système de management de la sécurité informatique (SMSI) et donne des exigences normatives pour le développement et l'utilisation d'un SMSI ;
3. **la norme ISO 27005[ISO08] :** qui décrit le processus de management du risque de la sécurité de l'information conforme à la norme ISO 31000. Elle s'appuie sur les concepts généraux spécifiés dans les normes 27000 et 27001 ;

Ce processus amène à la définition des éléments essentiels pour une bonne gestion de la sécurité des systèmes d'information. Ils ont par la suite été utilisés comme point de

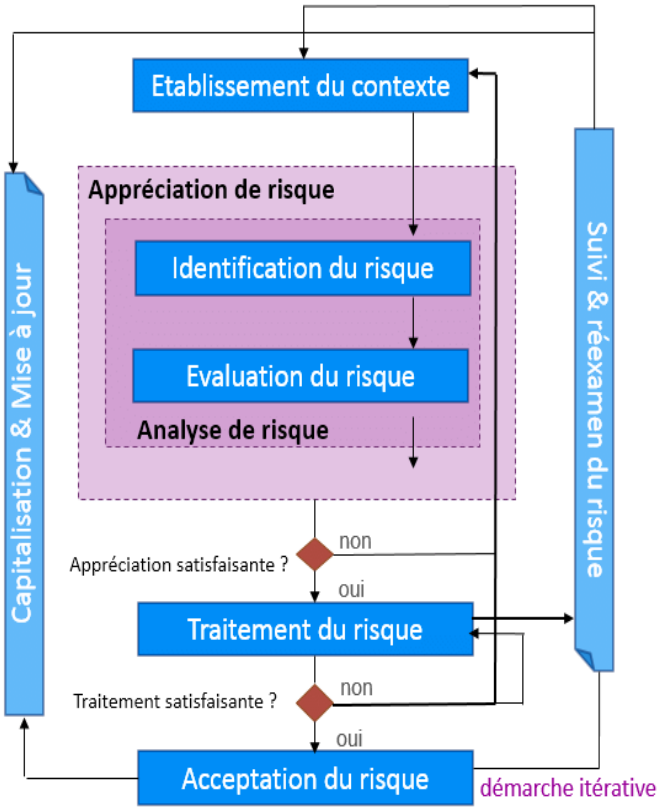


FIGURE 12: Processus de gestion des risques [Laj17]

départ pour la construction de méthodes d'analyse de risques reconnus au niveau international et utilisés dans les environnements industriels/opérationnels sous différents noms et représentations.

.3 Problématique

Les nouveaux besoins et exigences en matière de sécurité et notamment de cybersécurité se faisant de plus en plus importants, leurs intégrations dans les phases de conception des systèmes soulèvent des défis nouveaux et spécifiques [MBC+20]. Le domaine/secteur de la cybersécurité a connu une croissance exponentielle au cours de la dernière décennie, de nouvelles vulnérabilités sont identifiées quotidiennement et de nouvelles menaces continuent d'émerger et exploitent ces vulnérabilités [Run20], ce qui fait de la cybercriminalité l'un des risques les plus importants pour les industries de toutes tailles et de tous les secteurs

[Ven19][Wol10][Edd20]. La protection de ces systèmes industriels devient une tâche de plus en plus importante. En plus des problèmes de sécurité traditionnels, la complexité est amplifiée depuis que nous sommes entrés dans l'ère de l'industrie 4.0 [Sch17], dans laquelle notre dépendance vis-à-vis des services fournis par les systèmes cyber-physiques a augmenté de façon spectaculaire.

Lors du développement des systèmes complexes, l'analyse de risque reste une démarche coûteuse et souvent réalisée de façon épisodique/discontinue alors que le domaine de la cybersécurité se veut changeant et évoluant au jour le jour [MBC+20]. L'analyse de risque est fréquemment menée en amont ou en parallèle de la phase de conception par des ingénieurs et analystes en sécurité. Qui, à partir des exigences textuelles ainsi que de premières réflexions système vont, avec leurs vocabulaires, supports, méthodes et outils, définir et identifier les risques, leurs niveaux de menaces ainsi que les moyens de remédiation à mettre en œuvre. Une fois cela fait, l'intégration des résultats de l'analyse va être réalisée dans un premier temps à travers des propriétés fonctionnelles et non fonctionnelles qui par la suite devront transparaître à travers d'éléments de modèle ou choix d'architectures système à mettre en place (figure 13) au plus tôt pour réduire les coûts et identifier les points de sécurité clé à mettre en place. Les "architectes", responsables de la conception d'un système, connaissent bien la conception de l'architecture du système, mais ne sont pas toujours bien formés à la sécurité [MBC+20]. Ainsi, ils peuvent ne pas traiter et/ou prendre en compte de façon appropriée les aspects de sécurité, tels que les concepts d'actif, de vulnérabilité, d'attaque et de risque, lors de la conception de systèmes. Cependant, les architectes sont généralement capables d'imaginer une solution de conception préliminaire, en adaptant une solution "générique" à un contexte "particulier". Pour cela, ils peuvent utiliser soit un langage de description d'architecture (ADL) ad hoc, soit un langage générique standardisé tels que UML [OMG15b] ou SysML [OMG15a]. Pour aider les équipes d'architecte et de sécurité à mener à bien la sécurité par la conception, il est essentiel qu'ils puissent appréhender, échanger et prendre en compte les préoccupations de l'autre à travers une représentation et un vocabulaire partagé.

Néanmoins, à ce jour, aucune démarche ou processus de communication et de co-ingénierie n'ont été clairement définis avec les acteurs métiers du système [MBC+20]. L'absence de référence, représentation ainsi que vocabulaire partagé conduit à des incohérences, une mauvaise maîtrise de l'intégration ou corrections des éléments de sécurité [SDF16] lors de l'évolution du système, écosystème ou de son contexte. L'analyse de risque est dissociée de l'ingénierie du système d'un point de vue sémantique, méthodologique et du cycle de vie, et donc lorsque l'analyse de risque est modifiée/actualisée, la prise en compte et la com-

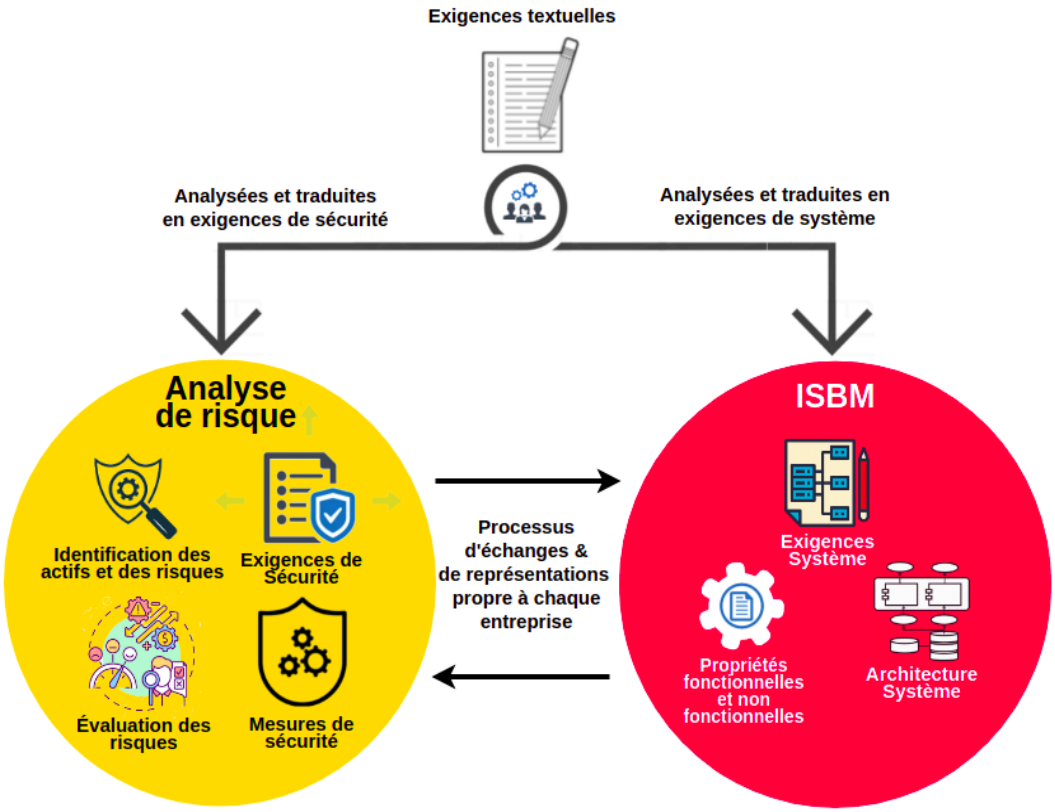


FIGURE 13: Représentation schématique du processus d'analyse de risque et de son intégration dans le déroulement et la conception du système.

munication de son impact sur l'ingénierie du système et ses équipes reste très limitées, et vice-versa.

Les approches et méthodologies d'analyse de risques récentes[CBB+16][ABB15], proposent et aident à consolider le processus collaboratif en mettant en avant des supports ainsi que des ateliers de collaboration pour intégrer et prendre en compte les préoccupations de chacun. Cependant, ils n'offrent pas les moyens de co-ingénierie des exigences de système et de sécurité, et ne proposent pas un processus structuré et sémantiquement justifié pour intégrer l'évaluation des risques de cybersécurité dans l'ingénierie des exigences.

.3.1 Domaine d'application : La Chaire de Cyberdéfense des Systèmes Navals

La cyberdéfense a été érigée au rang de priorité nationale par le Livre blanc de la défense et la sécurité nationale de 2013. L'École navale, l'ENSTA Bretagne, l'IMT Atlantique, Naval

Group et Thales ont depuis une vingtaine d'années une tradition d'échanges scientifiques et de collaborations dans les domaines des systèmes navals, des systèmes d'informations et de télécommunications. Dans cette vision, une Chaire de Cyberdéfense des Systèmes Navals a été créée pour mutualiser autour d'un programme de recherche les ressources humaines, scientifiques et techniques issues de la coopération académique et industrielle entre ces acteurs. À travers une production scientifique menée entre autres dans le cadre de doctorats, cette chaire industrielle participe à la réflexion et à la prospective en matière de cybersécurité des systèmes industriels, couvrant un large spectre de sa composante navale.

Comme nous l'avons évoqué précédemment, l'évolution de l'ingénierie système se dirige vers une co-ingénierie interdisciplinaire avec notamment la cybersécurité. L'application de la recherche en cybersécurité sur les processus d'ingénierie système des systèmes complexes est, en effet, particulièrement importante à l'heure où les navires/bâtiments – civils ou militaires sont considérés comme tels et utilisent un grand nombre de systèmes informatiques contrôlant notamment des actionneurs mécaniques d'importance critique, ou permettant au navire de communiquer, se localiser, percevoir son environnement opérationnel.

Toute bénéfique qu'elle soit en termes d'efficacité, de précision et de sûreté, la présence de ces systèmes informatiques peut ouvrir et amener des brèches ou vulnérabilités exploitables par l'attaquant ainsi que des exigences de sécurité entraînant des modifications de l'architecture du système. C'est pour cela qu'il est judicieux de réfléchir à ces problématiques dès les premières phases de modélisation/définition du système afin d'identifier, évaluer les risques et de mettre en place et tracer les éléments de sécurité adéquats ainsi que de suivre leurs évolutions et maintient tout au long du cycle de vie du système. La co-ingénierie des systèmes et de leur sécurité basée sur les modèles est au cœur des travaux de recherche présentés dans ce mémoire.

.3.2 Objectifs

À l'instar des approches utilisées pour la sûreté [SS04], la qualité [FFC09] et d'autres projets axés sur la performance, la cybersécurité ne doit pas être considérée comme un «projet» ponctuel. Elle doit plutôt être considérée à travers les éléments fonctionnels et les propriétés des éléments du système existant, ayant une définition, une représentation et un impact sur leur environnement afin de répondre aux besoins émergents de représentation et d'évaluation des risques lors des phases de définition des besoins et de modélisation [MBC+20] [NVPB19]. La sécurité des systèmes est passée d'une question technique unidimensionnelle à

une question bidimensionnelle qui comprend une dimension technique (liée aux défis et aux problèmes associés à la technologie disponible et à l'infrastructure des systèmes) et une dimension sociale (qui comprend les questions et les problèmes liés à l'élicitation et à l'analyse correctes des exigences de sécurité et à l'implication des humains dans la sécurisation des systèmes). Pour prendre en compte efficacement ces deux dimensions, nous soutenons qu'il est essentiel que la sécurité soit prise en compte dès les premières étapes et tout au long du cycle de vie du développement et qu'une méthodologie d'ingénierie système sécurisée solide doit être développée pour soutenir l'analyse simultanée des deux dimensions de la sécurité. Ce processus est une partie essentielle de ce que l'on appelle la «sécurité par la conception», dans laquelle les préoccupations de sécurité sont prises en compte dès le début de l'effort d'ingénierie du système, afin d'identifier et évaluer la gravité des événements redoutés et leur impact, de réduire les coûts et les risques globaux du projet [HCB+20], et de permettre des compromis entre les préoccupations de cybersécurité et d'autres préoccupations fonctionnelles et non fonctionnelles [Hon13] [EG12] [Pap17]. Cela est aussi appuyé par la Vision 2025 de l'INCOSE [BOF+14], qui a inclus la sécurité, et en particulier la cybersécurité, comme l'une des huit caractéristiques clés du système souhaitées par les parties prenantes. Elle propose que les ingénieurs système abordent la cybersécurité comme une propriété fondamentale du système qui doit être comprise, analysée et intégrée dans la conception du système. L'ISBM est une solution clé compte tenu de sa capacité à manipuler, créer, gérer et partager des modèles à un niveau d'abstraction plus élevé, à adapter le langage de modélisation générique (UML [13] et SysML [14]) avec les concepts liés à la sécurité, et à effectuer des analyses de sécurité avec des outils supplémentaires [NAY17].

Les objectifs de cette thèse sont : 1) de combler le fossé entre l'analyse et la modélisation des exigences fonctionnelles et non fonctionnelles du système ; et 2) l'analyse et la modélisation des risques de cybersécurité analogues et leur maintien et mise à jour tout au long de la durée de vie du système. Pour atteindre ces objectifs, nous devons répondre aux questions de recherche QR suivantes :

QR1 **Comment co-ingénierier et modéliser les exigences de système et les exigences de sécurité permettant l'intégration et l'évaluation des risques de cybersécurité tout au long de l'ingénierie système ?**

(a) **Comment permettre aux architectes et experts de sécurité de co-identifier et co-définir les besoins pour co-modéliser un système com-**

13. UML : Unified Modeling Language
14. SysML : Systems Modeling Language

plexe ?

(b) **Comment représenter les métriques et les concepts permettant l'analyse de risques dès les premières phases du cycle de vie (en particulier les phases d'analyse des besoins et d'architecture) ?**

QR2 **Comment assurer une mise à jour de l'architecture et de l'analyse de risque tout au long de la durée de vie du système ?**

L'analyse de risques de sécurité et l'ingénierie système travaillent sur le même sujet (le système), mais avec des points de vue et objectifs différents. Une collaboration entre ces deux domaines permettrait de regrouper les points fort inhérents à ces domaines et de renforcer la définition du contexte de l'analyse, sa cohérence globale ainsi que la prise en compte des préoccupations et les enjeux de l'un et de l'autre.

.3.3 Contributions

Les contributions de cette thèse s'illustrent par la méthode MoRiA : **Mo**del-based Cyber **Ri**sk **A**nalysis qui étend les méthodes ISBM existantes, adaptées et reposant sur des normes pour permettre l'analyse des risques à travers les modèles. Cette méthode permet de remplir le fossé entre deux domaines de recherche : les processus d'analyse de risque et d'ingénierie système dirigée par les modèles.

Pour répondre à la première QR1, la première contribution QR1.a est l'identification des éléments fondamentaux à la réalisation d'une analyse de risque ainsi que ceux nécessaires à la définition et la conception d'un système. Cette identification permet de distinguer les éléments structurants et inhérents aux deux processus et possédant des concepts partagés assurant ainsi la cohérence entre la vision des architectes système et les réflexions et résultats de l'analyse ainsi qu'une compréhension plus complète et conforme au système :

- Pour cela, nous proposons un alignement sémantique et conceptuel entre les concepts de modélisation de systèmes fonctionnels et les concepts d'analyse de risques, ces deux notions travaillent souvent sur les mêmes éléments, mais sous des formes ou des vocabulaires différents, par conséquent, un alignement est nécessaire pour identifier, coupler et implémenter les concepts partagés, ainsi que ceux qui ne sont pas partagés, mais nécessaires pour réaliser une analyse de risques ;

La seconde contribution QR1.b porte sur la représentation de ces concepts dans les

différentes perspectives de l'ingénierie système notamment à travers une représentation concrète de ces concepts comme extension d'un langage de modélisation existant. À travers cette contribution, MoRiA implique :

- Un langage de modélisation MoRiAML pour représenter les concepts et les mesures du risque de sécurité, permettant ainsi une modélisation précise du risque et son évaluation ultérieure ainsi que son processus d'utilisation ;
- MoRiA sera appliquée et évaluée à travers son implémentation comme une extension de la méthode industrielle existante ISBM Architecture Analysis and Design Integrated Approach (ARCADIA) et de son outil de modélisation Capella. Nous avons étendu ARCADIA en incorporant les concepts d'EBIOS Risk Manager, une méthode créée par l'Agence Nationale de la Sécurité et des Systèmes d'Information (ANSSI) permettant l'expression des besoins et l'identification des objectifs de sécurité.

Notre méthode permettra à l'instar de la figure 2 de regrouper le processus d'ingénierie système et d'analyse de risque afin de co-définir et co-modéliser les 2 domaines avec un vocabulaire et une représentation adaptés et compréhensibles pour l'un et l'autre (Figure 14).

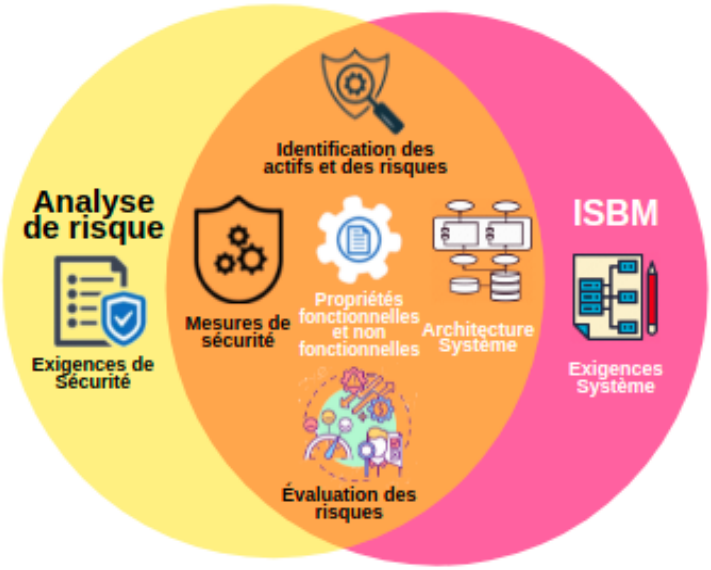


FIGURE 14: Représentation schématique des différents domaines étudiés et leurs axes d'application/d'interfaçage.

Pour répondre à notre QR2, nous proposons une extension de l'analyse de risque grâce à son couplage avec une méthode de modélisation des procédés d'intrusion sur un réseau

informatique appelée aussi kill chain dans les modèles d'ingénierie grâce aux éléments de sécurité définis et associés dès les premières étapes de l'analyse. Cet enrichissement permet à travers une couverture de tous les concepts de sécurité un suivi itératif du niveau de risque lors des modifications des exigences et critères de sécurité ou système et qui à travers le processus d'utilisation de MoRiA permettra donc de façon itérative et grâce au lien de traçabilité entre les modèles, une maintenance et un suivi de l'analyse accrus tout au long du cycle de vie du système. Cela contribue à un troisième interfaçage : Le principe de cyber kill chain apporté par l'ingénierie et implantant la démarche d'analyse de risque. La figure 15 illustre ce nouvel axe d'intersection.

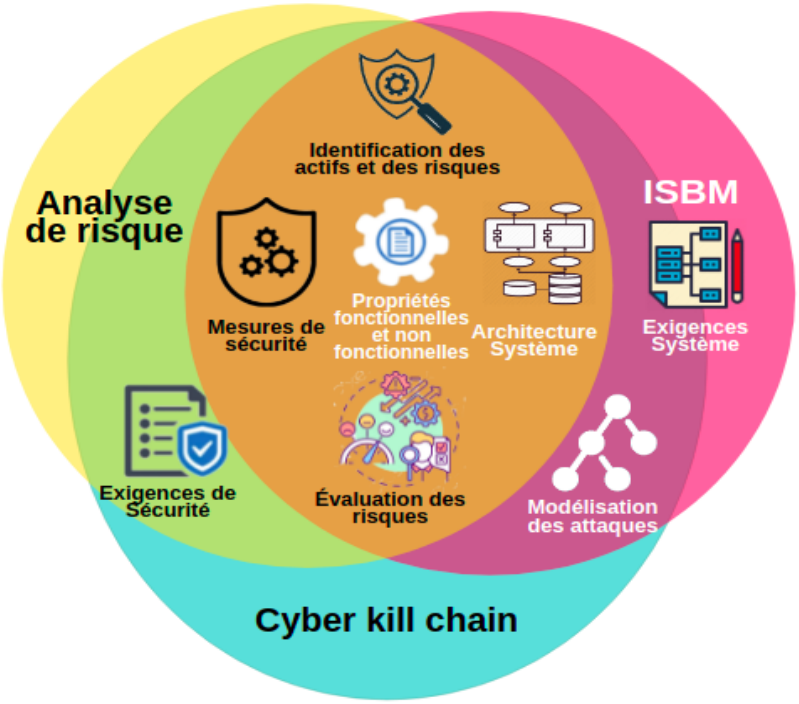


FIGURE 15: Représentation schématique des différents domaines étudiés et leurs axes d'application.

Pour illustrer et démontrer l'applicabilité de MoRiA, nous l'avons employé sur un cas d'étude représentant un système complexe de type naval. Le système étudié illustre une plateforme de simulation navale englobant toute l'architecture et tous les équipements d'un navire normalisé (boucle de propulsion, d'énergie... ainsi que la passerelle et les divers instruments et IHM [15] associées). L'application de notre méthode a pour objectif la modélisation

14. le principe de kill chain désigne dans le domaine de la sécurité des systèmes d'information une méthode de modélisation des procédés d'intrusion sur un réseau informatique.

15. IHM : Interactions homme-machine

de ce système en utilisant la méthode MoRiA afin d'identifier, de représenter et d'évaluer les risques de sécurité. Ensuite, nous avons évalué les résultats en les comparant à ceux obtenus avec une méthode d'analyses de risque actuellement utilisée en entreprise. Pour la validation de notre méthode, nous avons réalisé de nombreux échanges et retours d'expérience, d'architectes et d'experts en sécurité et en systèmes industriels. Quant aux résultats du cas d'étude, ils ont été validés par des experts industriels tant sur la pertinence de l'analyse de risque réalisée que sur le processus et les différentes perspectives/vues permettant sa co-ingénierie et prise de décisions.

.3.4 Plan du manuscrit

Le manuscrit est composé de quatre chapitres (Figure 16).

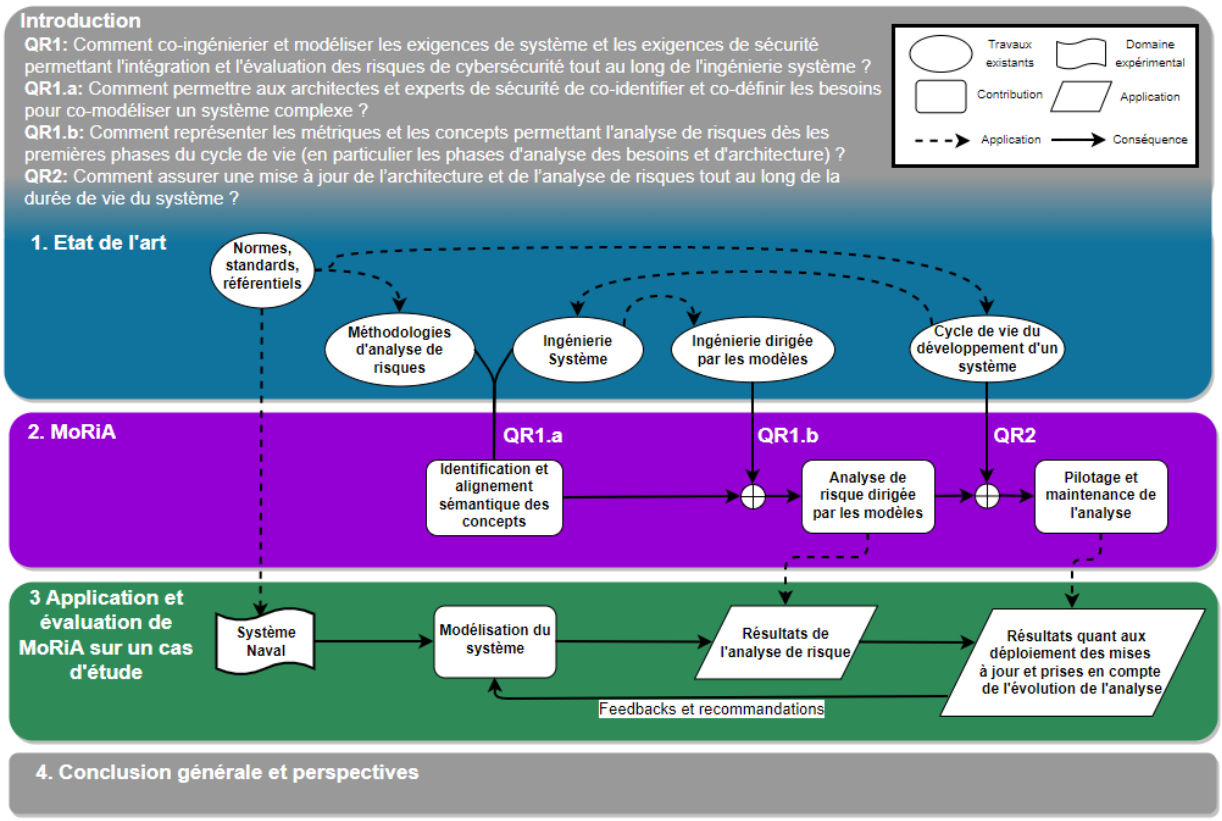


FIGURE 16: Description des relations entre les chapitres du manuscrit de thèse.

Le premier chapitre présente l'état de l'art des différents domaines qui sont explorés : les normes, standards et référentiels servant de socle et fils conducteurs aux méthodologies d'analyse de risque et d'ingénierie des systèmes et comment ces méthodes sont implémentées

afin de proposer une solution quant à leur co-ingénierie. À travers ce chapitre, nous cataloguons et parcourons la littérature afin d'identifier les méthodes, solutions et propositions répondant partiellement à nos travaux et questions de recherches ainsi que les manques ou écarts qui mèneront à la nécessité et la pertinence de nos contributions.

Dans le deuxième chapitre, nous présentons la méthodologie MoRiA ainsi que son langage de modélisation MoRiAML. L'objectif de ce chapitre est d'amener, illustrer et justifier notre alignement sémantique (QR1.a) des domaines, sa représentation concrète (QR1.B), son processus d'utilisation (QR1.B) ainsi que notre proposition d'implémentation et de pilotage de l'analyse de risque à travers le principe de cyber kill chain (QR2).

Dans le troisième chapitre, notre méthode MoRiA sera implémentée à travers une méthode d'analyse de risque et d'ingénierie système utilisée en entreprise. L'objectif de ce chapitre est de rendre la méthode opérationnelle à travers son implémentation.

Dans le quatrième chapitre, nous définissons et appliquons notre méthode implémentée sur notre cas d'étude : une plateforme de simulation navale composée d'une passerelle et de plusieurs sous-systèmes permettant la gestion de l'énergie, la propulsion, la sécurité, et des services auxiliaires. À travers cette application, nous cherchons à valider les résultats obtenus de l'analyse de risque lors des différentes étapes et perspectives de l'ingénierie ainsi que les moyens de communication et d'échanges mis en place. Nous validerons la pertinence de notre implémentation de l'analyse de risque et sa traçabilité et représentation quant à l'évolution de celle-ci ou du système.

Pour finir, nous conclurons le manuscrit en analysant des résultats obtenus, leur généralisation et en identifiant et dégageant les perspectives envisagées du travail réalisé.

Chapitre I

État de l'art

Sommaire

Nos travaux s'inscrivent et se concentre sur les phases (1)-d'exigences et de (2)-modélisation du cycle de vie du système (cf. figure 6) dans l'optique de proposer une solution permettant de développer, modéliser et prendre en compte l'analyse des risques et ses besoins en sécurité élicités des les premières phases de réflexion/définition du système. Ce chapitre décrit dans un premier temps les travaux de recherche antérieurs sur les différentes méthodes d'analyse de risque et quelles sont les propositions concernant leur intégration et alignement dans l'ingénierie système et ses modèles. Par la suite, nous nous intéressons aux processus/démarche/déroulement d'utilisation de l'analyse de risque à travers les modèles

avec notamment, comment elle peut être construite et maintenue à travers les différentes phases et perspectives de l'ingénierie système.

I.1 Introduction

Pour avoir une idée de l'état actuel de la recherche sur la modélisation de la sécurité dans les processus d'ingénierie système, nous avons passé en revue les approches existantes qui ont été publiées à ce jour [1].

Notre objectif est de permettre aux équipes de sécurité de pouvoir co-identifier et co-modéliser la sécurité et ses risques avec les équipes métier dans les modèles et s'inscrivant dans le processus d'ingénierie système. Pour mener à bien nos travaux, nous avons structuré notre état de l'art de la façon suivante. Dans un premier temps, nous rapportons dans ce chapitre les approches existantes qui traitent conjointement de nos deux questions de recherche (QR1 & QR2) : l'alignement et la modélisation des concepts de sécurité et plus exactement ceux de l'analyse de risque dans l'ingénierie système ainsi que son processus d'utilisation, maintien et évolution (catégorie A) ; Dans un second temps, nous rapportons les travaux portant exclusivement sur notre QR1 et nous peaufinerons ces recherches afin d'identifier les solutions répondant strictement à notre QR1.a OU QR1.b (catégories B, C, D et E) ; Pour finir, nous nous concentrerons uniquement sur les solutions concordantes avec notre QR2 (catégorie F dans le tableau I.1). Il est important de mentionner que les publications présentées et analysées dans ce chapitre sont des travaux connexes qui ont été extraits de plusieurs bases de données bibliographiques, principalement : Scopus [2], IEEE Xplore [3], Google Scholar [4].

Catégorie	Approches étudiées	Modélisation système	Modélisation sécurité	Analyse de risque	Cycle de vie
A	Mavzeika et al,. 2020 [MB20b]	✓	✓	✓	✓
	Khashooei et al, 2021 [KVKM21]	✓	✓	✓	✓
	Mili et al, 2021 [MNC21]	✓	✓	✓	✓
	Carter et al,. 2019 [CAB+19]	✓	✓	✓	✓
B	Navas et al,. 2019 [NVPB19]	✓	✓	✓	✗
	Zhang et al,. 2018 [ZHLL18]	✓	✓	✓	✗

1. 4 juillet 2021
2. https ://www.scopus.com/home.uri
3. Institute of Electrical and Electronics Engineers Xplore, http ://ieeexplore.ieee.org/Xplore/home.jsp
4. https ://scholar.google.com/

	Abdallah et al,. 2015 [ALR16]	✓	✓	✓	✗
	Mouratidis et al,. 2010[MJ10]	✓	✓	✓	✗
	CORAS 2002 [SdBD+02]	✓	✓	✓	✗
C	Apvrille et al,. 2016 [ALR16]	✓	✓	✗	✗
	Alam et al., 2015 [AHA15]	✓	✓	✗	✗
	Ahmed et al., 2014 [AM14]	✓	✓	✗	✗
	Muñante et al 2013., [MGA13]	✓	✓	✗	✗
	Matulevicius et al., 2012 [MMN+12]	✓	✓	✗	✗
	Altuhhova et al., 2012 [AMA12]	✓	✓	✗	✗
	Dubois et al., 2010 [DHMM10]	✓	✓	✗	✗
	Mellado et al., 2010 [MFMP10]	✓	✓	✗	✗
	Asnar et al., 2008 [AMSZ08]	✓	✓	✗	✗
	Mellado et al., 2007 [MFMP07]	✓	✓	✗	✗
	Gandhi et al., 2007 [GL07]	✓	✓	✗	✗
	Sindre et al., 2007 [Sin07]	✓	✓	✗	✗
	Mouratidis al., 2007 [MG07]	✓	✓	✗	✗
	Elahi et al., 2007 [EY07]	✓	✓	✗	✗
	Asnar et al., 2006 [AG06]	✓	✓	✗	✗
	Sindre et al., 2005 [SO05]	✓	✓	✗	✗
	Lamsweerde et al., 2004 [VL04]	✓	✓	✗	✗
	Lin et al., 2004 [LNIJ04]	✓	✓	✗	✗
	Lodderstedt et al., 2002 [LBD02]	✓	✓	✗	✗
	Jürjens et al., 2002 [Jür02]	✓	✓	✗	✗
	McDermott et al., 1999 [MF99]	✓	✓	✗	✗
D	Voirin et al., 2017 [Voi17]	✓	✗	✗	✗
	Feiler et al., 2016 [FDW16]	✓	✗	✗	✗
	Feiler et al., 2012 [FG12]	✓	✗	✗	✗
	Grammes et al., 2006 [Gra06]	✓	✗	✗	✗
E	EBIOS RM 2018 [ebi18]	✗	✗	✓	✗
	MAGERIT 2012[edap12]	✗	✗	✓	✗
	MEHARI 2012 [Mih12]	✗	✗	✓	✗
	EBIOS 2010 [ndlsdsdA10]	✗	✗	✓	✗
	OCTAVE-allegro 2007 [CSYW07]	✗	✗	✓	✗
	CRAMM 2005[Con05]	✗	✗	✓	✗
	NIST SP-800-30 2002 [SGF02]	✗	✗	✓	✗
F	Hoffmann et al., 2020 [HNPS20]	✗	✓	✓	✓
	Khan et al., 2018 [KSF18]	✗	✓	✓	✓
	Hahn et al., 2015 [HTLC15]	✗	✓	✓	✓
	Coleman et al., 2012 [Col12]	✗	✓	✓	✓
	Hutchins et al., 2011 [HCA+11]	✗	✓	✓	✓

L'extraction des publications a été faite de manière structurée en utilisant des mots-clés appropriés liés à nos sujets d'intérêt comme décrit ci-dessous, en plus de plusieurs critères d'inclusion et d'exclusion pour sélectionner les études pertinentes, cependant cette étude n'est pas une revue systématique complète de la littérature[KPB+10]. De plus, ces travaux connexes ont été analysés en tenant compte de nos questions de recherche que nous avons formulées dans l'introduction générale et des objectifs de cette thèse, au lieu de nous limiter au périmètre identifié par leurs propres auteurs.

Dans le tableau I.1, nous présentons les approches examinées et les analysons en fonction des sujets d'intérêt suivants :

1. **Modélisation de système :** Comme argumenté dans le chapitre d'introduction générale, l'ingénierie système basée sur les modèles (ISBM) est une approche efficace pour faire face à la complexité des systèmes complexes ainsi qu'aux défis de modélisation et d'évaluation liés à la sécurité. Dans cette thèse, nous nous intéressons tout d'abord à proposer une méthode pour réaliser l'analyse de risque dans la conception des différentes phases de l'ingénierie système. Par conséquent, pour inclure ce sujet dans notre revue, nous avons utilisé les mots-clés suivants : "Model Driven Systems Engineering" ou "Model Driven Architecture" ou "Model Bbased Systems Engineering" ou "Model Based Architecture" ou "MBSE" ou "System Engineering" ou "MDE" ;
2. **Modélisation de la sécurité :** Ensemble de préceptes et de règles nécessaires pour mesurer réellement le niveau de sécurité d'une organisation et faciliter la prise de décision ; les mesures de sécurité impliquent l'application d'une méthode de mesure à une ou plusieurs entités d'un système qui possèdent une propriété de sécurité évaluable afin d'obtenir une valeur mesurée. En conséquence, nous avons considéré les mots-clés "security metrics" ou "threat modeling" ou "security concepts" ou "security modeling" ou "security requirement" dans notre recherche ;
3. **L'analyse de risque :** Parmi les défis liés aux propriétés de sécurité et leur intégration dans le processus d'ingénierie, nous nous concentrons sur la globalité des métriques et concepts de sécurité nécessaires à la réalisation d'une analyse de risque. En conséquence, nous avons considéré les mots-clés "risk analysis" ou "risk assessment" ou "risk management" ou "Security Risk Management" ou "SRM" dans notre recherche ;
4. **Analyse continue lors des phases de modélisation des besoins et de l'architecture :** Ces phases se composent d'un certain nombre de phases de travail clairement

définies et distinctes, utilisées par les différentes équipes d'ingénieurs. Ici nous cherchons à identifier comment comment rendre l'analyse de risque dans les différentes perspectives de l'ingénierie système continu et itératif afin de suivre, maintenir et faire évoluer le niveau de sécurité du système. De plus, nous incluons les recherches sur le concept de cyber kill chain qui est un cadre permettant de décomposer une attaque complexe. En conséquence, nous avons considéré les mots-clés "continuous analysis" ou "iterative analysis" ou "cyber kill chain" dans notre recherche.

Nous avons organisé les approches étudiées en six catégories :

1. Catégorie A : Les approches couvrent à la fois l'intégration et la modélisation de concepts de sécurité issues de l'analyse de risque dans l'ingénierie système ainsi que sa démarche de construction, maintenance et d'évolution ("Modélisation système" et "Modélisation sécurité" et "Analyse de risque" et "Cycle de vie") ;

2. Catégorie B : Les travaux qui couvrent conjointement l'intégration et la modélisation de concepts de sécurité issues de l'analyse de risque dans l'ingénierie système ("Modélisation système" et "Modélisation sécurité" et "Analyse de risque") ;

3. Catégorie C : Les travaux qui portent exclusivement sur l'intégration et la modélisation de concepts de sécurité dans l'ingénierie système ("Modélisation système" et "Modélisation sécurité") ;

4. Catégorie D : Les travaux qui portent exclusivement sur les méthodes et outils d'ingénierie système utilisés dans l'industrie et implémentant les normes ("Modélisation système") ;

5. Catégorie E : Les travaux qui portent exclusivement sur les méthodes et outils d'analyse de risque utilisés dans l'industrie et implémentant les normes ("Analyse de risque") ;

6. Catégorie F : Les travaux qui portent exclusivement sur le maintien et l'évolution de l'analyse de risque dans les phases d'exigence et architecture lors de la modélisation ("Cycle de vie") ;

I.1.1 Catégorie A : Approches existantes intégrant le processus d'analyse de risque ainsi que ses concepts dans l'ingénierie système ainsi que sa construction et son maintien

Ces dernières années, diverses études dans le domaine de la modélisation de l'ingénierie système ont été publiées, beaucoup d'entre elles soulignant l'urgence et l'importance de prendre en compte la sécurité dès les premières phases de l'ingénierie [BOF+14] [MB20a] [JS07]. Malgré cela, jusqu'à ce jour et à notre connaissance, la modélisation de la sécurité et sa maintenance à travers les différentes phases/perspectives de l'ingénierie système sont à peine abordées.

Dans [MB20b], les auteurs présentent une méthode MBSEsec alignée sur l'ISO/IEC 27001, consistant en un profil basé sur SysML/UML, une définition du processus de sécurité et des recommandations, et comment ces concepts de sécurité basés sur le cadre d'architecture unifié pourraient être définis avec le profil SysML. Cette méthode présente de nombreux avantages, en particulier la mise en correspondance de certains concepts de sécurité avec des approches de modélisation de la sécurité et le fait qu'elle soit basée sur une norme et un profil communs. Néanmoins, cette méthode a été conçue pour être utilisée par des ingénieurs et analystes en sécurité et ne prend pas en compte les avantages de la co-définition de ces concepts de sécurité avec les ingénieurs système. De plus, les éléments de sécurité identifiés sont censés être "ajoutés" et non "intégrés" aux différents modèles, ce qui rend leurs définitions, leurs impacts et leurs cycles de vie disjoints.

Carter [CAB+19], présente une méthode et un outil connexes pour aborder la cybersécurité dès les premières étapes du cycle de vie d'un nouveau système. La méthode s'appelle Cyber Security Requirements Methodology (CSRM) [HBF+18] et elle vise à élaborer des exigences de cybersécurité lors de la définition du système à travers une représentation dans SysML. Ces exigences comprennent l'incorporation de solutions de sécurité traditionnelles et de résilience dans la conception du système, ainsi que des recommandations sur les pratiques d'ingénierie logicielle. L'outil Systems-Theoretic Resiliency Assessment Tools (STRAT) quant à lui se concentre sur l'identification et l'évaluation des stratégies de résilience. Cependant, les concepts de sécurité et de l'ingénierie système ne sont pas explicitement alignés et justifiés, la méthode ne se repose sur aucune norme de sécurité ou d'ingénierie ce qui rend difficile son implémentation à travers les processus et méthodes d'analyse de risque et/ou d'ingénierie déjà existantes.

Les travaux de [MNC21] proposent une approche appelée MBSAES à base de modèles pour l'analyse de la sécurité consistant en trois étapes : (i) modélisation conceptuelle des exigences de sécurité (ii) modélisation conceptuelle du système, et (iii) transformation des modèles pour la vérification. Ces trois étapes sont mises en correspondance avec les concepts de l'architecture dirigée par le modèle (MDA), en séparant la modélisation conceptuelle de la plate-forme technique. À travers le langage SysML, ils ont introduit un profil appelé Extended Attack Tree permettant une modélisation formelle et temporelle des attaques et un profil de connectivité permettant la propagation des flux entre les différents sous-systèmes communicants qui par la suite sont validés à travers deux processus de transformation suivant le paradigme MDA. Cette méthode combinant la modélisation semi-formelle et la vérification formelle, et pouvant être réalisée de manière automatique et précoce, permet de faciliter l'approche secure-by-design. Cependant, elle ne traite pas tous les aspects de l'analyse de risque, notamment ceux liés à l'établissement du contexte. Cela est bien sûr inhérent à leur approche basée sur les scénarios d'attaques qui ont besoin d'éléments concrets sur lesquels reposer, mais qui alors spécialise leur méthode et ne permet pas une couverture complète de l'analyse. De plus la méthode est pour aider et assister les équipes sécurité en modélisant la sécurité dans les modèles afin d'exécuter leurs processus de vérification, ce qui ne répond pas à nos objectifs de co-ingénierie entre les équipes métiers et de sécurité.

Khashooei [KVKM21], propose une méthode prenant place au début de la phase de modélisation et de l'analyse du système dans le contexte des systèmes de systèmes. Le résultat de la conception est un ensemble de vues holistiques du système, où les préoccupations de sécurité et de confidentialité sont liées aux blocs de construction du système et où les informations principales sur les solutions alternatives peuvent être présentées de manière simple et intuitive. Néanmoins, cette approche n'intègre l'analyse de risque qu'à un stade avancé de la modélisation et ne couvre pas toute la démarche d'analyse de risque. Elle reste spécifique à la sécurisation de systèmes au travers de solutions alternatives d'architecture sans traçabilité et prise en compte des spécificités de l'ingénierie des exigences. De plus, cette méthode cherche à créer des tableaux contenant les éléments d'analyse de risque afin de collaborer et de communiquer avec les décideurs et experts métiers. Cette approche n'est pas en adéquation avec notre objectif de co-ingénierie à travers les modèles.

L'analyse de ces approches montre qu'aucune de ces méthodes ne satisfait toutes les exigences étudiées. Les couplages proposés sont adaptés aux équipes sécurité en délaissant l'expertise métier qui peut être assimilée à travers des échanges supportés par les modèles. Pour cela, l'analyse de risque doit prendre place dans ceux-ci, couvrir les différentes phases

et évoluer en même temps que la définition du système.

I.1.2 Catégorie B : Approches existantes intégrant le processus d'analyse de risque ainsi que ces concepts dans l'ingénierie système

Ici, nous nous concentrons sur les approches existantes proposant un alignement des concepts de l'ingénierie système avec ceux de l'analyse de risque ainsi que les propositions de représentation de ces concepts. Nous avons sélectionné certaines des approches qui proposent une modélisation des différents ateliers de l'analyse de risque dans les différents modèles et perspectives de l'ingénierie système ainsi que les résultats obtenus.

Thales travaille actuellement sur une représentation et des perspectives de sécurité en tant d'extension de modèles. Ils ont mené une étude dans ce sens afin d'identifier au plus tôt les menaces possibles, les actifs à protéger (informations, capacités, etc.), et certaines mesures de sécurité pour y répondre [NVPB19]. Ce travail a conduit aux premières réflexions sur un travail de co-identification et de co-définition des éléments de sécurité par l'ingénierie système. Cependant, ce travail est encore à un stade très précoce, et il ne couvre pas tous les éléments nécessaires à la réalisation d'une analyse de risque. De plus, il ne prend pas en compte la dépendance et les impacts que ces concepts de sécurité ont les uns sur les autres pendant les phases d'exigence et de conception du cycle de vie du développement du système.

Dans un autre travail [AYL15], les auteurs proposent un cadre basé sur le modèle pour l'analyse de la sécurité en implémentant la méthode d'analyse de risque EBIOS et les arbres d'attaque comme profils UML. Ce travail a ces avantages, mais ne s'inscrit pas dans le nouveau paradigme de la sécurité plus collaboratif et transparent. Leur objectif reste d'équiper et d'aider les ingénieurs en sécurité en utilisant le langage et la propriété de l'ingénierie système sans chercher à collaborer avec les équipes système, dont le rôle se limite à définir les exigences des modèles de système. De plus, cette méthode est dissociée du cycle de vie du système, ça construction, maintenance et évolue peut donc être obsolète voir inapproprié.

La méthode CORAS [SdBD+02] est définie comme un cadre fondé sur un modèle pratique pour l'évaluation des risques pour les systèmes critiques. Elle fournit un langage graphique pour la modélisation du risque. Elle a été mise au point par le conseil norvégien de la recherche et de l'UE. Elle est fondée sur le standard australo-néo-zélandais : AS / NZS 4360 :

2004. CORAS est un modèle d'évaluation des risques basé sur le langage de modélisation normalisé UML qui vise à faciliter une meilleure communication pendant les évaluations de sécurité, en rendant les modèles semi-formels plus faciles à comprendre pour les non-experts, tout en les gardant bien définis et en documentant les résultats de l'évaluation des risques et les hypothèses dont dépendent ces résultats afin de favoriser la réutilisation et la maintenance. Cependant l'efficacité des mesures de sécurité n'est pas incluse, la mise en œuvre nécessite donc une connaissance approfondie de divers domaines.

Nous notons aussi l'article [ZHLL18], qui argumente le lien entre la discipline RAM (Fiabilité, disponibilité et maintenabilité) et l'ingénierie système (SE). À travers l'analyse, les auteurs proposent un cadre RAM-SE pour connecter les concepts et les modèles utilisés par ces deux disciplines, à la lumière des problèmes spécifiques rencontrés dans la conception sous-marine. Ce cadre identifie les avantages des différentes phases du processus SE sur lesquelles les ingénieurs RAM pourraient collaborer pour soutenir leurs techniques et méthodes et vice versa à travers un framework. Toutefois, ici il n'est question que du couplage/alignement des techniques en lien avec la sécurité dans les différentes phases et modèles dans l'ingénierie système. Ce travail est intéressant d'un point de vue abstrait, mais ne rentre pas en détail sur l'alignement, chevauchements et les intégrations des concepts inhérents à ces techniques dans les modèles.

Mouratidis et al. [MJ10] proposent et présentent l'intégration de deux approches importantes, une approche d'ingénierie des exigences de sécurité orientée vers les objectifs
ref appelés Secure Tropos et une approche MBSE appelée UMLsec. Pour les systèmes critiques en matière de sécurité, l'approche proposée permet d'éliciter et de raisonner sur les exigences de sécurité dès le début du processus de développement, dans le contexte du développement, et de manière transparente tout au long du cycle de développement. Ensuite, on peut vérifier que le système satisfait aux exigences de sécurité pertinentes au niveau de la conception en analysant le modèle. Cependant, ce travail porte en grande partie sur l'implémentation des concepts de sécurité déjà présents dans UMLsec avec ceux de Secure Tropos, ce qui une fois de plus aide à l'amélioration et la complétude de l'analyse, mais ne cherche pas à intégrer les expertises métier à travers des modèles collaboratifs.

L'analyse de ces approches montre qu'aucune de ces méthodes ne satisfait toutes les exigences nécessaires pour répondre à nos 2 questions de recherche. La co-ingénierie devrait être pensée pour servir et aider les équipes métier ainsi que celle de sécurité et cela à travers toutes les perspectives de l'ingénierie système et non pas seulement les experts en sécurité.

I.1.3 Catégorie C : Travaux portant exclusivement sur l'intégration et la modélisation de concepts de sécurité dans l'ingénierie système

Dans cette section, nous nous intéressons aux méthodes permettant aux équipes de sécurité de prendre en compte les questions de sécurité au cours et à travers les différents modèles de l'ingénierie système. Les méthodes adressées ici n'ont pas pour objectif de fournir une méthodologie complète d'analyse et de gestion des risques, mais plutôt de proposer des protocoles et des mécanismes de sécurité spécifiques aux besoins de modélisation.

Aux différentes étapes du développement d'un SI, la sécurité peut être abordée à l'aide de divers modèles ; par exemple, les "goal model" avec Tropos [BPG+04], i* [Yu97] ou KAOS [VL01] ; les diagrammes de classe UML SYSML [OMG15b][OMG15a], etc. Cependant, ces langages n'ont pas été conçus en prenant en compte les préoccupations et l'angle de la sécurité et, par conséquent, leur prise en compte est délicate et laborieuse.

Il existe également des langages de modélisation de la sécurité spécifiquement dédiés à l'analyse et à la modélisation des problèmes de sécurité des SI. Par exemple, Abuse frames [LNIJ04] qui propose des moyens de prendre en compte la sécurité dès le début de la phase d'ingénierie des exigences (RE). UMLsec [Jür02] et SecureUML [LBD02] qui sont utilisés quant à eux pour aborder la sécurité pendant la phase de conception/architecture du système. MoDELO [MGA13], une approche de politique de sécurité basée sur le modèle qui étend UMLSec avec les éléments de contrôle d'accès basés sur l'organisation, comme le rôle, le sujet, l'objet, l'action et le contexte, pour modéliser et évaluer les exigences de contrôle d'accès.

Les langages de modélisation des objectifs ont également été adaptés à la sécurité. Nous avons pour exemple Secure i* [EY07] qui traite des compromis en matière de sécurité entre les objectifs concurrents des systèmes à acteurs multiples. L'extension de sécurité de KAOS (Keep All Objectives Satisfied) [VL04] qui ajoute des modèles anti-objectifs conçus pour explorer et modéliser les raisonnements des attaquants. Tropos a été étendu à la méthodologie Secure Tropos [MG07] qui combine les concepts d'ingénierie des exigences, tels que l'acteur, le but, le plan, avec les concepts d'ingénierie de la sécurité, tels que la menace et les contraintes de sécurité avec par la suite une implémentation pour la gestion des risques [MMN+12].

Dans [ALR16] Apvrille et al. proposent SysML-Sec, une approche de la sécurité basée sur le modèle SysML. Il s'agit d'une approche formelle inspirée de la méthode KAOS pour

l'analyse des exigences et est défini en trois étapes : l'analyse du système (évaluation du système pour identifier les exigences et les menaces de sécurité), la conception du système (mise en œuvre des mécanismes de sécurité du logiciel) et la validation du système (vérification formelle et test des modèles conçus). Alam et al. [AHA15] quant à eux proposent l'utilisation subséquente de secure tropos et UMLsec en s'appuyant principalement sur le modèle Tropos pour l'analyse du système et UML/UMLsec pour la modélisation du système.

Dubois et al. [DHMM10] proposent d'étendre des langages Secure tropos et KAOS avec la notion de risque à travers un modèle de domaine conçu après la réalisation d'un alignement de différents concepts trouvés dans différents cadres, méthodologies et normes de gestion des risques, tels que les concepts d'actifs, de risque et d'impact. De même, Altuhhova et al ; dans [AMA12], proposent un alignement entre les concepts du modèle de Dubois et al. [DHMM10] et les modèles BPMN [Whi04] afin de permettre aux concepteurs de comprendre comment utiliser BPMN pour traiter la sécurité. Ahmed et al. [AM14] utilisent également le modèle de domaine de Dubois et al. [DHMM10] pour décrire quatre modèles orientés risque dans BPMN, et une méthodologie en sept étapes visant à sécuriser les processus métier. Néanmoins, l'analyste métier n'est pas guidé pour la sélection du modèle approprié.

Les diagrammes d'Abuse cases [MF99], de Misuse cases [SO05] et de Mal-activity [Sin07] abordent les problèmes de sécurité par le biais de scénarios négatifs ou de processus exécutés par l'attaquant.

En ce qui concerne le risque, Mellado et al. [MFMP07] et [MFMP10] ont présenté des travaux relatifs aux approches des exigences de sécurité basées sur le risque.

Le cadre Tropos Goal-Risk (GR) est une autre extension de Tropos qui considère le concept de "risque" [AG06] avec pour objectif d'évaluer le risque d'événements incertains sur les stratégies d'organisation et d'évaluer l'efficacité des traitements [AMSZ08]. Il est nécessaire de noter que l'éventail des risques pris en charge par le cadre Tropos GR n'est pas centré sur la sécurité des SI. Il est ouvert aux risques en général.

Enfin, dans [GL07], un modèle est proposé pour expliquer les relations entre les exigences de sécurité et les composants de risque, à des fins de certification et d'accréditation.

Dans la plupart des cas, les langages susmentionnés n'ont pas été spécifiquement conçus en tenant compte des aspects de sécurité. Ces aspects ont été introduits de manière incrémentale et ont enrichi les langages existants, en raison de l'importance croissante de la

sécurité. Par conséquent, ces langages ont progressivement intégré des concepts de sécurité, sans véritable approche systématique de la conception du langage. En outre, aucun des langages de modélisation présentés n'offre une correspondance formalisée avec la Gestion des risques liés à la sécurité des systèmes d'information (ISSRM) issue des normes et notamment celle de la famille 27000. Bien que certains langages incluent certains concepts de risque, aucun ne couvre tous les concepts nécessaires à la réalisation de l'ISSRM. Les langages manquent également de lignes directrices sur la façon dont ils peuvent répondre aux besoins des différentes parties prenantes, c'est-à-dire, représenter et unifier les points de vue et les préoccupations individuelles liées à la sécurité des SI, des exigences fonctionnelles métier et à la gestion des risques de sécurité. De plus, ces langages ne permettent pas une co-ingénierie en collaboration avec les experts système, cela pouvant amener un travail d'intégration ou de rectification supplémentaire.

I.1.4 Catégorie D : Les méthodes et outils d'ingénierie système utilisés dans l'industrie

Dans cette section, nous avons répertorié et comparé plusieurs langages de modélisation de système industriel. Nous avons identifié et choisi ces langages en fonction de leurs respects et adhésions par rapport aux différentes phases et perspectives des normes d'ingénierie système. De plus, nous avons considéré le fait qu'ils pourraient avoir des prédispositions quant au nouveau paradigme de la sécurité que nous voulions intégrer (prises en compte, modélisation de l'écosystème ainsi que des scénarii d'attaques).

Traditionnellement, de nombreuses approches ont été utilisées pour modéliser les exigences et l'architecture des systèmes, telles que : les approches formelles [Asn06][MUV+16][RB04][BKS10] qui décrivent les modèles d'architecture à l'aide d'expressions mathématiques et de prédicats ; les approches orientées vers les objectifs [HY16][DM17][JFS08] qui se concentrent sur la capture des exigences fonctionnelles et non fonctionnelles du système dans les modèles d'architecture ; et les langages de description architecturale (ADL) [Pan10] qui sont des langages utilisés pour décrire l'architecture logicielle du système, comme ses composants, ses connecteurs, ses règles et ses directives.

Nos travaux s'appuyant sur l'ingénierie basée sur les modèles (ISBM) afin de co-ingéniérer la sécurité dans les différentes perspectives et modèles de l'ingénierie système. Dans cette section, notre état de l'art s'est principalement posé sur les méthodes ISBMs

utilisées dans l'industrie et répandues dans le monde.

Les approches orientées sur les objectifs telles que KAOS [VL01] peuvent être utilisées pour modéliser des aspects comportementaux tels que les objectifs généraux du système, les fonctionnalités permettant leur réalisation ainsi que les interactions entre elles. Étant donné qu'un aspect crucial dans le contexte de notre travail est l'intégration de la sécurité dans les différentes phases de l'ingénierie système, les phases couvertes par l'approche par objectifs telles que celles des besoins et des exigences ne sont pas suffisantes et nous ne permettrons pas de modéliser les propriétés et les concepts tels que les vulnérabilités et les attaques et les extensions de sécurité. Les approches orientées vers les objectifs ne sont pas suffisantes pour décrire l'architecture structurelle d'un système et nécessitent un couplage avec un ADL [VVLPP05][LCS+09]. L'ADL fournissant un support pour la modélisation explicite des composants, des connecteurs, de leurs configurations et des contraintes.

ADL semble être une base plus adaptée pour l'extension/définition d'un langage de modélisation spécifique au domaine pour la modélisation d'architectures sécurisées comme le montrent d'autres revues de la littérature [EHPC+16][GNB+15][NGG+13]. Compte tenu de la diversité des approches récemment proposées pour la modélisation des systèmes et sur la base de notre étude et des résultats de revues récentes, nous limitons notre revue aux ADLs, nous présentons et analysons ci-dessous les dernières ADLs destinées à modéliser les différentes phases de l'ingénierie système.

Le langage AADL [FG12] (Architecture Analysis and Design Language) est un langage de conception d'architectures standardisé par la SAE (Society of Automotive Engineers). Il est destiné à la conception et l'analyse de systèmes embarqués complexes et temps réel. AADL permet de décrire à la fois les parties logicielles et matérielles d'un système. Il se concentre sur la définition d'interfaces de blocs claires et sépare les implémentations de ces interfaces. Il peut être exprimé à l'aide d'une syntaxe graphique et textuelle. À partir de la description de ces blocs, on peut construire un assemblage de blocs qui représente le système complet. Pour prendre en compte les multiples façons de connecter des composants, l'AADL définit différents patrons de connexion : sous-composant, connexion et liaison. Feiler et al. [FDW16] ont travaillé l'utilisation de ReqSpec avec des modèles AADL afin de définir et d'intégrer les objectifs des parties prenantes ainsi que les exigences du système permettant ainsi une couverture totale des phases d'ingénierie.

SDL (Specification and Description Language) [BHS91] est un langage graphique formel qui a été standardisé par l'ITU (International Telecommunication Union). Il est destiné à

la description des systèmes temps réels événementiels complexes. Il utilise une sémantique formelle contrairement à UML qui définit des "Points de variations sémantiques" (un élément de langage peut être interprété différemment), ne couvre pas les phases d'exigences et des besoins et ne peut être intégré à d'autres langages que de manière propriétaire, pour cette raison la création du profil UML pour SDL [BKV02] [Gra06] permettant l'utilisation de tous les diagrammes UML et de profiter de la sémantique formelle de la conception SDL a été étudiée.

UML existe maintenant depuis plus de 20 ans et est devenu un standard international. Il est le résultat d'années de travail d'experts de renommée internationale, qui ont doté le langage de riches capacités d'expression et d'une excellente couverture des besoins de modélisation les plus courants [AR15]. SysML est une spécialisation d'UML destinée à répondre aux préoccupations de l'ingénierie des systèmes. De nombreux outils de modélisation offrant divers degrés d'extensibilité et de personnalisation supportent SysML. L'approche la plus courante pour mettre en œuvre les orientations méthodologiques de l'ISBM consiste à enrichir le langage SysML avec des profils spécifiques aux méthodes, en ajoutant de la sémantique, et en fournissant des outils permettant sa réalisation et sa validation. Les langages standards ou universels tels que SysML ciblent une grande variété de domaines et d'intentions de modélisation. À l'inverse, les langages de modélisation spécialisés sont destinés à fournir des solutions pour des domaines ou des intentions de modélisation particulières. Les DSML (Domain-Specific Modeling Language, langage de modélisation spécifique à un domaine) ont généralement une couverture réduite et plus d'efficacité.

Ces caractéristiques les rendent plus susceptibles de fournir une sémantique plus riche et un formalisme amélioré. Malgré l'émergence d'environnements dédiés favorisant le développement de DSML, les coûts de développement peuvent être importants étant donné le niveau de maturité qu'un utilisateur final attend généralement d'une solution industrielle. Cependant, ce coût peut être contrebalancé par le fait que les outils DSML sont généralement moins complexes et plus faciles à apprendre.

Arcadia [Voi17] couvre l'analyse opérationnelle et la conception architecturale des systèmes. Il s'inspire d'une grande variété de langages standard, des cadres d'architecture (tels que NAF [Org16] ou DoDAF [G+03]) à SysML. L'approche intégrée (ARCADIA) est une méthode structurée d'ingénierie de l'architecture pour définir et valider des systèmes multi-domaines, basée sur des activités d'ingénierie centrées sur l'architecture et pilotées par les modèles. ARCADIA est une méthode basée sur l'analyse fonctionnelle et se concentre sur le développement du système en partant de l'analyse des besoins et du développement de

solutions jusqu'à la vérification et la validation intégrées. ARCADIA est très flexible et peut être mis en œuvre en utilisant une approche de développement descendante, ascendante ou intermédiaire, selon les besoins. Ces perspectives/phases sont implémentées à travers l'outil de modélisation/éditeur graphique Capella. La démarche et le langage ARCADIA et son outil Capella sont activement maintenus avec une documentation bien établie et ils sont extensibles et interopérables avec les langages et outils existants basés sur SysML. En effet, ARCADIA, ainsi que Capella, sont des logiciels libres, largement utilisés dans le monde entier par des fabricants tels que RollsRoyce (UK), Virgin Hyperloop (USA), Deutsche Bahn (GER), Comac (Chine) sans oublier l'industrie française, et en particulier, leur auteur Thales [5], une société multinationale française [She19].

ARCADIA est conforme aux normes MBSE, en particulier le processus ISO 15288 & IEEE 1220 et propose une démarche d'ingénierie en cinq phases d'analyse. Capella n'est donc ni un profil SysML ni un DSML. Le méta modèle central de Capella a été fortement inspiré par SysML et les diagrammes proposés sont très similaires. Cependant, en considérant le langage SysML comme une référence, le méta modèle de Capella est simplifié, modifié et enrichi [BVEN16]. Le principal avantage de cette approche hybride est que les diagrammes Capella peuvent être lus et compris par des ingénieurs n'ayant aucune connaissance particulière d'Arcadia.

En résumé, les ADLs industriels sont bien adaptés pour modéliser l'architecture et la définition des besoins et exigences des systèmes. SysML est activement utilisé et constitue une base solide pour toute définition/extension de langage traitant de la modélisation de l'architecture. Cependant, SysML n'est qu'un langage, et chaque entreprise doit élaborer une stratégie de modélisation adaptée et l'enseigner à ces outils de modélisation. À l'inverse d'ARCADIA qui propose sa méthode et son outil.

I.1.5 Catégorie E : Les méthodes et outils d'analyse de risque utilisés dans l'industrie

Comme présenté dans l'introduction, la norme ISO 27005 :2008 établit des lignes directrices pour la gestion des risques dans les systèmes d'information. Elle est complémentaire et s'appuie sur les concepts généraux spécifiés dans les normes ISO/IEC 27000 et ISO/IEC 27001 et ISO/IEC 27002 qui définissent la nécessité de gérer les risques liés à la sécurité

5. https ://www.thalesgroup.com/en

de l'information, sans préciser comment. Elle est perçue comme la formalisation d'exigences internationales à satisfaire par une méthodologie de gestion des risques de la sécurité de l'information. Elle permet la définition d'un cadre méthodologique utilisé comme référence pour la formulation et structure des méthodes appliquées de management des risques et utilisées dans l'industrie.

Afin de réaliser le processus de management du risque reposant sur ces éléments, un certain nombre de méthodes d'analyse de risques ont été développées : EBIOS 2010 [ndlsdsdA10] et EBIOS RM [ebi18], MEHARI [dlsdlf10], OCTAVE [CSYW07], NIST SP 800-30 [SGF02]... La plupart de ces méthodes suivent les étapes proposées dans la norme ISO 27005 et présentent donc des similitudes. La réalisation d'une analyse de risques est une tâche complexe qui nécessite d'être à la fois précise et de garder une vue d'ensemble, couvrant tous les risques et toutes les situations, tout en restant homogène. Afin de rendre la démarche la plus rigoureuse possible, l'apport de la méthode consiste tout d'abord à proposer une approche systématique composée d'étapes simples, qui consistent généralement à inventorier le système, à le représenter d'une manière ou d'une autre, puis à identifier les risques à partir de listes génériques et à les évaluer selon une échelle bien définie.

I.1.5.1 MAGERIT [edap12]

Magerit a été élaboré et promu par CSAE (Conseil supérieur de l'administration électronique espagnol) en réponse à la perception que le gouvernement (et, en général, toute la société) dépend de plus en plus des technologies de l'information pour atteindre ses objectifs de service. L'analyse de risque utilisant Magerit suit les étapes suivantes : 1 - Déterminer les actifs, 2 - Déterminer les menaces, 3 - Déterminer les mesures de protection disponibles et leur efficacité par rapport au risque, 4 - Estimer l'impact en connaissant la valeur des actifs et les dommages causés par les menaces 5 - Estimer le risque, défini comme l'impact pondéré sur le taux d'occurrence de la menace.

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
MAGERIT	CSAE Espagne	1997	2012	Gouvernement	Solution gratuite (EAR / PILAR)	Qualitative et quantitative	Disponible (licence GNU)

TABLE I.2: Fiche descriptive MEGERIT

La méthode Magerit suit les trois premières étapes générales de l'analyse des risques : (1) identification de la menace, (2) identification de la vulnérabilité, et (3) détermination du risque. Cependant elle ne comprend pas de recommandation de contrôle. Les recomman-

dations de contrôle sont incluses dans l'étape suivante de la gestion de la sécurité, après l'analyse des risques. Cependant Magerit fournit des documents supplémentaires pour aider à l'évaluation des risques.

I.1.5.2 OCTAVE-Allegro [CSYW07]

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) est une méthode, développée et publiée par le Software Engineering Institute (SEI) du Carnegie Mellon University à travers son programme CERT. Elle est reconnue dans le domaine de la sécurité des systèmes d'information notamment par la Federation of computer Emergency & Response Team-CERTS. La méthode se concentre sur l'étude des risques organisationnels, principalement dans les aspects liés au travail quotidien dans les organisations. L'une de ses particularités est qu'elle doit être réalisée par du personnel appartenant aux unités fonctionnelles et au domaine des technologies de l'information. Il existe : OCTAVE (pour les grandes organisations), OCTAVE-S (pour les petites organisations) et OCTAVE Allegro (défini pour analyser les risques en se concentrant davantage sur les actifs informationnels, par opposition à l'approche en ressources informationnelles). OCTAVE-Allegro est la dernière version et est orientée vers l'évaluation des risques de sécurité de l'information. Elle décrit les étapes et fournit des feuilles de calcul des risques et des questionnaires, comme des guides et des modèles pour évaluer les risques de l'organisation ou plus précisément, ses actifs. OCTAVE-Allegro fournit un framework d'évaluation des risques, composé de 8 étapes couvertes à travers quatre phases : 1 - Définir les paramètres, 2 - Définir les profils d'actifs, 3 - Identifier les menaces, 4 - Identifier et atténuer les risques.

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
Octave-allegro	CERT USA	2007	2007	Universitaire	Logiciel propriétaire	Qualitative et quantitative	Disponible (licence GNU)

Table I.3: Fiche descriptive d'Octave-allegro

Cette méthode comprend de nombreux documents et outils et met en oeuvre une évaluation des risques d'un point de vue opérationnel. Elle traite exclusivement les actifs informationnels et leur conteneur en les corrélant aux risques intentionnels et non intentionnels et évaluant leurs risques à travers des arbres de menaces et des scores de risque. Cette approche adopte le point de vue forteresse en étant exhaustive, une vulnérabilité, une mesure et ne prend en considération que l'atténuation et l'acceptation du risque, mais pas son évitement.

I.1.5.3 CRAMM [Con05]

- La méthode CRAMM est une méthode d'analyse et de maîtrise des risques concernant le système d'information d'une entreprise. Créée en 1986 par Siemens en Angleterre, cette méthode est entièrement conforme aux normes BS2 7799 et ISO 27001. CRAMM est utilisé par l'OTAN, les forces armées néerlandaises et des entreprises travaillant activement sur la sécurité, comme Unisys. Il est mis en œuvre en quatre phases : 1 - Identification et évaluation des actifs, 2 - Évaluation des menaces et des vulnérabilités, 3 - Analyse du risque, 4 - Management du risque.

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
CRAMM	Insight Consulting Royaume-Uni	1985	2003	Gouvernement	Solution industrielle	Qualitative et quantitative	Disponible (licence GNU)

TABLE I.4: Fiche descriptive de CRAMM

Cette méthode couvre les différentes menaces et vulnérabilités auxquelles le système d'information est exposé, qu'elles soient délibérées ou accidentelles. L'entreprise doit évaluer ses risques, mais également décider du niveau de sécurité voulu pour chaque menace. La méthode CRAMM est associée à un logiciel possédant une base de données de plus de 400 types d'actifs, plus de 25 types d'impacts, 38 types de menaces, 7 types de mesures de risque et plus de 3 500 mesures de protection. Cependant cette méthode adopte le point de vue de la forteresse (une vulnérabilité, une mesure) ce qui rend sa mise en place, réalisation et maintien très exigeant. Ni la méthode ni l'outil n'ont suivi l'évolution de la menace dans notre contexte actuel et donc ne prennent pas en compte l'écosystème dans leur analyse et sont incapables d'analyser des scénarios complexes.

I.1.5.4 NIST SP-800-30 [SGF02]

Le "SP 800-30 Guide for Conducting a Risk Assessment" est une directive du National Institute of Standards and Technology (NIST). Selon le NIST SP 800-30, l'objectif de l'évaluation des risques est d'aider les organisations à fournir aux dirigeants et aux cadres supérieurs les informations nécessaires à la mise en œuvre de stratégies de gestion des risques adaptées à leur profil de risque unique et au rapport coûts-avantages des stratégies d'atténuation. Pour cela, il propose de conduire une analyse de risque sous 4 étapes : 1 - Préparation de l'évaluation, 2 - Effectuer une évaluation, 3 - Communiquer les résultats, 4 - Maintenir l'évaluation.

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
NIST SP 800-30	NIST USA	2012	2012	Gouvernement	X	Qualitative et quantitative	Disponible (licence GNU)

Table I.5: Fiche descriptive du NIST SP 800-30

Contrairement à ISO 27005, et les méthodes l'implémentant, la NIST SP 800-30 ne peut pas être utilisée pour l'évaluation des risques organisationnels. Il n'y a pas d'identification des actifs dans le NIST SP 800-30. En tant que telle, elle se concentre uniquement sur une infrastructure spécifique et ses limites à un moment donné. Bien que la norme ISO 27005 soit influencée par le NIST SP 800-30, contrairement à la norme ISO 27005, le NIST SP 800-30 ne permet de calculer le risque que d'une seule manière en étant très normative, puisque l'objectif est de réaliser une analyse des risques techniques de l'infrastructure informatique centrale.

I.1.5.5 MEHARI [Mih12]

MEHARI (Méthode Harmonisée d'Analyse des Risques) est une méthodologie française développée par une organisation de sécurité de l'information sans but lucratif (CLUSIF). La méthode fait usage d'une méthode fondée sur la connaissance des procédures de support semi-automatiques pour l'évaluation des risques. Elle offre la possibilité d'évaluer et de gérer les risques liés aux scénarios de risque grâce à des formules d'évaluation directe et le choix des moyens de les réduire. La démarche MEHARI comprend trois phases : 1 - La phase préparatoire, 2 - La phase d'analyse des risques, 3 - La phase de planification du traitement des risques.

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
MEHARI	CLUSIF France	1995	2017	industriels	source ouverte	Qualitative et quantitative	Disponible (licence GNU)

Table I.6: Fiche descriptive de MEHARI

La base de connaissances complète de MEHARI, construite à l'aide d'Excel, est disponible en anglais et en français sous la forme d'un outil interactif, ou plus exactement d'une suite d'outils qui peuvent être utilisés individuellement, mais sont conçus comme une suite cohérente. Au fur et à mesure de l'avancement du processus, la base de connaissances s'enrichit automatiquement des informations obtenues, fournissant des données pour les étapes suivantes. Ce qui amène une mise en œuvre limitée réalisable uniquement avec le logiciel

dédié et le démarrage de l'analyse nécessite une adaptation complexe de la "base de connaissances".

I.1.5.6 EBIOS [ndlsdsdA10]

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode française développée en 1995, et revue en 2010, par la DCSSI (Direction centrale de la Sécurité des systèmes d'information) devenue par la suite l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Elle fournit une approche méthodologique complète en accord avec les principales normes internationales en matière de gestion des risques. EBIOS 2010 se définit comme une « Une démarche itérative en cinq modules » :

1. **Module 1 – Étude du contexte :** Ce module a pour objectif de formaliser le cadre de gestion des risques dans lequel l'étude va être menée en identifiant, de délimitant et décrivant le périmètre de l'étude à travers l'identification des biens et de leurs critères de sécurité, des sources de menaces, ainsi que des mesures de sécurité déjà mises en place ;
2. **Module 2 & 3 - Étude des évènements redoutés et des scénarios de menaces :** Ces modules sont complémentaires et permettent pour le premier de dresser une liste des événements redoutés et pour le second d'analyser les modes opératoires/scénarios portant atteinte à la sécurité dans le cadre de l'étude ;
3. **Module 4 - Étude des risques :** A pour objectifs de corréler les événements redoutés avec les scénarios de menaces afin d'identifier les seuls scénarios réellement pertinents vis-à-vis du périmètre de l'étude ainsi que la stratégie de traitement à appliquer ;
4. **Module 5 - Étude des mesures de sécurité :** A pour objectif de déterminer les moyens de traiter les risques et de suivre leur mise en œuvre, en cohérence avec le contexte de l'étude.

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
EBIOS	ANSSI France	1995	2010	Gouvernement Club EBIOS	X	Qualitative et quantitative	Disponible (licence GNU)

TABLE I.7: Fiche descriptive d'EBIOS

Cette méthode a pour avantage la réutilisation de chaque module afin d'améliorer progressivement l'analyse. Elle traite les actifs de haut niveau ainsi que des actifs support

permettant leur réalisation en les corrélant aux risques intentionnels et non intentionnels et évaluant leurs risques à travers des matrices de gravité et de vraisemblance. Cette approche adopte le point de vue forteresse en étant exhaustive, une mesure pour chaque vulnérabilité
.

Depuis bientôt 10 ans, EBIOS 2010 propose une méthode centrée sur la notion de menaces unitaires tirant parti de vulnérabilités et de prévention de leurs impacts sur des processus métier. Cette méthode remettait, à l'époque, le métier au centre de l'analyse de risques, mais n'était pas conçue pour identifier et traiter des menaces complexes. Ces menaces sont composées de rebonds de l'attaquant d'une vulnérabilité à une autre parfois exploitant l'environnement du système pour atteindre ses fins, constituent ainsi une part majeure de l'univers des risques SSI et ont été mises à l'ordre du jour de nombreux comités exécutifs à la suite des dernières attaques majeures comme NotPetya ou WannaCry.

I.1.5.7 EBIOS RM [ebi18]

EBIOS RM vise à compléter les faiblesses d'EBIOS 2010 par une approche menant une étude poussée des intentions des attaquants potentiels et dans un second temps une prise en compte plus formelle de l'écosystème pour finir avec une identification des scénarios d'attaques complexes. L'objectif final de cette étude n'est plus l'alignement des mesures de sécurité à des failles unitaires comme pour EBIOS 2010, mais vise désormais la capacité à maîtriser des risques aux facettes multiples.

EBIOS RM consiste en une approche itérative en 5 ateliers. L'approche par conformité est utilisée pour déterminer le socle de sécurité (atelier 1) sur lequel s'appuie l'approche par scénarios (atelier 2, 3 et 4) pour élaborer des scénarios de risque particulièrement ciblés ou sophistiqués. Cela suppose que les risques accidentels et environnementaux sont traités a priori via une approche par conformité au sein du socle de sécurité permettant à la méthode de se concentrer sur les menaces intentionnelles.

1. **Atelier 1 : Cadrage et socle de sécurité :** permet de suivre une approche par « conformité ». Il vise à identifier l'objet de l'étude, les participants et le cadre temporel. L'objectif est de recenser les missions, valeurs métier et biens supports relatifs à l'objet étudié. Les participants identifient ensuite les événements redoutés associés aux valeurs métier et évaluent la gravité de leurs impacts ;
2. **Atelier 2 : Sources de risque :** Sert à identifier les sources de risque (SR) et leurs

objectifs visés (OV), en lien avec le contexte particulier de l'étude. Au final, les couples SR/OV jugés les plus pertinents sont retenus permettant la formalisation d'une cartographie des sources de risque qui sera utile lors de la construction des scénarios des ateliers 3 et 4 ;

3. **Atelier 3 : Scénarios stratégiques :** Sert à acquérir une vision claire de l'écosystème (ensemble des parties prenantes qui gravitent autour de l'objet de l'étude et concourent à la réalisation de ses missions (partenaires, sous-traitants, filiales, etc.)). Cela va nous permettre de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ils représentent les chemins d'attaque qu'une source de risque est susceptible d'emprunter pour atteindre son objectif (i.e. un des couples SR/OV sélectionnés lors de l'atelier 2). Ces scénarios se conçoivent à l'échelle de l'écosystème et sont évalués en termes de gravité. À l'issue de cet atelier, nous pouvons déjà définir des mesures de sécurité sur l'écosystème et les scénarios stratégiques retenus constitueront la base des scénarios opérationnels de l'atelier 4 ;
4. **Atelier 4 : Scénarios opérationnels :** Schématisent les modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques et sont évalués en termes de vraisemblance. Cet atelier adopte une démarche similaire à celle de l'atelier précédent, mais se concentre sur les biens supports ;
5. **Atelier 5 : Traitement du risque :** synthèse des scénarios de risque identifié en vue de définir une stratégie de traitement du risque. Cette stratégie aboutit à la définition de mesures de sécurité, recensées dans un plan d'amélioration continue de la sécurité (PACS). On identifie ensuite les risques résiduels ainsi que le cadre de suivi de ces risques.

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
EBIOS RM	ANSSI France	2018	2018	Gouvernement Club EBIOS	Solution industrielle	Qualitative et quantitative	Disponible (licence GNU)

TABLE I.8: Fiche descriptive d'EBIOS RM

Cette méthode a pour avantage un processus itératif en deux temps (une itération stratégique et une opérationnelle) permettant d'améliorer et de raffiner progressivement l'analyse et ces scénarios ainsi que des supports collaboratifs permettant les échanges trans disciplinaires entre les analystes de sécurité et les équipes métiers. Elle traite les actifs de haut niveau ainsi que des actifs support permettant leur réalisation en les corrélant aux risques intentionnels et l'écosystème (les parties prenantes) comme possibles sources de risques ou chemins d'attaque. Les risques non intentionnels sont quant à eux traités par le socle de

sécurité complexe. Cette approche adopte le point de vue de l'attaquant, défense adaptée en fonction des chemins d'attaques.

Cette méthode est cependant très dépendante de ses acteurs et participants. Elle nécessite que les équipes métiers et sécurité trouvent les bonnes équivalences de vocabulaire et de points de vue afin d'échanger sur leurs besoins et exigences propres à leurs métiers et ainsi intégrer leurs préoccupations et leurs expertises dans l'analyse.

I.1.5.8 Conclusion

Méthode	Éditeur	Date de création	Dernière mise à jour	Soutenu par	Outils	Type d'analyse	Documentation
EBIOS RM	ANSSI France	2018	2018	Gouvernement Club EBIOS	Solution industrielle	Qualitative et quantitative	Disponible (licence GNU)
EBIOS	ANSSI France	1995	2010	Gouvernement Club EBIOS	X	Qualitative et quantitatif	Disponible (licence GNU)
MEHARI	CLUSIF France	1995	2017	industriel	source ouverte	Qualitative et quantitative	Disponible (licence GNU)
NIST SP 800-30	NIST USA	2012	2012	Gouvernement	X	Qualitative et quantitative	Disponible (licence GNU)
CRAMM	Insight Consulting Royaume-Uni	1985	2003	Gouvernement	Solution industriel	Qualitative et quantitative	Disponible (licence GNU)
Octave-allegro	CERT USA	2007	2007	Universitaire	Logiciel propriétaire	Qualitative et quantitative	Disponible (licence GNU)
MAGERIT	CSAE USA	2012	2012	Gouvernement	Solution gratuite (EAR / PILAR)	Qualitative et quantitative	Disponible (licence GNU)

Table I.9: Fiche descriptive d'EBIOS RM

Toutes ces méthodes couvrent partiellement ou intégralement la famille des normes 2700X et sont efficaces pour identifier et analyser les risques. Cependant, cette dernière décennie le contexte cyber a évolué et elles ont du mal à s'adapter à l'évolution de la menace et les nouveaux besoins en termes d'analyse tels que l'appréciation et la prise en compte de l'ensemble des parties prenantes qui gravitent autour de l'objet de l'étude (écosystème) et concourent à la réalisation de ses missions ainsi que la réalisation de scénarios complexes exploitant par exemple les maillons les plus vulnérables de cet écosystème pour atteindre leur objectif. La méthode EBIOS RM semble pour le moment la seule à proposer des ateliers dans ce sens permettant l'étude, l'identification, l'évaluation et la maîtrise des dangers stratégiques et opérationnels. L'ANSSI a fait évoluer sa méthode initiale en tenant compte des nombreux retours d'expérience tout en faisant converger concepts et normes internationales relatives au système de management de la sécurité de l'information. La méthode EBIOS Risk Manager se distingue par une approche qui réalise une synthèse entre conformité et scénarios et de nombreux prestataires industriels souhaitent développer une solution logicielle conforme aux principes et aux concepts de la méthode EBIOS Risk Manager [6].

6. https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-man

I.1.6 Catégorie F : Les travaux qui portent exclusivement sur le maintien et l'évolution de l'analyse de risque dans les phases d'exigence et architecture lors de la modélisation

Le processus de gestion des cyber-risques est un processus continu, qui devrait prendre la forme d'une séquence ordonnée d'événements, d'activités et de décisions ultérieures qui aboutissent à la cybersécurité de l'organisation [HKS16].

Comme le montre la figure 12, nous percevons le processus de gestion des risques relatifs à la cybersécurité d'une organisation comme étant itératif. L'approche itérative du processus d'évaluation des risques cybernétiques peut prendre la forme d'une augmentation du niveau de détail de chaque itération ou d'un arrêt du processus après chaque étape, il existe des points de décision (continuer, terminer, revenir). Il faut savoir que l'évaluation du risque, y compris l'analyse du risque, est un élément fondamental du système de gestion du risque dans l'organisation, car au cours du processus d'évaluation du risque, nous obtenons les informations indispensables pour prendre les bonnes décisions concernant la stratégie de traitement du risque, le choix efficace des mesures de réduction du risque, l'évaluation de la validité du transfert, l'acceptation ou l'évitement du risque. Une fois que le risque a été identifié, estimé et évalué, la direction de l'organisation est censée adopter les bonnes stratégies pour l'atténuer. Les stratégies doivent inclure des activités liées aux risques comme la réduction, le transfert, l'acceptation et l'évitement des cyber-attaques.

Dans les approches itératives menant à une augmentation du niveau de détail, nous avons ceux portant sur les cyber-attaques. Les cyber-attaques ne durent pas un instant, mais sont un processus, c'est-à-dire un ensemble d'activités qui doivent être réalisées dans le bon ordre et qui ont leur durée et leur lieu. Ces activités sont combinées en groupes logiques et sont exécutées par étapes, créant ainsi un processus de cyber-attaque qui a généralement une durée limitée. Les processus de cyber-attaque qui sont divisés en phases peuvent être appelés "cyber kill chains" [HCA+11]. En d'autres termes, les cycles de vie des cyberattaques sont des modèles pratiques qui consistent en différentes étapes d'intrusion liées à la sécurité des réseaux et des systèmes d'information. Il existe différents cycles de vie des cyber-attaques chacun ayant des phases diversement nommées, définies et décrites. Par exemple, selon [Col12], le cycle se compose de cinq étapes : reconnaissance, balayage, accès au système, activité malveillante et exploitation. Dans [HCA+11][KSF18], le processus

ager/label-ebios-risk-manager-des-outils-pour-faciliter-le-management-du-risque-numeriq
ue/

de cyber-attaque et quant a lui défini comme la séquence de sept étapes : reconnaissance, armement, livraison, exploitation, installation, commandement et contrôle, actions sur les objectifs. D'autres chercheurs [HTLC15] indiquent qu'une attaque contre une infrastructure critique doit être considérée comme une séquence de six phases : reconnaissance, armement, livraison, exploitation, installation, commandement et contrôle, réalisation des objectifs.

Yadav et al. [YR15] et Jonsson et al. [JP11], explique qu'un aspect important de l'analyse continue à travers la cyber kill chain est l'acquisition d'informations. L'évaluation des risques ne sera complète que si, d'une part, elle se concentre sur les détails et, d'autre part, elle est replacée dans le contexte des autres informations recueillies. L'évaluation de la cyber kill chain est appliquée comme le produit de la probabilité d'un événement indésirable à chaque étape de la chaîne et de son impact négatif. De l'avis de Hoffmann [HNPS20], la cyber kill chain, est un concept tourné vers l'avenir qui combinera diverses lois, normes, réglementations et bonnes pratiques concernant le traitement de l'information, l'échange d'informations et la protection des données, y compris les données personnelles et permettra l'augmentation du niveau de détail de chaque itération de l'analyse. Pour toutes ces raisons, nous utiliserons la cyber kill chain afin de rassembler et travailler les éléments d'analyse de façon itérative afin de réinjecter les résultats obtenus afin de raffiner et adapter l'analyse en fonction de l'évolution et correction du système.

I.1.7 Conclusion

Par conséquent, les approches et les outils récemment proposés aident à consolider le processus d'analyse des risques, ils n'offrent pas les moyens de co-ingénierie des exigences de système et de sécurité, et ne proposent pas un processus structuré et sémantiquement justifié pour intégrer l'évaluation des risques de cybersécurité dans l'ingénierie des exigences. De plus, dans ces approches, l'analyse de risque est dissociée de l'ingénierie système (d'un point de vue sémantique, méthodologique et du cycle de vie), et donc lorsque l'analyse de risque est modifiée/actualisée, la prise en compte de son impact sur l'ingénierie système reste très limitée, et vice versa. Par conséquent, les approches et outils existants ne répondent pas à notre question de recherche, et ne satisfont pas pleinement les besoins actuels.

Toutes ces raisons justifient la nécessité de proposer un langage de modélisation ou d'étendre un langage existant, tel que SysML/ARCADIA, pour établir une formalisation plus avancée des exigences de sécurité sous la forme d'une modélisation des exigences et concepts de sécurité amenés et élicités par les modèles, par opposition à la modélisation de sécurité

basée sur les exigences habituellement employées. Les éléments de sécurité des modèles résultants doivent alors être considérés, pour l'ingénierie, comme des exigences portées par le modèle. Ces éléments doivent être co-définis et co-modélisés, et leurs dépendances, impacts et traitements doivent être tracés à travers tous les modèles et points de vue. De plus, le langage de modélisation doit permettre l'échange et la communication des résultats de façon intelligible et précise avec les décideurs.

Pour cela, nous allons dans un premier temps déterminer le processus d'analyse de risque en nous référant aux normes associées, afin d'identifier le processus ainsi que tous les éléments nécessaires à sa réalisation. Par la suite, nous réaliserons la même démarche pour l'ingénierie système afin d'intégrer/assimiler/fusionner ces deux processus ainsi qu'aligner les éléments les définissant.

Chapitre II

Méthode basée sur les modèles pour l'évaluation des risques de cybersécurité (MoRiA)

Sommaire

II.1 Introduction

Dans ce chapitre, nous présentons une méthode basée sur l'IDM, MoRiA, **Mo**del-based **Ri**sk **A**nalysis (MoRiA) ainsi que son langage spécifique au domaine MoRiA **M**odeling **L**anguage (MoRiAML) et son processus d'utilisation.

La méthode MoRiA, vise à travers son langage de modélisation MoRiAML à étendre et aligner les concepts d'ingénierie système fonctionnels avec les concepts spécifiques au processus d'analyse de risques décrit dans les normes 2700X.

MoRiA, repose d'une part sur des normes d'ingénierie système et d'une autre part sur les normes de sécurité pour enrichir d'une part les techniques de modélisation conceptuelle utilisées par les équipes métiers et système dans l'industrie avec des concepts de sécurité et d'autre part l'analyse de risque de sécurité avec des précisions sur le discernement et la compréhension des détails structurels et fonctionnels du système ainsi que l'assurance d'une cohérence entre la vision des architectes système et sécurité. La mise en œuvre de techniques de modélisation conceptuelle est une occasion d'améliorer les pratiques d'ingénierie entre autres en minimisant la probabilité d'exigences incomplètes, peu claires, incohérentes et/ou erronées, en constituant la base de la vérification du modèle et en guidant sa validation. Cependant, si l'on veut augmenter les chances d'acceptation [RAB+15], ces pratiques ne doivent pas remettre en cause les savoir-faire existants, comme les éléments d'exigences, scénarios de conception, règles de cohérence qui devront être satisfaits. Pour cela, pour répondre à notre QR1, nous proposons l'utilisation d'un langage "dédié" (DSML) qui structure un langage de l'ingénierie système spécifique au domaine fonctionnel ainsi que la définition de la représentation que les nouveaux concepts vont prendre, nous permettant ainsi de modéliser les éléments de sécurité associés à l'analyse de risque avec les différents éléments fonctionnels de l'ingénierie système et cela dans les différentes phases/perspectives de conception. Par la suite, nous proposons une analyse itérative et continue des concepts de sécurité des normes 2700X afin de suivre la prise en compte de l'évolution des scénarios de risques au fur et à mesure de l'évolution de la modélisation du système et de l'évolution de contexte des menaces cyber. Un accent particulier a été mis sur l'aspect "représentation" des éléments de l'analyse de risque, la collaboration et la communication entre les équipes métiers, les experts de sécurité et les décideurs tout au long de la méthode afin de permettre une compréhension et une intervention de tous ainsi qu'une itération du processus tout au long du cycle de modélisation du système répondant ainsi à nos questions de recherche QR1 et QR2.

Pour définir un DSML, il faut définir une syntaxe abstraite, une ou plusieurs syntaxes concrètes et une sémantique. Dans les sections qui suivent, nous présentons l'IDM et son utilisation pour la définition d'un DSML dans la section II.2, par la suite nous proposerons notre langage MoRiAML dans la section II.3 à travers ces trois composants II.3.1, II.3.2 et II.3.2.1.

II.2 Ingénierie Dirigée par les Modèles (IDM)

L'IDM et l'ISBM ont suscité un intérêt notable d'activité dans le domaine de la recherche et de la pratique ces dernières années [AGD18][BSAN17]. Ces approches sont des solutions clés afin de surmonter les problèmes émergents de l'industrie 4.0 introduits dans la section .1.3.1 et portant sur la prise en compte et le respect des domaines transversaux ainsi que de leur comportement émergent et leurs propriétés non fonctionnelles, en particulier la sécurité tant au niveau de la modélisation des exigences qu'au niveau architectural de la solution et cela tout au long du cycle de conception. Ainsi ces deux approches vont nous servir de fondation pour répondre à nos questions de recherches portant sur la co-ingénierie et modélisation des exigences système et sécurité afin de construire, appliquer et maintenir l'évaluation des risques de cybersécurité tout au long du processus d'ingénierie système.

L'Ingénierie Dirigée par les Modèles (IDM) du domaine de l'informatique permet de «mécaniser» le processus de développement logiciel et système par la modélisation. Cette «mécanisation» s'appuie sur les connaissances d'ingénieurs expérimentés et leurs bonnes pratiques en matière de développement. L'ordonnancement de l'ensemble des transformations de modèles est alors vu comme un processus de conception. Ce processus doit inclure toutes les étapes de modélisation des plus conceptuelles à celles se rapprochant le plus de la solution finale. Ces dérivations successives "mono-métier" sont ce que l'on appelle l'ingénierie dirigée par les modèles. Or, il arrive aussi de vouloir transformer un modèle d'un métier pour qu'un autre métier apporte sa contribution dans son cycle de vie. L'Ingénierie Système Basée sur les Modèles (ISBM/MBSE) répond à cette problématique en établissant des ponts sémantiques entre des concepts identiques ou proches, mais représentés dans des formalismes différents. Ces deux approches sont donc complémentaires et nécessaires et permettent de s'appuyer sur un cadre d'architecture permettant de se centrer et se focaliser sur le système et ses éléments constitutifs ainsi que de balayer l'ensemble des points de vue métiers qui participent à son cycle de vie [Auz09].

L'IDM vise à définir des modèles, des méthodes et des outils adaptés à la représentation précise et efficace de systèmes à forte intensité logicielle et au raisonnement sur ces systèmes. Ces modèles, méthodes et outils ont pour objectif d'aider les ingénieurs métiers et les autres parties prenantes du système tout au long de son cycle de vie, de l'élaboration des exigences à la mise en œuvre et à sa maintenance. Ce soutien facilite toutes les tâches liées au système et la prise de décision impliquée, entre autres, dans les étapes de transformation, vérifications, visualisation, coopération et intégration. En outre, IDM caractérise les langages

de modélisation spécifiques au domaine (DSML) les mieux adaptés à la description d'activités spécifiques au domaine. Dans IDM, les modèles et les méthodes sont considérés comme des objets de première classe qui peuvent être étudiés pour eux-mêmes. Cette réification permet de développer des outils, des méthodes et des processus génériques.

L'Ingénierie système Basée sur les modèles (ISBM) ou l'Ingénierie Dirigée par les Modèles (IDM) est un processus de développement logiciel itératif et incrémental. La prise en charge de l'analyse et de la vérification des systèmes complexes développés selon le paradigme IDM nécessite la construction/l'utilisation d'une description du système à plusieurs niveaux d'abstraction en utilisant des modèles. Le *modèle* est le concept principal qui guide l'ensemble du processus de développement IDM [KBJV06][EH17] et est une *représentation* simplifiée [1] d'un système du monde réel conçu dans un but précis. Le modèle lui-même est *conforme* à un niveau plus abstrait, le *métamodèle*, qui définit les concepts utilisés pour décrire le modèle et ses relations [Béz04]. Ce métamodèle est également conforme à un niveau d'abstraction supplémentaire, le méta-métamodèle, qui est conforme à lui-même, comme le montre la figure II.1.

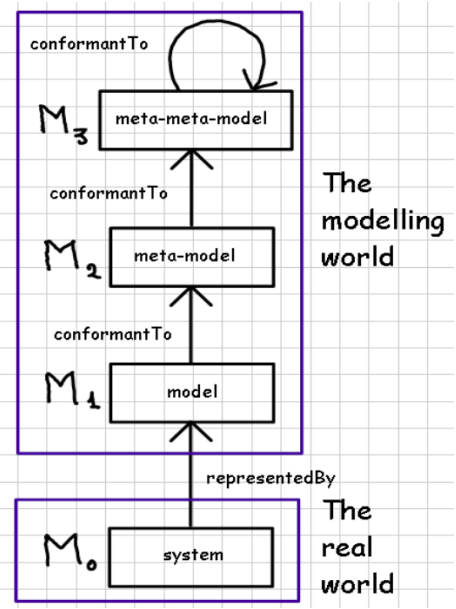


FIGURE II.1: Description du système sous plusieurs niveaux d'abstraction [Béz04]

La vision globale du développement du système IDM Figure II.2 va des *modèles* d'application jusqu'à la réalisation opérationnelle, en passant par des *transformations* de modèles consécutives. Cela permet la réutilisation des *modèles* et l'exécution de systèmes

1. https://fr.wikipedia.org/wiki/Mod%C3%A8le_scientifique

sur différentes *plateformes*. IDM recherche des solutions selon des dimensions orthogonales : la conceptualisation (colonnes de la figure II.2) et la mise en œuvre (lignes de la figure II.2). La question de *l'implémentation* concerne la mise en correspondance des modèles avec certains systèmes existants ou futurs. Par conséquent, elle consiste à définir trois aspects fondamentaux :

1. **Le niveau de modélisation :** où les modèles sont définis ;
2. **Le niveau de réalisation :** où les solutions sont mises en œuvre par le biais d'artefacts qui sont réellement utilisés dans les systèmes en cours d'exécution ;
3. **Le niveau d'automatisation :** où les mappings entre les niveaux de modélisation et de réalisation sont mis en place.

La question de la *conceptualisation* est orientée vers la définition de modèles conceptuels pour décrire la réalité. Elle peut être appliquée à trois niveaux principaux :

1. **Le niveau application :** où les modèles des applications sont définis, les règles de transformation sont exécutées et les composants réels en fonctionnement sont générés ;
2. **Le niveau du domaine d'application :** où l'on définit le langage de modélisation, les transformations et les plates-formes de mise en œuvre pour un domaine spécifique ;
3. **Le méta-niveau :** où la conceptualisation des modèles et des transformations est définie.

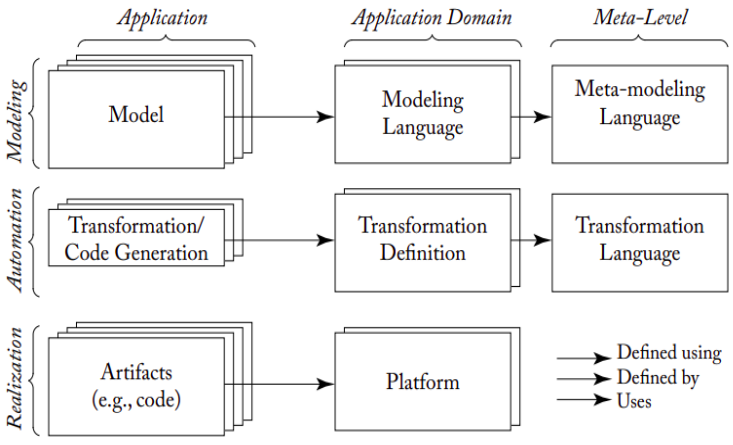


FIGURE II.2: Déroulement de la méthode IDM [BCW17]

Le modèle est défini à l'aide d'un langage de modélisation qui est défini par un méta-langage de modélisation, qui peut être défini par lui-même. Les transformations sont définies

par une définition de transformation qui est définie en utilisant un langage de transformation. Le résultat peut être mis en correspondance avec le code/les artefacts d'une plate-forme spécifique par transformation/génération de code.

Pour des raisons évoquées dans [EH17] telles que le soutien quant à la séparation des préoccupations en matière de conception, l'assurance d'une meilleure compréhension du comportement des modèles, la réduction des efforts des utilisateurs, la diminution des problèmes liés à la conception de systèmes complexes, le support lors de la manipulation des modèles ainsi que la garantie de l'interopérabilité et de la portabilité des modèles, l'IDM est de plus en plus liée à l'ingénierie des langages de modélisation des domaines spécifiques (DSML). En effet, un DSML est un langage qui définit des notations et des abstractions appropriées pour représenter efficacement un problème dans le domaine spécifique qu'il décrit [Slo02], qui est dans notre cas la co-modélisation du système et de la sécurité pour une meilleure évaluation des risques de sécurité lors des phases d'exigence et de conception du cycle de vie de développement. Un langage spécialisé va cibler plus particulièrement un domaine spécifique, ou intention de modélisation particulière. Ce langage permettra de capturer l'information avec un plus grand degré de précision et laissera moins de place à l'interprétation. Grâce à sa couverture moindre, les DSML embarquent une sémantique plus riche/formelle et sont souvent utilisables pour une vérification et une génération plus avancées. De plus un langage spécialisé est plus explicite pour l'expert puisqu'il utilise son vocabulaire métier, les concepts du domaine, au lieu de concepts plus généraux éloignés de la culture de l'utilisateur. De même, le nombre de concepts de diagrammes est beaucoup plus limité, facilitant l'apprentissage du langage. Sa mise en œuvre est également facilitée avec des outils dédiés, qui peuvent être très compacts et performants. En permettant la spécification, la visualisation et la vérification d'un système, avec une correspondance entre le monde du problème et le monde de la solution, les DSML améliorent la qualité, la fiabilité, la maintenabilité, la ré-utilisabilité et la flexibilité [KBJV06]. C'est pour cela, que l'utilisation d'un DSML pour modéliser des propriétés non fonctionnelles, comme la sécurité conduira à de meilleures solutions [EH17].

Tout cela explique notre choix quant à l'utilisation de l'ISBM/IDM pour définir notre DSML, MoRiAML ainsi que son outil de modélisation graphique pour concevoir des architectures de systèmes sécurisés. Nous implémenterons ces modèles dans des méthodes d'ingénierie système et d'analyse de risque utilisées dans l'industrie afin d'analyser, représenter et de prendre en compte les risques dans la modélisation système et en particulier, l'identification et la traçabilité des attaques.

Une approche, fréquemment utilisée pour définir les langages de modélisation graphique, est l'approche de méta-modélisation pour la définition des langages [EH17][Chi12]. Elle définit un langage de modélisation comme un ensemble de cinq composants (figure II.3) :

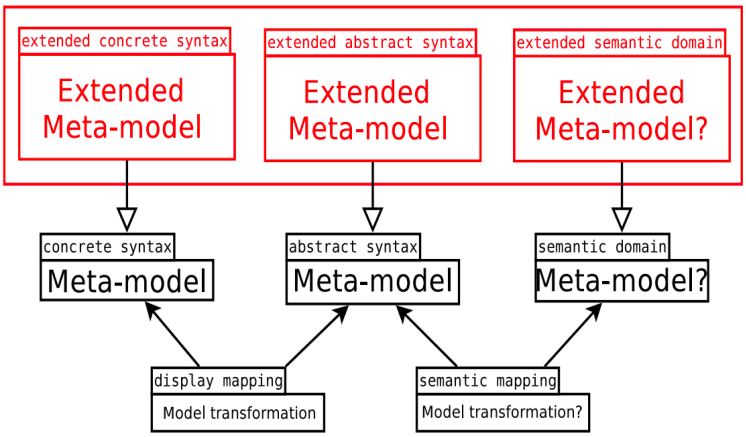


FIGURE II.3: Approche de méta-modélisation pour la définition de DSML [EH17]

1. **Syntaxe abstraite :** Elle exprime un ensemble de notations (concepts et relations) spécifiques au domaine du langage. Dans l'ingénierie dirigée par les modèles, le domaine est modélisé par l'utilisation d'un métamodèle. Par conséquent, le métamodèle décrivant le domaine représente la syntaxe abstraite du langage de modélisation. Les métamodèles jouent le même rôle pour les langages de modélisation que les grammaires pour les langages de programmation [Chi12] ;
2. **Syntaxe concrète :** Définit un ensemble de symboles, qui sont utilisés pour représenter les concepts du métamodèle. Un langage de modélisation peut avoir une ou plusieurs syntaxes concrètes, chacune étant définie par un métamodèle de "surface d'affichage" ;
3. **Le domaine sémantique :** Définit la signification des concepts et des relations dans le langage. Dans l'IDM, la sémantique pourrait être définie par le biais du mappage sémantique vers la sémantique précise d'un langage de programmation ou d'une plate-forme existante. Par conséquent, une sémantique bien définie garantit l'absence d'ambiguïté lors de l'exécution des modèles [EH17] ;
4. **Le mapping d'affichage :** Représente le lien entre la syntaxe abstraite et la syntaxe concrète. Il est défini à l'aide de transformations de modèles ;
5. **Le mapping sémantique :** Représente le lien entre la syntaxe abstraite et la sémantique. Il est défini à l'aide de transformations de modèle, principalement la génération de code ;

Notre langage MoRiAML englobe les trois premiers composants. Dans II.3.1, II.3.2 et II.3.2.1, nous décrivons respectivement les syntaxes abstraite et concrète de MoRiAML ainsi que son domaine sémantique. La dernière section de ce chapitre présente le processus d'utilisation de MoRiA.

II.2.0.1 Mécanisme d'extension de profil

Il existe trois méthodes principales pour définir un DSML [Sel09] :

1. Raffiner un langage de modélisation existant : En spécialisant certains de ses concepts généraux afin de représenter les concepts spécifiques du domaine ;
2. Étendre un langage de modélisation existant : En enrichissant le langage existant en ajoutant de nouveaux concepts spécifiques au domaine et en implémentant les concepts existants ;
3. Définir le nouveau DSML à partir de zéro.

Définir un nouveau langage à partir de zéro présente des inconvénients, tels que l'absence de structure de support, des difficultés liées au développement d'un support d'outils précis et peu coûteux en raison de la sémantique sophistiquée du langage de modélisation et de son interprétation. Par conséquent, le raffinement ou l'extension d'un langage de modélisation est l'occasion d'améliorer ses pratiques d'ingénierie en bénéficiant de la réutilisation, à un certain niveau, de la structure du langage et des outils existants [Sel09][DCB+15].

Dans le contexte de notre travail, nous proposons d'étendre le langage existant SysML [OMG15a] ; La mise en œuvre efficace du langage SysML nécessite l'utilisation d'un cycle de conception systématique comme celui avancé dans la norme 15288 [Tur08]. Nous proposons donc d'étendre les concepts d'ingénierie système inhérents aux normes 15288, 1220 portant sur les activités menées au cours des phases du cycle de vie d'un système. Ainsi, MoRiAML étend le langage de modélisation existant SysML pour couvrir la modélisation des systèmes sécurisés notamment avec de nouveaux concepts spécifiques provenant de la norme 27001 portant sur la gestion des risques numériques à travers une représentation SysML. Même si elle relève d'une pratique particulière, la modélisation conceptuelle doit permettre la pratique métier et non pas l'inverse, sous peine d'un rejet ou d'un mauvais usage de la part des équipes et donc d'une inefficacité de la technique. Ce point sera notamment important lors de la définition des concepts de sécurité dans les modèles de l'ingénierie système. Notre langage se veut être un support aidant la co-identification et co-définition des

concepts de sécurité tout en prenant en compte le point de vue ainsi que les préoccupations des différentes équipes et corps de métiers impliqués dans le projet : architectes système, analystes de sécurité, responsables de la sécurité des systèmes d'information (RSSI), gestionnaire de budgets, communicants et décisionnaires/responsables. De ce fait les concepts de sécurité amenés dans l'ingénierie système se doivent d'être clairs de par leur définition et alignement avec les concepts système existants ainsi que proches des représentations utilisées par les équipes métier afin de faciliter l'apprentissage et l'utilisation.

À travers ce travail nous proposons, une méthode de co-ingénierie permettant en outre la communication entre les acteurs métiers et sécurité du système. En mettant à disposition un vocabulaire et une représentation partagée entre les domaines conduisant ainsi à faciliter et renforcer l'analyse de risque, éviter les incohérences ou les oublis ainsi que de permettre une meilleure maîtrise de l'intégration ou corrections des éléments de sécurité. Cette méthode sera basée sur l'ISBM/IDM.

II.3 Présentation de la méthode MoRiA

Comme indiqué dans le chapitre l'Introduction et l'État de l'art, les standards ISO/IEC/IEEE 15288 et 1220 constituent une bonne base pour la modélisation d'un système complexe. Cependant, ces standards spécifiques aux processus de l'ingénierie système ne traitent pas les concepts de sécurité, en particulier ceux nécessaires à la réalisation de l'analyse de risque. Par conséquent, pour co-ingénierer et co-modéliser les exigences de système et les exigences de sécurité permettant l'intégration et l'évaluation des risques de cybersécurité lors de la définition du système (QR1) ainsi qu'assurer la mise à jour de l'architecture et de l'analyse de risque (QR2), nous proposons la méthode MoRiA (**Mo**del-based Cyber **Ri**sk **A**nalysis) permettant la co-ingénierie des concepts fonctionnels d'ingénierie système avec ceux de la sécurité nécessaires à la réalisation d'une analyse de risque numérique comme décrite dans la famille des normes 2700X. MoRiA comporte :

1. Un langage de modélisation MoRiAML défini par une syntaxe abstraite, une syntaxe concrète et une sémantique.

2. Un processus d'utilisation de MoRiAML qui décrit les acteurs et les étapes à suivre et à utiliser lors de la définition et modélisation d'un système sécurisé ;

II.3.1 Syntaxe abstraite du langage de modélisation MoRiAML

Les concepts fonctionnels de l'ingénierie système permettent aux différents acteurs de la modélisation de collaborer autour d'un modèle commun pour définir un système. La conception de système donne souvent lieu à une accumulation de documentations et perceptives/vues qui doivent toutes être croisées et mises à jour pour maintenir la cohérence et respecter les spécifications du système. Les concepts fonctionnels de l'ingénierie système n'abordent pas la conception avec la notion de classes, mais avec la notion de blocs qui à partir d'exigences système deviendront des parties mécaniques, électroniques, informatiques ou autres. Les concepts fonctionnels de l'ingénierie système sont un moyen de regrouper à travers un modèle commun à tous les corps de métiers, les spécifications, les contraintes, et les paramètres de l'ensemble du système. Cependant, ces concepts et les méthodes d'ingénierie système les utilisant manquent de notions permettant de modéliser et prendre en compte les besoins de sécurité.

En conséquence, la syntaxe abstraite (métamodèle) de MoRiAML étend la syntaxe abstraite de concepts fonctionnelle de l'ingénierie système avec plusieurs concepts spécifiques au domaine de la sécurité. Nous présentons d'abord dans la sous-section suivante, un aperçu du métamodèle des concepts fonctionnels de l'ingénierie système lors de la définition d'un système, en particulier leurs représentations à travers SysML et nous détaillons l'intégration des concepts de sécurité pour la définition de la syntaxe abstraite de MoRiAML.

II.3.1.1 Métamodèle des concepts fonctionnels de l'ingénierie système

Dans notre travail, le premier défi que nous relevons est celui de l'identification des concepts fonctionnels de l'ingénierie système définis et raffinés à chaque perspective de l'ingénierie système (de la définition des exigences à l'implémentation de l'architecture physique du système) et sur lesquels nous allons rattacher nos concepts non fonctionnels de sécurité. Avec comme objectif par la suite d'aligner ces concepts de sécurité avec ceux spécifiques à l'analyse de risque numérique. Comme présenté dans notre état de l'art, l'ingénierie des systèmes utilise des normes qui décrivent les activités menées au cours des phases du cycle de vie d'un système. Nous nous sommes basés sur une description fonctionnelle des concepts et de leurs relations définies, mises en œuvre, implémentées et raffinées tout au long de ces quatre perspectives de conception (figure II.4) pour élaborer un métamodèle.

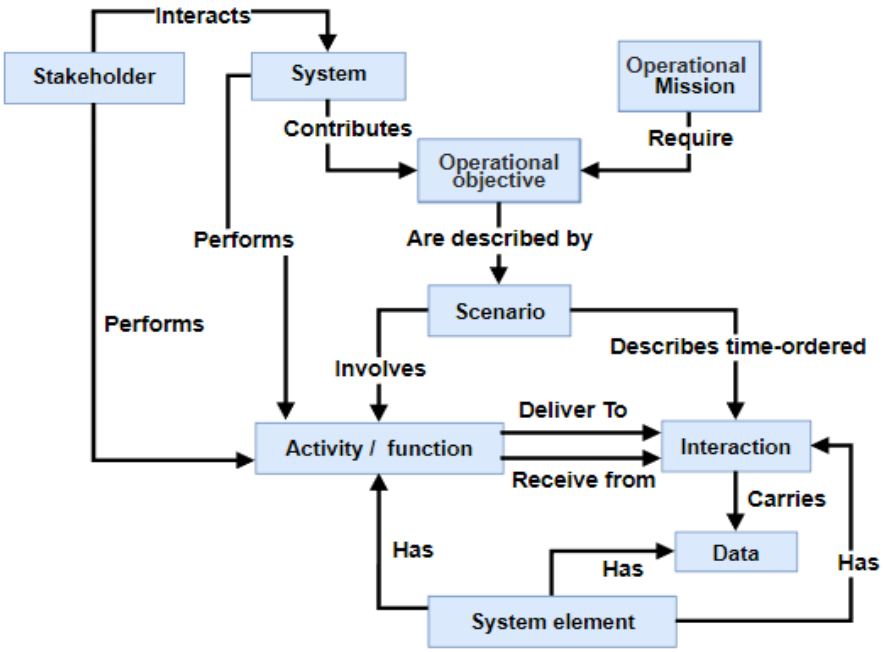


FIGURE II.4: Métamodèle représentant les concepts fonctionnels de l'ISBM et leurs relations

1. **Partie prenante :** Individu ou organisation ayant un droit, une part, une revendication ou un intérêt dans un système ou dans sa possession de caractéristiques qui répondent à leurs besoins et attentes ;
2. **Mission opérationnelle :** La tâche, le devoir ou la fonction spécifique définie pour être accomplie par un système ;
3. **Objectif opérationnel :** La capacité d'un système à exécuter un plan d'action particulier ou à obtenir un effet souhaité dans un ensemble de conditions spécifiées ;
4. **Scénario :** Description d'une séquence d'événements qui comprend l'interaction du produit ou du service avec son environnement et ses utilisateurs, ainsi que les interactions entre les composants du produit ou du service ;
5. **Activité :** Tâche ou action effectuée pour atteindre le résultat souhaité ;
6. **Interactions :** Communications, coopérations et collaborations entre les différents nœuds (système, parties prenantes, etc.) qui agissent ensemble, par le biais de fonctions et d'interactions réalisées, pour résoudre des problèmes locaux et stratégiques ;
7. **Données :** Une donnée doit être prise dans son sens le plus large, elle peut représenter un signal, une image, une information, un état physique, ou une unité de grandeur ;
8. **Système :** Ensemble organisé d'éléments fonctionnant comme un tout, répondant à la demande et au besoin du client et des utilisateurs.

9. **Élément du système :** Un membre d'un ensemble d'éléments qui constitue un système. Un élément de système est une partie discrète d'un système qui peut être mise en œuvre pour répondre à des exigences spécifiées.

SysML est à l'ingénierie des systèmes complexes et/ou hétérogènes ce qu'UML est à l'informatique. SysML doit permettre à des acteurs de corps de métiers différents de collaborer autour d'un modèle commun pour définir un système. La conception de système donne souvent lieu à une accumulation de documentations qui doivent toutes être croisées et mises à jour pour maintenir la cohérence et respecter les spécifications du système. SysML n'aborde plus la conception avec la notion de classes, mais avec la notion de blocs qui deviendront des parties mécaniques, électroniques, informatiques ou autres. SysML est un moyen de regrouper dans un modèle commun à tous les corps de métiers, les spécifications, les contraintes, et les paramètres de l'ensemble du système. MoRiAML à travers ces concepts fonctionnels de l'ingénierie système s'inscrit principalement dans trois diagrammes SysML : le diagramme de cas d'utilisation, le diagramme d'activité et le diagramme d'exigences voir la section II.3.2.

Dans notre contribution, nous utiliserons ces abstractions/concepts de l'ingénierie système ci-dessus pour exprimer la sémantique des concepts syntaxiques de l'ingénierie système, en alignant chacun des concepts du métamodèle qui articule un sens similaire/analogue avec ceux de la sécurité, comme détaillé dans la section suivante.

II.3.1.2 Métamodèle des concepts de sécurité de la norme 27001

Comme présenté précédemment, les normes internationales prescrivent des lignes de base pour la sécurisation des actifs, tant numériques que physiques. La norme ISO (International Organization for Standardization) 27001 relative aux systèmes de gestion de la sécurité de l'information (SI), en particulier, se concentre sur la sécurisation des actifs informationnels, mais propose également des contrôles de sécurité physique. La norme ISO 27001 définit des concepts et des pratiques de mise en œuvre de la sécurité de l'information dans les organisations, en fournissant des lignes directrices flexibles sur la manière dont ces méthodes et pratiques doivent être mises en œuvre. Comme c'est le cas avec les normes ISO en général, l'implémentation de ces lignes directrices est laissée aux entreprises, afin qu'elles puissent les développer et les mettre en œuvre en fonction de leurs contextes et spécificités. Sur la base d'une approche de catégorisation inductive, les auteurs dans [MG11][MG10b][MG10a] ont développé un métamodèle (figure II.5) de la norme ISO 27001 ISS (Annexe A spécifiquement) ainsi que son évaluation sémantique.

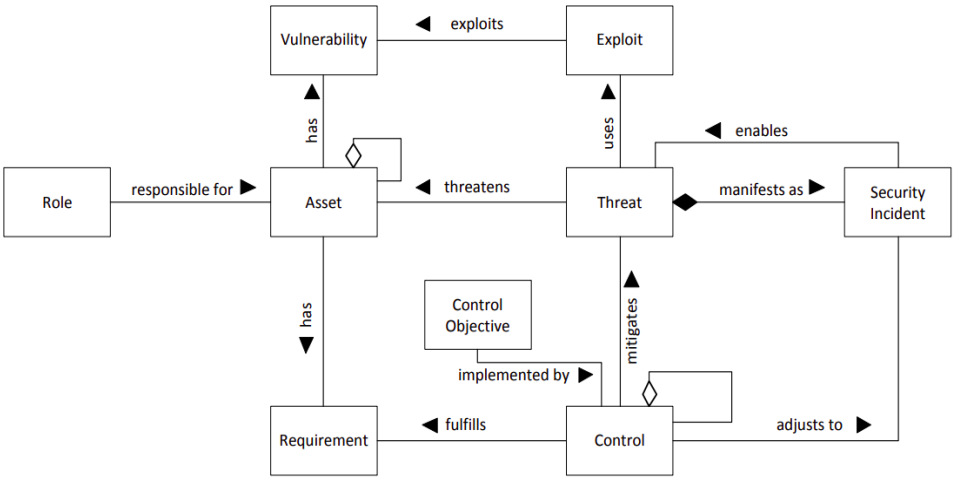


FIGURE II.5: Métamodèle représentant les concepts de sécurité de la norme ISO 27001 [MG11]

1. **Actif :** Éléments pouvant être considérés comme un sujet d'analyse de sécurité / Quelque chose dans le système et/ou son environnement à protéger des conséquences négatives ;
2. **Rôle :** Le propriétaire de l'actif est responsable de la gestion efficace de l'actif tout au long de son cycle de vie. Cette responsabilité peut être différente de la propriété légale et peut être assumée par un individu, un service ou une autre entité ;
3. **Exigence :** Un type de règle qui saisit une déclaration formelle pour définir les lois, les règlements, les directives et les politiques de sécurité ;
4. **Menace :** Cause potentielle d'un incident indésirable, qui peut entraîner un préjudice pour un système ou une organisation ;
5. **Incident de sécurité :** Un seul ou une série d'événements/exploitations de sécurité de l'information non désirés ou inattendus qui ont une probabilité significative de compromettre les opérations commerciales et de menacer la sécurité de l'information ;
6. **Vulnérabilité :** Une faiblesse d'un actif ou d'un contrôle qui peut être exploitée comme une menace ;
7. **Exploitation :** Il s'agit d'une occurrence identifiée d'un système, d'un service ou d'un état de réseau indiquant une violation possible de la politique de sécurité de l'information ou une défaillance des contrôles, ou une situation précédemment inconnue qui peut être pertinente pour la sécurité ;
8. **Contrôle :** Moyens de gestion des risques, y compris les politiques, les procédures, les

lignes directrices, les pratiques ou les structures organisationnelles, qui peuvent être de nature administrative, technique, de gestion ou juridique ;

9. **Objectif de contrôle :** Déclaration décrivant ce qui doit être réalisé à la suite de la mise en œuvre des contrôles ;

La norme ISO/IEC 27001 régit la mise en place d'un système de management de la sécurité de l'information (SMSI) et des concepts de sécurité qui doivent nécessairement être intégrés à un processus de gestion du risque. La gestion du risque est l'approche préconisée dans l'ISO/IEC 27001 qui sert de ce fait de base à la politique de sécurité de l'organisme concerné. Le SMSI s'appuie sur un modèle d'amélioration continue (appelé PDCA ou « Roue de Deming » [THI03]) qui conduit dans un premier temps à fixer les objectifs du SMSI (Plan), à le déployer (Do), puis à vérifier les écarts éventuels entre ce qui a été défini et ce qui est mis en œuvre (Check), enfin à mettre en place les actions qui permettront de corriger ces écarts et améliorer le SMSI (Act). L'ISO/CEI 27001 ne fait que fixer un cahier des charges spécifiant chacune des étapes clefs de l'appréciation des risques. L'organisme a le libre choix, de développer sa propre méthode en suivant les objectifs fixés par l'ISO/CEI 27001 ou d'en appliquer une déjà éprouvée (voir chapitre État de l'art pour la liste des méthodes d'analyse de risque implémentant la famille des normes 27000).

Nous avons utilisé les concepts de sécurité précédemment décrits comme base pour définir notre profil MoRiAML. Afin de réaliser ce travail, la famille des normes 2700X nécessite l'utilisation et la définition de matrices d'évaluation afin de coter certains de ces concepts. Dans ce qui suit, nous présentons certaines de ces matrices.

II.3.1.2.1 Besoin de sécurité et impact

Le concept d'*actif* a le concept *exigence*. Selon le contexte dans lequel elles sont utilisées, elles résument à elles seules les *exigences* de sécurité de l'entité à travers un "besoin de sécurité", ou les moyens mis en œuvre pour répondre au besoin exprimé, sans pour autant définir l'élément de *contrôle*.

En temps que "besoin de sécurité" on associe une valeur numérique, généralement comprise entre 0 et 4, qui permet d'évaluer, en fonction de la complétude des matrices, l'importance de chaque besoin de sécurité. Les plus utilisés étant : disponibilité, intégrité, confidentialité et traçabilité (DICT)[CSG18].

1. **Disponibilité :** une ressource doit être accessible et utilisable par son destinataire

autorisé à l'endroit et à l'heure prévue ;

2. **Intégrité :** les données sont bien celles que l'on croit être ;
3. **Confidentialité :** une ressource n'est accessible qu'aux seules personnes autorisées ;
4. **Traçabilité :** garantie que les accès et tentatives d'accès aux ressources sont tracés et que ces traces sont conservées et exploitables.

Ces métriques peuvent être définies en choisissant une option parmi un ensemble de postulats, comme dans la figure suivante II.6.

Disponibilité

Niveau	Définition
4	Le bien ne peut pas être indisponible plus d'une heure
3	Le bien ne peut pas être indisponible plus de 4 heures
2	Le bien ne peut pas être indisponible plus d'une journée
1	Le bien ne peut pas être indisponible plus d'une semaine

Confidentialité

Niveau	Définition
4	Donnée secrète
3	Donnée confidentielle
2	Donnée à accès restreint
1	Donnée interne
0	Donnée publique

Intégrité

Niveau	Définition
4	Aucune modification intempestive tolérée
3	Toute modification intempestive doit être détectée et corrigée
2	Toute modification intempestive doit être détectée
1	Aucune exigence, la donnée peut être modifiée

Traçabilité

Niveau	Définition
4	Exigence légale
3	Besoin métier
2	Besoin pour information
1	Aucune exigence

FIGURE II.6: Exemple de matrices DICT [2]

Par la suite, le calcul de l'impact de la perte ou altération de ce besoin de sécurité est calculé. Cette perte/altération sera une première formulation du concept d'*incident de sécurité*. Les impacts sont généralement répartis sur 4 niveaux et 5 grandes catégories : impacts sur la mission, impacts juridiques, impacts financiers, impacts humains, impacts d'image. L'objectif est d'attribuer un niveau global d'impact pour la perte/l'altération du besoin de sécurité de l'actif. Comme mentionné précédemment, les normes n'imposent rien quant aux détails d'implémentation. Les matrices enrichissant et spécifiant ces critères sont donc à adapter en fonction du contexte et des besoins de l'étude.

2. `https://unitedstatesofsecurity.net/dict-ladn-de-la-cybersecurite/`

ÉCHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

FIGURE II.7: Exemple de matrice d'impact [ebi18]

II.3.1.2.2 Vraisemblance de la menace

Le concept de *Menace* peut être identifié et défini à partir de métriques telles que la motivation et les ressources, comme l'illustrent les bases de connaissances proposées dans les fiches méthodologiques de l'ANSSI[II.3.3] pour estimer le niveau de vraisemblance/dangerosité.

		Motivation		
		+	++	+++
Ressources	+++	MOYEN	ÉLEVÉ	ÉLEVÉ
	++	FAIBLE	MOYEN	ÉLEVÉ
	+	FAIBLE	FAIBLE	MOYEN

FIGURE II.8: Exemple de matrice de vraisemblance de la menace[II.3.3]

II.3.1.2.3 Pertinence de l'incident de sécurité

La pertinence est établie à travers le couplage de l'impact de la perte/altération du besoin de sécurité avec la vraisemblance de la menace (figure II.9).

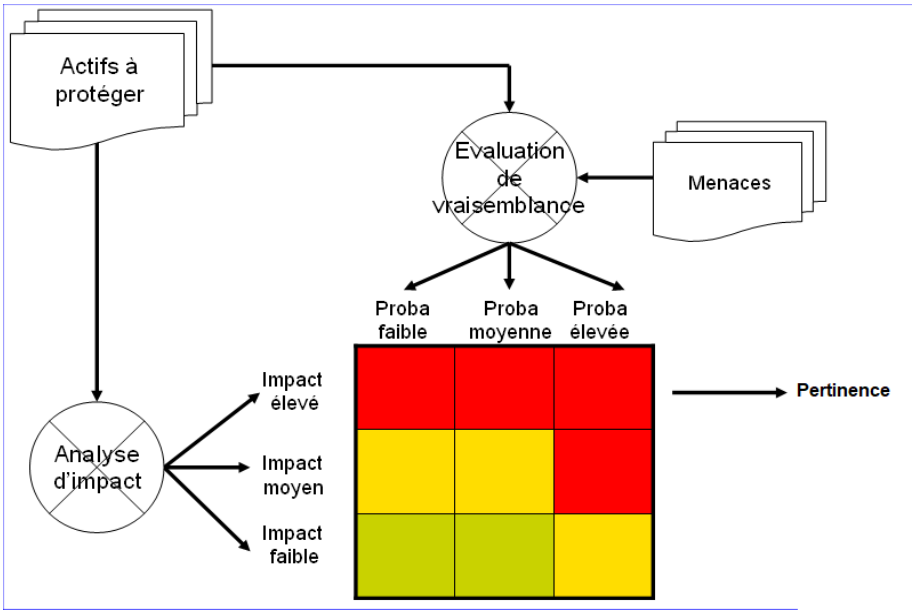


FIGURE II.9: Calcul simplifié de la pertinence de l'incident de sécurité [Ins05]

II.3.1.2.4 Niveau de menace des parties prenantes

Les parties prenantes constituent une partie du risque cependant la norme 27001 ne les prend pas en compte. Seules les méthodes d'analyse de risque implémentant la norme (voir I.1.5) proposent des moyens de calculer leur niveau de menace. La méthode EBIOS RM est la plus récente et celle qui propose des matrices les plus génériques permettant de traiter de nombreux contextes d'étude. La menace en tant que partie prenante se voit donc attribuer des métriques spécifiques [II.3.3] (dépendance, exposition, confiance ...) pour définir leur niveau de menace vis-à-vis du sujet étudié.

	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFIANCE
1	Relation non nécessaire aux fonctions stratégiques.	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2	Relation utile aux fonctions stratégiques	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3	Relation indispensable mais non exclusive.	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	Relation indispensable et unique (pas de substitution possible à court terme).	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisation.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

FIGURE II.10: Calcul du niveau de menace[II.3.3]

Les concepts de sécurité, issus des normes 2700X ainsi que les concepts d'ingénierie système, issus des normes 15288 et 1220 et précédemment décrits, constituent une base pour le métamodèle de MoRiAML.

II.3.1.3 Métamodèle de MoRiAML

Le métamodèle MoRiAML spécialise le métamodèle des concepts fonctionnels de l'ingénierie système II.4 pour permettre la définition, la réalisation et la prise en compte de la sécurité II.5 dans la définition du système.

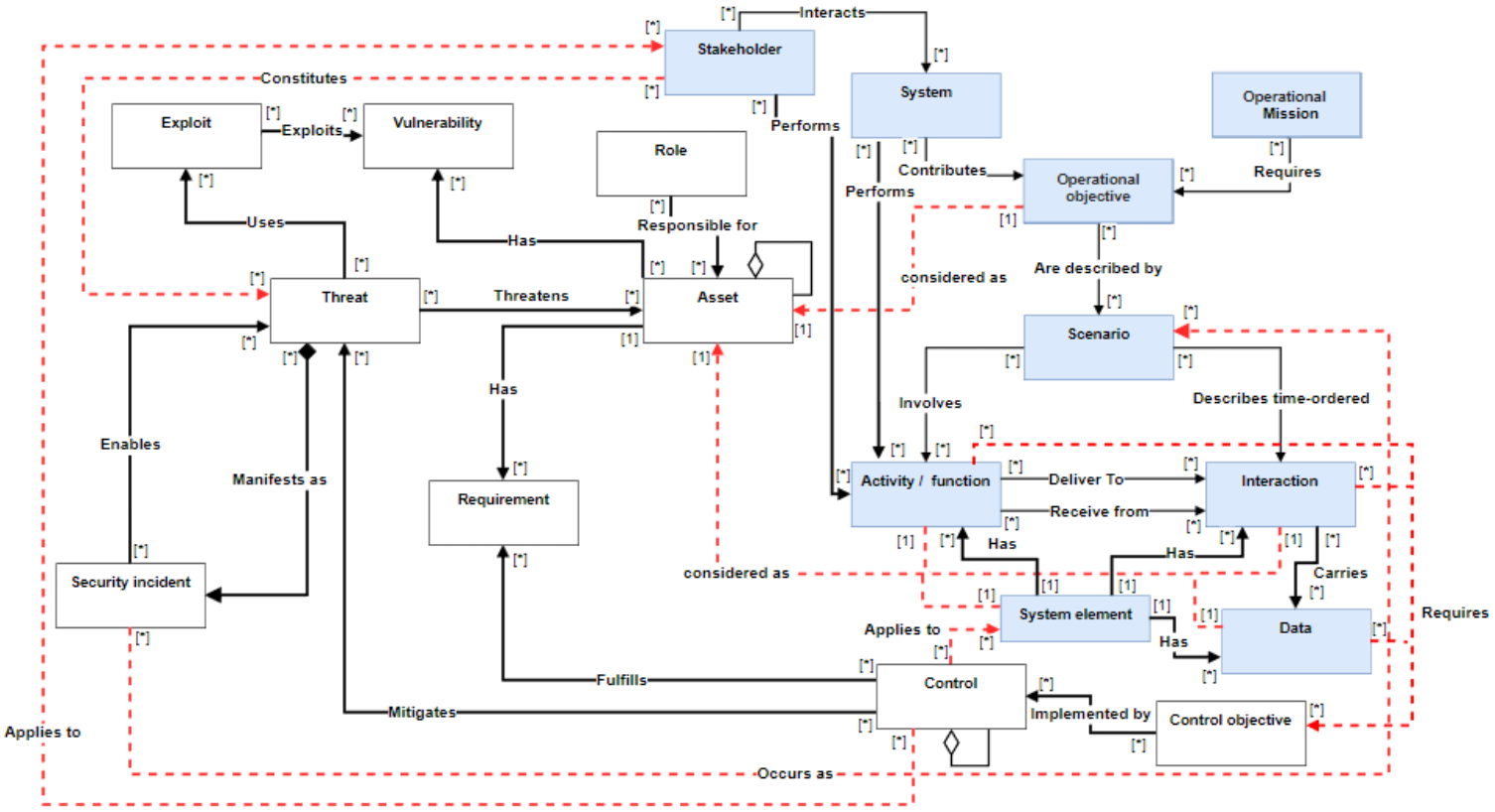


FIGURE II.11: Syntaxe abstraite MoRiAML (métamodèle)

Dans la figure II.11, nous illustrons notre métamodèle. Nous présentons nos extensions dans une seule figure comprenant les concepts fonctionnels de l'ingénierie système en bleu, en blanc ceux de sécurité et les nouvelles relations entre les deux domaines en pointillé. À travers MoRiAML, nous alignons les concepts de *partie prenante* avec celui de *menace*, de *scénario* avec *incident de sécurité*, celui d'actif avec les *activités/fonctions*, *interactions*, *données*, *élément système* et *objectif opérationnels*, le concept de sécurité *contrôle* avec le concept d'*élément système*, et de *partie prenante* et pour finir le concept de sécurité *objectif de contrôle* avec les concepts d'*activités/fonctions*, *interactions* et *données*. Nous décrivons en détail dans la section II.3.2.1 l'alignement de ces concepts.

II.3.2 Syntaxe concrète du langage de modélisation MoRiAML

Comme indiqué précédemment, la définition d'un DSML consiste à faire correspondre une ou plusieurs syntaxes concrètes à sa syntaxe abstraite. La syntaxe concrète est la notation lisible par l'utilisateur et sert pour la présentation et la visualisation des modèles. Il s'agit d'un ensemble de notations textuelles ou visuelles qui facilitent la présentation et la construction du langage. Le fait de garder la syntaxe abstraite séparée et indépendante de sa ou ses syntaxes concrètes permet à un langage de modélisation d'avoir plusieurs représentations concrètes différentes pour divers contextes ou points de vue [Sel09]. La syntaxe concrète peut être définie de manière textuelle ou visuelle/graphique. Dans une syntaxe textuelle, les modèles sont décrits à l'aide de formes textuelles/mots clés structurées, tandis que dans une syntaxe visuelle, les modèles sont représentés à l'aide de formes/icônes de manière schématique, par exemple en visualisant les notations des nœuds et des bords par des rectangles et des flèches. Pour notre syntaxe concrète MoRiAML, nous avons choisi d'utiliser une approche graphique afin de permettre aux acteurs de corps de métiers différents de collaborer autour d'un modèle commun pour définir un système, notamment ceux du domaine de l'ingénierie système et de l'analyse de sécurité. En fait, pour bénéficier du mécanisme d'extension du DSML, nous avons réutilisé les notations visuelles de SysML pour représenter les nouveaux concepts que nous avons introduits dans la syntaxe abstraite afin de faciliter la compréhension et manipulation de ces derniers par les équipes métiers. Nous présentons dans le tableau II.1 une partie de la syntaxe concrète de MoRiAML héritée de la syntaxe concrète de SysML.

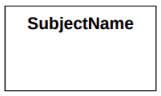
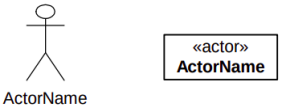
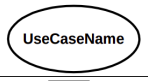
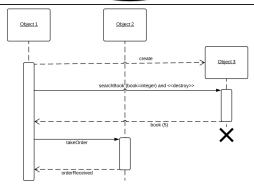
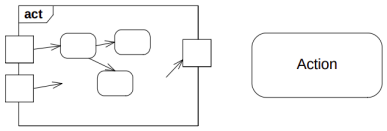
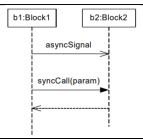
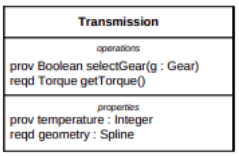
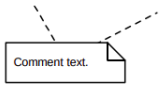
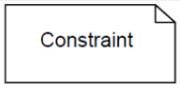
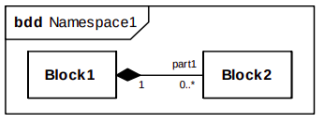
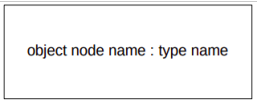
MoRiAML Concepts	SysML Concepts	Syntaxe concrète
Système	Sujet	
Partie prenante - Menace	Acteur	
Objectif - mission opérationnelle - Actif	Cas d'utilisation	
Scénario - incident de sécurité	Diagramme de séquence	
Activité / fonction - Exploitation, Contrôle	Activité / action	
Interaction	Message	
Donnée	Propriété du flux	
Rôle	Commentaire	
Exigences, objectif de contrôle	Contrainte	
Contrôle, élément du système	Bloc	
Vulnérabilité	Nœuds d'objets	

TABLE II.1: Syntaxe concrète de MoRiAML, modifiée à partir de [OMG15a]

II.3.2.1 Sémantique du langage de modélisation MoRiAML

MoRiAML étant un langage, pour le compléter et répondre entièrement à nos QRs sur la co-ingénierie et la modélisation des exigences de système et les exigences de sécurité permettant l'intégration et l'évaluation des risques de cybersécurité lors de la définition du système (QR1). La sémantique de MoRiAML a été réalisée à travers l'alignement conceptuel et sémantique entre le domaine de la sécurité et le domaine de l'ingénierie système. Cela consiste à aligner les entités (termes, concepts, rôles) appartenant aux deux domaines afin de parvenir par la suite à une sémantique d'un vocabulaire commun et partagé entre ces disciplines permettant ainsi la co-modélisation/ingénierie. Le tableau II.2 présente les similarités/alignements essentielles entre les concepts du métamodèle MoRiAML. Dans ce qui suit, nous argumentons et expliquons ces similitudes.

Concepts fonctionnels de l'ingénierie des systèmes (ISO 15288 et 1220)	**Concepts de cybersécurité (ISO 27001)**	**Alignement conceptuel**
Partie prenante	Menace	Éléments (personne, système d'information, organisation ou source de risque) qui interagissent directement ou indirectement avec le système. Une menace peut être interne ou externe à l'organisation à laquelle appartient l'objet de l'étude.
Objectif opérationnel, activité/fonction, interaction et données, élément du système	Actif	Les ressources d'information, les processus de mission/d'entreprise et/ou les programmes critiques qui présentent un intérêt particulier pour les adversaires potentiels ou réels. Un actif peut être matériel (par exemple, un élément physique tel que du matériel, un micrologiciel, une plate-forme informatique, un dispositif de réseau ou tout autre composant technologique) ou immatériel (par exemple, des êtres humains, des données, des informations, un logiciel, une capacité, une fonction, un service, une marque, un droit d'auteur, un brevet, une propriété intellectuelle, une image ou une réputation).
Élément du système, partie prenante	Contrôle	Les éléments opérationnels et techniques (ses composants, processus, données, sauvegardes ou contre-mesures) prescrits pour qu'un système puisse atteindre ses objectifs ou pour protéger le système.
Activité/fonction, interaction et données	Objectif de contrôle	Les objectifs de contrôle sont définis en fonction des besoins et exigences des actions, données, interactions et englobent la spécification des "exigences fonctionnelles" pour l'architecture de gestion de la sécurité de l'information d'une organisation.
Scénario	Incident de sécurité	Comment le système et ses acteurs interagissent dans le contexte d'une capacité ou d'un service du système. Ces interactions prennent souvent la forme de séquences d'actions et, dans le cas d'un attaquant, son objectif est de détourner ces actions pour atteindre son propre objectif.

TABLE II.2: Alignement conceptuel et sémantique entre les concepts fonctionnels et non fonctionnels de MoRiAML

Les parties prenantes du système constituant une partie de la menace

La **Menace** est alignée avec le concept de **partie prenante** par le biais de la relation ***constitue***. Une **menace** englobe toutes les causes potentielles d'un incident. Par conséquent, d'un point de vue fonctionnel, les **parties prenantes** de l'ingénierie conventionnelle, conçus comme légitimes, ***constituent*** une partie des risques de **menace** potentiels - parfois involontairement par leur proximité et leur interaction avec le **système**.

Objectifs opérationnels, activités/fonctions, interactions, données et éléments du système considérés comme actifs à protéger

Actif est aligné avec **Objectif opérationnel**, **activité/fonction**, **interaction**, **données** et **élément du système** par la relation ***considéré comme***. Le concept d'**Actif** englobe les éléments clés à prendre en compte dans l'analyse de sécurité. D'un point de vue fonctionnel, les services et fonctionnalités que le système réalise, les actions et tâches nécessaires à leur réalisation, les moyens de communication entre ces éléments et les informations transmises doivent être ***considérés comme*** les **actifs** (de type service ou d'information) à protéger.

Les contrôles de sécurité appliqués aux éléments du système et parties prenantes

Contrôle est aligné avec **élément du système** et **partie prenante** par la relation ***s'applique à***. Le concept **contrôle** comprend les moyens de gérer un risque, et d'un point de vue fonctionnel, ces mesures seront ***appliquées aux*** éléments du système ainsi que sur les parties prenantes interagissant avec.

Incident de sécurité se produisant en tant que scénario

Incident de sécurité est aligné avec **Scénario** par la relation ***se produit en tant que***. Les deux concepts s'appuient sur la notion de séquence d'événements, et tous deux basent leur séquence sur les concepts précédemment alignés **activité/fonction**, et **interaction**. Un **Incident de sécurité** ***se produit en tant que*** scénario spécifique du point de vue de l'attaquant, reliant ainsi les séquences d'événements que l'attaquant réalisera ou traversera pour atteindre ses objectifs.

Les besoins et exigences des activités/fonctions, interactions, données définissent les Objectifs de contrôle

Objectif de contrôle est aligné avec **activités/fonctions**, **interaction** et **donnée** par la relation ***nécessite***. Le concept **Objectif de contrôle** comprend les exigences et besoins de sécurité qui nécessiteront une implémentation fonctionnelle à travers le concept de **contrôle**.

II.3.2.2 Implémentation de l'analyse continue, itérative et contextuelle

Par ailleurs, pour répondre à la QR2 consistant à réaliser la mise à jour de l'architecture et de l'analyse de risque (QR2), nous proposons d'enrichir son métamodèle avec le concept de "Cyber Kill Chain" en bénéficiant et en capitalisant l'alignement conceptuel et sémantique effectué afin de proposer une représentation et une élaboration plus fine et opérationnelle de la Cyber Kill Chain directement dans les modèles du système permettant ainsi de façon continue et itérative l'analyse des risques. Dans un second temps, nous proposons aussi d'enrichir le métamodèle avec le concept d'"état" afin d'incorporer et de prendre en compte la notion de contexte dans lequel se trouve un acteur, le système ou un de ces composants, afin de produire des contextes/profils de risque/sécurité adaptés aidant ainsi à la réalisation et au maintien de l'analyse lors de la définition et modélisation de ces différents "états" durant son cycle de vie.

Cyber Kill Chain

Il existe différentes façons d'aborder et de construire une analyse de risque. Le point de vue du monde de la technique recherche à mettre en œuvre directement les meilleures mesures de sécurité disponibles. Néanmoins les actions et mesures choisies doivent être pertinentes et surtout justifiables aux yeux des décideurs. Pour justifier les actions à mener, ils utilisent des référentiels de sécurité composés et approuvés par des experts et des professionnels du domaine. Pour cette approche "remontante" (figure II.12), ils partent donc des actions opérationnelles pour construire la stratégie de sécurité de l'entreprise. En ayant comme objectif d'être conforme à ces référentiels, on se trouve alors dans une approche dite de mise en conformité [CLU12]. Une approche dont l'avantage réside dans sa rapidité et simplicité de mise en œuvre. Les équipes sécurité ne partent pas de rien, mais implémentent rapidement les actions pertinentes, avant de passer aux actions plus spécifiques. De plus, le besoin de recruter une ressource spécialisée en cybersécurité est moins prépondérant, car le plan d'action existe déjà au travers d'une expertise sous forme de guide qu'il faudra mettre en œuvre.

Cependant cette approche présente aussi ces inconvénients. Sur un système d'information existant, un premier travail de comparaison avec le guide choisi doit être réalisé pour éviter l'implémentation de mesures en doublon. De plus, cette approche ne prend pas en compte les besoins des métiers qui utilisent le système d'information. L'approche par la conformité a donc ses limites. Les guides de sécurité restent génériques et ne seront pas toujours adaptés aux ressources et connaissances métier de l'entreprise.

3. `https://matthieulobry.fr/securiser-son-entreprise/`

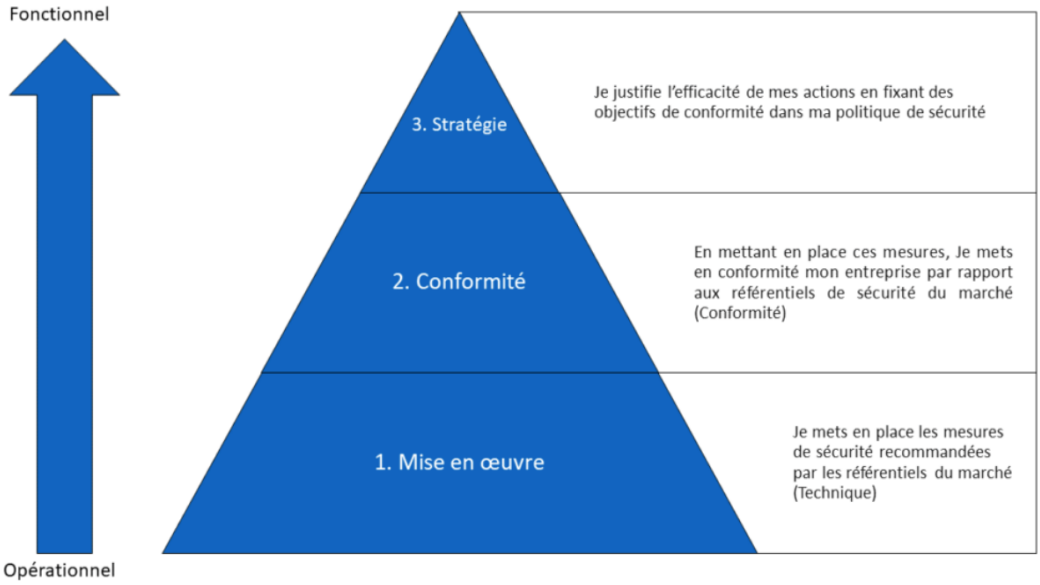


FIGURE II.12: Approche par la mise en conformité [3]

Dans le cas d'une analyse "descendante" (figure II.13), les équipes sécurité n'abordent pas dans un premier temps le sujet avec un regard technique. L'idéal est de pouvoir réfléchir avec les différents métiers de l'entreprise pour choisir les mesures de sécurité les plus efficaces et les moins contraignantes pour les utilisateurs. Cette analyse se base sur les connaissances que nous avons du système et les premières phases de son cycle de vie ne permettent qu'une étude superficielle. La réflexion se fait au fur et à mesure de l'avancement des travaux sur le sujet, par raffinements successifs, en fonction de ce que les équipes de sécurité connaissent et sont capable de modéliser. Dans un premier temps, ils s'intéressent aux grands enjeux pour identifier des « risques liés aux sources de risques », dans un second temps ils affinent la description du sujet et élaborent des « risques au niveau des éléments à protéger », puis étudient les « risques au niveau des supports » pour obtenir des risques détaillés et des mesures. C'est donc en réalisant des itérations successives et des activités supplémentaires que la gestion des risques accompagne le cycle de vie du sujet de l'analyse.

Ce processus d'itérations pourrait néanmoins être raffiné afin d'être plus intelligible, efficient et facilement mis en place à travers l'utilisation de la Cyber Kill Chain dans les modèles. L'objectif est de rassembler et travailler simultanément sur les entrées (*actifs*), intermédiaires (*menaces*) et sortie (*mesures de sécurité*) dans la même vue afin de calibrer et éliciter la notation des uns et des autres à travers la Cyber Kill Chain de façon itérative afin de réinjecter les résultats dans les différents diagrammes et éléments de modèles impliqués, permettant ainsi, dans notre contexte, une mise à jour de l'architecture réalisée avec

MoRiAML.

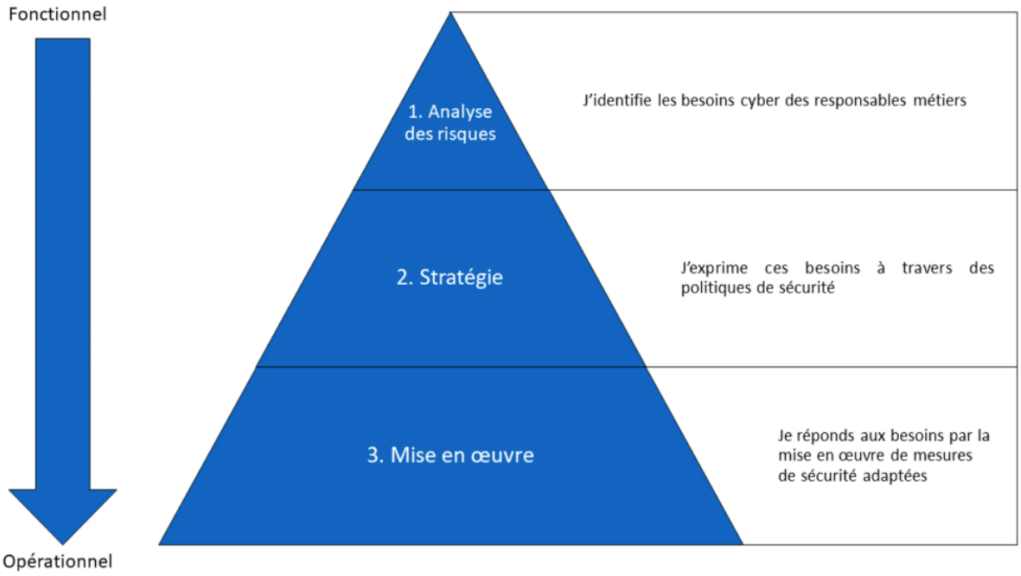


FIGURE II.13: Approche par l'analyse des risques [4]

Comme cela est le cas avec la norme ISO 27005 qui propose une méthodologie de gestion des risques descendante conforme et aux normes et concepts des ISO/CEI 2700X (figure II.14).

Le contexte est la première chose qui est établie. Une appréciation du risque est ensuite réalisée. Si cette appréciation donne suffisamment d'éléments pour déterminer les actions nécessaires pour ramener le risque à un niveau acceptable, alors la tâche est terminée. Sinon, une nouvelle itération est réalisée avec un contexte révisé (par exemple les critères d'évaluation du risque, les critères d'acceptations ou les critères d'impacts) et éventuellement sur des parties limitées de l'ensemble du domaine d'application. L'efficacité du traitement du risque dépend des résultats de l'appréciation du risque. Si le traitement du risque ne donne pas satisfaction, le risque sera qualifié de risque résiduel non acceptable, alors une nouvelle appréciation du risque est nécessaire avec éventuellement de nouveaux paramètres de contexte (comme des critères d'impact), suivi d'un traitement des risques. L'activité d'acceptation du risque doit fournir nécessairement des risques résiduels acceptables par les dirigeants. Une analyse du coût des mesures est alors proposée permettant l'acceptation des risques résiduels. Il est donc important que le plan de traitement des risques et son coût, dont des éventuelles et les mesures correctives, soit communiqués aux décideurs.

4. `https://matthieulobry.fr/securiser-son-entreprise/`

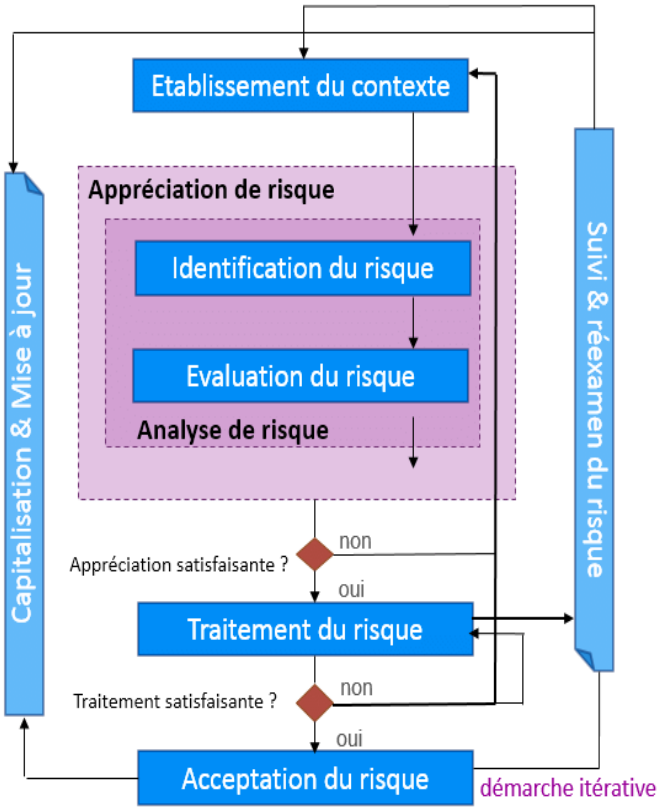


FIGURE II.14: Processus de gestion des risques [ISO08]

Le bon établissement du contexte ainsi que son appréciation et de son analyse sont les points cruciaux ainsi que pivots qui détermineront tout le déroulement de la démarche. Notamment à travers le concept d'*incident de sécurité*, il convient d'apprécier la vraisemblance des scénarios d'incidents, et cela à travers une estimation qualitative ou quantitative. Il convient d'estimer le niveau de risque de chaque scénario d'incidents. L'estimation du risque est basée sur l'appréciation des conséquences et de la vraisemblance.

Cependant, l'un des principaux problèmes auxquels sont confrontées les organisations aujourd'hui est l'émergence d'attaques ciblées menées par des adversaires qui ont facilement accès à des outils et des technologies sophistiquées dans le but d'établir une présence persistante et non détectée dans la cyber-infrastructure/architecture ciblée. Ces attaques en plusieurs étapes deviennent aujourd'hui plus complexes, impliquant des mouvements verticaux et horizontaux à travers de multiples éléments de l'organisation. La communauté des chercheurs en sécurité a donné un nom à cette chaîne d'événements en plusieurs étapes : la

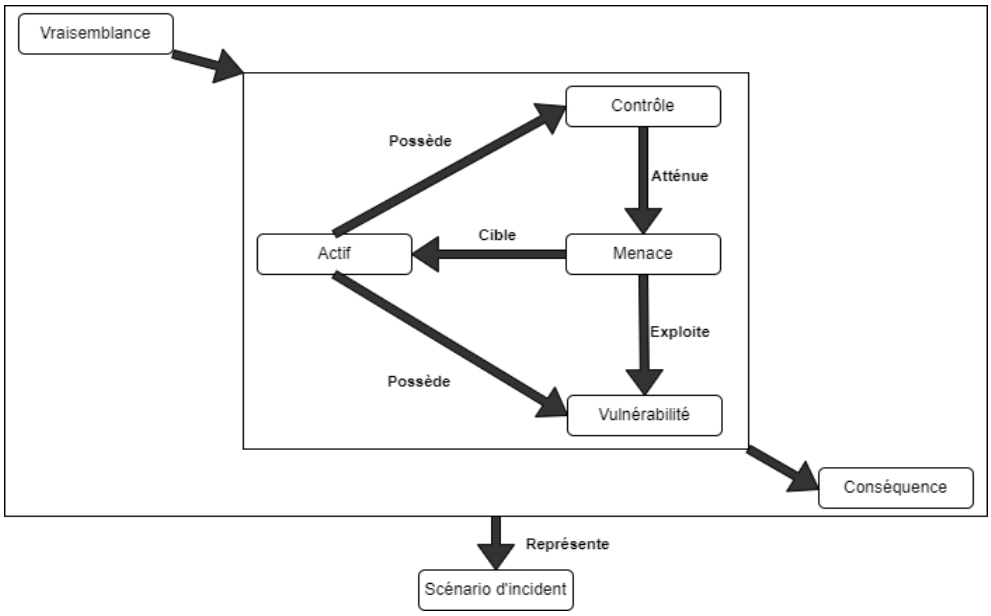


FIGURE II.15: Modélisation simplifiée du niveau de risque d'un scénario d'incident de sécurité

"Cyber Kill Chain"[YR15].

La Cyber Kill Chain est un modèle permettant aux équipes de réponse aux incidents, aux enquêteurs en criminalistique numériques et aux analystes de logiciels malveillants de travailler de manière ordonnée. Elle consiste à modéliser et à analyser les actions offensives d'un cyberattaquant. Ainsi, pour un analyste de sécurité qui développe des contre-mesures défensives [Sag14], il est pertinent d'étudier cette chaine. Cette connaissance peut aider à penser sur le même modèle que celui d'un attaquant ce qui conforte le changement de paradigme vu dans les méthodes d'analyse. Chaque phase de la Cyber Kill Chain constitue en soi un vaste domaine de recherche à aborder et à analyser. Ces dernières années, les cyberattaques sont devenues plus complexes qu'auparavant, de multiples vecteurs d'attaques redondants et complémentaires sont exploités dans les cyberattaques, non seulement pour en multiplier l'effet, mais aussi pour rendre l'analyse plus difficile pour l'équipe d'intervention. Pour analyser de telles attaques, la Cyber Kill Chain fournit un cadre permettant de décomposer une attaque complexe en étapes ou en couches non exclusives les unes des autres. Une telle approche par couches permettra aux analystes de s'attaquer à des problèmes plus petits et plus faciles et, dans le même temps, elle aidera également les défenseurs à maîtriser chaque phase en développant des défenses et des mesures d'atténuation pour chacune d'entre elles. La Cyber Kill Chain se compose principalement de 7 phases [Harb],[Hara],[Eng14] (figure II.16).

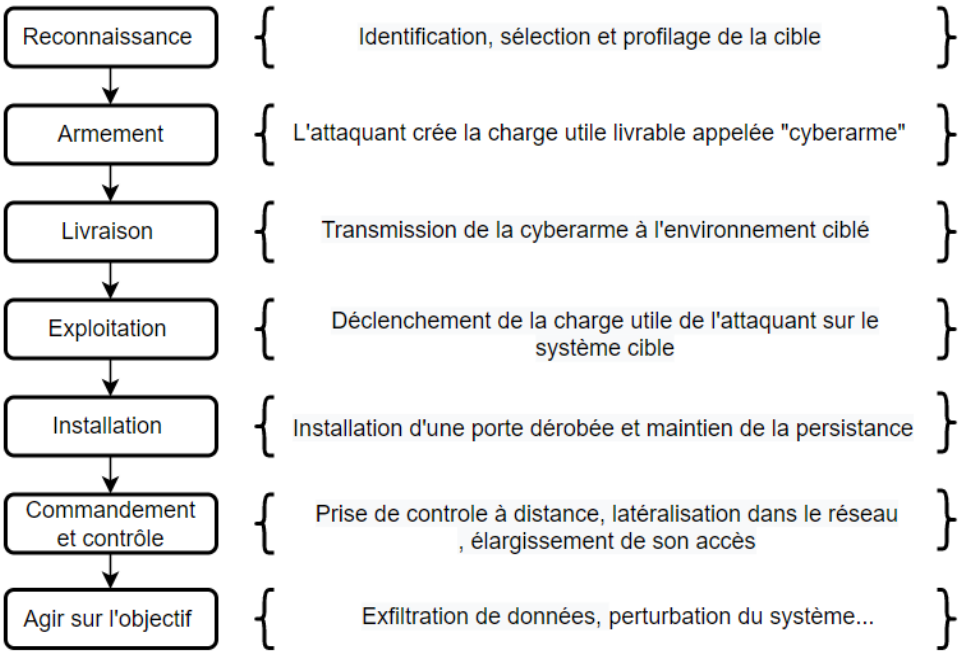


FIGURE II.16: Les 7 phases de la cyber kill chain

MoRiAML offre, au-delà du couplage entre le domaine de la sécurité et celui de l'ingénierie système, un enrichissement du concept *incident de sécurité* avec celui de la cyber kill chain. Ceci permet de bénéficier de l'apport des modèles dans l'analyse de risques : scénario fonctionnel servant de fondation pour la cyber kill chain avec entre autres : les liens entre les éléments, mettant en avant les possibles zones de latéralisation ainsi que l'identification du chemin nominal et des parties prenantes concernées pour sa réalisation.

La *cyber kill chain* est une vision plus sophistiquée de l'*incident de sécurité* lui-même aligné avec les *scénarios* de l'ingénierie système par la relation ***se produit en tant que*** (cf. figure II.11). Les deux concepts s'appuient sur la notion de séquence d'événements, et tous deux basent leur séquence sur les concepts précédemment alignés **activité/fonction**, et **interaction** mais avec une perspective et un découpage diffèrent. La *cyber kill chain* ***se produit en tant que*** scénario spécifique du point de vue de l'attaquant, reliant ainsi les séquences d'événements que l'attaquant réalisera ou traversera pour atteindre ses objectifs.

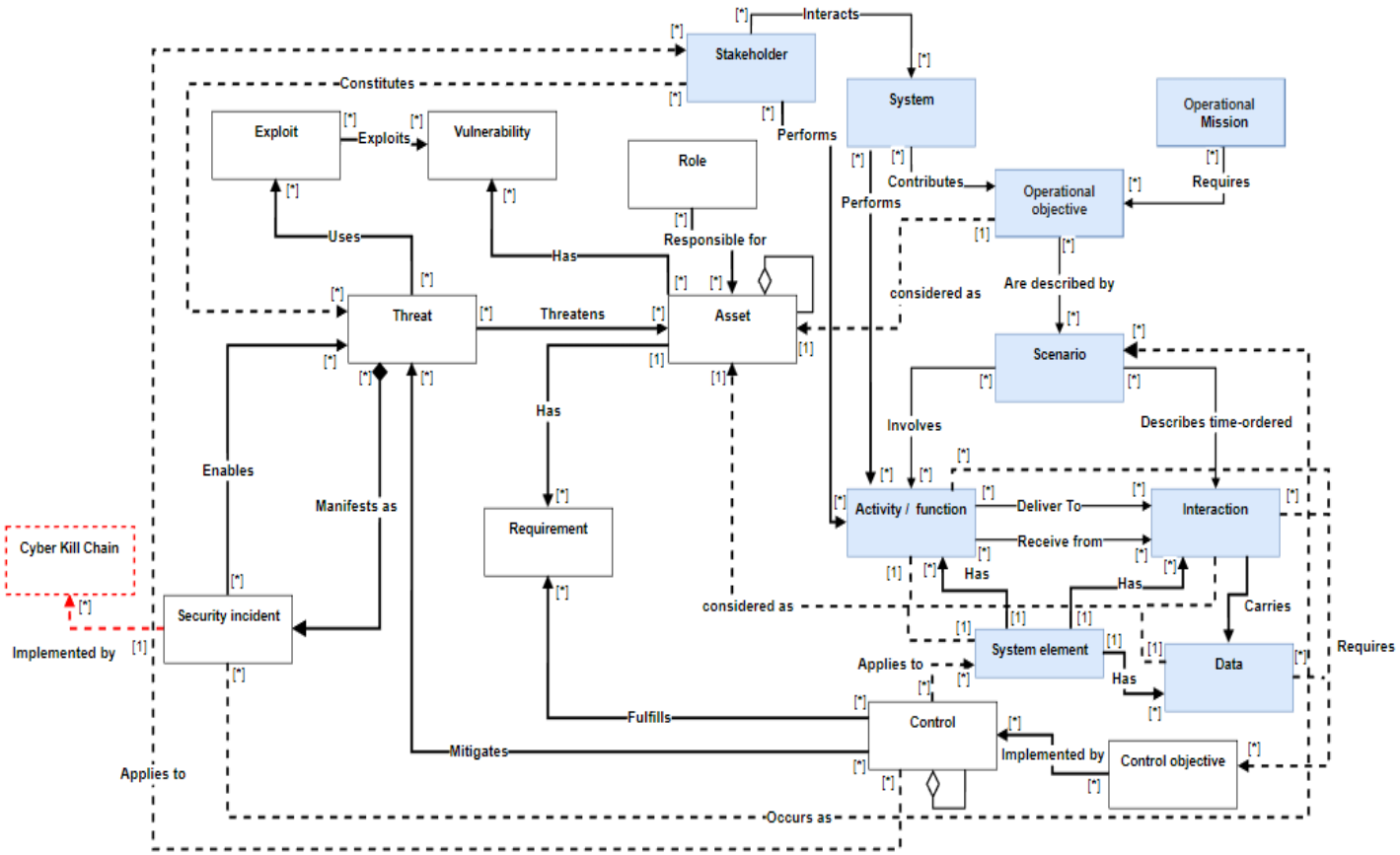


FIGURE II.17: Métamodèle de MoRiAML enrichi avec les concepts de la Cyber Kill Chain

Le couplage de la Cyber Kill Chain avec MoRiAML a pour avantage de se baser et d'utiliser tous les éléments et alignements de MoRiA et cela de façon directe ou indirecte. Nous proposons donc d'utiliser les concepts à notre disposition à travers les modèles pour guider et aider la notation de la vraisemblance de réalisation de chaque étape de la Cyber Kill Chain à travers la définition de métriques notables grâce à l'expertise de l'ingénierie et qui contribuent à la vulnérabilité de nos éléments de modèles (figure II.18).

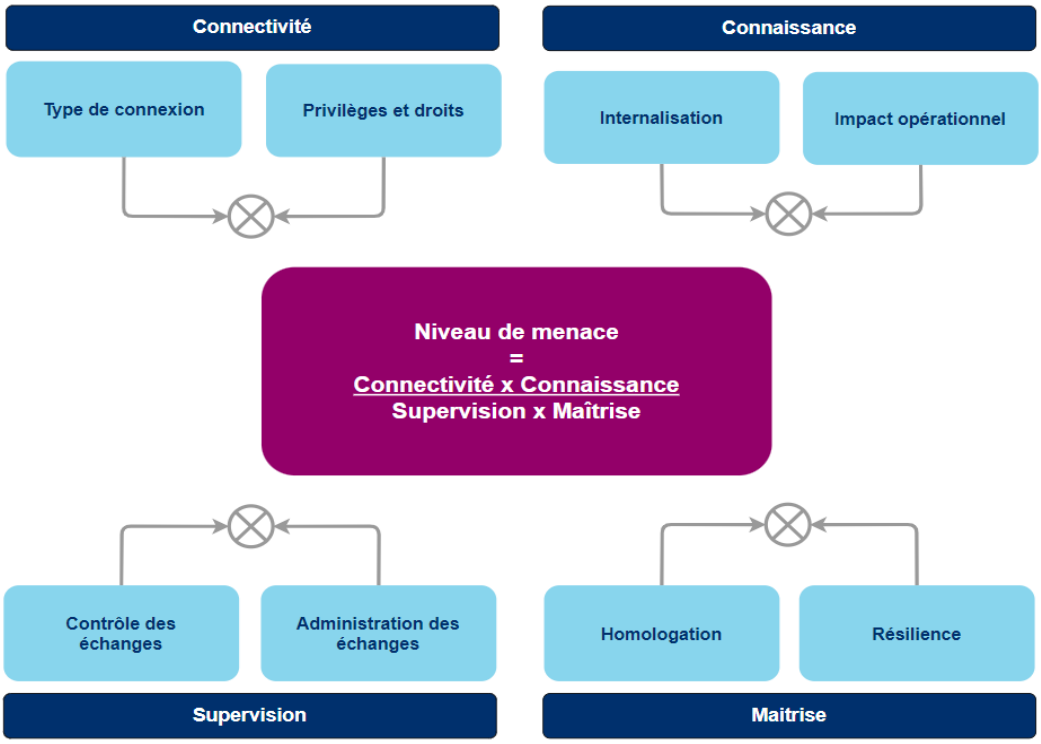


FIGURE II.18: Métriques de calcul de vulnérabilités élémentaires

1. **connectivité :**
   (a) **type de connexion :** englobe le nombre d'interconnexions ainsi que le type (analogique, numérique, Wi-Fi...) ;
   (b) **privilèges et droits :** englobe les privilèges de l'élément ainsi que les éléments avec qui il échange ;
2. **supervision :**
   (a) **contrôle des échanges :** englobe le chiffrement ainsi que le sens des échanges ;
   (b) **administration des échanges :** englobe la gestion des privilèges adaptés au besoin ;
3. **connaissance :**
   (a) **internalisation :** englobe la provenance ainsi que l'importance de l'élément ;
   (b) **impact opérationnel :** englobe les différentes classifications d'impact au cas où l'élément ne serait plus opérationnel ;
4. **maîtrise :**
   (a) **homologation :** englobe la politique et hygiène de sécurité à mettre en œuvre ;

(b) **résilience :** englobe la facilité d'intervention et de remplacement ;

Nous avons dans un premier temps la métrique "connectivité" séparée en deux sous métriques : 1) métrique de type connexions qui va englober le nombre d'interconnexions ainsi que le type (analogique, numérique, Wi-Fi...) ; et 2) métriques sur les privilèges et droits portant sur le type de privilège de l'élément ainsi que les éléments avec qui il échange. Cette métrique sera opposée à la métrique "Supervision" elle aussi séparée en 2 sous métriques contrebalançant les 2 métriques précédemment exposées. La sous-métrique de contrôle des échanges porte sur le chiffrement ainsi que le sens des échanges, il a pour objectif de réduire le niveau de menace amené par la sous-métrique type de connexions. L'intérêt de ces métriques est qu'elles sont "influençables" en fonction des mesures de sécurité mises en place. La sous-métrique privilège et droits est quant à elle mitigée par l'administration des échanges englobant la gestion des privilèges adaptés au besoin.

Dans un second temps, nous avons la métrique "connaissance" séparée elle aussi en 2 sous métriques une de type internalisation qui va porter sur la provenance ainsi que l'importance de cet élément. Il sera secondé par la sous-métrique impact opérationnel englobant les différentes classifications d'impact au cas où l'élément ne serait plus opérationnel. Cette métrique "connaissance" est contrebalancée par la métrique "maîtrise" de notre système elle-même composée de deux sous métrique une d'homologation portant sur la politique et hygiène de sécurité à mettre en œuvre chez notre prestataire et une seconde englobant la résilience notamment la facilité d'intervention et de remplacement.

Notion d'état dans les différentes perspectives

La Cyber Kill Chain permet d'étudier et représenter l'état du système et de son écosystème à un moment donné. La prise en compte du concept d'état devient donc plus qu'important à intégrer dans l'analyse afin de contextualiser l'analyse et la cyber kill chain. Un *état* caractérise un contexte choisi (respectivement subi) dans lequel se trouve un acteur, le système ou un composant de celui-ci, et définit son comportement dans ce contexte. Ce comportement est le plus souvent défini par les fonctions et les échanges, voire composants, disponibles ou non dans l'*état* considéré. Un *état* peut traduire divers concepts, comme une phase d'une mission ou d'un processus, un fonctionnement particulier requis du système, des conditions d'emploi comme un *état* de test ou de maintenance, d'entraînement, etc. Le passage d'un *état* à un autre correspond en général à une décision explicite, par exemple celle d'un changement d'utilisation du système pour répondre à des besoins ou des situations nouvelles. Il est donc conditionné par des choix effectués par le système, des utilisateurs ou acteurs externes, à travers la réalisation d'un échange fonctionnel ou l'activation d'une fonction particulière. Les états associés à un élément sont en général définis par une machine d'états, qui décrit ceux-ci et les transitions possibles entre eux, ainsi que les conditions de ces transitions.

À travers cette notion, notre objectif est de pouvoir définir des contextes de sécurité/risques en fonction du contexte et du comportement du système. Les acteurs, le système ainsi que ses composants et fonctions n'ont pas le même besoin en sécurité, impacts et vraisemblance en termes de risque en fonction de leur contexte et état.

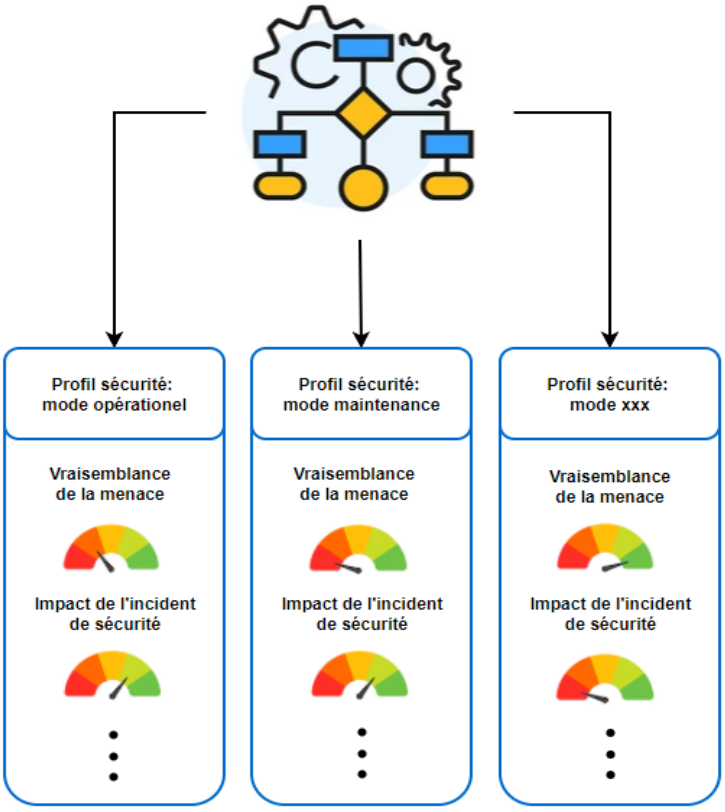


FIGURE II.19: Profils de sécurité en fonction du contexte et du comportement du système

Par exemple, dans le contexte d'un navire : certaines zones, doivent être accessibles en « Mode opérationnel » mais devront être surveillées et nécessiter des mesures de sécurité dans le « Mode à quai/amarre » où la vraisemblance qu'un intrus accède physiquement au système est plus vraisemblable. L'intérêt est de diminuer la pertinence du scénario de menace de façon adaptée sans pénaliser les aspects fonctionnels et organisationnels du système nécessaires dans les autres modes). Pour cela, les équipes de sécurité et système, les clients et les responsables budget devront statuer en fonction de leur finesse d'analyse voulue par les contexte et comportement qui nécessiteront un profil et une analyse de risque adaptée.

Ainsi, nous avons enrichi MoRiAML avec les concepts et relations suivants :

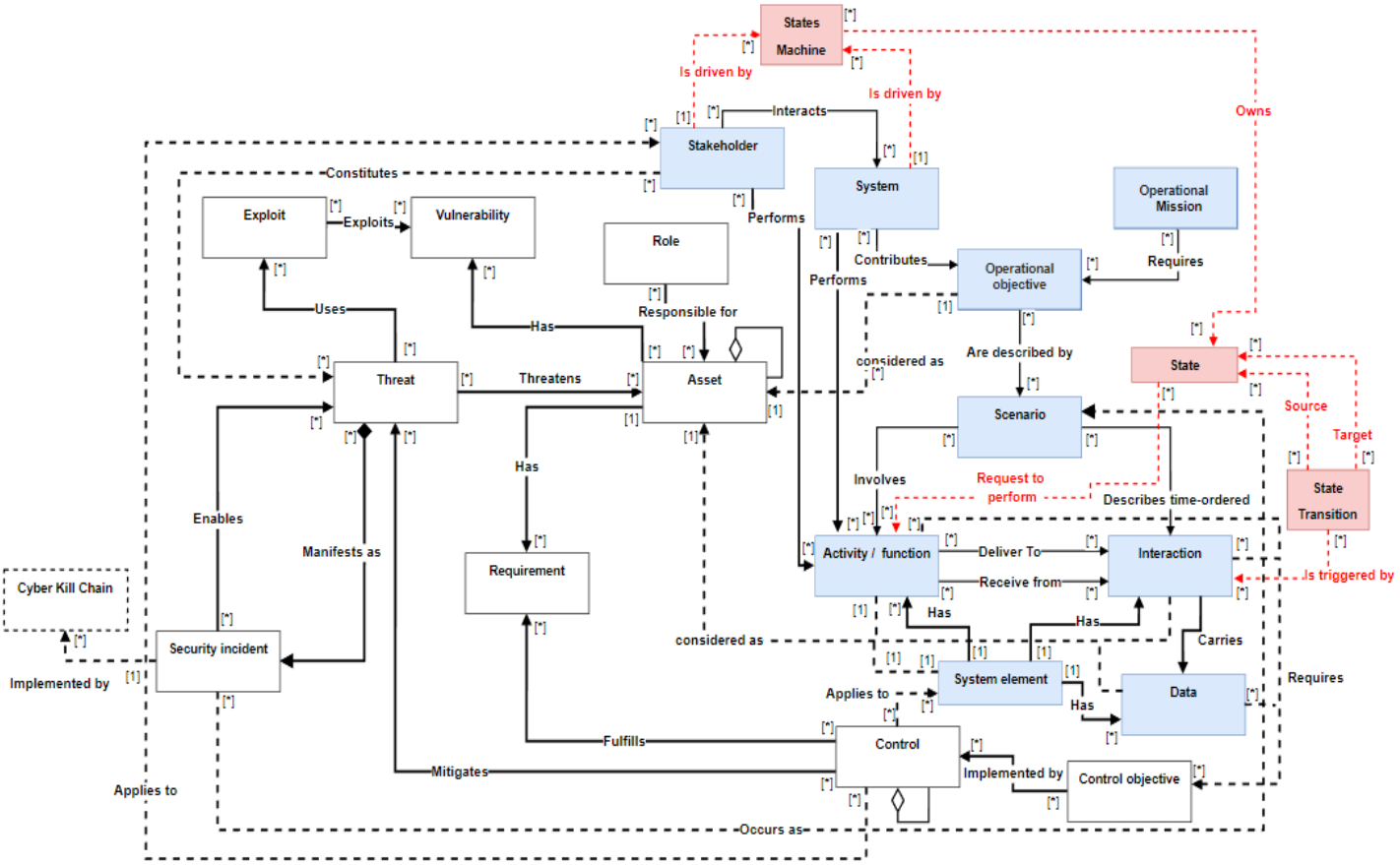


FIGURE II.20: Métamodèle de MoRiAML enrichie avec les concepts et relations entre états et descriptions fonctionnelle

1. **Transition d'état :** Une transition est un changement d'un état à un autre (appelés respectivement « source » et « cible de la transition ») ;
2. **État :** Un état est une contrainte ou une situation dans le cycle de vie d'un objet, dans laquelle une contrainte est maintenue, l'objet exécute une activité ou attend un événement ;
3. **Machine d'état :** L'ensemble des états et transitions dont la syntaxe est basée sur SysML (machine d'états) ;

À travers cet enrichissement du métamodèle (syntaxe abstraite), nous pouvons définir différents profils de sécurité en fonction des différentes machines d'état du système. Ces différents profils nous permettent de réévaluer la vraisemblance et pertinence de la menace ainsi que l'impact et la faisabilité des incidents de sécurité en fonction du contexte d'utilisation choisi ou subi. Cela permettant aux équipes participant à l'analyse de produire des profils

de sécurité contextuels et adaptés aux besoins de sécurité ainsi qu'au besoin fonctionnel en fonction des circonstances.

II.3.3 Processus d'utilisation de MoRiAML

MoRiA étant une méthode, nous avons élaboré un processus de modélisation adapté pour guider l'utilisation du langage MoRiAML. Ce processus permet de réaliser l'analyse de risque dans les modèles, d'exploiter l'expertise métier, construire des vues adaptées cross-disciplinaire afin d'échanger et communiquer autant avec les équipes d'ingénierie que les décideurs ainsi que de mettre en place un processus d'analyse itératif dans la lignée de la norme 27005 permettant la mise à jour de l'analyse en fonction de l'évolution du système et de son environnement à travers nos scénarios d'incidents (implémenté avec la cyber kill chain) et de ses composants. Ce processus décrit les activités qui doivent être suivies lors de l'utilisation de MoRiAML pour réaliser l'analyse de risque dans les différentes phases de la conception d'un système.

Il existe de nombreuses façons (figure II.21) d'aborder et construire une analyse fonctionnelle, en fonction du contexte propre à chaque projet et organisation, aucune n'étant nécessairement meilleure qu'une autre.

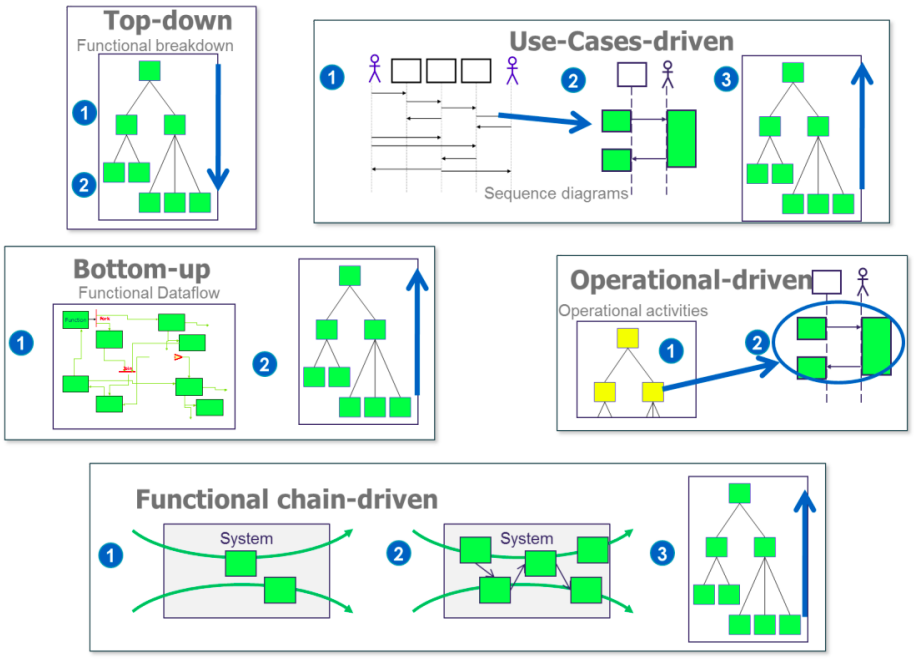


FIGURE II.21: Différentes approches d'analyse/définition fonctionnelle [5]

- **L'approche hiérarchique descendante** traditionnelle telle que promue par [Ros77] et ses dérivés, exprime les fonctionnalités requises sous la forme d'un nombre limité de fonctions de premier niveau, puis détermine les échanges nécessaires entre ces fonctions. Cette vision synthétique, de haut niveau, est ensuite raffinée, fonction par fonction, en définissant des sous-fonctions – ou fonctions filles – pour chaque fonction identifiée, et ce, de manière récursive, créant de ce fait une décomposition hiérarchique des fonctions.

- **L'approche remontante par regroupement** fonctionnel définit d'abord l'ensemble des fonctions élémentaires (fonctions filles) et leurs échanges, puis construit des vues synthétiques en regroupant a posteriori ces fonctions filles dans des fonctions mères (éventuellement sur plusieurs niveaux hiérarchiques).

- **L'approche par construction/allocation fonctionnelle** vise à définir le contenu fonctionnel d'un ensemble d'éléments structurels (système, composants, opérateurs ou acteurs externes au système, etc.), à partir d'un ensemble d'activités ou services. Il ne s'agit pas le plus souvent de raffinement à proprement parler, mais de création d'une solution par partie guidée par un besoin exprimé comme un graphe de dépendances fonctionnelles.

- **Approche par fonctions de services et chaînes fonctionnelles traversantes** commence par identifier les cas d'usage du système par les utilisateurs et acteurs externes et pour chacun d'eux les services fonctionnels requis, c'est-à-dire les interactions principales des utilisateurs et acteurs externes avec le système, pour définir le contenu fonctionnel attendu de celui-ci et les échanges externes associés.

- **Approche par cas d'usages et scénarios** identifie les cas d'usage et situations d'emploi principales du système, en les formalisant sous la forme de scénarios temporels d'interactions avec les utilisateurs et autres acteurs externes.

Les démarches et approches précédentes sont pratiquées dans les projets opérationnels, mais très rarement de manière exclusive [Voi18]. La plupart du temps, une démarche pragmatique emprunte à chacune des approches ce qui correspond le mieux à son contexte propre, quitte à les mélanger. Ainsi, quand bien même une démarche descendante hiérarchique est possible pour démarrer l'analyse fonctionnelle, il est très fréquent de devoir basculer sur une approche remontante lorsque des évolutions de besoin sont nécessaires, ou sur une approche par construction/allocation si l'architecture structurelle doit être revue. De même, la définition des scénarios de tests et d'intégration, ou l'ingénierie des performances ou de la sécurité conduisent à appliquer partiellement les approches par chaînes fonctionnelles et

5. `https://download.eclipse.org//capella/publis/INCOSE_Capella_SysML_paper.pdf`

scénarios.

L'utilisation de processus d'ingénierie et d'analyse de risque descendant est la plus pertinente quant à nos questions de recherche. Ce processus permet de commencer la construction de l'analyse dès les premières phases d'ingénierie portant sur la définition de fonctions de premier niveau qui seront par la suite raffinées. De plus ces processus sont tous deux familiers avec les itérations successives qui seront nécessaires à son maintien et évolution. À travers MoRiA, nous proposons un processus d'utilisation structuré qui guide l'utilisation du langage proposé pour co-définir et co-modéliser l'analyse de risque et les modèles d'architecture système, ainsi que les acteurs correspondants et les outils nécessaires.

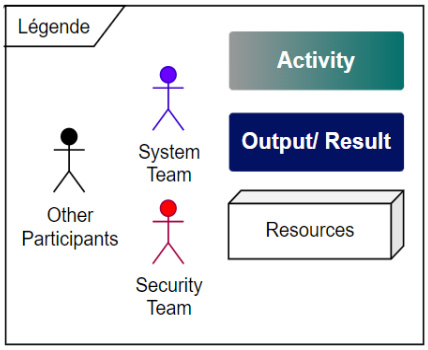


FIGURE II.22: MoRia processus d'utilisation - légende

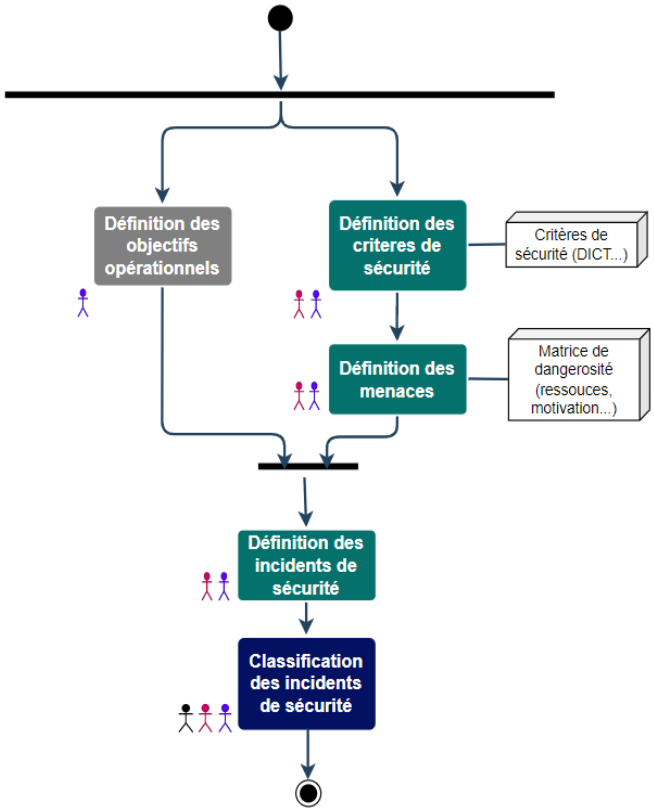


FIGURE II.23: MoRia processus d'utilisation - phase analyse opérationnelle - identification des actifs, menaces et incidents de sécurité 1ère partie

Dans la phase de modélisation de notre processus d'utilisation de MoRiA, pour chaque concept fonctionnel identifié, différentes équipes d'architecte système et de sécurité co-définissent et co-modélisent les concepts de sécurité, possiblement liés à ces concepts et cela pour les quatre phases de l'ingénierie.

Les équipes d'ingénierie système dans une approche descendante mettent l'accent sur l'analyse du problème avant de définir directement la solution. Pour cela l'ingénierie système propose une première perspective appelée analyse opérationnelle. Cette perspective analyse la problématique des utilisateurs opérationnels, en identifiant les grandes fonctionnalités, acteurs devant interagir avec le système, leurs buts, les activités, les contraintes et les conditions d'interactions entre eux.

La Figure II.22 illustre en gris les actions actuellement réalisées par l'équipe système pour définir le système, en vert les actions nécessaires à la réalisation d'une analyse de risque, en blanc les ressources sur lesquelles s'appuyer, en bleu des vues dites de synthèse ayant pour objectif de regrouper le travail réalisé afin de brainstormer entre équipes techniques et com-

muniquer, argumenter sur l'avancement et les choix à faire avec les équipes non techniques. Le stickman violet représente l'équipe système (architectes et ingénieurs système), en rouge l'équipe sécurité (les ingénieurs et analystes de sécurité) et en noir les autres participants (RSSI, juriste, décideurs, responsable budget...).

MoRiA permet d'initier les premières réflexions sur les grandes fonctionnalités appelées **objectifs opérationnels** (figure II.23). Conformément à l'alignement II.2, les **objectifs opérationnels** sont alignés sur les **actifs** et sont traités comme tels. L'équipe système définissant l'**objectif opérationnel** aidera à la définition des critères de sécurité, notamment grâce à sa connaissance de l'importance de celle-ci dans la réalisation globale et fonctionnelle du projet.

L'équipe sécurité apporte la matrice d'évaluation [6] et les **critères de sécurité** afin d'apprécier l'importance de l'actif. Les **objectifs opérationnels** grâce aux échanges entre les équipes se verront attribuer une valeur numérique, généralement entre 0 et 4, en fonction de la complétude des matrices et qui permet d'évaluer l'importance de chaque critère de sécurité : disponibilité, intégrité, confidentialité et traçabilité (DICT) [CSG18].

Pour exemple, la notation [4301] attribuée à un **objectif opérationnel** indiquerait que : 1) l'**objectif opérationnel** manipulé doit absolument rester disponible, 2) son exigence d'intégrité est importante sans être critique, 3) les informations utilisées par cet **objectif opérationnel** sont publiques, et 4) il n'y a pas de besoin spécifique de traçabilité des accès.

Par la suite des profils de **Menace** peuvent être identifiés et définis à partir de métriques telles que la motivation et les ressources, comme l'illustrent les bases de connaissances proposées dans les fiches méthodologiques de l'ANSSI[II.3.3] pour estimer le niveau de vraisemblance/dangerosité, pour par la suite associer les **Menace** aux **actifs** qu'ils sont le plus susceptibles de menacer. Lorsque les équipes système et sécurité auront conjointement cessé de produire de nouveaux couples Menace/actif, ils évalueront par la suite la pertinence de chaque couple. Si le retour d'expérience des participants peut constituer une première base d'évaluation, l'utilisation de critères et métriques de caractérisation apporteront une certaine objectivité.

6. https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-going_further-en-v1.0.pdf

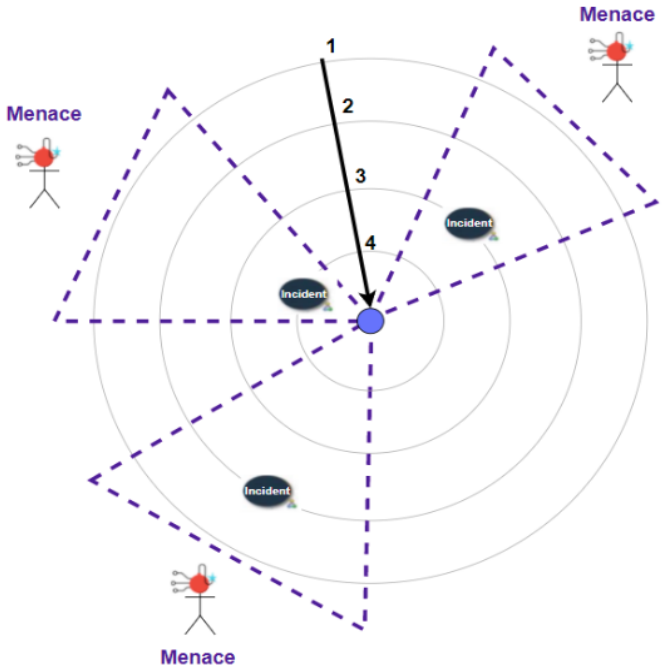


FIGURE II.24: Vue de synthèse des couples incident de sécurité - menace

Le niveau de pertinence de chaque couple est là pour nous aider à identifier au mieux les incidents de sécurité les plus pertinents. Ici aussi, MoRiA permet une représentation sous forme de radar-pie (voir figure II.24) ou la menace serait représenté en tant que "pie" et englober plusieurs actifs. La distance radiale correspondrait au niveau de pertinence évaluée pour le couple (plus le couple est proche du centre, plus il est estimé dangereux pour l'objet de l'étude). L'**actif** avec un **critère de sécurité** jugé critique ou suffisamment important pour être pris en compte sera alors associé à une menace pour être développé sous la forme d'**incident de sécurité**. Les **incidents de sécurité** gardés se verront par la suite attribuer un score de sévérité en fonction du type et de la gravité des impacts engendrés (impact humain, matériel, sur la mission, juridique, image...)[II.3.3] L'objectif étant de pouvoir à la fin de cette étape créer une première vue de synthèse regroupant et positionnant les **incidents de sécurité** en fonction de leur pertinence. Cette vue de synthèse sert de support afin d'échanger avec les acteurs non techniques. Ici, le RSSI, les juristes, décideurs, responsables budget sont invités à échanger et prendre connaissance de la pertinence des différents incidents de sécurité.

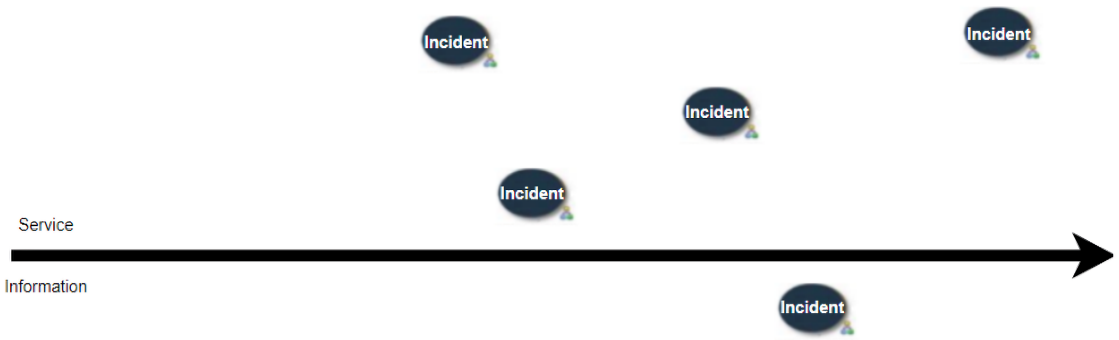


FIGURE II.25: Vue de synthèse de l'impact des incidents de sécurité

De plus, les impacts des incidents de sécurité peuvent être nuancés à travers une seconde vue de synthèse où les incidents de sécurité seraient organisés les uns par rapport aux autres et où les événements redoutés concernant les processus seraient au-dessus et ceux informationnels au-dessous de l'axe. Ici, même si le niveau de l'impact spécifique a été attribué à l'événement à travers les matrices, ce qui est important, c'est sa position relative par rapport aux autres actifs et sa position absolue sur l'axe. Un actif positionné à droite d'un autre actif a un niveau de gravité plus fort et vice versa (figure II.25). Ici, le RSSI, les juristes, décideurs, responsables budget sont invités à échanger sur leurs préoccupations quant à la bonne notation des impacts.

Dans la suite logique de définition de système, le second élément d'ingénierie est celui des **parties prenantes** qui vont être susceptibles de réaliser ou d'interagir avec les **objectifs opérationnels** (figure II.26).

Conformément à l'alignement II.2, les parties prenantes constituent une partie du risque et se voient donc attribuer des métriques [II.3.3] (dépendance, exposition, confiance ...) pour définir leur niveau de menace vis-à-vis des **objectifs opérationnels**. Une représentation sous forme de radar est conseillée. La distance radiale correspondant au niveau de menace selon l'échelle d'évaluation utilisée. Plus une **partie prenante** fait peser une menace numérique importante pour l'objet de l'étude, plus elle se situe près du centre et plus elle est de confiance et sensibilisée au risque, plus sa couleur se rapprochera du bleu et au contraire virera sur le rouge. Ici, le RSSI, les juristes, décideurs, responsables budget sont invités à échanger sur leurs préoccupations quant au niveau de menace des différentes parties prenantes afin de nuancer voire planifier les mesures à prendre.

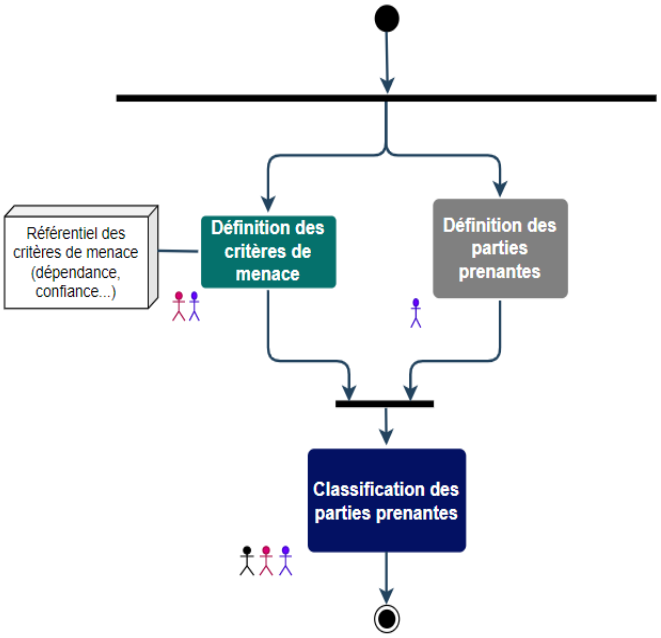


FIGURE II.26: MoRia processus d'utilisation - phase analyse opérationnelle - identification des parties prenantes constituant la menace 1ère partie

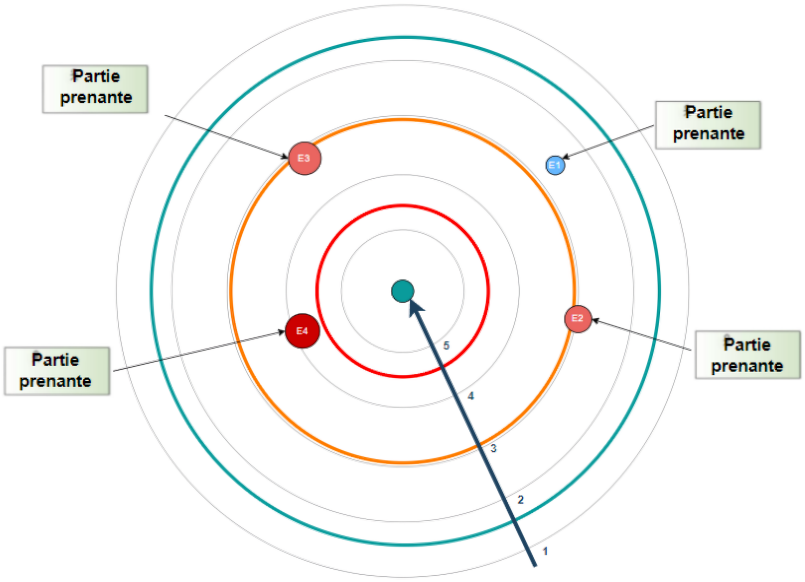


FIGURE II.27: Vue de synthèse du niveau de menace des différentes parties prenantes

Par la suite dans le processus d'ingénierie fonctionnel, les **objectifs opérationnels** sont découpés en **activités**, **interactions** et **données** que les **parties prenantes** vont devoir réaliser (figure II.28). Les **fonctions**, **interactions**, **données** définies ultérieurement

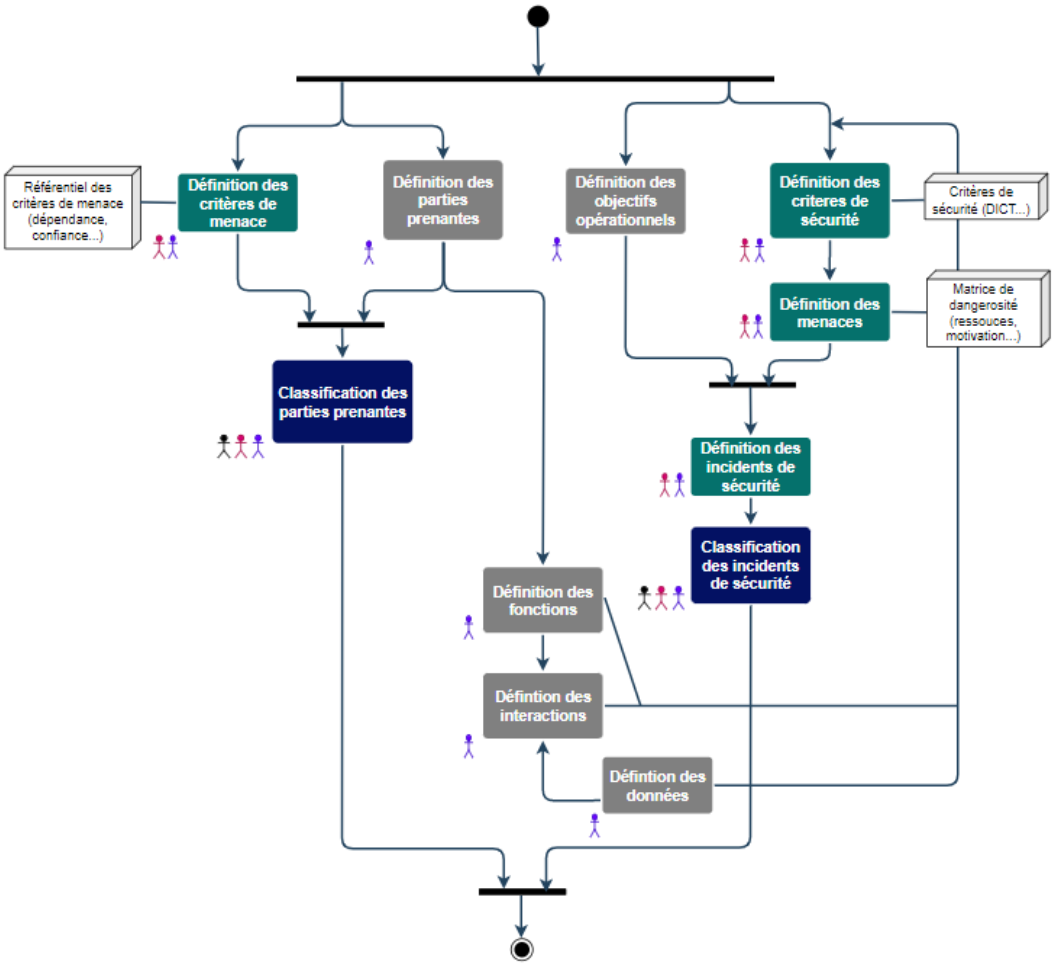


FIGURE II.28: MoRia processus d'utilisation - phase analyse opérationnelle - identification des actifs 2ème partie

peuvent, si elles sont jugées critiques (par exemple, une **donnée** nécessitant un certain niveau de classification (Défense ou Confidentiel Secret ...)) modifier le score d'un de plusieurs **objectifs opérationnels**, ou du moins être considérés comme des **incidents de sécurité** spécifiques détaillant les **objectifs opérationnels**. Cette première itération nous permettant de compléter la liste d'**incidents de sécurité** afin d'identifier au mieux les éléments ciblés ainsi que les profils d'attaquants les plus vraisemblables.

À travers cette première perspective, les équipes de sécurité et système devront identifier quelles sont les grandes fonctionnalités à protéger ainsi que certaines plus spécifiques en fonction des critères de sécurité. Les incidents de sécurité sont couplés avec leurs sources de menaces les plus vraisemblables et sont comparés afin de garder seulement les couples les plus pertinents. En parallèle à cela, les équipes sécurité et métier ont évalué le niveau

de menaces des parties prenantes. L'analyse opérationnelle n'a que pour objectif d'identifier et de représenter ce que les utilisateurs du système doivent accomplir ; dans la seconde perspective, la notion de ce que le système doit réaliser pour les utilisateurs apparaît.

II.3.3.1 Analyse Système

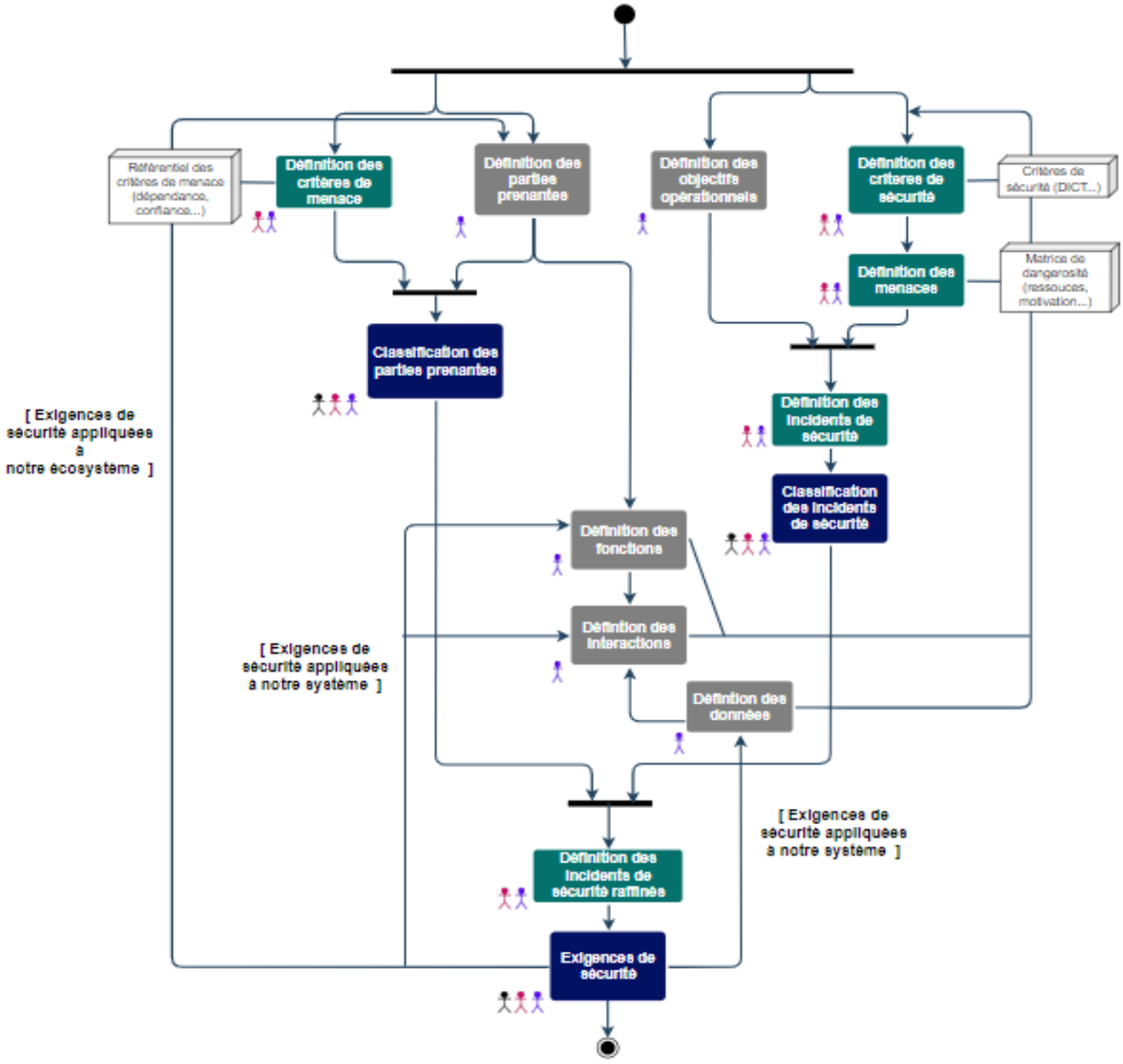


FIGURE II.29: MoRia processus d'utilisation - phase analyse système - définition des incidents de sécurité raffinés

Cette perspective construit une analyse fonctionnelle externe, bâtie à partir de l'analyse opérationnelle et des exigences textuelles d'entrée modélisées, pour identifier en réponse les fonctions ou services du système nécessaires à ses utilisateurs, sous contrainte des propriétés non fonctionnelles demandées. Ici les **fonctions**, **interactions** et **données** définies

précédemment sont raffinées et assignées au **système** ou à ces **parties prenantes**. Cette nuance permet aux équipes système et sécurité d'identifier les éléments propres au système et ceux qui vont faire partie de son écosystème et qui donc nécessiteront un traitement spécial quant aux **exigences** et **contrôles** de sécurité. Après ces attributions et la nette démarcation du système avec son écosystème, il est possible que les **activités/fonctions**, **interactions/échanges** et les **données** se soit précisés dans leur définition. Une itération est alors réalisée pour redéfinir et re-évaluer les couples afin de raffiner les incidents de sécurité (figure II.29).

Les **incidents de sécurité** raffinés vont être décrits en une séquence d'exploitation réalisée par la **menace** en passant possiblement à travers les **parties prenantes** pour atteindre son objectif. Ici, les équipes sécurité et système ont : le point de départ (la menace), les possibles points d'entrées à travers nos **parties prenantes** et l'objectif visé sous la forme d'une **activité**, **interaction** ou **donnée** dans notre système. Les actifs traversés au sein de notre système se verront assigner des exigences de sécurité de type protection (cloisonnement, contrôle d'accès, chiffrement...), défense (surveillance d'évènements, détection et classification d'incident, réponse à un incident cyber...) et résilience (continuité d'activité (sauvegarde/restauration, gestion en mode dégradé), reprise d'activité...) afin de prévoir et de réfléchir à l'architecture logique et physique de façon sécurisée dès cette phase. Les **parties prenantes** auront quant à eux des exigences à appliquer de type gouvernance et anticipation (audit de sécurité, processus d'homologation...) afin d'appréhender et réduire leur niveau de menaces. Une autre solution pourrait alors à ce stade de changer de prestataire pour quelqu'un ayant un niveau de menace inférieur ou d'internaliser le processus. Les exigences de sécurité appliquées aux parties prenantes réduiront leur niveau de menaces, permettant dans un premier temps de réduire voire de contrôler les points d'entrée du système.

II.3.3.2 Architecture logique

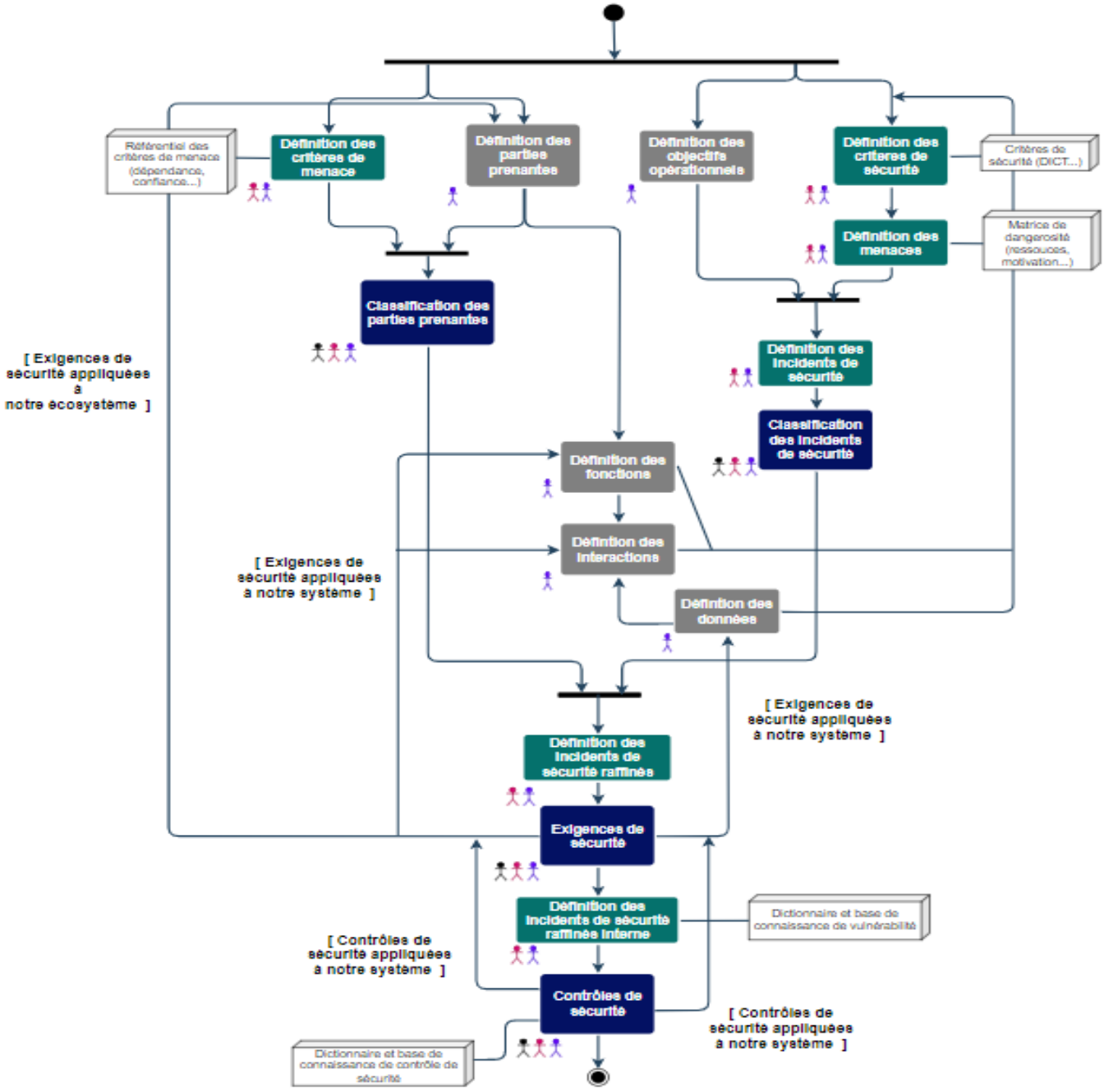


FIGURE II.30: MoRia processus d'utilisation - phase analyse système - définition des incidents de sécurité interne

En réponse au besoin exprimé par les deux perspectives précédentes, l'architecture logique porte les premiers grands choix de conception de la solution. D'abord via une analyse fonctionnelle interne du système : elle décrit les fonctions à réaliser et à assembler pour réaliser les fonctions de service identifiées lors de la phase précédente et elle se poursuit par l'identification des composants de principe réalisant ces fonctions solution, en y intégrant les contraintes non fonctionnelles que les équipes système et sécurité ont choisi de traiter à ce niveau. Maintenant que l'analyse du contexte et de son écosystème a été réalisée, les équipes système et sécurité concentrent leur analyse sur le système. Les équipes système et sécurité ont leurs points d'entrée à travers les **parties prenantes** ainsi que les interventions physiques (exploitation) de la **menace** dans le système. Les équipes système et sécurité vont par la suite raffiner la partie de l'incident de sécurité se déroulant dans le système et constituée **d'activités/fonctions**, **interactions**, **échanges** et de **données** qui vont être exploités et détournés à travers leur vulnérabilité pour réaliser l'incident. À travers la Cyber Kill Chain les équipes système et sécurité identifieront et peaufineront les scénarios de menaces de façon itérative et les mitigeront à travers l'élicitation de contrôles de sécurité.

Ici dans la figure II.30, les équipes système et sécurité ont un niveau d'abstraction suffisant pour ajouter les **contrôles** de sécurité directement sur les actifs exploités dans les incidents de sécurité, permettant après itération de diminuer la dangerosité globale du scénario. Arrivé à ce stade d'analyse dans la dernière phase d'ingénierie "architecture physique" modélise les contrôles de sécurité élicités dans cette phase.

Tout ce processus nous permet de modéliser l'analyse de risque tout le long de la définition du système de façon corrélée répondant ainsi à notre QR1, permettant ainsi à la moindre modification de l'architecture ou du besoin d'itérer l'analyse afin de modifier les différentes vues pour ensuite communiquer sur la marche à suivre. C'est également le cas si nous modifions nos métriques de sécurité afin de rester à jour en termes de sécurité répondant ainsi à notre QR2. Ce processus a pour objectif de guider les équipes d'architectures système et d'architectures cybersécurité dans leur démarche intellectuelle d'analyse ainsi que d'assurer la cohérence entre les deux visions. MoRiA permet la co-ingénierie et co-modélisation des concepts de sécurité dans l'ingénierie système, ainsi les points forts de notre méthode enrichissent et améliorent la cohérence à la fois de l'analyse de risque et de la définition et de l'architecture du système.

II.3.3.2.1 Discussion

Les apports des modèles et des éléments de diagrammes dans l'analyse de risque :

- La modélisation permet le discernement et la compréhension des détails structurels et fonctionnels du système supportant ainsi une identification plus pertinente des *actifs*, *parties prenantes*, à analyser et protéger ainsi que des *incidents de sécurité*.

- La modélisation permet de plus une compréhension plus fine du système à travers la réalisation de réflexions adaptées en fonction du contexte et cohérentes avec les besoins fonctionnels. Appuyant ainsi la cohérence en contenu et en niveau de détails entre les architectes système et experts sécurité à travers une identification conjointe et claire des activités perturbées ainsi que des entrées et données possiblement interrompues ou dégradées lors de la réalisation des événements redoutés et cela à travers les différentes perspectives.

- L'utilisation de la modélisation permet de supporter l'analyse de risque à travers l'utilisation de ces outils, éléments et diagrammes comme instrument/support de représentation, d'échanges et de communication entre les équipes métiers et non métiers. Permettant ainsi la prise en compte des préoccupations de chacun pour mener à bien l'analyse de risque dans la définition du système.

Les apports de l'analyse de risque dans les modèles et les éléments de diagrammes :

- L'analyse de risque dans les modèles permet la prise en compte des concepts et métriques en lien avec la sécurité, à travers l'identification, modélisation de ces concepts dans les différents modèles.

- L'analyse de risque permet l'identification des points d'entrée utilisables par la menace ainsi que les parties prenantes, fonctions et composants susceptibles d'être détournés à travers leur vulnérabilité par les attaquants.

- L'analyse de risque apporte aux modèles les exigences non fonctionnelles de sécurité, leur efficacité ainsi que leur dérivation en choix d'architecture.

La modélisation apporte un cadre d'analyse conjointe entre les architectes système et les analyses de sécurité permettant l'identification de manière précise des éléments critiques, permettant ainsi une évaluation encadrée et ciblée sans manque de pertinence causé par un

manque de connaissance du domaine ou une explosion combinatoire de risques et d'actifs et incidents non essentiels. Grâce à nos discussions avec des collaborateurs industriels, nous avons pu constater la pertinence de l'expertise métier lors de la réalisation d'une analyse de risque appuyant ainsi les éléments de discussion.

II.4 Conclusion

Pour conclure, nous avons présenté dans ce chapitre les syntaxes abstraite et concrète de notre DSML appelée MoRiAML. Nous avons choisi de définir notre DSML comme une extension de SysML. Pour les raisons invoquées dans ce chapitre, nous nous sommes concentrés sur les concepts fonctionnels de l'ingénierie système. Par conséquent, le métamodèle MoRiAML est défini comme un profil étendant le métamodèle des concepts fonctionnels de l'ingénierie système des normes 15288 et 1220, avec les concepts ainsi que leurs relations correspondantes présentes et nécessaires à la réalisation d'une analyse de risque suivant la famille des normes 2700X. Ces concepts couvrent les aspects inhérents à la définition d'un système et sont raffinés au fur et à mesure de son avancée à travers différents éléments et perspectives de modèle, notre extension permet la définition du système prenant en compte non seulement les caractéristiques spécifiques de celui-ci, mais aussi les concepts de sécurité reposant sur les éléments de modèle produit et nécessaire à son analyse de risque. En alignant ces concepts, nous offrons une représentation de tous les aspects de la sécurité d'une analyse de risque numérique lors de la définition du système. Ce qui permet aux ingénieurs d'associer et d'aligner leurs concepts afin de co-identifier, co-définir et représenter les éléments de sécurité dans les modèles. Par conséquent, MoRiAML, répond à notre QR1 en offrant une extension de langage de modélisation de la structure fonctionnelle d'un système avec un accent particulier sur les aspects de sécurité pour permettre la réalisation d'une analyse de risque dans les différentes perspectives d'architectures. De plus nous proposons à travers MoRiA une représentation du concept d'incident de sécurité afin d'affiner l'analyse et de faciliter son itération de par sa couverture et point de vue. La cyber kill chain permet dans la même vue de rassembler et travailler simultanément sur les entrées (*actifs*), intermédiaires (*menaces*) et sorties (*mesures de sécurité*) afin d'analyser et éliciter la notation des uns et des autres de façon itérative afin de réinjecter les résultats dans les différents diagrammes et éléments de modèles impliqués. La cyber kill chain nous sert donc de fil conducteur et de vue pivot afin de mettre à jour l'analyse de risque tout au long de la définition du système et lors de ces modifications, pour répondre ainsi à notre QR2. Après avoir présenté les syntaxes abstraites

et concrètes de notre langage ainsi que son processus d'utilisation, nous présentons dans le chapitre suivant l'implantation de MoRiAà travers 2 méthodes industrielles : une méthode d'ingénierie (ARCADIA) et une méthode d'analyse de risque EBIOS RM.

Chapitre III

Implémentation de la méthode MoRiA comme une extension de deux méthodes industrielles : ARCADIA (ingénierie système) et EBIOS RM (analyse des risques)

Sommaire

III.1 Introduction

Après avoir défini la méthode MoRiA, nous l'avons implémentée, en tant qu'extension des méthodes industrielles d'analyse de risque et d'ingénierie système suivantes, elles-même implémentant les normes présentées dans les sous-sections II.3.1.1 et II.3.1.2 et constituant une base solide pour l'implémentation de notre méthode comme argumentée dans le chapitre I. De plus, ces méthodes industrielles sont utilisées par nos collaborateurs industriels.

III.2 ARCADIA : Une méthode d'ingénierie des systèmes industriels

Pour présenter les valeurs MBSE appropriées, Architecture Analysis Design Integrated Approach (ARCADIA) sert de méthode d'ingénierie appropriée et de choix de langage de modélisation, ainsi que Capella, son outil de modélisation/éditeur graphique correspondant. ARCADIA et Capella sont activement maintenus avec une documentation bien établie, et ils sont extensibles et interopérables avec les langages et outils existants basés sur SysML. En effet, ARCADIA, ainsi que Capella, sont open-source, largement utilisés dans le monde entier par des constructeurs tels que Rolls Royce (UK), Virgin Hyperloop (USA), Deutsche Bahn (GER), Comac (Chine) sans oublier l'industrie française, et en particulier, leur créateur Thales [1], une société française qui conçoit et réalise des systèmes critiques et fournit des services pour les marchés de l'espace, de l'aérospatiale, de la défense, du transport et de la sécurité. Thales est le 8 ème plus grand contractant de défense dans le monde [She19] et un leader européen dans la cybersécurité [2].

ARCADIA est une méthode d'ingénierie d'architecture structurée pour définir et valider

1. https ://www.thalesgroup.com/en
2. https ://www.thalesgroup.com/en/markets/defence-and-security/cyberdefence-solutions

des systèmes multi-domaines et basée sur des activités d'ingénierie centrées sur l'architecture et pilotée par les modèles. Il s'agit d'une méthode basée sur l'analyse fonctionnelle. Elle se concentre sur le développement du système à partir de l'analyse des besoins en décrivant le raisonnement détaillé pour comprendre les besoins réels du client, pour définir et partager l'architecture du produit entre toutes les parties prenantes de l'ingénierie, pour valider et justifier sa conception à un stade précoce, pour valider rapidement sa conception de développement de solutions et la justifier, pour faciliter et maîtriser l'intégration, la validation et la vérification. ARCADIA est très flexible et peut être mis en œuvre en utilisant une approche de développement descendante, ascendante ou intermédiaire, selon les besoins. Elle applique une approche structurée à travers les perspectives/phases d'ingénierie définies dans les normes, qui établissent une séparation claire entre les besoins (analyse des besoins opérationnels et analyse des besoins du système) et les solutions (architectures logiques et physiques). ARCADIA est conforme aux normes MBSE, notamment à travers l'implémentation (tableau III.1 et figure III.1) des concepts MBSE des normes ISO 15288 et 1220 que nous avons utilisée comme bases pour notre langage MoRiaML. Dans ce qui suit, nous allons présenter le métamodèle d'ARCADIA, puis dans la section III.4 l'implémentation du métamodèle MoRiAML comme extension de celui d'ARCADIA.

1. **Entité et acteur :** Elle appartient au monde réel (par exemple, une organisation, un système existant) dont le rôle est d'interagir avec le système ou avec ses utilisateurs (par exemple, l'équipage, Navire, etc.). Un acteur est un cas particulier d'une entité opérationnelle (humaine) qui ne peut être décomposée (par exemple, un pilote) ;
2. **Activité :** Étape du processus réalisée pour atteindre un objectif spécifique par une entité opérationnelle, qui peut avoir besoin d'utiliser le futur système pour le faire (par exemple, détecter une menace, collecter des données météorologiques) ;
3. **Interaction :** Unidirectionnel pour échanger des informations ou du matériel entre les activités (par exemple, des données météorologiques) ;
4. **Capacité :** La capacité d'une organisation à fournir un niveau de service élevé pour atteindre un objectif opérationnel (par exemple, fournir des prévisions météorologiques, etc.). Il s'agit de la capacité, attendue d'une ou plusieurs entités opérationnelles, à fournir un service contribuant à la réalisation d'une ou plusieurs missions opérationnelles ;
5. **Fonction :** Une action, une opération, ou un service, réalisés par le système ou l'un de ses composants, ou également par un acteur interagissant avec le système ;
6. **Échange fonctionnel :** Interaction entre une fonction source et une fonction destination, pour transmettre des éléments d'échange de l'une à l'autre ;

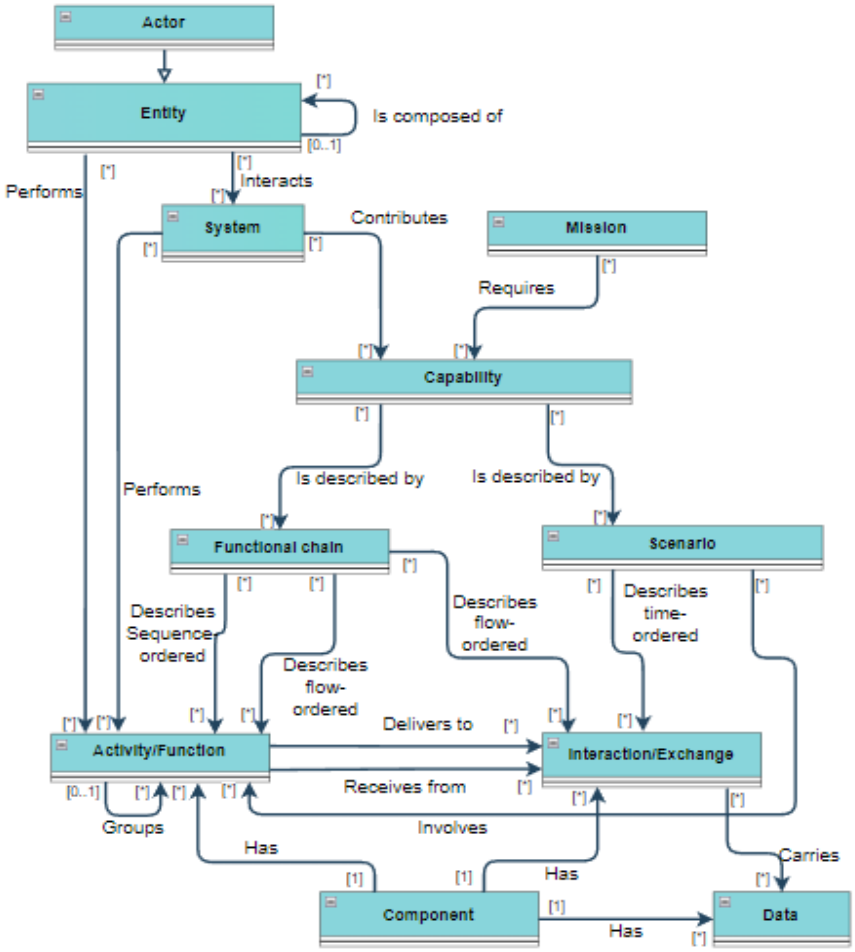


FIGURE III.1: Arcadia métamodèle modifié de [Voi18]

7. **Chaîne fonctionnelle :** Est l'arrangement spécifique des fonctions et des échanges, formant un chemin entre tous les chemins possibles à travers les flux de données du système, soit pour décrire un comportement attendu du système dans un contexte donné, soit pour exprimer des propriétés non fonctionnelles sur ce chemin ;
8. **Donnée :** Élément produit/utilisé par des fonctions ou des composants et acheminé par un ou plusieurs échanges entre eux.
9. **Composant :** Un composant est une part constitutive du système, contribuant au comportement et/ou aux propriétés de celui-ci, en lien avec d'autres composants et les acteurs externes au système.

Une chaîne fonctionnelle est un ensemble organisé (ordonné) de références à des fonctions et des échanges fonctionnels qui les relient, décrivant un chemin possible parmi tous les chemins constituant : le Dataflow. Ce dernier est souvent utilisé pour mettre l'accent sur

des chemins spécifiques soumis à des contraintes de latence, des attentes de sûreté, etc.

Concepts fonctionnels de l'ingénierie système -normes 15288 et 1220	**Concepts fonctionnels de l'ingénierie système - ARCADIA**
Partie prenante	Entité et acteur
Mission opérationnelle	Mission
Objectif opérationnel	Capacité
Scénario	Scénario
Activité	Activité et fonction
Interaction	Interaction et Échange fonctionnel
Donnée	Donnée
Élément du système	Composant

Table III.1: Alignement des concepts MBSE dans ARCADIA

III.3 EBIOS RM : Une méthode d'analyse des risques industriels

Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager (EBIOS RM) est une méthode récente d'évaluation et de traitement des risques numériques utilisée dans l'industrie. EBIOS est née d'une réflexion et d'une collaboration entre l'Agence Nationale de la Sécurité et des Systèmes d'Information (ANSSI) et plusieurs acteurs majeurs, regroupés par le Club EBIOS. Il est issu de l'expérience accumulée depuis de nombreuses années et de nouveaux besoins industriels. S'appuyant sur des concepts éprouvés, tels que les notions de moyens de soutien et d'événements redoutés, elle a actualisé l'approche de l'analyse des risques en prenant en compte la relation avec leur écosystème, les moyens d'évaluer et de valider le niveau de risque acceptable pour une démarche d'amélioration continue. En outre, elle met à disposition des ressources et des arguments utiles à la communication et à la prise de décision au sein de l'organisation et vis-à-vis de ses partenaires. Comme présenté dans notre état de l'art, EBIOS RM est composée de 5 ateliers (cadrage et socle de sécurité, sources de risque, scénario stratégique, scénario opérationnel, traitement du risque). EBIOS RM est conforme aux normes 2700X, notamment à travers l'implémentation (tableau III.2 et figure III.2) des concepts de sécurité que nous avons utilisés comme base pour notre langage MoRiaML. Dans ce qui suit, nous allons présenter le métamodèle d'EBIOS RM, puis dans la section III.4 l'implémentation du métamodèle de MoRiAML comme extension de celui d'EBIOS RM.

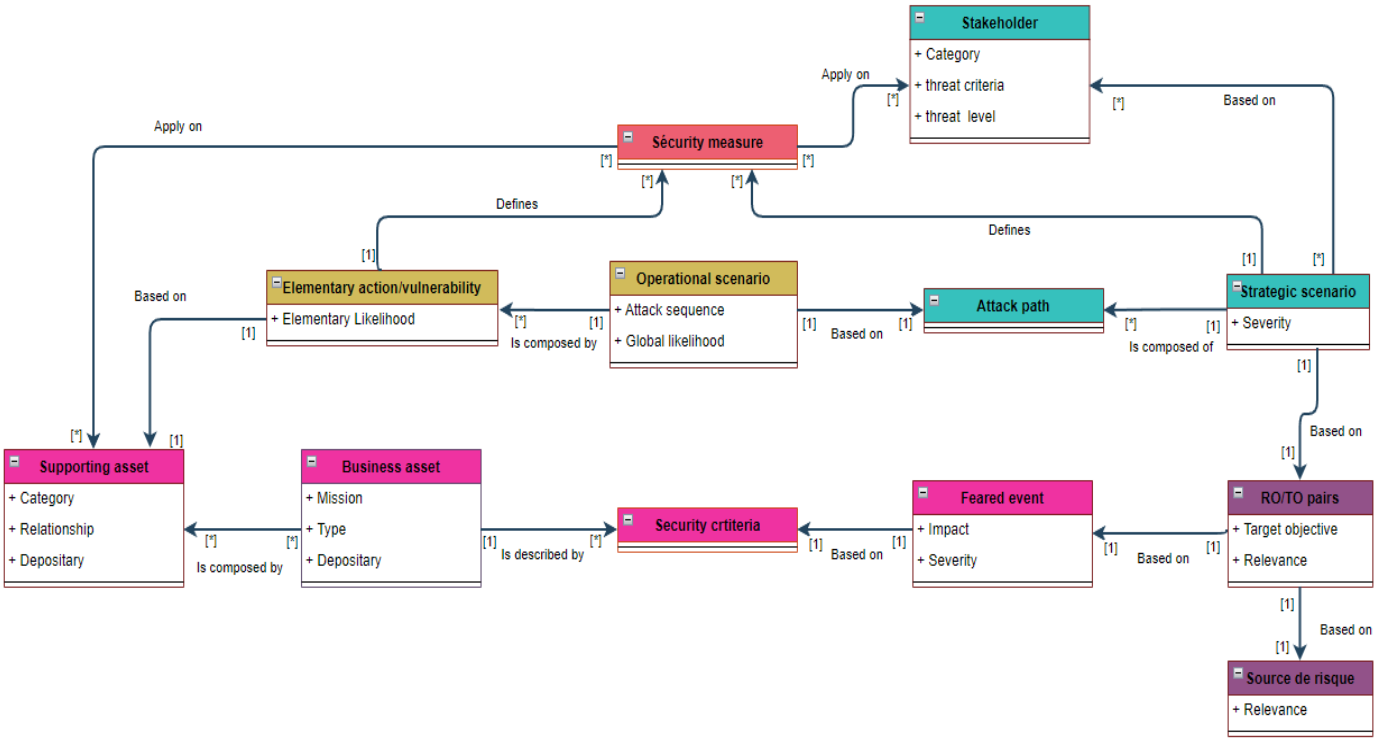


FIGURE III.2: EBIOS RM métamodèle

1. **Actif métier :** Dans le cadre de l'étude, composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé ;
2. **Actif support :** Composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle ;
3. **Critère de sécurité :** Propriété de sécurité à garantir pour une valeur métier. Elle traduit un enjeu de sécurité pour la valeur métier ;
4. **Origine du risque :** Élément, personne, groupe de personnes ou organisation susceptibles d'engendrer un risque. Une source de risque peut être caractérisée par sa motivation, ses ressources, ses compétences, ses modes opératoires (de prédilection) ;
5. **Partie prenante :** Élément (personne, système d'information, organisation, ou source de risque) en interaction directe ou indirecte avec l'objet de l'étude. On entend par interaction toute relation intervenant dans le fonctionnement normal de l'objet de l'étude. Une partie prenante peut être interne ou externe à l'organisation à laquelle appartient l'objet de l'étude ;

6. **Événement redouté :** Un événement redouté est associé à une valeur métier et porte atteinte à un critère ou besoin de sécurité de la valeur métier ;
7. **Scénario opérationnel :** Enchaînement d'actions élémentaires portées sur les biens supports de l'objet étudié ou de son écosystème. Planifiés par la source de risque en vue d'atteindre un objectif déterminé ;
8. **Scénario stratégique :** Chemins d'attaque allant d'une source de risque à un objectif visé en passant par l'écosystème et les valeurs métier de l'objet étudié ;
9. **Vulnérabilité :** Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système ;
10. **Action élémentaire :** Action unitaire exécutée par une source de risque sur un bien support dans le cadre d'un scénario opérationnel ;
11. **Mesure de sécurité :** Moyen de traiter un risque prenant la forme de solutions ou d'exigences pouvant être inscrites dans un contrat ;
12. **Traitement du risque :** La stratégie de traitement du risque formalise les seuils d'acceptation du risque et un niveau de sécurité à atteindre en cas de non-acceptation. Elle se réalise à partir de la cartographie du risque initial : pour chaque risque issu des activités d'appréciation du risque, la stratégie de traitement doit définir l'acceptabilité du risque.

À travers l'implémentation de la famille des normes 2700X via EBIOS RM, les concepts sont découpés en une plus grande variété permettant une analyse plus ciblée et sous différents niveaux d'abstraction et point de vue. Notamment avec la notion d'actif support et métier permettant de nuancer les besoins de sécurité au niveau des objectifs et missions du système avec ceux plus spécifiques au composant, l'architecture ou l'humain. De même, 3 niveaux de nuance ont été ajoutés au concept scénario afin de l'appréhender sous différents aspects : l'événement redouté qui est un scénario haut niveau ayant pour objectif d'identifier et évaluer le lien entre les sources de menace et nos actifs métiers, les scénarios stratégiques portés sur l'identification du chemin d'attaque allant d'une source de risque à un objectif visé en passant par l'écosystème et pour finir les scénarios opérationnels qui vont porter exclusivement sur le système afin d'identifier et évaluer les enchaînements d'actions élémentaires portées sur les biens supports pour réaliser l'attaque. Le code couleur utilisé est le même que celui utilisé par la méthode pour ces différents ateliers : rose pour le cadrage et socle de sécurité, violet pour

l'atelier sources de risque, turquoise pour l'atelier scénarios stratégique, ocre pour l'atelier scénarios opérationnels et enfin rouge pour l'atelier Traitement du risque.

Concepts de sécurité de la famille de normes 2700X	**Concepts de sécurité d'EBIOS RM**
Actif	Valeur métier, actif support
Rôle	Entreprise, Gestionnaire de dépôt, Propriétaire
Exigence	Critère et exigence de sécurité
Menace	Origine du risque, partie prenante
Incident de sécurité	Événement redouté, scénario opérationnel et stratégique,
Vulnérabilité	Vulnérabilité
Exploitation	Action élémentaire
Contrôle	Mesure de sécurité
Objectif de contrôle	Traitement du risque

TABLE III.2: Alignement des concepts de sécurité des normes 2700X dans EBIOS RM

III.4 Implémentation de MoRiaML

Les méthodes d'analyse de risque (EBIOS RM) et d'ingénierie système (ARCADIA) implémentent les normes utilisées pour la définition de notre métamodèle MoRiaML. Nous pouvons retracer les concepts de ces méthodes industrielles afin d'implémenter notre propre métamodèle de MoRiaML comme extension de ces 2 méthodes. Cette implémentation couvre donc la syntaxe abstraite, concrète, la sémantique ainsi que le processus d'utilisation du langage.

III.4.1 Implémentation de la syntaxe abstraite de MoRiAML comme extension du métamodèle d'ARCADIA

Le métamodèle MoRiAML implémenté spécialise le métamodèle des concepts fonctionnels de l'ingénierie système et de sécurité à travers leurs implémentations dans les méthodes industriels.

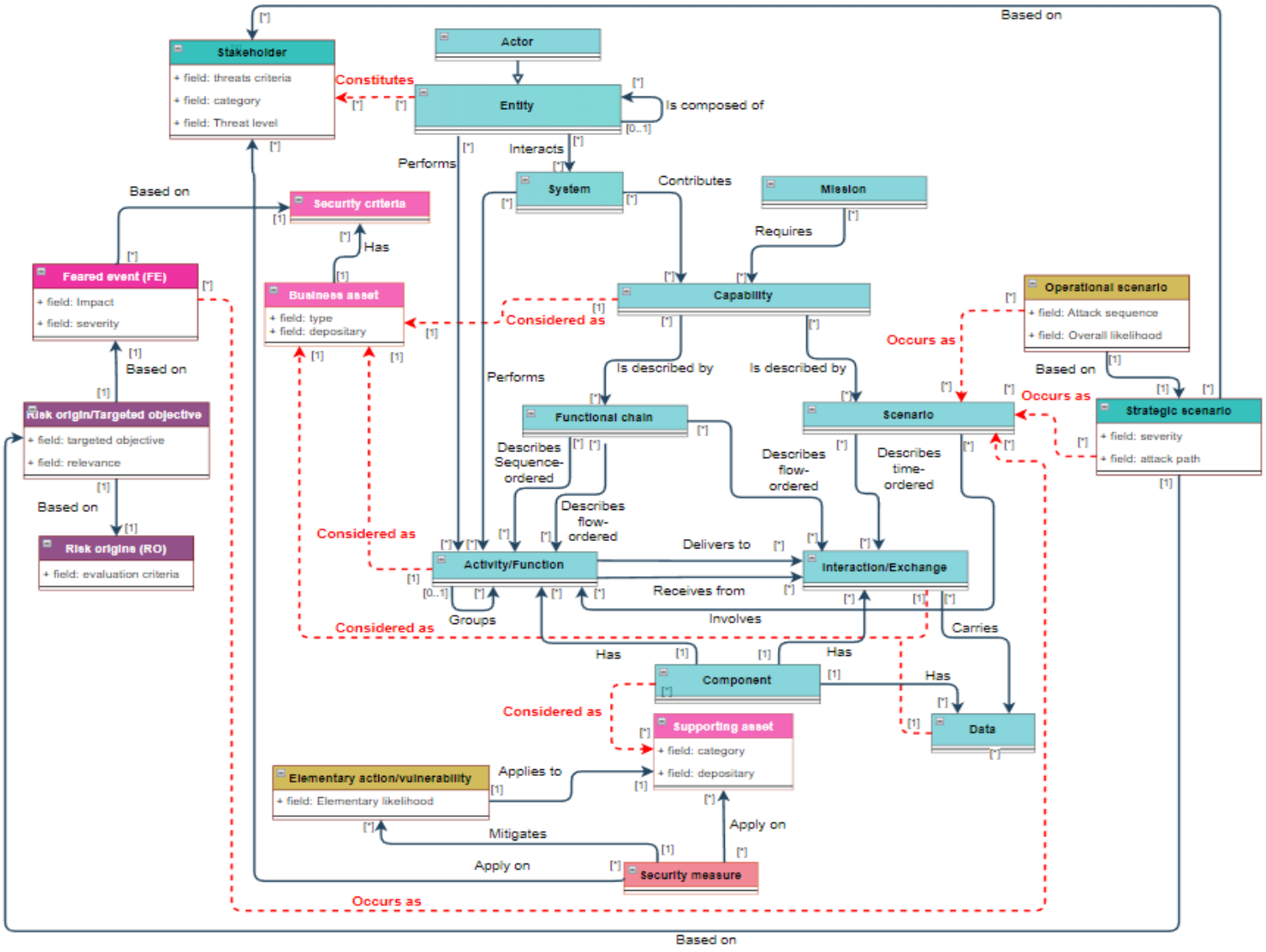


FIGURE III.3: Implémentation de la syntaxe abstraite MoRiAML (MetaModel)

Dans la figure III.3, nous illustrons notre métamodèle implémenté. Nous présentons nos extensions dans une seule figure comprenant les concepts fonctionnels d'ARCADIA en bleu et en rose, violet, turquoise, ocre et rouge les différents concepts d'EBIOS RM, ceux de sécurité et les relations entre les 2 domaines en pointillés rouge. À travers MoRiAML implémenté, nous alignons les concepts de *partie prenante* avec celui d'*entité*, de *scénario* avec les *événements redoutés*,*scénarios stratégiques* et les *scénarios opérationnels*, celui d'actif métier avec les *activités/fonctions*, *interactions*, *données* et *capacité* et pour finir le concept d'actif support avec le concept *composant*. Nous décrivons en détail dans la section III.4.3 l'alignement de ces concepts.

Cyber kill chain

Dans EBIOS RM, le concept *incident de sécurité* se voit affiné à travers différents degrés d'abstraction et points de vue : les *événements redoutés*, les *scénarios stratégiques* et les *scénarios opérationnels*. C'est à travers le concept de *scénarios opérationnels* que nous avons le niveau d'abstraction suffisant pour implémenter les concepts de MoRiAML représentant la cyber kill chain.

Notion d'état dans les différentes perspectives

La méthode ARCADIA intègre le concept *d'état* mais le catégorise sous deux concepts :

- Le concept de *mode* qui caractérise le contenu fonctionnel attendu du système. Un mode peut traduire divers concepts, comme une phase d'une mission ou d'un processus, un fonctionnement particulier requis du système, des conditions d'emploi comme un mode de test ou de maintenance, un mode d'entraînement, etc.

- Le concept *d'état* indique une situation en dehors des règles prévues, ou à laquelle on ne peut rien. Le plus souvent, un état se traduit sur les éléments structurels (présence ou absence d'un composant, disponibilité ou panne, intégrité ou pas, indisponibilité d'un acteur externe ou perte de connexion avec lui, etc.). Ceci permet d'implémenter facilement le concept d'état du métamodèle de MoRiAML.

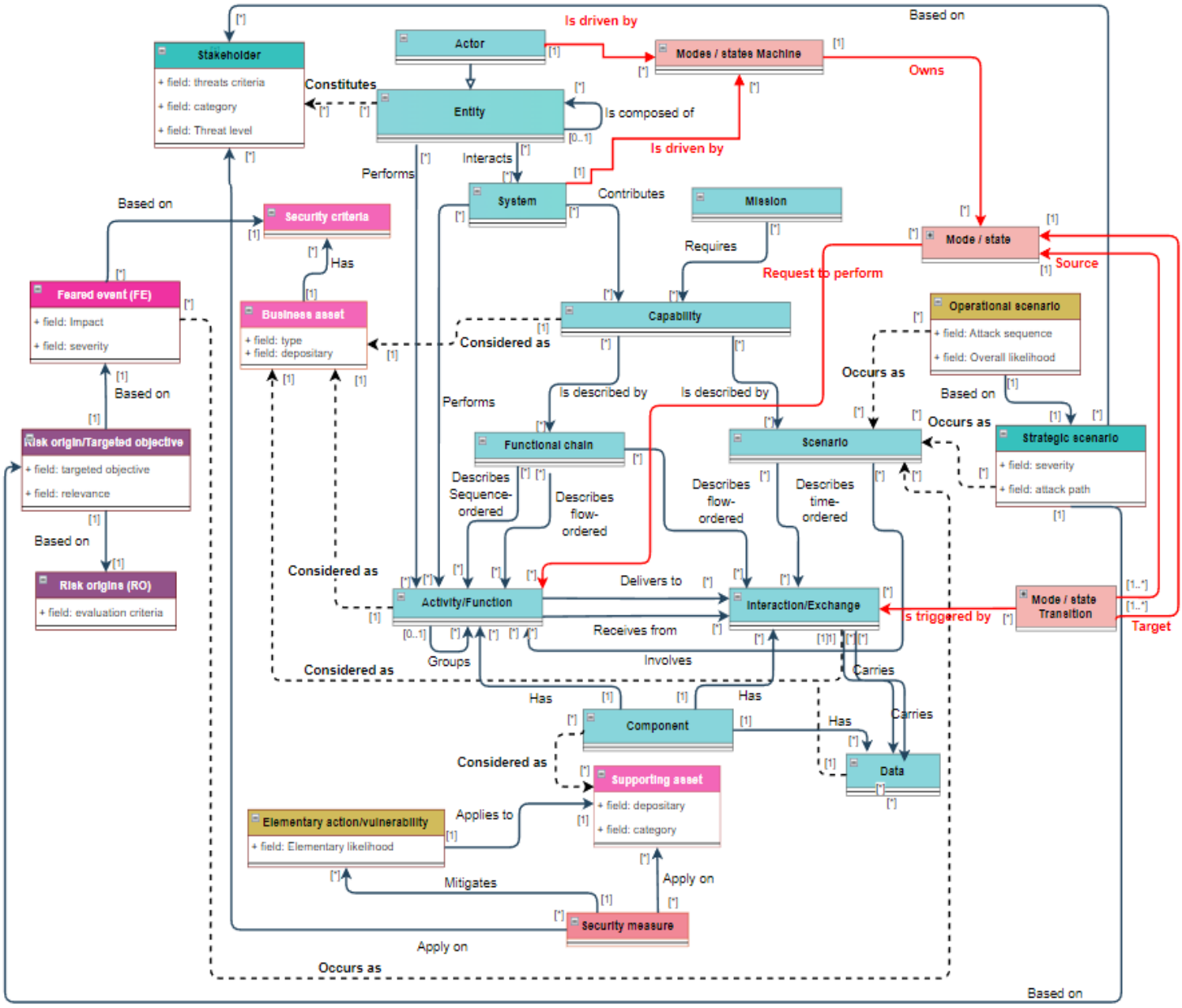


FIGURE III.4: Métamodèle de MoRiAML enrichi avec les concepts et relations entre état et mode et description fonctionnelle

Conformément à la sémantique de MoRiAML, ces concepts sont définis comme suit ;

1. **Transition d'état ou de mode :** Une transition est un changement d'un mode à un autre mode, ou d'un état à un autre état (appelés respectivement « source » et « cible de la transition ») ;
2. **État :** Un état est un comportement subi, dans certaines conditions imposées par

l'environnement, par le système, par un composant, par un acteur ou par une entité opérationnelle ;

3. **Mode :** Un mode est un comportement attendu, dans certaines conditions choisies, du système, d'un composant, ou encore d'un acteur ou d'une entité opérationnelle ;
4. **Machine d'états/modes :** Une machine de mode (respectivement d'états) est un ensemble de modes (respectivement d'états) liés les uns aux autres par des transitions. Des modes et des états ne peuvent cohabiter dans une même machine ;

Les notions de *mode* et *état* sont, comme présentées dans la figure, III.4 toujours associées au concept de *fonctions/activités* par l'association *demande d'effectuer*. La notion de *transition de mode* et de *transition d'état* est toujours associée aux interactions/échanges par l'association *est déclenché par*. Les notions de *machine de mode* et de *machine d'état* sont toujours associées aux concepts de *système* et d'*acteurs* par l'association *est entraîné par*.

À travers ces notions, l'objectif reste le même que pour la section II.3.2.2, de pouvoir définir des profils/contextes de sécurité/risques en fonction du contexte et du comportement du système. Les acteurs, le système ainsi que ses composants et fonctions n'ont pas le même besoin en sécurité, impacts et vraisemblance en termes de risque en fonction de leur contexte et état.

III.4.2 Implémentation de la syntaxe concrète de MoRiAML comme extension de Capella

III.4.2.1 Outil graphique de modélisation correspondant à MoRiaML

Comme discuté précédemment, la définition/extension d'un DSML implique la définition de son ensemble d'outils correspondant, principalement un éditeur graphique et un générateur de code. L'IDM offre des mécanismes automatisés et des méta-outils tels que le cadre de modélisation Eclipse (EMF), le cadre de modélisation graphique (GMF) et des normes d'échange comme l'échange de métadonnées XML (XMI), pour soutenir et automatiser la définition des outils du langage de modélisation, réduisant ainsi le temps et l'effort de développement des outils. Les principaux avantages de la définition d'un outil selon IDM sont de le rendre standardisé, modifiable, extensible et réutilisable.

Processus de construction de l'outil de modélisation de MoRiaML

Les mécanismes de l'IDM permettent l'utilisation de l'EMF pour définir un outil de modélisation logicielle pour MoRiaML. La figure III.5 illustre le processus suivi pour construire l'éditeur graphique visuel MoRiaML. Ce processus décrit les activités, les artefacts et les Méta-outils utilisés pour définir l'éditeur graphique. Un développeur Java, qui peut être assisté par un expert IDM, utilise le cadre de modélisation Eclipse pour définir le métamodèle/syntaxe abstraite MoRiaML et sa syntaxe concrète, ainsi que le mappage (semi-)automatique entre eux en utilisant le mécanisme de mappage/les règles de transformation de l'affichage EMF. Nous proposons une démarche pour étendre l'éditeur graphique Capella [3] spécifié, conçu et développé par Thales [4] une société française qui conçoit et réalise des systèmes critiques et fournit des services pour les marchés de l'espace, de l'aérospatiale, de la défense, du transport et de la sécurité. Capella est open source et activement maintenue avec une documentation bien établie, et est extensible et interopérable avec les langages et outils existants basés sur SysML.

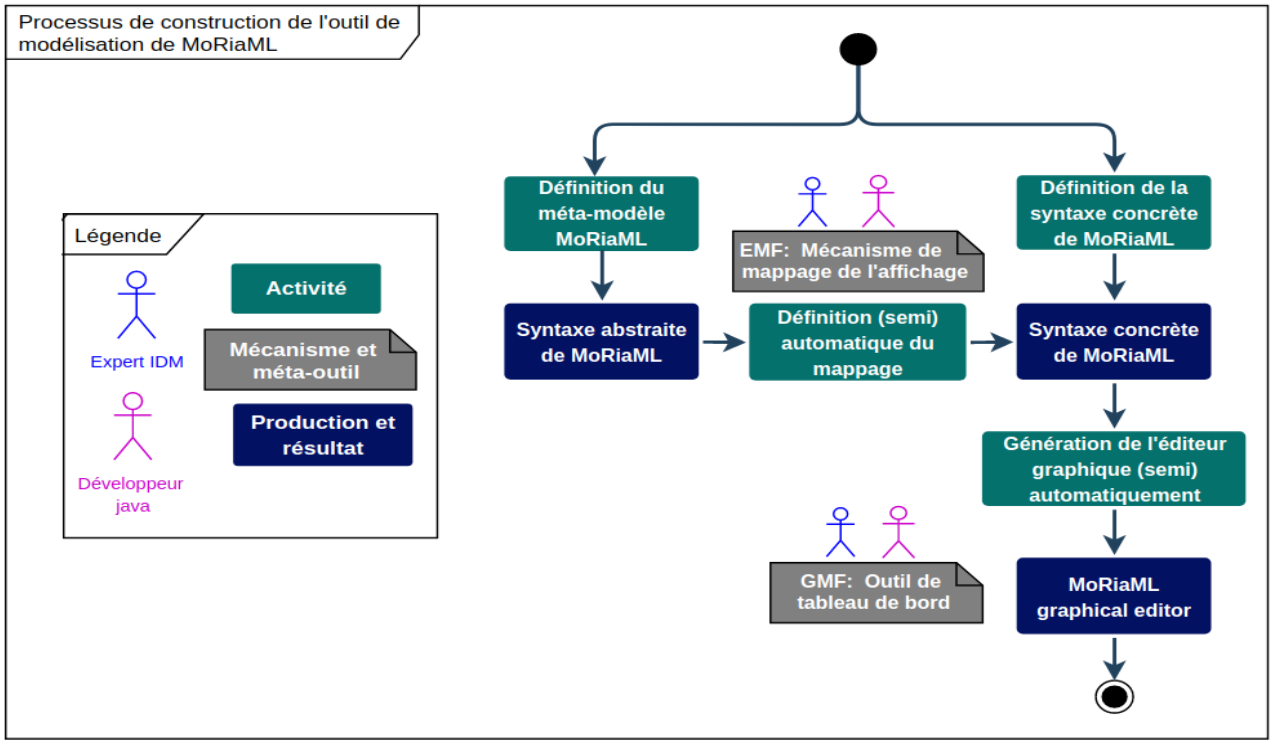


FIGURE III.5: Processus de construction de l'outil de modélisation de MoRiaML

3. https ://www.eclipse.org/capella/
4. https ://www.thalesgroup.com/en

III.4.3 Implémentation de la sémantique héritée du couplage ARCADIA - EBIOS RM

concepts de sécurité (ISO 27001)	**concepts de sécurité (EBIOS RM)**	**concepts d'ingénierie système (ISO 15288 et 1220)**	**concepts d'ingénierie système (ARCADIA)**	**Alignement conceptuel**
Menace	Origine du risque, Partie prenante	Partie prenante	Entité et acteur	Éléments (personne, système d'information, organisation ou source de risque) qui interagissent directement ou indirectement avec le système. Une menace peut être interne ou externe à l'organisation à laquelle appartient l'objet de l'étude.
Actif	Actif support et Valeur métier	Objectif opérationnel, activité/fonction, interaction, donnée, élément du système	Capacité, fonction / activité, interaction, donnée et composant	Les ressources d'information, les processus de mission/d'entreprise et/ou les programmes critiques qui présentent un intérêt particulier pour les adversaires potentiels ou réels. Un actif peut être matériel (par exemple, un élément physique tel que du matériel, un micrologiciel, une plate-forme informatique, un dispositif de réseau ou tout autre composant technologique) ou immatériel (par exemple, des êtres humains, des données, des informations, un logiciel, une capacité, une fonction, un service, une marque, un droit d'auteur, un brevet, une propriété intellectuelle, une image ou une réputation).
Contrôle	Mesure de sécurité	Activité/fonction, interaction, donnée et élément du système	Fonction/activité, interaction, donnée et composant	Les éléments opérationnels et techniques (ses composants, processus, données, sauvegardes ou contre-mesures) prescrits pour qu'un système puisse atteindre ses objectifs ou pour protéger le système.
Incident de sécurité	Évènement redouté, scénario stratégique et opérationnel	Scénario	Scénario	Comment le système et ses acteurs interagissent dans le contexte d'une capacité ou d'un service du système. Ces interactions prennent souvent la forme de séquences d'actions et, dans le cas d'un attaquant, son objectif est de détourner ces actions pour atteindre son propre objectif.

TABLE III.3: Cartographie entre les concepts de cybersécurité (EBIOS RM) et d'ingénierie des systèmes (ARCADIA)

La sémantique de MoRiAML implémenté a été réalisée à travers l'alignement sémantique entre les deux domaines et à travers leur implémentation dans leur méthode industrielle. Le tableau III.3 résume les principaux alignements sémantiques entre les concepts de cybersécurité ISO 27001 et leurs implémentations dans EBIOS RM (colonnes 1 & 2) ; et les concepts MBSE ISO 15288, 1220 et leurs implémentations dans ARCADIA (colonnes 3 & 4), avec la justification de ces alignements (colonne 5). En outre, la figure III.3 détaille la mise en œuvre des alignements sémantiques précédemment définis dans la section II.3.2.1 et illustrés dans la figure II.11 comme une extension d'ARCADIA et d'EBIOS RM.

— **Menace** est mis en œuvre à travers les concepts **Parties prenantes** et **Origine du risque** dans la méthode EBIOS RM. L'**Origine du risque** représente tout élément externe, personne, groupe de personnes ou organisation pouvant générer un risque. Le concept **Partie prenante** couvre les éléments faisant partie de l'écosystème du système et susceptibles de constituer un vecteur privilégié d'attaques. De même, le concept d'ingénierie système **Partie prenante** est mis en œuvre à travers le concept **entity** (entité) dans ARCADIA pour représenter les éléments (personne, système d'information, organisation) qui interagissent directement ou indirectement avec le système et ses utilisateurs. Par conséquent, conformément au tableau II.2, **Origine du risque** a été aligné sur **entity** (entité) en utilisant la relation ***constitutes*** (constitue).

— Le concept d'**actif** est mis en œuvre à travers l'**actif métier et support** dans la méthode EBIOS RM. L'**actif métier** comprend tous les composants importants permettant à une organisation d'accomplir ses missions sous deux formes : **type Service** et **type Information**. L'**actif support** couvre les **composants** du système sur lesquels un ou plusieurs **actifs métier** sont basés. De même, les concepts d'ingénierie système **objectif opérationnel**, **activité / fonction**, **interaction**, et **données** sont mis en œuvre dans ARCADIA à travers **capacité**, **fonction / activité**, **interaction / échange**, et **données**. Par conséquent, conformément à II.2, les **biens métier** du type service sont alignés sur la **capacité** du système, la **Fonction / Activité** critique et les moyens spécifiques d'**Interaction** par le biais des relations ***considéré en tant que***. De même, les **données** échangées qui requièrent des exigences ou une vigilance particulières sont traitées elles aussi comme un **bien métier** de nature informationnelle. Quant aux **biens support** ils couvriront l'ensemble des **composants** permettant la réalisation des **capacités** à travers les relations ***considérées en tant que***.

— **Contrôle** est mis en œuvre par le biais du concept **mesure de sécurité** dans la méthode EBIOS RM. **Mesure de sécurité** représente les moyens de traiter un

risque, d'abord sous la forme d'exigences, puis sous la forme de mesures de sécurité. De même, les concepts SE **activité/Fonction**, **interaction**, **données** et **éléments du système** sont mis en œuvre dans ARCADIA à travers **fonction/Activité**, **interaction/Échange**, **données** et **composants**. Par conséquent, la conformité à la II.2 **mesure de sécurité** est alignée sur les concepts **activité/fonction**, **interaction** et **données** par le biais du ***appliqué à*** .

— **Incident de sécurité** est mis en œuvre à travers les concepts **Événement redouté** , **Scénario stratégique** et **Scénario opérationnel** dans la méthode EBIOS RM. En effet, les **Événements redoutés** ***Basé sur*** **Critères de sécurité** et associés au **Actif métier** du système, représentent une attaque dommageable pour le système. Les **Scénarios stratégiques** avec l'évaluation de l'écosystème à travers les **Parties prenantes**, définissent les premiers scénarios partant de l' **Origine du risque** et évoluant vers le **Objectif visé**, en tenant compte du point d'entrée apporté par les **Parties prenantes**. Enfin, le **Scénario opérationnel** est une chaîne de **Actions élémentaires** s'appliquant au **Actif support** de l'objet étudié. De même, le concept d'ingénierie système **scénario**, se retrouve dans ARCADIA sous le même nom. Par conséquent, conformément à II.2 **Événements redoutés, le scénario stratégique et opérationnel** a été aligné avec **Scénario** à travers la relation ***Occurs as***.

III.4.4 Processus d'utilisation correspondant à l'implémentation de la méthode MoRiA dans ARCADIA et EBIOS RM

Dans cette section, nous reprenons le processus d'utilisation de MoRiA et nous l'étayons avec les implémentations dans les méthodes ARCADIA et EBIOS RM.

Comme expliqué dans le chapitre précédent, les équipes d'ingénierie système dans une approche descendante mettent l'accent sur l'analyse du problème avant de définir directement la solution. Pour cela ARCADIA propose une première perspective appelée analyse opérationnelle. Cette perspective analyse la problématique des utilisateurs opérationnels, en identifiant les grandes fonctionnalités, acteurs devant interagir avec le système, leurs buts, les activités, les contraintes et les conditions d'interactions entre eux.

La Figure III.6 illustre en gris les actions actuellement réalisées par l'équipe système pour définir le système avec ARCADIA, en vert les actions nécessaires à la réalisation d'une analyse de risque avec EBIOS RM, en blanc les ressources sur lesquelles s'appuyer, en bleu des

vues dites de synthèse ayant pour objectifs de regrouper le travail réalisé afin de brainstormer entre équipes techniques et communiquer, argumenter sur l'avancement et les choix à faire avec les équipes non techniques. Le stickman violet représente l'équipe système (architectes et ingénieurs système), en rouge l'équipe sécurité (les ingénieurs et analystes de sécurité) et en noir les autres participants (RSSI, juriste, décideurs, responsable budget...).

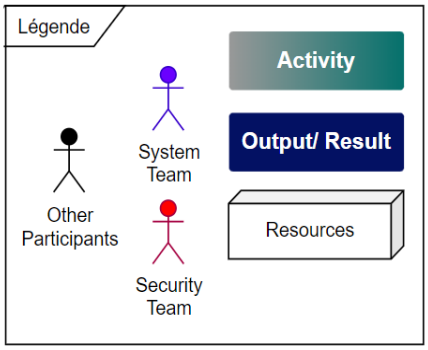


FIGURE III.6: MoRia processus d'utilisation - légende

III.4.4.1 Analyse opérationnelle

MoRiA commence dès les premières réflexions sur les grandes fonctionnalités appelées **capacité** dans Arcadia (figure III.7). Conformément à l'alignement III.3, les **capacités** sont alignées sur les **actifs métier** et sont traitées comme telles. L'ingénieur système définissant la **capacité** aidera à la définition des exigences de sécurité, notamment grâce à sa connaissance de l'importance de celle-ci dans la réalisation globale et fonctionnelle du projet. L'ingénieur sécurité apporte la matrice d'évaluation [5] et les **critères de sécurité** afin d'échanger et d'évaluer l'événement redouté avec les ingénieurs système utilisant leur expertise et leur connaissance du système. Les **capacités** grâce aux échanges entre les équipes se verront attribuer une valeur numérique, généralement entre 0 et 4, en fonction de la complétude des matrices et qui permet d'évaluer l'importance de chaque **critère de sécurité** : disponibilité, intégrité, confidentialité et traçabilité (DICT) [CSG18]. Par exemple, la notation [4301] attribuée à une **capacité** indiquerait que : 1) la **capacité** manipulée doit absolument rester disponible, 2) son exigence d'intégrité est importante sans être critique, 3) les informations utilisées par cette **capacité** sont publiques, et 4) il n'y a pas de besoin spécifique de traçabilité des accès. La **capacité** avec un **critère de sécurité** jugé critique

5. https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-going_further-en-v1.0.pdf

ou suffisamment important pour être pris en compte sera alors développé sous la forme d'**événements redoutés**. Les événements redoutés gardés se verront par la suite attribuer un score de sévérité en fonction du type et de la gravité des impacts engendrés (impact humain, matériel, sur la mission, juridique, image...)[andlsdsdA19] L'objectif étant de pouvoir à la fin de cette étape créer une première vue de synthèse regroupant et positionnant les événements redoutés en fonction de leur gravité. Cette première synthèse contient en son centre une abscisse horizontale représentant le niveau de gravité des événements redoutés, les actifs métier seraient organisés au-dessus de l'axe et ceux informationnels au-dessous de l'axe. Ici, même si un niveau de gravité spécifique a été attribué à l'événement, ce qui est important, c'est sa position relative par rapport aux autres actifs et sa position absolue sur l'axe. Un actif positionné à droite d'un autre actif a un niveau de gravité plus fort et vice versa. Dans la suite logique de définition de système, le second élément d'ingénierie est celui

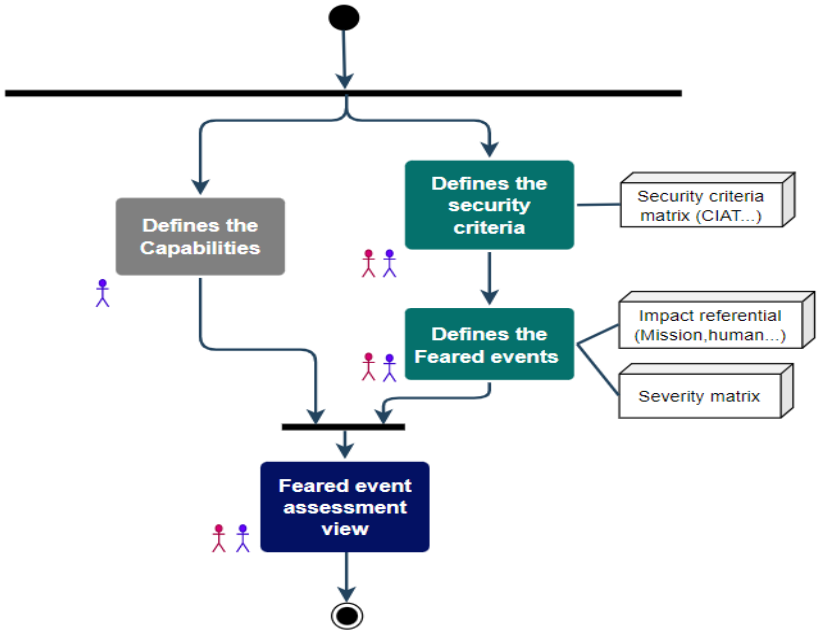


FIGURE III.7: MoRia processus d'utilisation - phase analyse opérationnelle - identification des actifs 1ère partie

des entités et des acteurs qui vont être susceptibles de réaliser ou d'interagir avec nos capacités (figure III.8). Conformément à l'alignement III.3, le concept de **partie prenante** est aligné avec **entité** et **acteur**, ils sont donc traités comme tel. Les parties prenantes se voient attribuer des métriques [andlsdsdA19] (dépendance, exposition, confiance ...) pour définir leur niveau de menace vis-à-vis des **capacités**. Une représentation sous forme de radar est conseillée, la distance radiale correspondant au niveau de menace selon l'échelle

d'évaluation utilisée. Plus une partie prenante fait peser une menace numérique importante pour l'objet de l'étude, plus elle se situe près du centre. En parallèle de l'identification et de

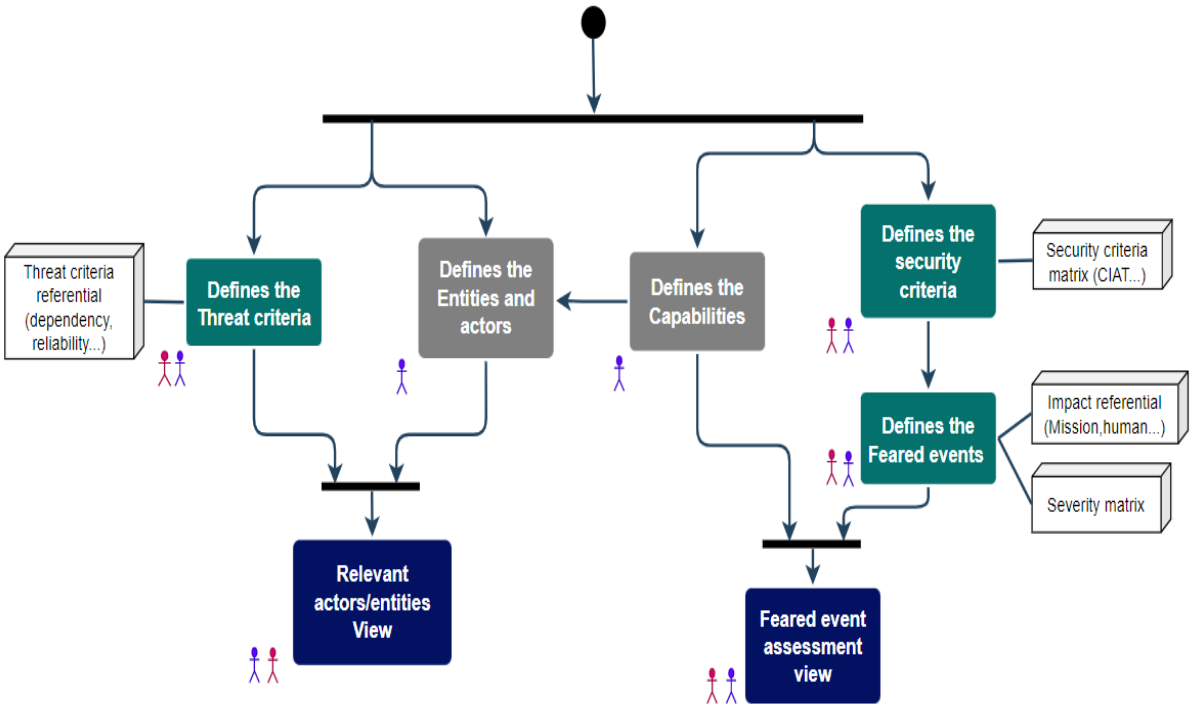


FIGURE III.8: MoRiA processus d'utilisation - phase analyse opérationnelle - identification de l'écosystème 1ère partie

l'évaluation du niveau de menaces des entités et acteurs interagissant avec notre système, nous pouvons travailler nos événements redoutés en élaborant des profils de menace (origine du risque)(figure III.9). Les profils **origines du risque** peuvent être définis à partir de métriques telles que la motivation et les ressources, comme l'illustrent les bases de connaissances proposées dans les fiches méthodologiques de l'ANSSI [andlsdsdA19] pour estimer le niveau de vraisemblance/dangerosité, pour par la suite associer les **origines du risque** aux **événements redoutés** qu'ils sont le plus susceptibles de réaliser. Lorsque l'équipe aura cessé de produire de nouveaux couples Origine du risque/Événement redouté, nous pourrons évaluer la pertinence de chaque couple. Si le retour d'expérience des participants peut constituer une première base d'évaluation, nous recommandons également d'utiliser des critères et métriques de caractérisation qui apporteront une certaine objectivité. La métrique de vraisemblance de l'origine de risque ainsi que celle de la gravité de l'impact de l'événement redouté sont là pour nous aider à identifier au mieux les couples les plus impactants. Ici aussi, nous conseillons une représentation sous forme de radar-pie (l'origine du risque représenté

en tant que “pie” et pouvant englober plusieurs événements redoutés). La distance radiale correspondrait au niveau de pertinence évalué pour le couple (plus le couple est proche du centre, plus il est estimé dangereux pour l’objet de l’étude). Par la suite dans le proces-

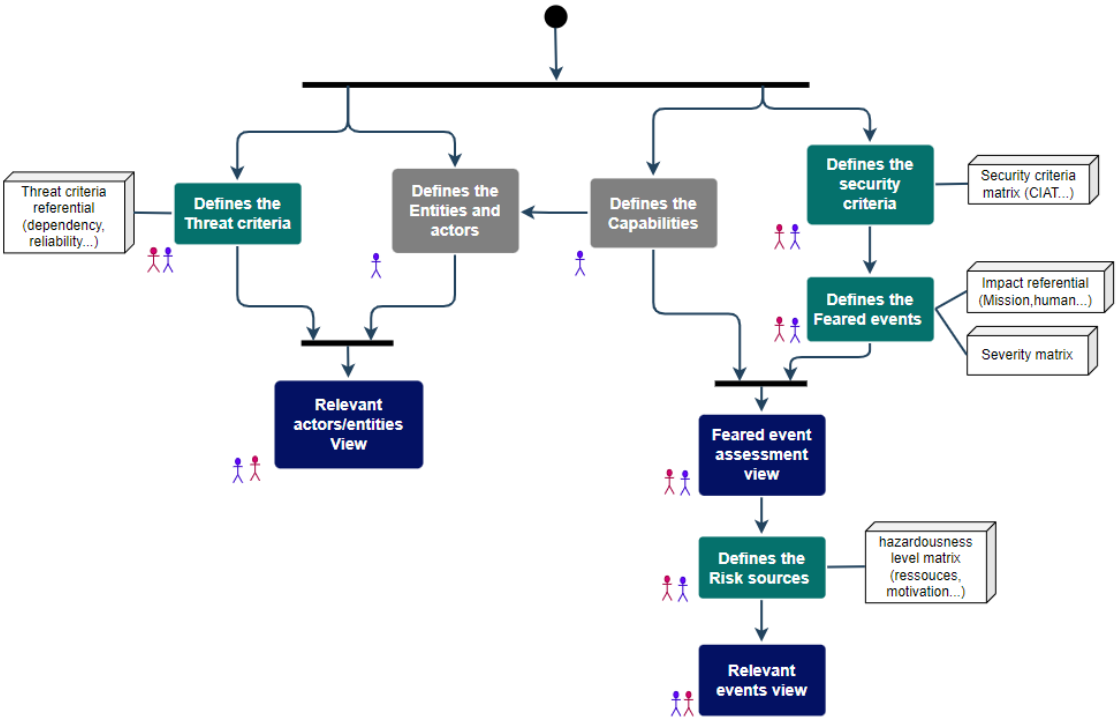


FIGURE III.9: MoRiA processus d’utilisation - phase analyse opérationnelle - identification des couples événement redouté/origine du risque

sus d’ingénierie d’Arcadia, les capacités sont découpées en activités, interactions et données que les entités et acteurs vont devoir réaliser (figure III.10). Les **fonctions**, **interactions**, **données** définies ultérieurement peuvent, si elles sont jugées critiques (par exemple, une **donnée** nécessitant un certain niveau de classification (Défense ou Confidentiel Secret ...)) qui va modifier le score d’une ou de plusieurs **capacités**, ou du moins être considérés comme des **événements redoutés** spécifiques détaillant les **capacités**. Cette première itération nous permettant de compléter nos listes d’événements redoutés afin d’identifier au mieux les éléments ciblés ainsi que les profils d’attaquants les plus vraisemblables.

À travers cette première perspective, nous arrivons à identifier quelles sont les grandes fonctionnalités que nous allons devoir protéger ainsi que certaines plus spécifiques à nos exigences de sécurité. Nous les avons couplées avec leurs sources de menaces les plus vraisemblables et nous les avons comparés afin de garder seulement les plus pertinents. En parallèle à cela, nous avons évalué le niveau de menaces de nos parties prenantes. À partir

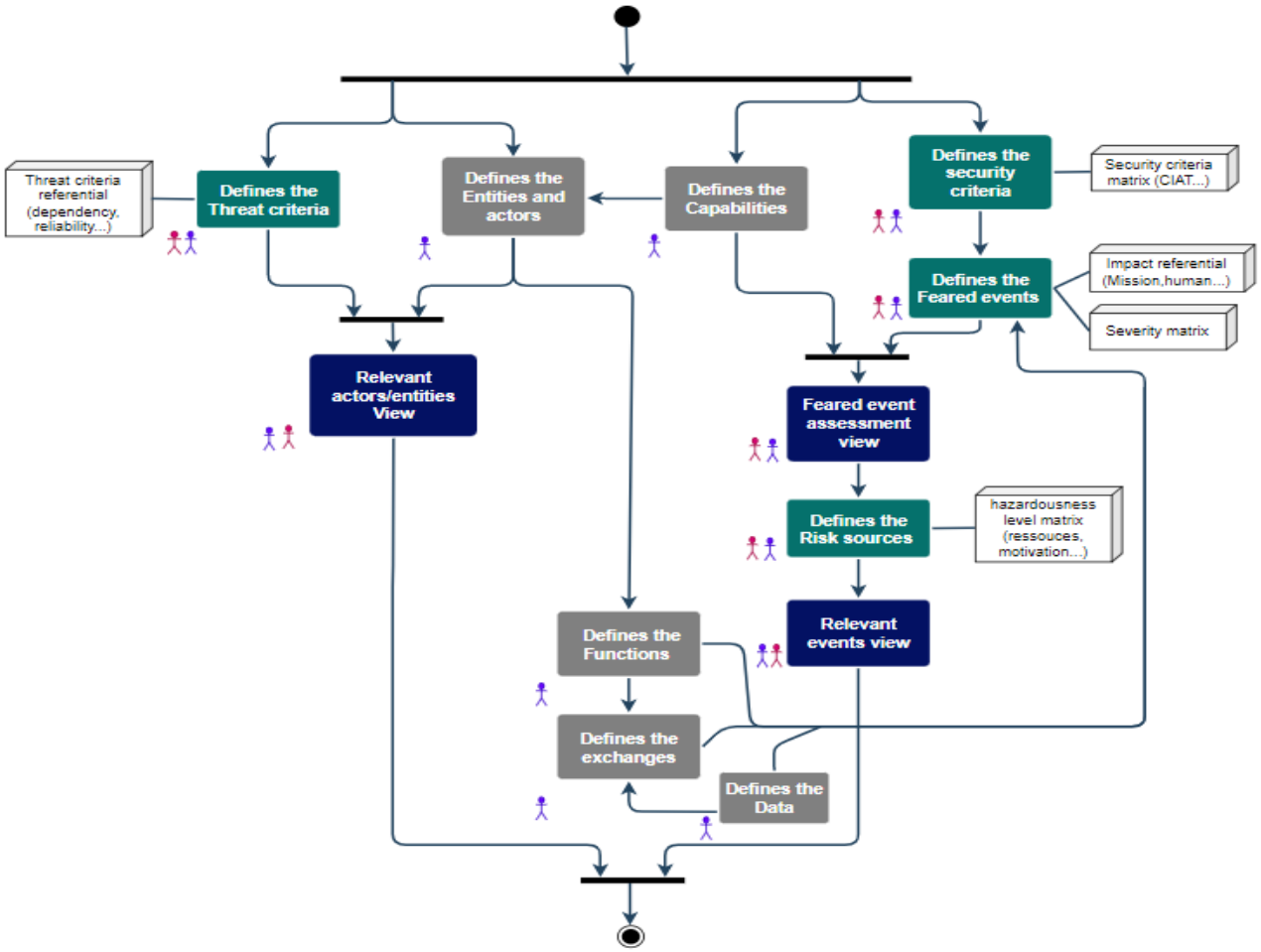


FIGURE III.10: MoRiA processus d'utilisation - phase analyse opérationnelle - identification des actifs 2ème partie

de cela, le concept de *mode* nous permet de re-contextualiser et nuancer nos analyses. Afin de définir comme précédemment l'impact des événements redoutés, la pertinence de menace, la pertinence des couples événements redoutés/origine du risque ainsi que le niveau de menace des parties prenantes en fonction du contexte du système.

L'analyse opérationnelle n'a que pour objectif d'identifier et de représenter ce que les utilisateurs du système doivent accomplir ; dans la seconde perspective, la notion de ce que le système doit réaliser pour les utilisateurs apparaît.

III.4.4.2 Analyse Système

Cette perspective construit une analyse fonctionnelle externe, bâtie à partir de l'analyse opérationnelle et des exigences textuelles d'entrée et modélisées, pour identifier en réponse les fonctions ou services du système nécessaires à ses utilisateurs, sous contrainte des propriétés non fonctionnelles demandées. Ici les activités, interactions et données définies précédemment sont raffinées et assignées au système ou à ces entités et acteurs. Cette nuance nous permet d'identifier les éléments propres à notre système et ceux qui vont faire partie de notre écosystème et que donc nécessiteront un traitement spécial quant aux exigences et en mesures de sécurité. Après ces attributions et la nette démarcation de notre système avec son écosystème, il est possible que les activités/fonctions, interactions/échanges et les données se soit précisés dans leur définition. Une itération est alors réalisée pour reconfigurer et réévaluer nos couples afin de les élaborer à travers des scénarios stratégiques (figure III.11). Le scénario stratégique issu du couple origine du risque/événement redouté va être décrit en une séquence d'événements réalisés par la source de risque en passant possiblement à travers nos parties prenantes pour atteindre son objectif. Ici, nous avons le point de départ (origine du risque), les possibles points d'entrées à travers nos entités et acteurs et l'objectif visé sous la forme d'une activité, interaction ou donnée dans notre système. Les événements réalisés au sein de notre système se verront assigner des exigences de sécurité de type protection (cloisonnement, contrôle d'accès, chiffrement...), défense (surveillance d'événements, détection et classification d'incident, réponse à un incident cyber...) et résilience (continuité d'activité (sauvegarde/restauration, gestion en mode dégradé), reprise d'activité...) afin de prévoir et de réfléchir à l'architecture logique et physique de façon sécurisée dès cette phase. Les entités et acteurs auront quant à eux des exigences et des mesures à appliquer de leur côté de nature de type gouvernance et anticipation (audit de sécurité, processus d'homologation...) afin d'appréhender et réduire leur niveau de menaces. Une autre solution pourrait alors être à ce stade de changer de prestataire pour quelqu'un ayant un niveau de menace inférieur ou d'internaliser le processus. Les mesures de sécurité appliquées à nos parties prenantes réduiront leur niveau de menaces, permettant dans un premier temps de réduire voire de contrôler les points d'entrée de notre système.

III.4.4.3 Architecture logique

Comme définit dans le processus de MoRiA, l'analyse du contexte et de l'écosystème à ce stade a été réalisée, les équipes système et sécurité concentrent alors leur analyse sur

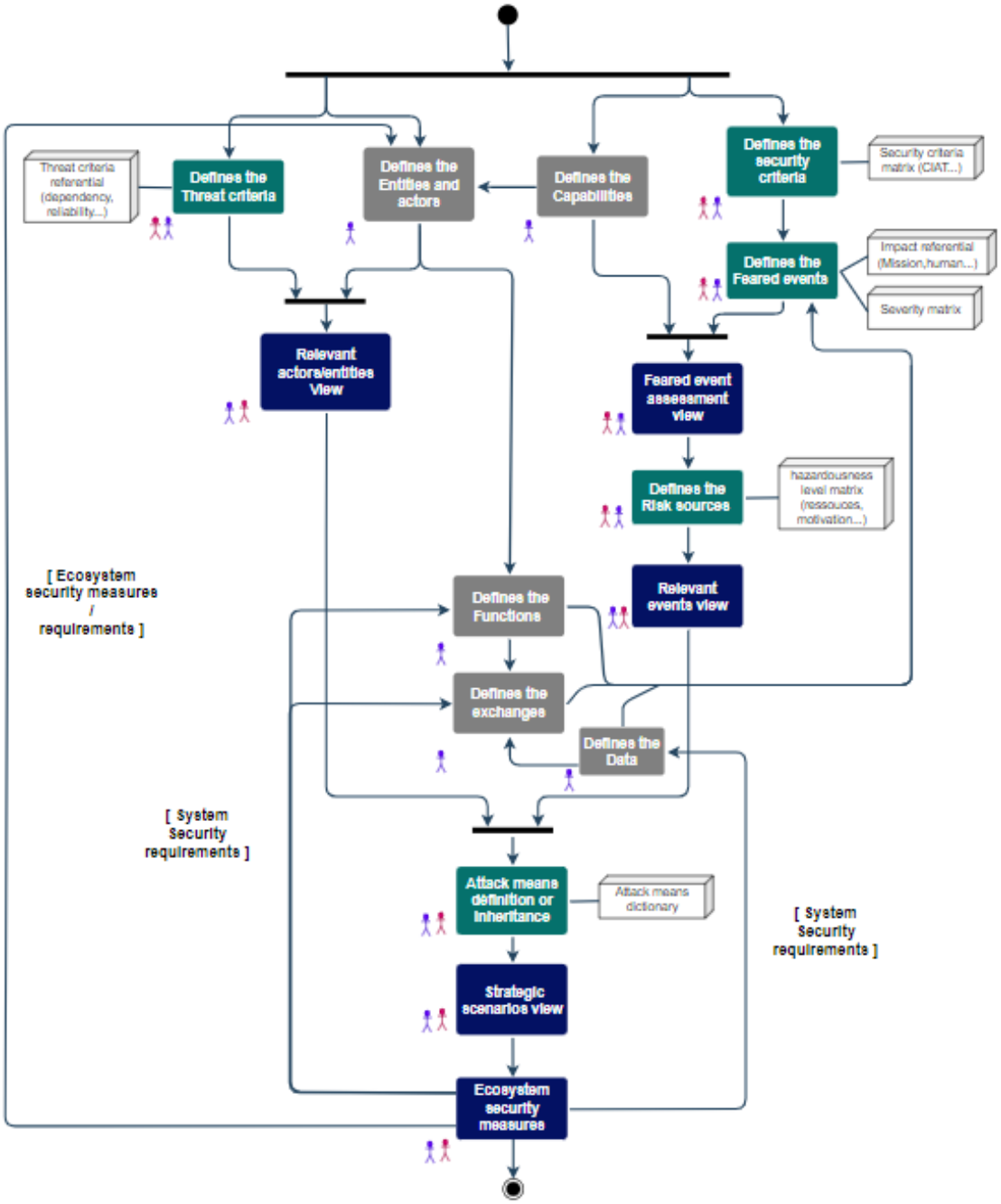


FIGURE III.11: MoRiA processus d'utilisation - phase analyse système - définition des scénarios stratégiques

le système. Les points d'entrées à travers les parties prenantes ainsi que les interventions physiques de la source de risque dans notre système sont identifiés. Les équipes système et sécurité vont par la suite identifier la chaîne fonctionnelle constituée d'activités/fonctions, interactions, échanges et de données qui vont être utilisées et détournées pour réaliser son

objectif qui est notre valeur métier sous la forme d'événement redouté.

Comme proposé dans la méthode EBIOS RM nous définissons le *scénario opérationnel* et à travers l'alignement de celui-ci avec *incident de sécurité* nous proposons de le décrire sous la forme de "Cyber Kill Chain" comprennent cinq phases : (i) reconnaissance externe ; (ii) intrusion ; (iii) reconnaissance interne ; (iv) déplacement latéral ; (v) exploitation. Ainsi que l'utilisation de métriques afin de noter la vraisemblance de la réalisation de chaque étape de la cyber kill chain.

Comme nous pouvons le voir dans la figure III.12 nous ajoutons les exigences et mesures de sécurité directement sur les biens support impactés dans le scénario permettant après itération de diminuer la dangerosité globale du scénario. À ce stade de l'analyse, il nous faut appliquer les mesures de sécurité physique dans la dernière phase de l'architecture physique. Tout ce processus nous permet de modéliser l'analyse de risque tout au long de la définition du système de façon corrélée répondant ainsi à notre QR1, permettant ainsi à la moindre modification de l'architecture ou du besoin d'itérer l'analyse afin de modifier les différentes vues pour ensuite communiquer sur la marche à suivre. C'est également le cas si nous modifions nos métriques de sécurité afin de rester à jour en termes de sécurité répondant ainsi à notre QR2.

III.5 Conclusion

Dans ce chapitre, nous avons implémenté MoRiA comme extension de 2 méthodes connues, basées sur les normes et utilisées dans l'industrie française et internationale. Cette implémentation nous a permis de démontrer que la méthode générale et applicable telle quelle sur des méthodes industrielles implémentant les mêmes normes. De plus, cette implémentation permet son utilisation dans l'industrie et donc sur des cas d'étude opérationnels. Dans la section suivante, nous allons illustrer la méthode MoRiA implémentée sur un cas d'étude de système naval.

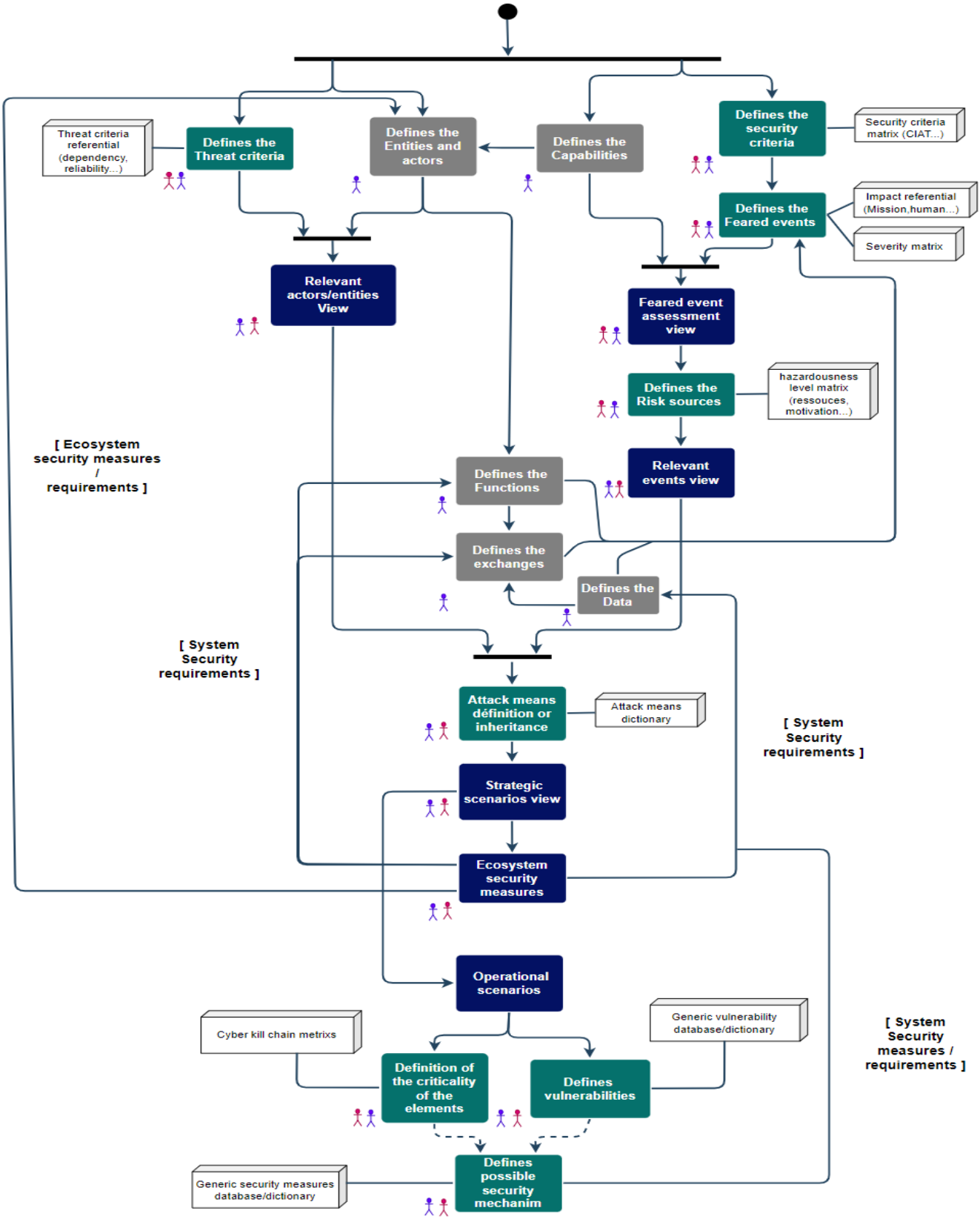


FIGURE III.12: MoRiA processus d'utilisation - phase analyse système - définition des scénarios opérationnels

Chapitre IV

Cas d'étude : Modélisation et analyse de risque d'un système naval à l'aide de la méthode MoRiA

Sommaire

IV.1 Introduction

Après avoir présenté la partie modélisation de notre méthode MoRiA ainsi que son implémentation à travers deux méthodes industrielles et le processus d'utilisation à suivre lors de l'utilisation de la méthode, nous présentons dans ce chapitre l'application de notre méthode MoRiA sur une étude de cas d'un système naval.

Environ 80% du commerce international est transporté par voie maritime [SHJ+19]. Les

navires sont de plus en plus sophistiqués et, dans de nombreux cas, les équipages sont de plus en plus réduits. Les Systèmes d'information et réseaux informatiques ont progressivement envahi le monde du transport maritime et sont désormais omniprésents sur les navires : systèmes de navigation, postes bureautiques utilisés par l'équipage, systèmes « métier » tels que, par exemple, le poste de contrôle de la cargaison d'un super tanker, ou les systèmes de gestion de plate-forme (propulsion, électricité, fluides...). Cette évolution s'est accompagnée de l'émergence de nouveaux risques et les chiffres parlent d'eux-mêmes : les grands ports maritimes subissaient en moyenne 10 à 12 cyber-attaques par jour en 2017 [Cer17]. Cette tendance ne fait que s'accentuer, puisque le nombre de cyber-attaques dans le transport maritime a augmenté de 400% selon le spécialiste israélien de la cybersécurité Naval Dome [Dom20], ces tentatives de piratage ont augmenté depuis février 2020, ce qui coïncide avec une période où le secteur maritime s'est tourné vers une plus grande utilisation de technologies en raison de la pandémie de coronavirus. Nous pouvons nous attendre à ce que cette tendance se poursuive, avec une augmentation des attaques contre les navires et les ports.

La gestion efficace des menaces cybernétiques exige un ensemble d'outils proactifs et l'instauration d'une culture de sécurité globale. Conscient de cela l'Union européenne a financé le projet FORESIGHT visant à développer une solution fédérée de «cyber range» pour améliorer la préparation des professionnels de la cybersécurité à tous les niveaux et faire progresser leurs compétences en matière de prévention, de détection, de réaction et d'atténuation des cyberattaques sophistiquées. Un écosystème de plates-formes de formation et de simulation réalistes en réseau a été mis en place dans les domaines de l'aviation, des réseaux intelligents et de la marine. Ces plateformes permettent la création de scénarios complexes inter-domaines/hybrides basés sur les tendances identifiées et prévues des cyberattaques et des vulnérabilités extraites de la littérature ; cela permettra le développement de modèles avancés d'analyse des risques et d'économétrie ce qui s'avérera précieux pour estimer l'impact des cyber-risques, sélectionner les mesures de sécurité les plus appropriées et les plus abordables, et minimiser le coût et le temps de récupération après une cyber-attaque. La chaire de cyberdéfense navale [1] est le concepteur et le responsable de la plateforme navale. Cette plateforme se veut générique et au plus proche de ce qui est utilisé à bord des navires de commerces et de transport tant dans l'architecture que sur les composants utilisés afin de pouvoir conduire et tester en conditions opérationnelles diverses expérimentations (analyse de risques, scénario de cyber-attaques, analyse réseau...). C'est pour cela, que nous utilisons la plateforme navale comme étude de cas tout au long de ce chapitre, sur lequel nous appliquons notre méthode MoRiA pour prouver son efficacité dans la modélisation et l'ana-

1. `https://www.chaire-cyber-navale.fr/`

lyse de risque et de l'architecture sécurisée en découlant. Le système naval étudié comprend son système de navigation, de propulsion, d'énergie, de sécurité et de systèmes auxiliaires ainsi que ses interactions et connexions avec les parties prenantes nécessaires ou présentes (équipage, passagers, prestataires...).

Dans ce chapitre, nous illustrons la partie modélisation de la méthode MoRiA sur la plateforme navale. Par conséquent, nous utilisons le langage MoRiAML proposé pour modéliser les différentes perspectives d'ingénierie de la définition du système. Ce travail a été réalisé en collaboration avec une équipe technique de l'entreprise Thales et les ingénieurs sécurité et plateforme du projet Foresight. Ce chapitre est organisé comme suit : dans la section IV.2, nous présentons le protocole que nous avons suivi pour définir et concevoir notre cas d'étude, principalement la phase de collecte de données. La section IV.3 décrit la phase de modélisation du système naval : le processus détaillé d'utilisation de MoRiA qui décrit capacité, fonction et acteur du système ainsi que les éléments de sécurité co-définis et co-modélisés rattachés et qui seront raffinés lors des différentes phases/perspectives de l'ingénierie à travers l'évolution de l'analyse de risque et des choix d'architecture et composants y découlant. Par la suite dans la section IV.4.1, nous discuterons des retours des utilisateurs de la méthode et nous comparerons les résultats obtenus avec les résultats d'une analyse de risque dite classique et nous conclurons ce chapitre dans la section IV.5.

Le système naval peut être représenté à travers 5 "couches" : la partie extérieure du navire "off ship", la partie générale où l'on retrouve le réseau des passagers ainsi que de l'équipage "general ship layer", la partie où la gestion des automates est réalisée "integrated ship control layer", puis la partie "process layer" où nous retrouvons nos différents systèmes tels que les boucles de propulsion, d'énergie, de sécurité et d'énergie et auxiliaires, pour finir la couche "instrument layer" comprend les capteurs et systèmes permettant la réalisation des services et fonctionnalités du système naval.

2. `https://club-ebios.org/site/approche-de-gestion-des-risques-de-type-obeya/`

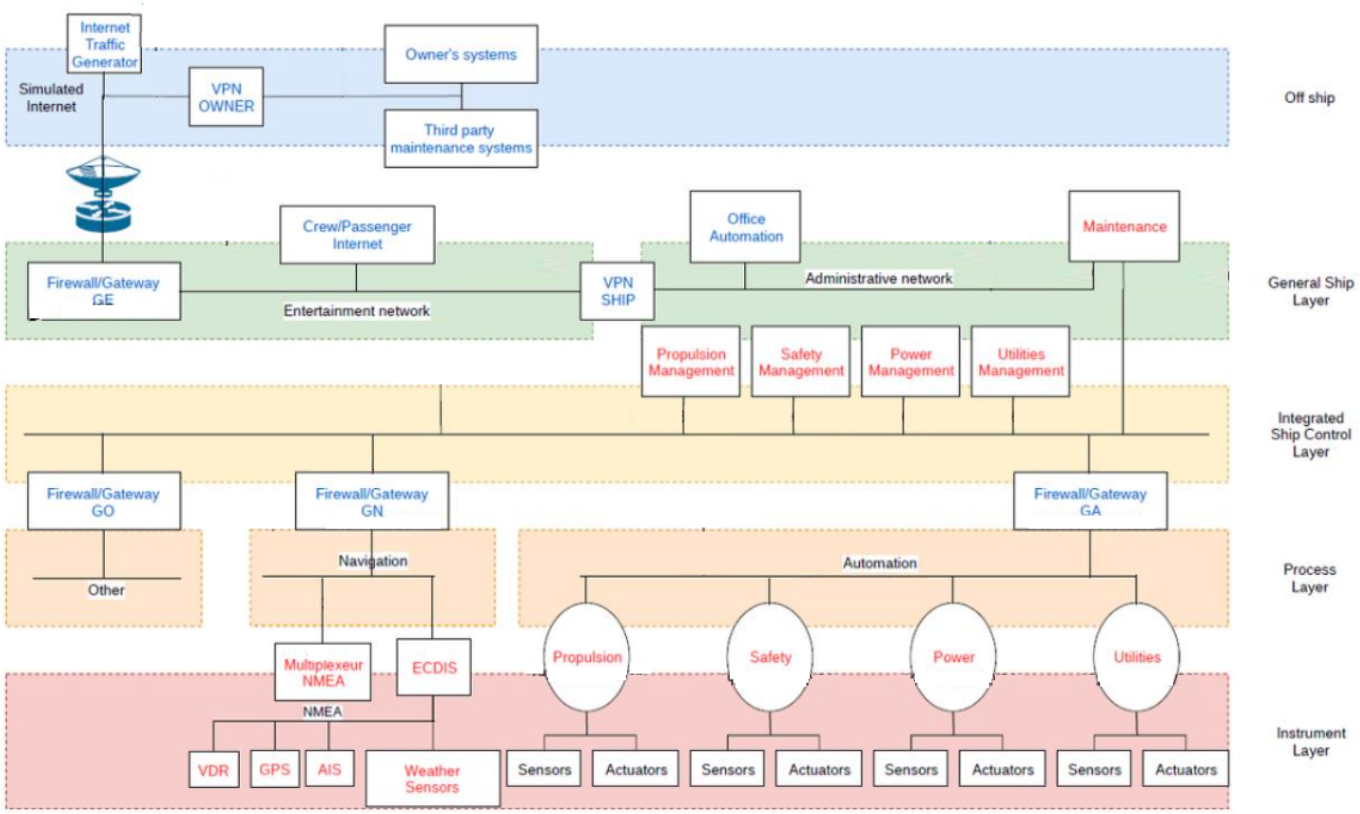


FIGURE IV.1: schéma du système naval [2]

IV.2 Protocole de planification de l'étude de cas

Pour réaliser notre étude de cas, nous avons suivi le modèle de protocole de planification présenté dans [bre]. Ce modèle de protocole améliore la précision de l'étude de cas en assurant que la collecte de données et les procédures répondent rigoureusement aux objectifs définis. Il identifie plusieurs étapes qui garantissent un processus de planification cohérent. Conformément à ces étapes, nous présentons dans les sous-sections suivantes le protocole de planification de l'étude de cas de la plateforme navale que nous avons mis en œuvre.

Introduction

L'objectif de cette partie est de définir les questions de recherche qui seront abordées par l'étude de cas. Pour notre travail, après une première réunion avec l'équipe de Thales, nous avons présenté notre méthode MoRiA (englobant le langage et le processus d'utilisation) et discuté de son application et pertinence dans le cadre de son utilisation sur la plateforme navale. Nous avons convenu que l'étude de cas devrait répondre aux questions suivantes :

- Comment pouvons-nous utiliser la méthode MoRiA pour modéliser le système naval tenant compte des concepts nécessaires pour l'analyse de risque ?
- Comment maintenir l'analyse lors des modifications du système ou de son écosystème ?

Description du cas d'étude

Les éléments centraux d'une étude de cas sont la définition de l'objet/du but de l'étude, et l'identification des propositions théoriques dérivées de chaque question de recherche. Pour notre étude de cas, le but de l'utilisation de MoRiA pour co-définir et co-modéliser l'analyse de risque dans l'ingénierie système afin d'aider les équipes d'architecture et de sécurité à atteindre les objectifs suivants :

1. Meilleure compréhension des préoccupations des deux domaines : cet objectif pourrait être atteint en co-identifiant et modélisant la sécurité avec les éléments fonctionnels et non fonctionnels de l'ingénierie système en fonction de leur raffinement, en se conformant au langage de modélisation MoRiA (MoRiAML) ;
2. Introduire et prendre en compte les mesures de sécurité dans l'architecture logique et physique de la plateforme : en définissant des scénarios de menaces et en identifiant les vulnérabilités/faiblesses possibles amenant à sa réalisation ainsi que les mesures à mettre en place ;
3. Avoir un retour sur les impacts de ces mesures sur notre système : en prenant en compte la modification de l'architecture dans notre analyse afin de la mettre à jour et d'identifier les nouveaux scénarios et vulnérabilités émergents.

En outre, la conception doit identifier le type de cas et son unité d'analyse. En se référant à [rob] :

- Un cas : il représente le sujet intéressant de l'étude. Les cas peuvent être uniques si les cas semblent représenter un test critique de la théorie existante ; ou multiples si une "logique de réplication" est censée révéler un soutien aux propositions théoriques ;
- Une unité d'analyse : la source réelle d'information. Il peut s'agir de conceptions holistiques ou intégrées. Les conceptions holistiques comprennent une seule unité d'analyse pour étudier la nature globale du phénomène. Les conceptions intégrées comprennent plusieurs unités d'analyse au sein d'un cas.

Puisque nous avons mené une seule étude de cas dans une seule entreprise/organisation pour tester notre méthode MoRia, notre étude de cas est une étude de cas unique. De plus,

notre objectif est de réaliser et modéliser l'analyse de risque ainsi que l'architecture sécurisé découlant de notre étude de cas, notre étude de cas est donc un cas holistique.

Choix du cas

Les critères de sélection de l'organisation et de l'équipe avec lesquelles nous avons collaboré pour réaliser notre étude de cas étaient les suivants :

- Une étude de cas réaliste et opérationnelle dans le contexte du domaine naval ;
- Capacité à collaborer avec les équipes d'architecture et de sécurité sur les tâches suivantes :
  - Collecter les données nécessaires ;
  - Comprendre les exigences fonctionnelles du système et de ses composants ;
  - Recueillir les problèmes de sécurité éventuels auprès de l'équipe de sécurité, s'ils existent, ou les définir, dans le cas contraire ;
  - Définir une liste de vulnérabilités de sécurité possibles pour chaque élément de nos scénarios.

Sachant que plusieurs lignes directrices de sécurité [McN16] existent pour aider les états et industriels à sécuriser leurs systèmes navals (navires et ports), il est plus raisonnable de concevoir et de mettre en œuvre des solutions à une échelle plus petite, mais néanmoins réaliste.

Procédures et rôles de l'étude de cas

Afin de planifier correctement les exigences de notre étude de cas, tels que les données nécessaires et leur analyse, nous détaillons dans ce qui suit les procédures suivies pour chacune de ces exigences (plan de collecte des données, stratégie d'analyse des données). En outre, nous avons clarifié les rôles des participants à cette étude de cas comme suit :

— L'équipe de recherche MoRiA (un étudiant en doctorat Mr Naouar supervisé par les Prof. KERMARREC et Dr. EL HACHEM) sont responsables de l'application de la méthode MoRia pour définir et modéliser l'analyse de risque dans les différentes phases de l'ingénierie système ainsi que son architecture sécurisée ;

— L'équipe Thales est chargée d'évaluer le résultat de cette étude, sa validité et son utilité pour la co-modélisation et co-analyse du système naval ainsi que sa mise à jour.

— L'équipe chaire cyber-plateforme chargée de fournir les données nécessaires à l'étude de cas

Collecte des données

1. Pour réaliser cette étude de cas, nous avons recueilli auprès de l'équipe d'architecture de la plateforme l'ensemble des données suivantes :

- Le but/la mission globale du système naval ;
- Les composants du système naval ;
- Les exigences fonctionnelles du système naval ;
- Des informations détaillées sur les interactions entres les différentes parties du système ;
- Les exigences de sécurité non fonctionnelles découlant des normes et devant être appliquées ;
- Des détails sur les composants du système et acteurs gravitant au tour de celui-ci, afin de définir une liste possible de vulnérabilités ou chemins d'attaque.

En plus de ces données, nous avons effectué une revue de la littérature pour étudier les publications/documentations existantes sur les problèmes de sécurité ou les scénarios d'attaque ciblant le domaine naval ainsi que les sources de ces problèmes.

2. Les données décrites ci-dessus ont été recueillies auprès de deux sources :

- Réunions/Interviews : De multiples réunions avec l'équipe de la chaire cyber défense via des discussions et réunions ;
- Étude de la documentation : En outre, nous avons étudié les publications existantes telles que [McN16].

Plan de validation

L'objectif de cette étude de cas est de valider notre méthode MoRiA en l'utilisant pour co-définir et modéliser l'analyse de risque et l'architecture sécurisée d'un système naval existant. Cela peut être considéré comme une étude de cas exploratoire pour identifier l'efficacité de la méthode MoRiA, ses avantages et ses limites. Les résultats de l'étude de cas ont été discutés et analysés lors de plusieurs réunions avec les équipes Thales qui certifient l'efficacité des résultats et leur utilité dans l'amélioration de la sécurité d'un système naval actuel.

Limitations de l'étude

Les limites des études de cas sont généralement liées à des problèmes de validité de l'étude plutôt que du plan. Voici quelques-unes des limites de notre étude de cas :

- Critères de sélection des études de cas : les caractéristiques utilisées pour sélectionner la recherche de l'étude de cas peuvent présenter certaines limitations dans son utilisation pour différents domaines d'application (la plateforme respectant et soumises aux réglementations et normes européennes).
- Généralisation : La généralisation pourrait être formalisée ou laissée au lecteur qui détermine ce qui peut s'appliquer à son contexte. Nous notons cependant que le choix de la plateforme du projet FORESIGHT a été pensé pour sa généricité qu'en besoins, fonctionnalités et architectures des systèmes navals et en appliquant la méthode MoRia sans aucun besoin de la raffiner, nous supposons qu'elle pourrait être généralisée à d'autres domaines d'application sans complications.

De plus, nous avons limité notre étude tant sur la modélisation et l'analyse à une partie du système, néanmoins suffisamment significatives pour nos besoins d'application, réflexions et validation. En supplément, les éléments du système naval, leurs vulnérabilités ainsi que la réalisabilité des chemins d'attaques sont simplifiés et ne reflète pas la situation opérationnelle des systèmes navals utilisés dans l'industrie.

Planning

L'étude de cas a été réalisée sur une période de 3 mois. Dans ce qui suit, nous décrivons le processus détaillé que nous avons suivi, par rapport aux étapes précédentes du protocole, pour réaliser notre étude de cas du système naval. Nous décrivons les acteurs/équipes et leurs rôles, ainsi que les différentes entrées et sorties de l'étude de cas en ce qui concerne les réunions et les échanges entre les équipes.

Lors d'une première réunion, l'équipe MoRia a présenté la méthode MoRia (le langage, les processus) et a discuté avec l'équipe Thales et la plateforme de la manière dont la méthode pourrait être utile pour la définition et la modélisation de l'analyse de risque dans l'architecture de la plateforme en tant que système naval. Par la suite, nous avons lors de plusieurs réunions discuté plus en détail des objectifs globaux, contextes et parties prenantes du système naval. Sur la base de ces informations et des directives de l'organisation maritime internationale (OMI), l'équipe MoRiA utilise la méthode afin de définir conjointement les éléments fonctionnels d'ingénierie système ainsi que de sécurité. Les résultats ont ensuite été discutés avec l'équipe Thales et suite à leurs retours, les éléments de modèles système et

sécurité ont été successivement raffinés plusieurs fois, jusqu'à la validation de celle-ci et cela pour les quatre perspectives d'ingénierie.

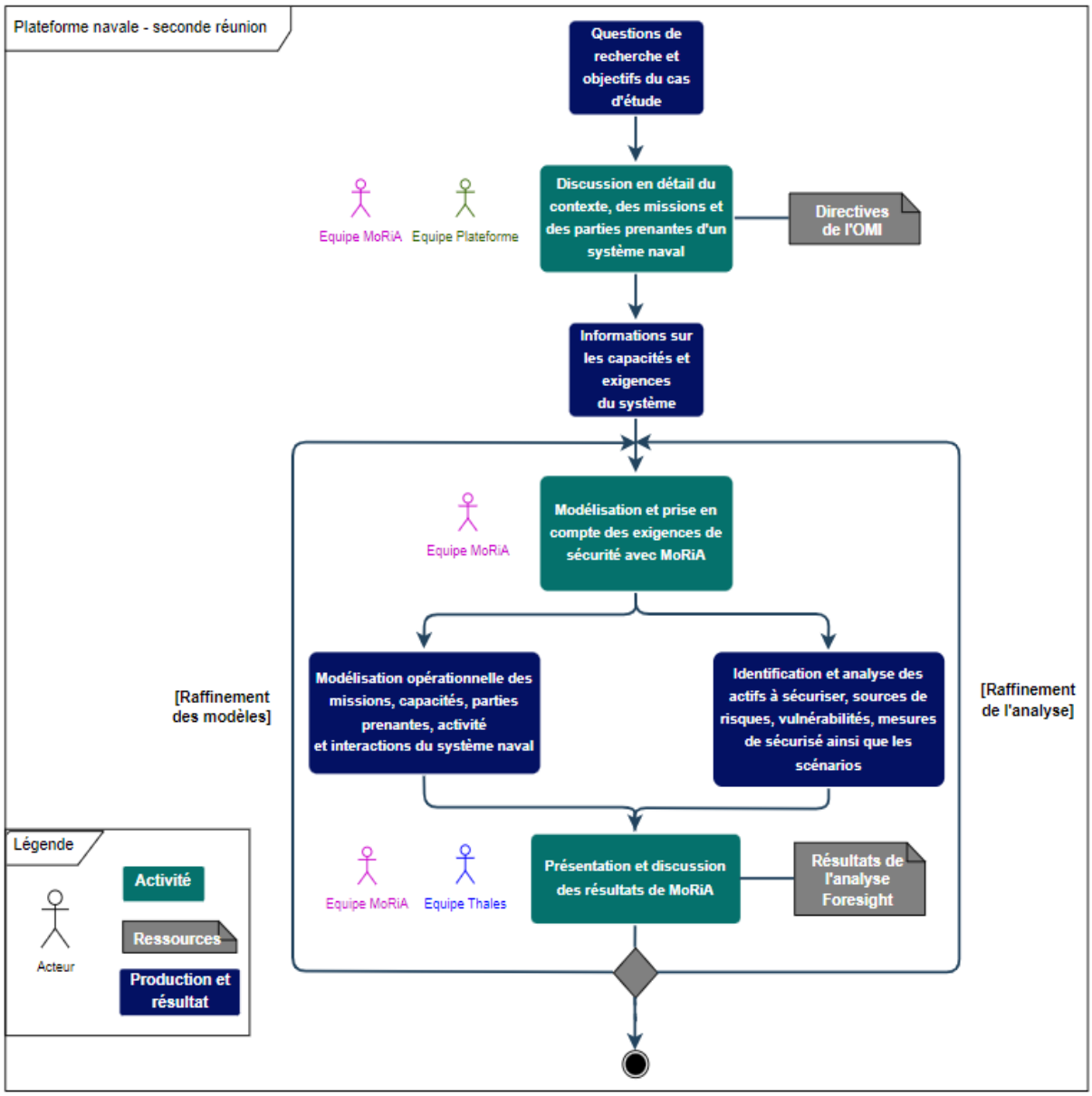


FIGURE IV.2: Protocole de planification

Il est important de mentionner que les données relatives aux composants du système naval ont été anonymisées pour des raisons de non-divulgation, et que toutes les informations relatives aux vulnérabilités réelles des composants du système naval ne sont pas présentées pour des raisons de sécurité. En effet, pour définir et modéliser les vulnérabilités de sécurité et pour définir les scénarios de menaces, nous avons suggéré quelques vulnérabilités possibles inspirées de notre étude des travaux relatifs à la sécurité des systèmes navals, y compris les

nouvelles attaques, qui ont été validées par l'équipe de Thales et plateforme comme étant réalistes.

IV.3 Modélisation et analyse de risques du système naval

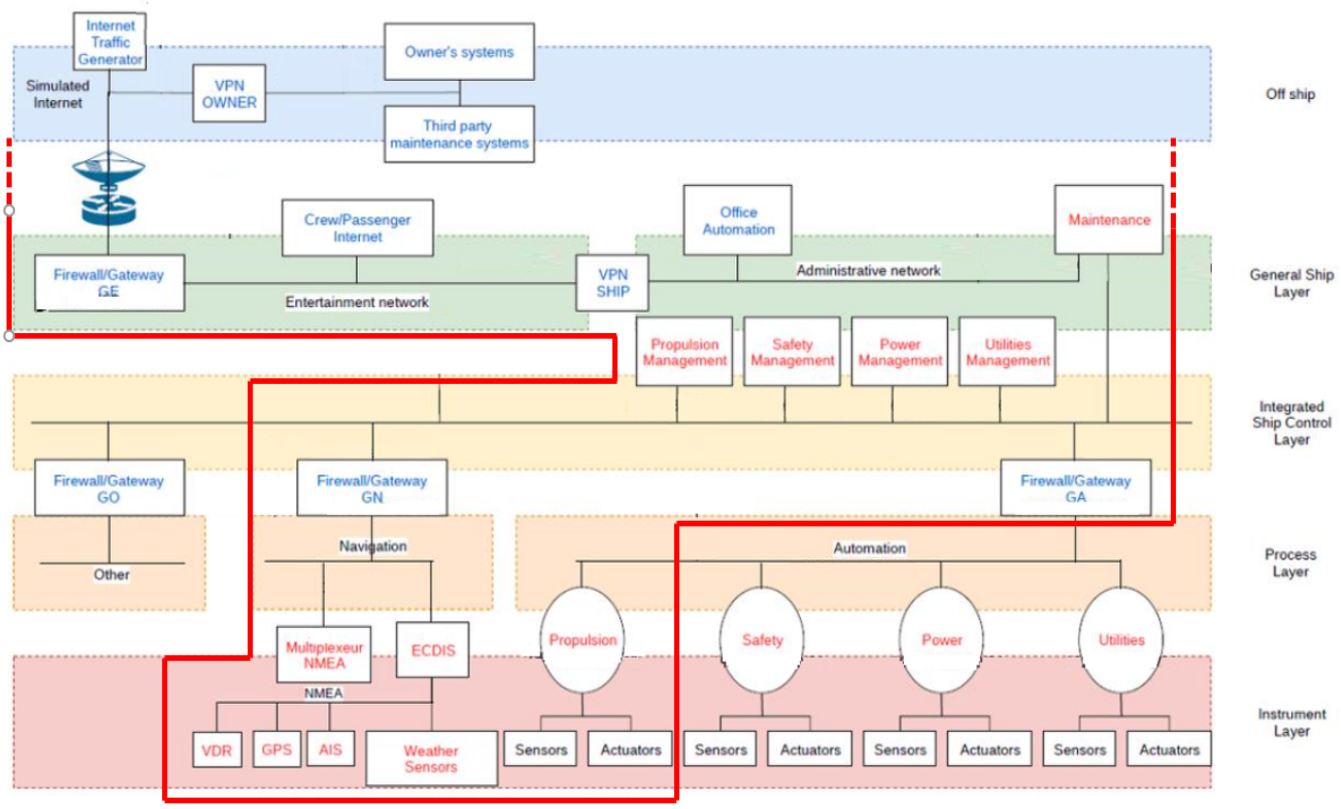


FIGURE IV.3: schéma du système naval [3]

Un navire est un système complexe d'ingénierie cyber-physique qui englobe à la fois des activités et des systèmes et des éléments distants tels que les signaux de navigation. Il a pour objectif d'assurer différentes missions et services :

- La gestion de la propulsion et de la direction :
  . Assure la gestion et le contrôle du système de propulsion (moteur, arbre, engrenage, hélice, etc.) ;

3. https://club-ebios.org/site/approche-de-gestion-des-risques-de-type-obeya/

. Assure la gestion et le contrôle du système de direction (gouvernail, propulseur, jet d'eau, etc.) ;

- La gestion de la génération et de la distribution de l'énergie :

  . Assure le contrôle et la gestion du système pour : moteur, turbine, générateur, batterie et autres sources d'énergie ;

- La gestion de la sécurité :

  . Les systèmes utilisés pour maintenir l'intégrité, la sûreté et/ou la sécurité du navire et sa cargaison (SMDSM (Système mondial de détresse et de sécurité en mer), AMVER (Sauvetage mutuel automatisé des navires), SSAS (Système d'alerte de sécurité des navires), NavTechnica (Système d'alerte de sécurité des navires), alarmes incendie...) ;

- La gestion des services auxiliaires :

  . Les systèmes qui sont en charge de l'alimentation en combustible, en air, en huile, de la production d'eau douce, du traitement des eaux grises et noires ou encore de la réfrigération des vivres ;

- La gestion de la navigation :

  . Les systèmes qui sont soient directement destinés, soit fournis en soutien à la navigation du navire (Système de navigation et de visualisation des cartes électroniques (ECDIS), GPS et gyrocompas du navire, radar de marine, échosondeur, AIS, enregistreur de données de voyage (VDR)...) ;

- La gestion des systèmes d'accès :

  . Un système d'accès pour les passagers ou l'équipage est tout système auquel ils peuvent accéder ou s'interfacer directement avec le système. Cela inclut les systèmes qui donnent accès à des services multimédias tels que des films ou de la musique et les systèmes qui permettent de se connecter à l'Internet.

Nous nous concentrons dans cette section à la modélisation et l'analyse des services de navigation et de propulsion afin d'identifier et d'évaluer les évènements redoutés ainsi que les éléments amenant à leurs réalisations (encadré en rouge dans la figure IV.3). À travers la méthode MoRiA et conformément à son processus d'utilisation décrit dans les chapitres II et III, section II.3.3 et III.4.4 les architectes système commencent par définir et modéliser les grandes fonctionnalités du système sous le nom de capacités opérationnelles (Figure IV.4). À cela les équipes sécurité et les architectes système discutent des métriques à utiliser ainsi que leur différent niveau de notation, ici l'objectif et de pouvoir établir rapidement à travers

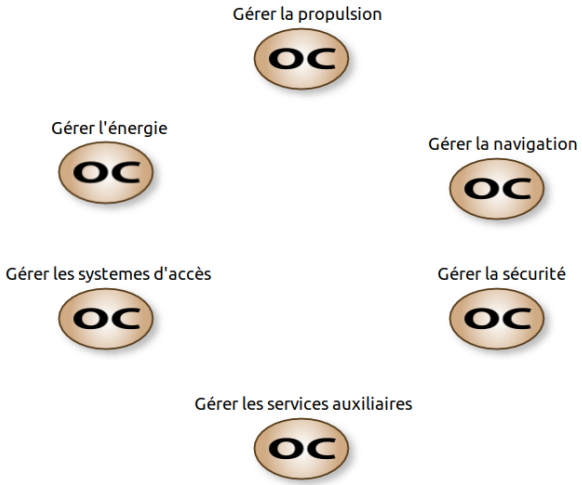


FIGURE IV.4: Définition des capacités opérationnelles par les architectes systèmes

cela les types d'évènements redoutés vraisemblables dans le cadre de notre étude. Nous avons choisi dans notre cas les matrices D.I.C.T génériques présentées précédemment (Figure II.6).

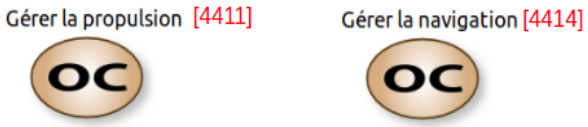


FIGURE IV.5: Définition du besoin de sécurité des capacités opérationnelles par les architectes système et sécurité

À travers ces échanges les équipes déterminent que la capacité de propulsion [4411] doit absolument rester disponible, son niveau d'intégrité est critique, les informations utilisées sont internes et il n'y a pas de besoin spécifique de traçabilité des accès. Pour la capacité de navigation[4414] elle aussi doit rester absolument rester disponible, son niveau d'intégrité est critique, les informations utilisées sont interne et cependant un besoin d'exigence légale est nécessaire. Ces réflexions sont par la suite exprimées et modélisées par les équipes sécurité à travers des évènements redoutés dits de haut niveau (figure IV.6) pour chaque besoin de sécurité estimé suffisamment important pour être traité. Pour le cas de la gestion de la propulsion, les équipes décident de garder le besoin de disponibilité et d'intégrité et pour la gestion de la navigation, ceux de disponibilité, d'intégrité et de traçabilité. Ces évènements redoutés de haut niveau ont par la suite été raffinés par les équipées d'ingénierie système ainsi que des intervenants du domaine s'appuyant sur des normes, exigences et réglementations du

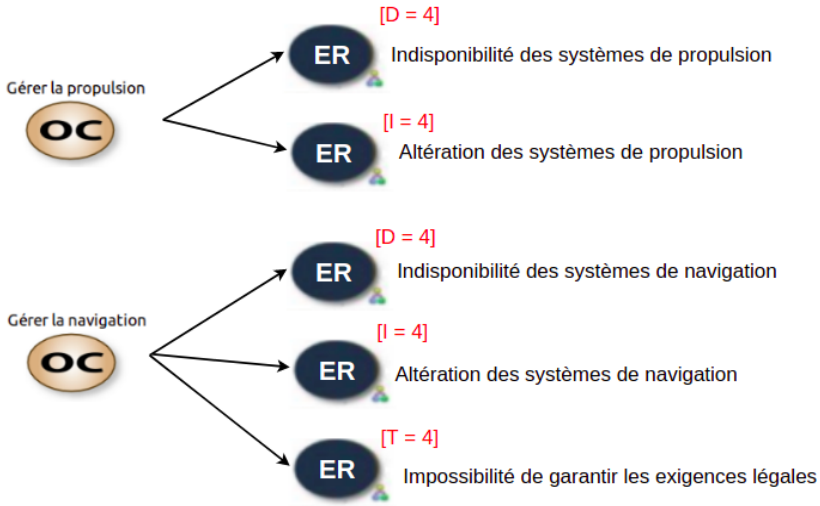


FIGURE IV.6: Définition des évènements redoutés de haut niveau par les architectes système et sécurité

domaine maritime tels que le BIMCO [NM10] et les exigences SOLAS [Sol02]. La figure IV.7 illustre les nouveaux évènements redoutés définis et rattachés à la capacité de propulsion.

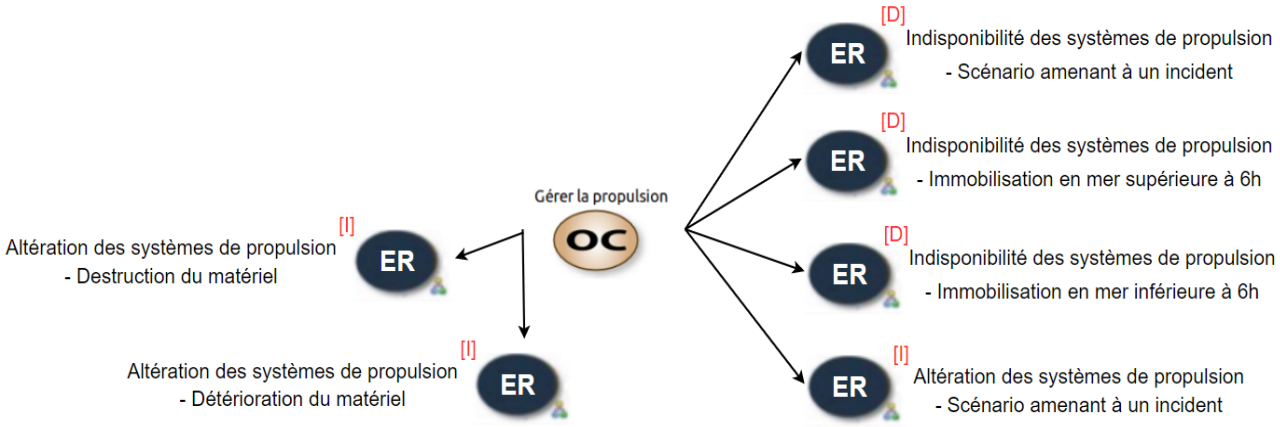


FIGURE IV.7: Enrichissement des évènements redoutés par les architectes système, sécurité et intervenants du domaine naval

Une fois cela fait, les différents intervenants de l'analyse (équipes du domaine naval, système, sécurité, service juridique ainsi que le client et les responsables) se rassemblent afin d'échanger et d'intervenir à travers la vue de synthèse suivante (Figure IV.8) afin de placer les évènements redoutés les uns par rapport aux autres en fonction de leur gravité/impact ainsi que des priorités de l'organisation.

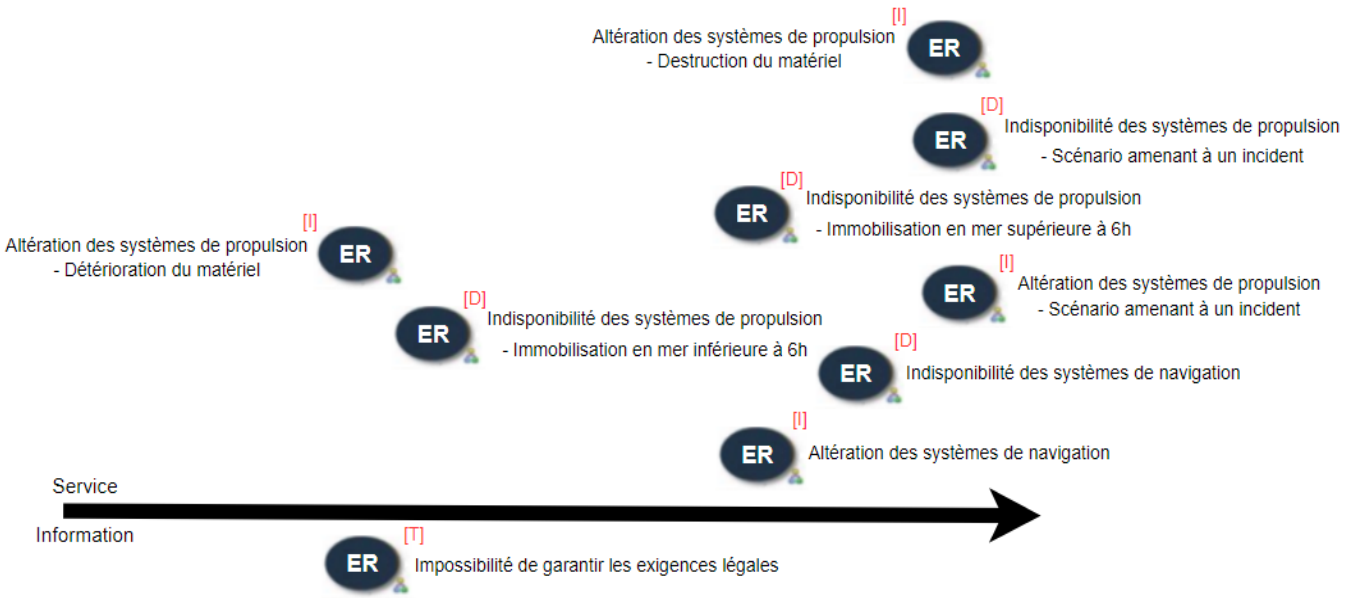


FIGURE IV.8: Classement des évènements redoutés par tous les acteurs de l'analyse

Par la suite, les équipes système et sécurité et du domaine naval établissent les profils de menaces et leurs objectifs visés. Les acteurs de la menace peuvent être classés dans l'une des sept catégories suivantes :

- les individus : l'intention peut être de voler ou de divulguer des informations sensibles, de saboter ou d'interrompre les opérations du navire, etc. L'ampleur des dommages qu'ils peuvent infliger dépend de leur rôle, des droits d'accès au système et de l'efficacité des mesures de cybersécurité liées aux systèmes et aux données du navire ;
- les groupes d'activistes : ces groupes sont constitués d'individus motivés par une idéologie. Leurs actions sont en fait des protestations en ligne, qui peuvent avoir pour but de perturber des systèmes ou d'acquérir des informations confidentielles ou sensibles pour les publier ou les diffuser afin d'embarrasser leur(s) cible(s). L'impact des petits groupes d'activistes peut être considérablement amplifié lorsque, comme certains groupes l'ont démontré, ils recrutent ou persuadent des tiers de les rejoindre en permettant par exemple l'installation de logiciels malveillants sur les ordinateurs ;
- les concurrents commerciaux : ce groupe est généralement constitué de grandes entreprises qui cherchent à créer un avantage concurrentiel. Elles peuvent agir directement ou par l'intermédiaire de tiers, dans le but de nuire à un rival en recueillant des renseignements commerciaux, en volant la propriété intellectuelle, en recueillant des renseignements concurrentiels sur les appels d'offres ou en perturbant les opérations pour causer des pertes financières ou de réputation ;

- les cyber-criminels : Il s'agit de groupes criminels sophistiqués perpétrant un large éventail de crimes illégaux liés aux technologies de l'information. Leur motivation est de tirer profit d'activités illégales, et ils se concentrent principalement sur la fraude, les vols de comptes et le vol de propriété intellectuelle. Cependant, les activités cybercriminelles comprennent également le chantage et l'extorsion par l'utilisation de logiciels malveillants pour chiffrer les données ou les menaces d'attaques par déni de service sur les sites Web des entreprises ;
- les terroristes : Les terroristes sont de plus en plus sensibilisés aux technologies de l'information et font déjà un usage intensif de l'Internet pour diffuser leur propagande et communiquer. Les groupes bien financés pourraient profiter des services offerts par les cybercriminels, chercher le soutien d'un État-nation ou encourager leurs membres internes à adopter ces méthodes d'attaque. Les terroristes pourraient s'appuyer sur les diverses boîtes à outils disponibles au téléchargement pour perturber ou endommager les navires en attaquant les systèmes du navire et/ou les systèmes connectés à terre et peuvent également exploiter des données de navires mal sécurisées pour permettre la reconnaissance à distance de cibles par des groupes hostiles, réduisant ainsi le temps d'attente qu'ils doivent passer dans ou près de leur cible.
- les États-nations et les acteurs parrainés par des États : il est reconnu que certains États-nations participent activement à des cyber-attaques contre un large éventail d'organisations afin d'acquérir des secrets d'État, des informations commerciales sensibles ou des propriétés intellectuelles. Les acteurs de la menace parrainés par l'état ont effectivement la capacité et le soutien technique sophistiqué dont dispose un État-nation.

Ces profils de menace peuvent viser l'activité globale, le navire ou les sous-systèmes du navire et sont regroupés dans les catégories suivantes :

- Détruire : les exemples peuvent inclure la destruction d'une fonctionnalité, d'un système ou sous-système de sorte qu'ils ne puissent plus être utilisés.
- Dégrader : il peut s'agir, par exemple, d'avoir une incidence sur la vitesse ou la manœuvrabilité du navire, sur la capacité de naviguer avec précision ou de surveiller avec précision l'environnement local, au point de compromettre de manière significative la capacité du navire à fonctionner.
- Refuser : il peut s'agir, par exemple, de refuser l'accès aux systèmes ou aux informations/données du navire, éventuellement pour des raisons telles que l'extorsion à des fins de gain financier ou pour organiser une attaque physique sur le navire à des fins d'enlèvement et de rançon.

- Retarder : il peut s'agir, par exemple, de retarder l'exploitation en temps voulu du navire ou de ses sous-systèmes de telle sorte que l'effet d'entraînement puisse avoir une incidence sur les opérations commerciales ou entraîner des pénalités.
- Dissuader : il peut s'agir par exemple d'empêcher l'entreprise d'opérer dans certaines zones des océans du monde, d'opérer sur des marchés spécifiques ou d'accéder à certains ports spécifiques d'un point de vue commercial.
- Détecter : il peut s'agir, par exemple, de détecter l'emplacement de personnes, de cargaisons ou de navires et de les suivre de manière à ce qu'un vol physique ou une manipulation de cargaison planifiée puisse avoir lieu.
- Distraire : il peut s'agir, par exemple, de la capacité de modifier l'état d'un capteur afin de fournir une distraction pendant qu'une extraction de données ou d'informations a lieu.

Suite aux échanges entre les équipes, les profils de menaces/objectifs visés retenus sont les suivants (figure IV.9).

Sources de risque	Objectifs visés	Motivation	Ressources	Activité	Vraisemblance
Activistes	- la destruction des données - la publication de données sensibles - l'attention des médias - refus d'accès au service ou au système ciblé	+++	++	++	Moyenne
Criminels	- vendre des données volées - rançonner des données volées - le rançonnement de l'exploitabilité du système	++	+++	++	Haute
Opportunistes (passagers)	- percer les défenses de la cybersécurité	+	+	+	Faible
Employés mécontents	- la destruction des données - la publication de données sensibles - refus d'accès au service ou au système ciblé	+++	+++	+++	Haute

FIGURE IV.9: Liste et notation des sources de risques de l'étude

Après discutions, les sources de menace criminelles et les employés mécontents ont été identifiés comme les plus susceptibles de nuire au système en réalisant leurs objectifs visés. Subséquemment, les équipes systèmes et sécurité ont créé les couples de sources de risque et d'évènements redoutés les plus pertinents en fonction de la proximité des objectifs visés avec la réalisation des évènements redoutés afin d'identifier le couple le plus pertinent (figure IV.10). Les objectifs visés définis des activistes, employés mécontents, et criminels étant assez

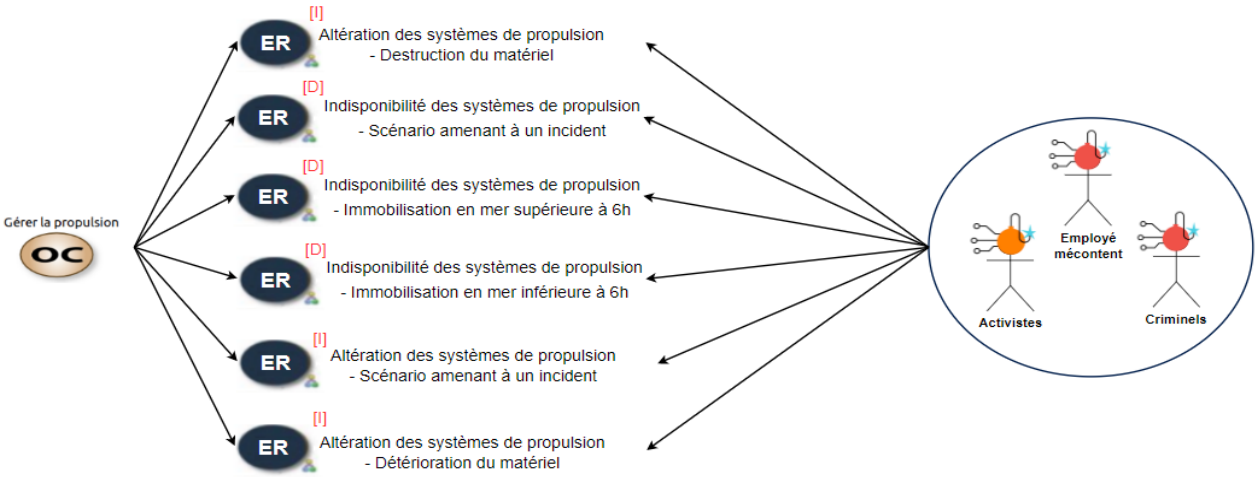


FIGURE IV.10: Définition des couples Évènement redouté/Source de risque

proches, il est naturel qu'ils soient à ce niveau couplés avec les mêmes évènements redoutés. C'est à travers la vue de synthèse suivante (figure IV.11) où la pertinence de ces différents couplages est véritablement définie et illustrée à travers les échanges entre analystes de sécurité, experts navals et architectes système.

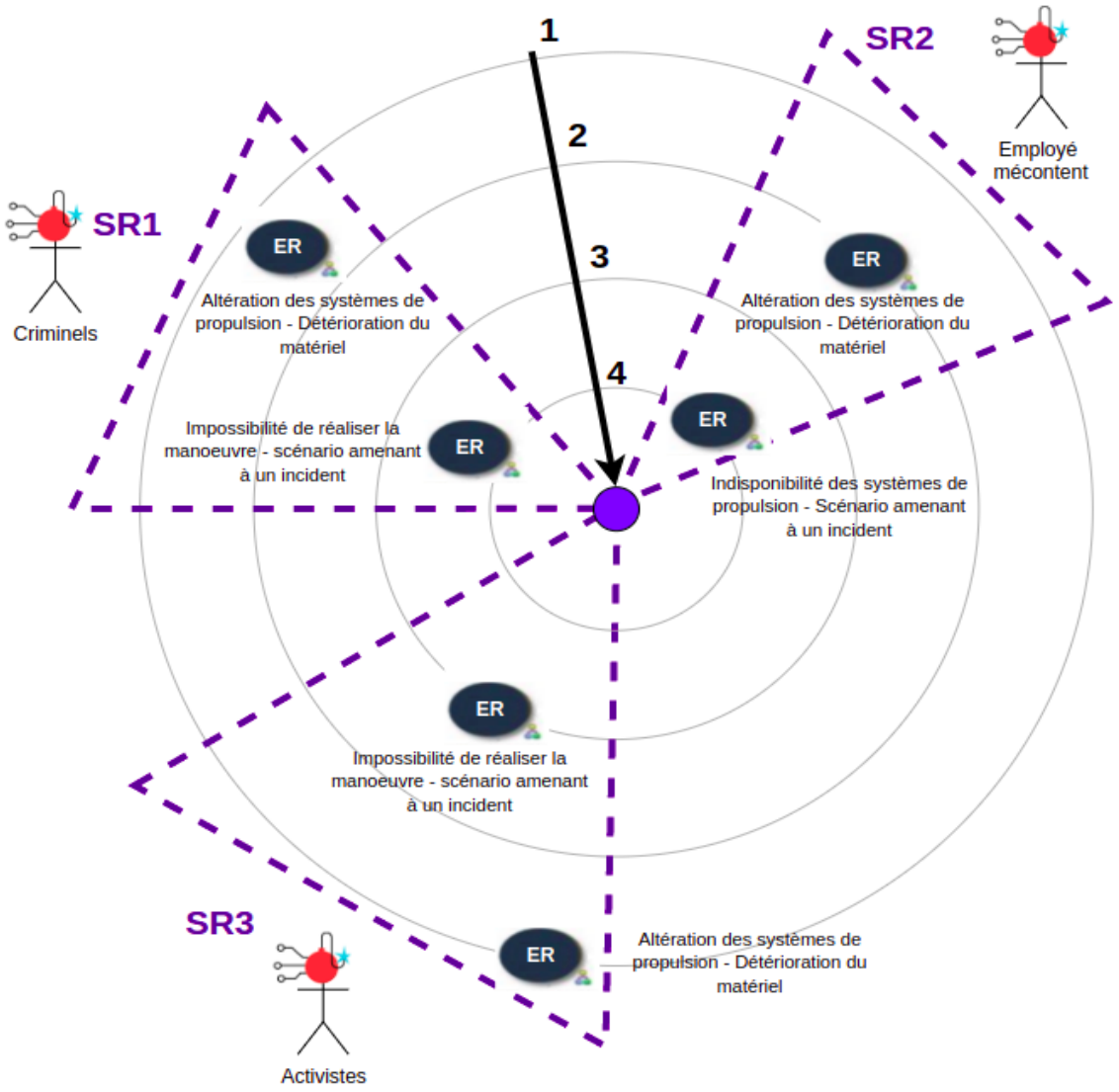


FIGURE IV.11: Vue de synthèse représentant la pertinence des couples

Par souci de clarté et de lisibilité, nous nous concentrerons sur la modélisation de l'événement redouté "indisponibilité des systèmes de propulsion - Scénario amenant à un incident" pour la suite de l'analyse.

Les équipes ayant classé l'événement redouté "indisponibilité des systèmes de propulsion - Scénario amenant à un incident" comme un des événements les plus graves (figure IV.8) et les sources de risque "criminels" et "employé mécontent" étant classées comme fortement vraisemblables, la pertinence de ces couples s'illustre par leur proximité avec le centre du radar. À l'opposé l'événement redouté "altération des systèmes de propulsion - détérioration du matériel" ayant été classé comme étant le moins grave, il a été placé plus au large du

radar. L'objectif de cette vue est de pouvoir illustrer les couples et les comparer, ici encore nous ne cherchons pas une valeur absolue de notation pour les couples, mais plutôt de les placer les uns par rapport aux autres en fonction de leur pertinence ainsi que des priorités de l'organisation.

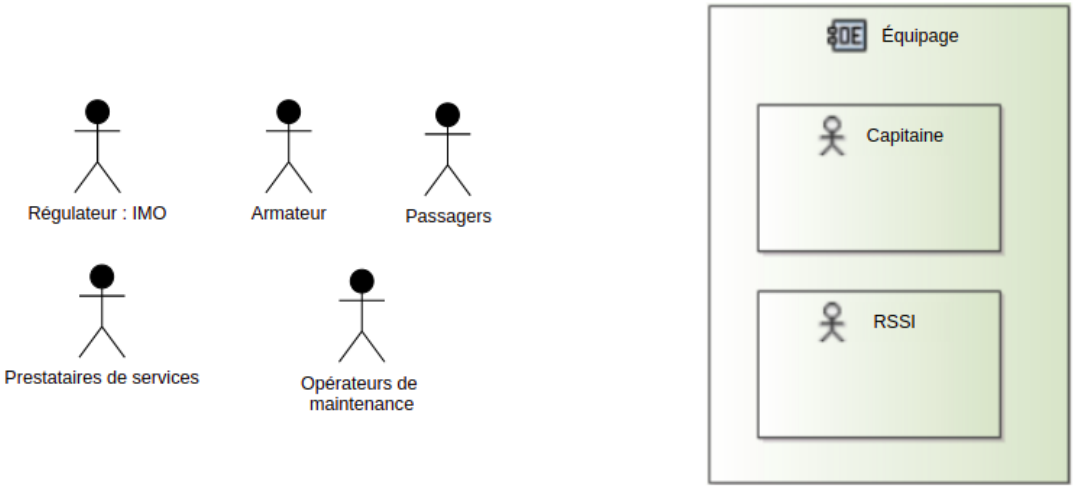
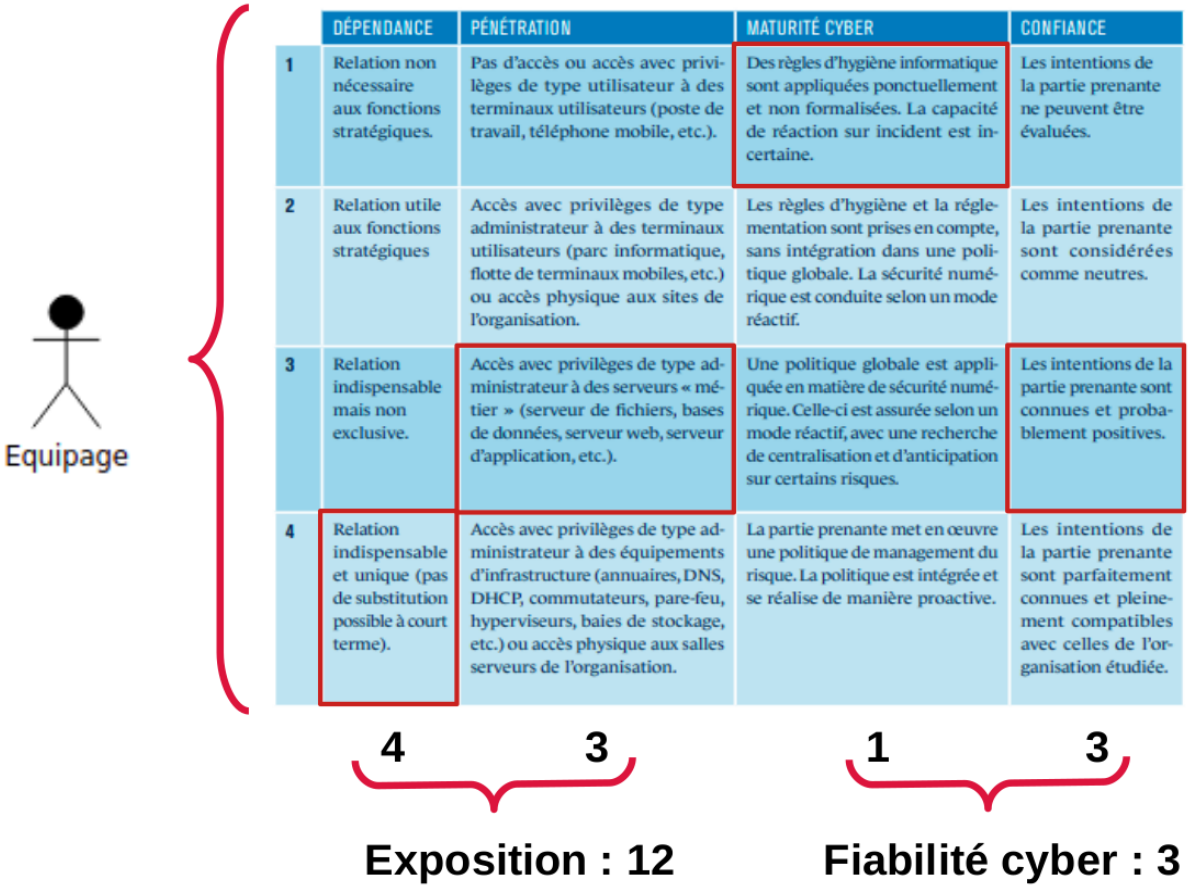


FIGURE IV.12: Modélisation des entités et acteurs du système

Par la suite les architectes et ingénieurs système modélisent les entités et acteurs (équipage, prestataire de service, opérateur de maintenance, passagers...) contribuant et nécessaires à la réalisation des capacités du système.



	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFIANCE
1	Relation non nécessaire aux fonctions stratégiques.	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2	Relation utile aux fonctions stratégiques	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3	Relation indispensable mais non exclusive.	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	Relation indispensable et unique (pas de substitution possible à court terme).	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisation.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

FIGURE IV.13: Notation des entités et acteur du système

Subséquemment, les équipes de sécurité, système et du domaine naval argumentent et définissent le niveau d'exposition et de fiabilité cyber de ces parties prenantes avec les métriques de l'ANSSI (figure II.10). Dans le cas de l'équipage, les équipes ont défini son niveau de dépendance comme indispensable et unique (niveau 4), comme ayant un niveau de pénétration assez élevé avec des accès avec privilèges de type administrateur à des systèmes et serveurs (niveau 3), comme ayant une maturité cyber non formalisée et incertaine (niveau 1) et un niveau de confiance assez haut (niveau 3). Cela donnant un niveau d'exposition (dépendance*pénétration) de 12 et un niveau de fiabilité (maturité*confiance) de 3.

FIGURE IV.14: vue de synthèse illustrant le niveau de menace des parties prenantes

L'objectif de cette vue est de pouvoir illustrer les parties prenantes et leur niveau de menace afin de pouvoir en discuter et les renoter si besoin. À travers la notation des parties prenantes, les équipes ont identifié 2 d'entre elles à surveiller. L'équipage et l'opérateur de maintenance ont tous deux été identifiés comme ayant un fort niveau d'exposition (supérieur à 9) et un faible niveau de fiabilité (inférieur à 3).

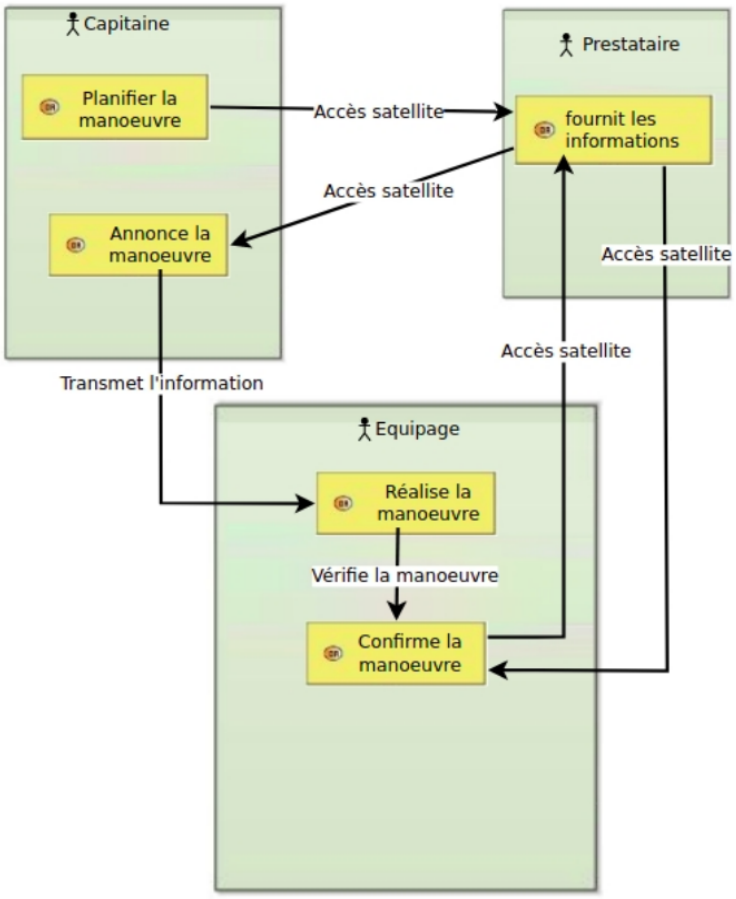


FIGURE IV.15: Modélisation des activités et interactions

Suite à cela les architectes et ingénieurs système modélisent les activités et interactions que devront réaliser les parties prenantes pour la réalisation des capacités. Notamment pour la capacité gérer la propulsion si nous voulons réaliser une manoeuvre les activités et interactions suivantes (figure IV.16) sont nécessaires.

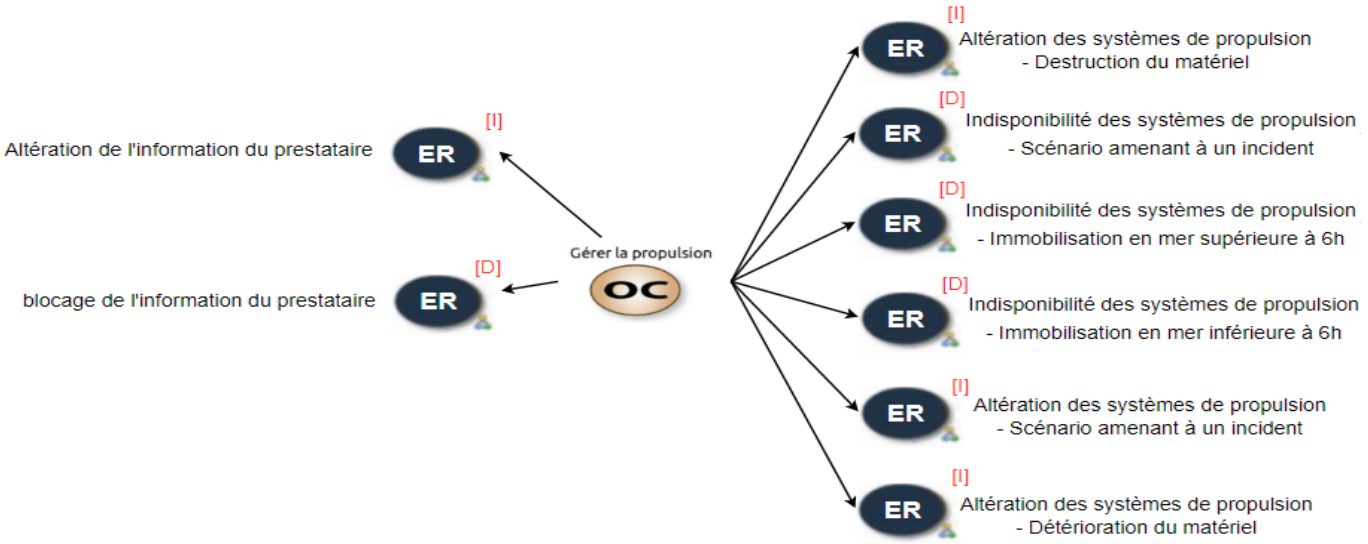


FIGURE IV.16: Enrichissement des évènements redoutés

Grâce à ces nouvelles informations les équipes, on a pu identifier à travers l'interaction "accès satellite" un besoin de sécurité menant à 2 nouveaux événements redoutés touchant l'intégrité et la disponibilité de cette interaction pour la réalisation de cette capacité.

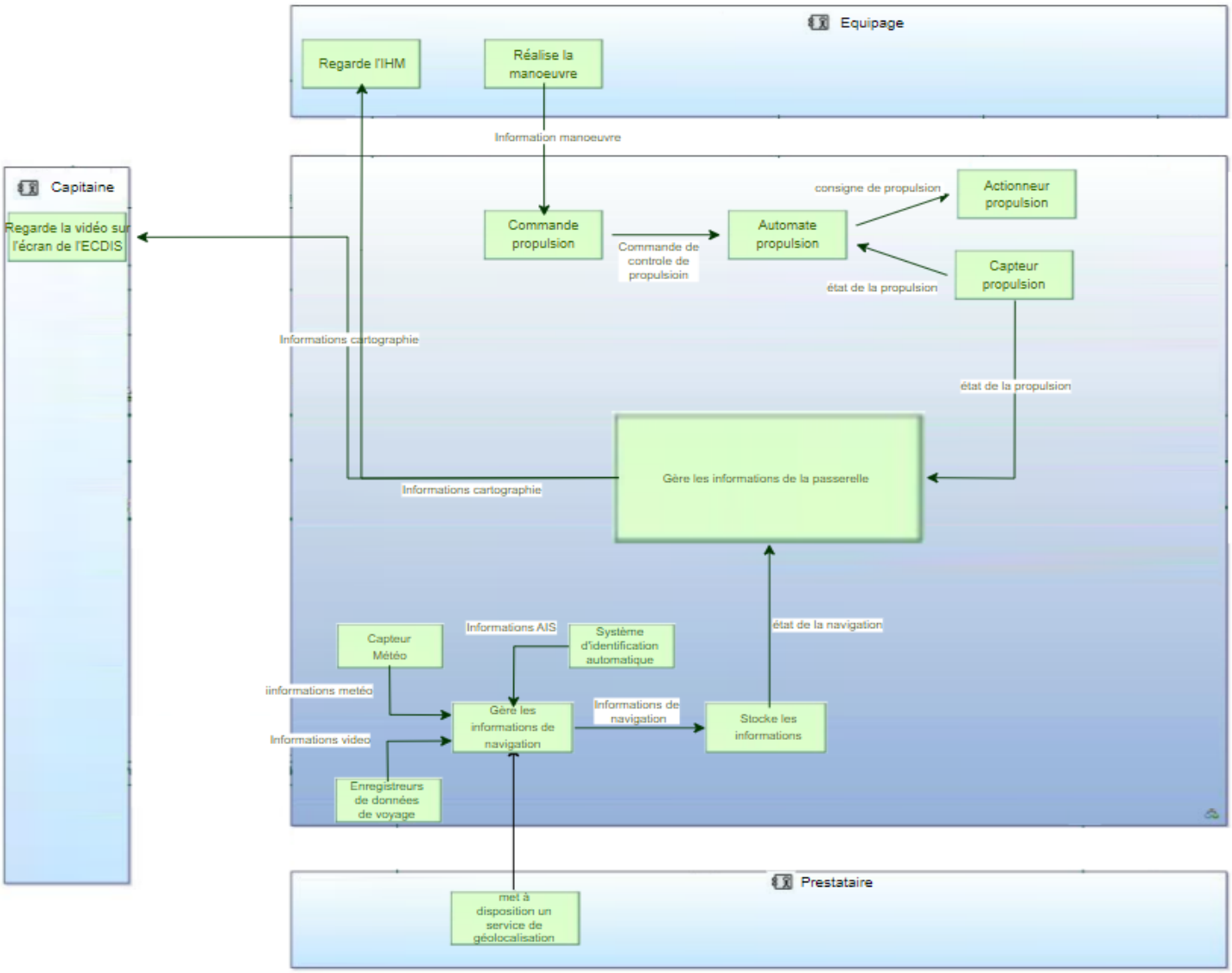


FIGURE IV.17: Transition de l'analyse opérationnelle à l'analyse système

Suite à cela, les équipes système réalisent la transition de l'analyse opérationnelle à l'analyse système, faisant ainsi émerger le système au centre des parties prenantes et en réassignant, en développant et précisant les activés à réaliser.

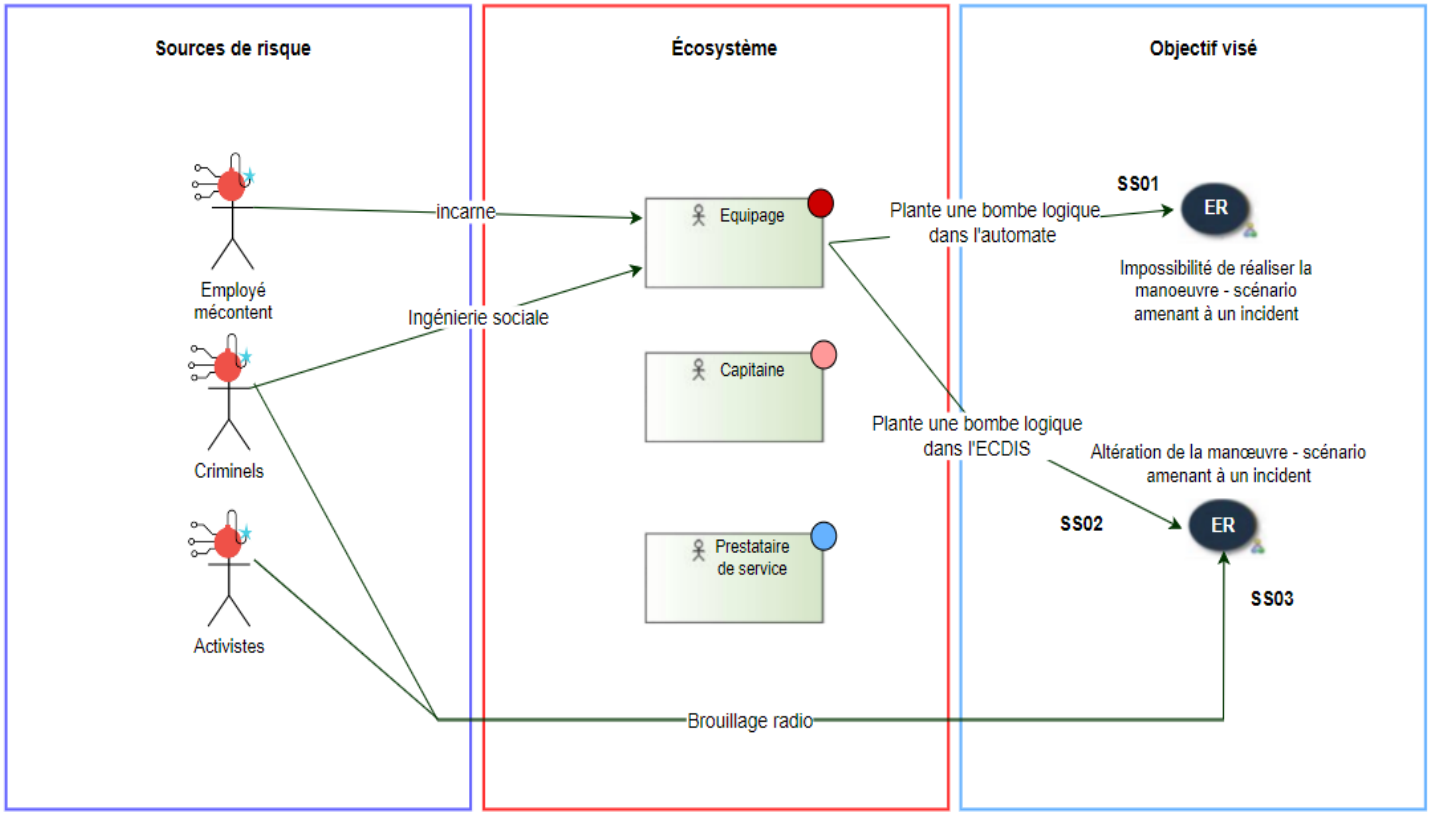


FIGURE IV.18: Définition des scénarios stratégiques

Subséquemment à cela les équipes sécurité et système définissent les scénarios stratégiques menant aux évènements redoutés. Un grand scénario stratégique concernant l'évènement redouté "indisponibilité des systèmes de propulsion - Scénario amenant à un incident" a été défini :

- **SS01 :** L'employé mécontent ou le criminel plante une bombe logique dans l'automate de propulsion en incarnant, corrompant ou réalisant du chantage à travers de l'ingénierie sociale sur l'équipage ;

Quant à l'évènement redouté "Altération de la propulsion - Scénario amenant à un incident", deux scénarios stratégiques ont été définis :

- **SS02 :** L'employé mécontent ou le criminel plante une bombe logique dans le système d'affichage (ECDIS) afin d'altérer ces informations en incarnant, corrompant ou réalisant du chantage à travers de l'ingénierie sociale sur l'équipage ;
- **SS03 :** L'activiste ou le criminel plante réalise un brouillage radio afin de perturber les capteurs du système afin d'altérer les informations d'affichage.

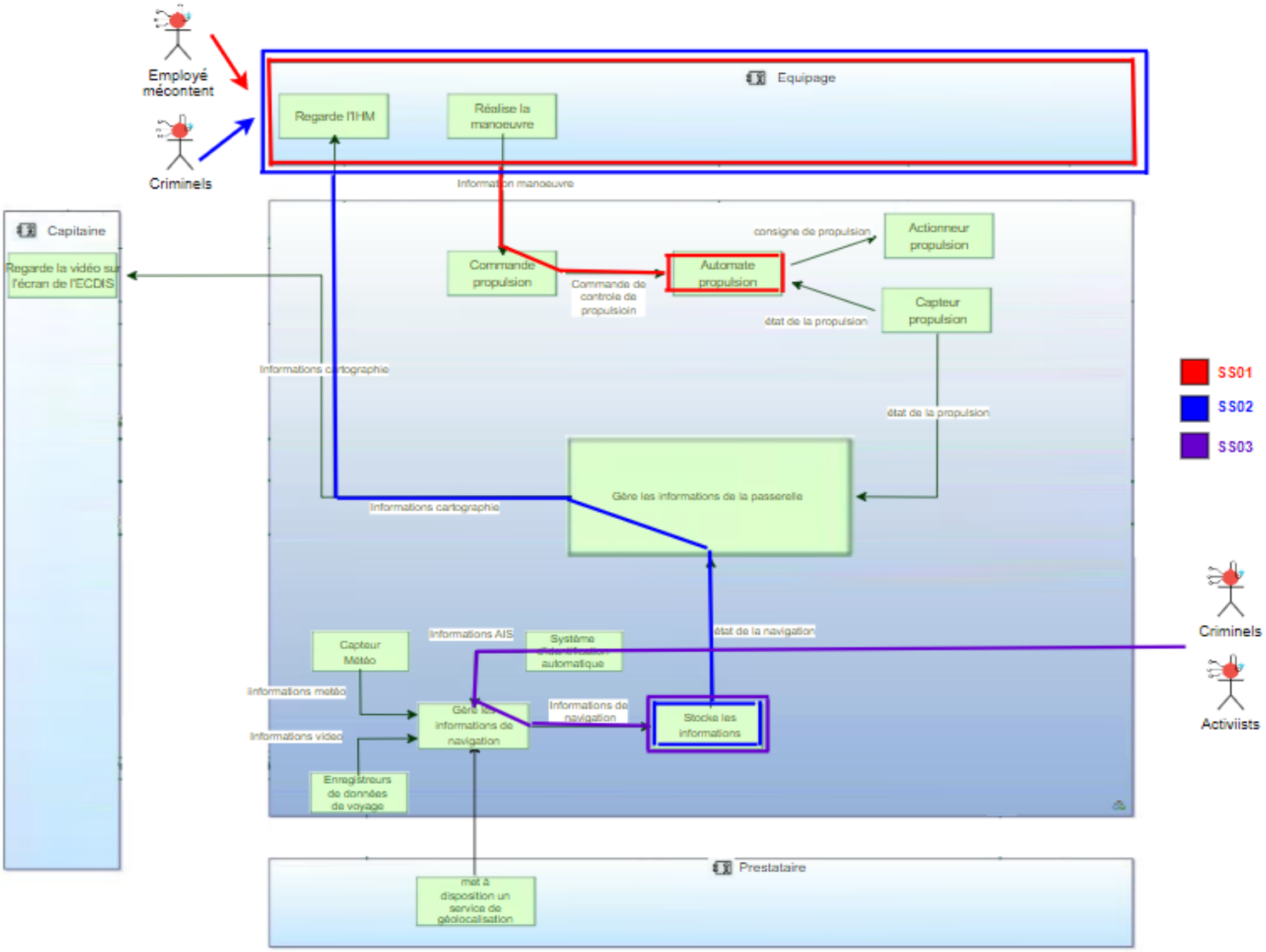
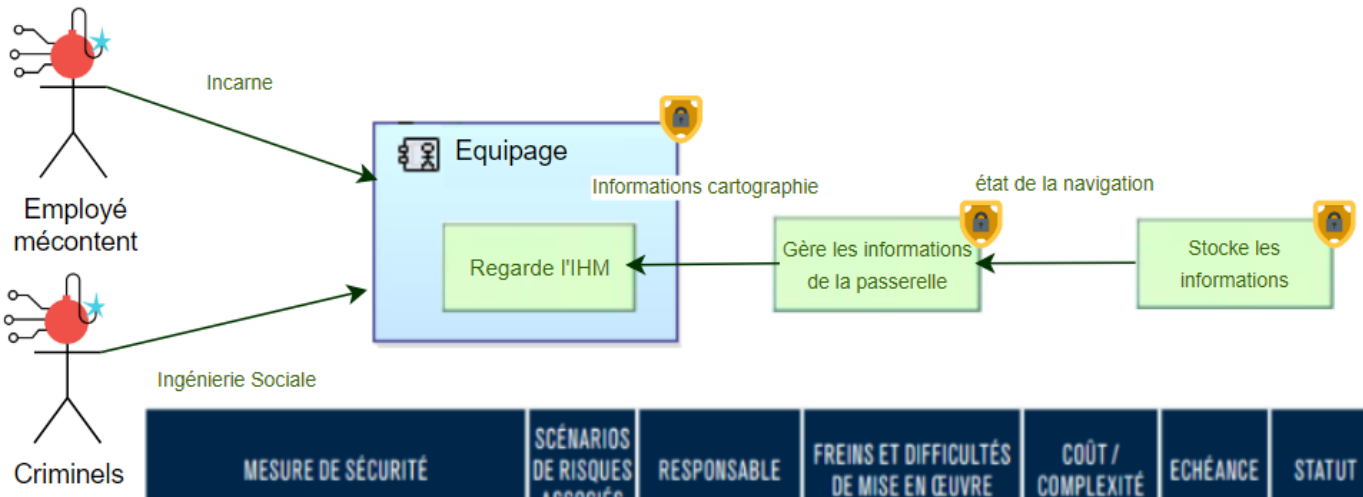


FIGURE IV.19: Modélisation des scénarios stratégiques dans l'architecture du système

Ces scénarios ont par la suite été modélisés dans l'architecture du système et ont permis aux équipes systèmes et sécurité d'identifier les chaînes fonctionnelles de réalisation des attaques ainsi que des premières mesures de sécurité à éliciter.



MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN ŒUVRE	COÛT / COMPLEXITÉ	ECHÉANCE	STATUT
GOUVERNANCE						
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	SS01, SS02	RSSI	Validation du CHSCT indispensable	+	6 mois	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	SS01, SS02	RSSI		++	3 mois	À lancer
PROTECTION						
Renforcement du contrôle d'accès physique	SS01, SS02	Équipe sûreté		++	3 mois	Terminé

FIGURE IV.20: Identification de la chaîne fonctionnelle SS02 et élicitation des mesures de sécurité

Sur cette chaîne fonctionnelle liée au scénario stratégique SS02 les équipes sécurité ont identifié et proposé des mesures de sécurité à mettre en place. Plusieurs mesures ont été définies, une mesure dite de gouvernance sur l'équipage afin de le sensibiliser, une autre de gouvernance et consistant en un audit sur l'équipage et le système d'information et pour finir une mesure de protection et de contrôle d'accès sur l'élément de stockage d'information. À travers ces mesures, celles appliquées à l'équipage ont un impact direct sur l'analyse, elles nous permettent de recalculer son niveau de maturité cyber et de le repositionner dans l'analyse des niveaux de menace des parties prenantes (figure IV.14).

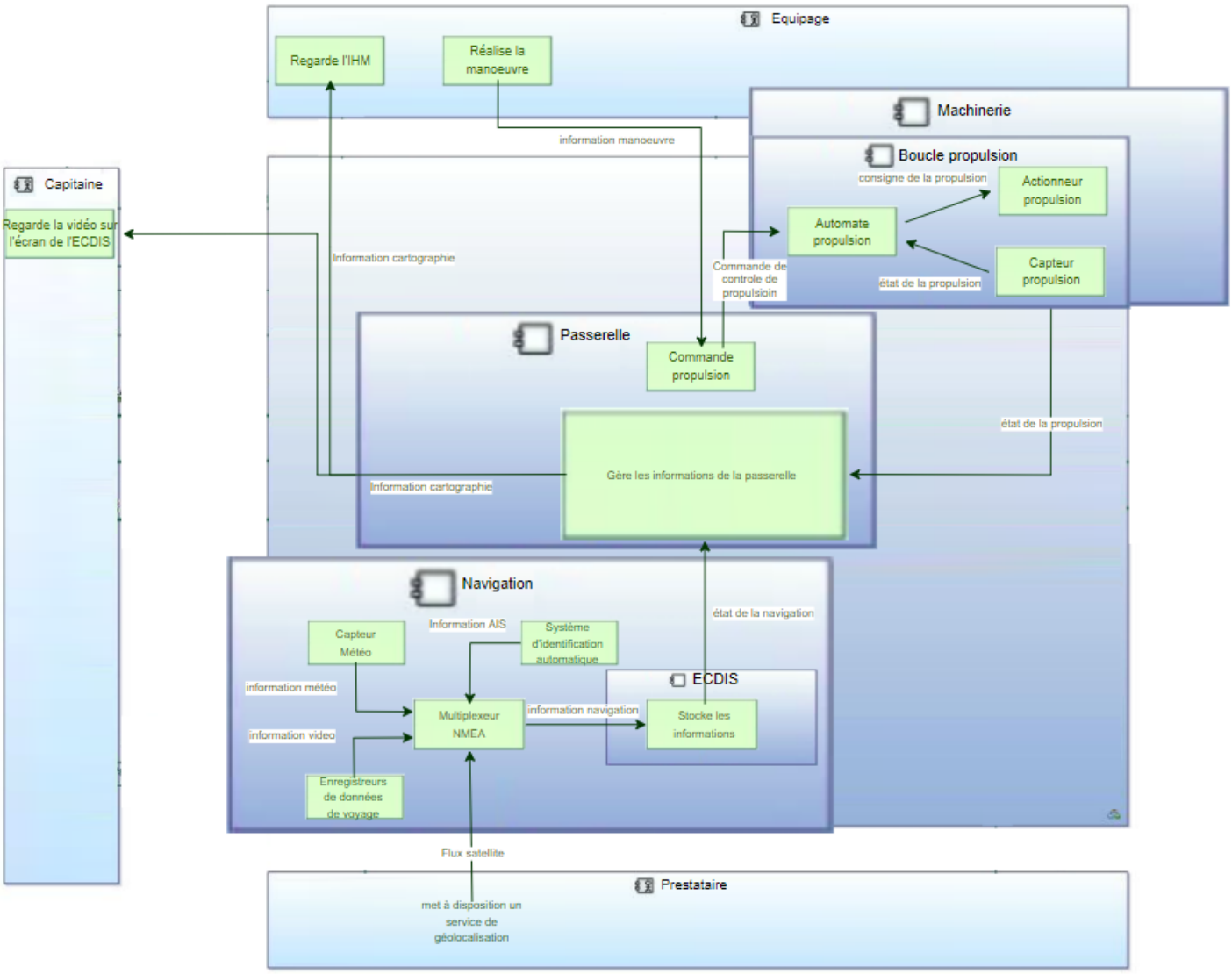


FIGURE IV.21: Transition de l'analyse système à l'architecture physique

Suite à cela, les équipes d'ingénierie système, réalisent la transition de l'analyse système à l'architecture logique et modélise les blocs de système logique suivant : Navigation, ECDIS, Passerelle, Machinerie et Boucle de propulsion. Les équipes sécurité en collaboration avec les équipes systèmes ont par la suite co-ingénieré les cyber kill chains associées aux scénarios stratégiques.

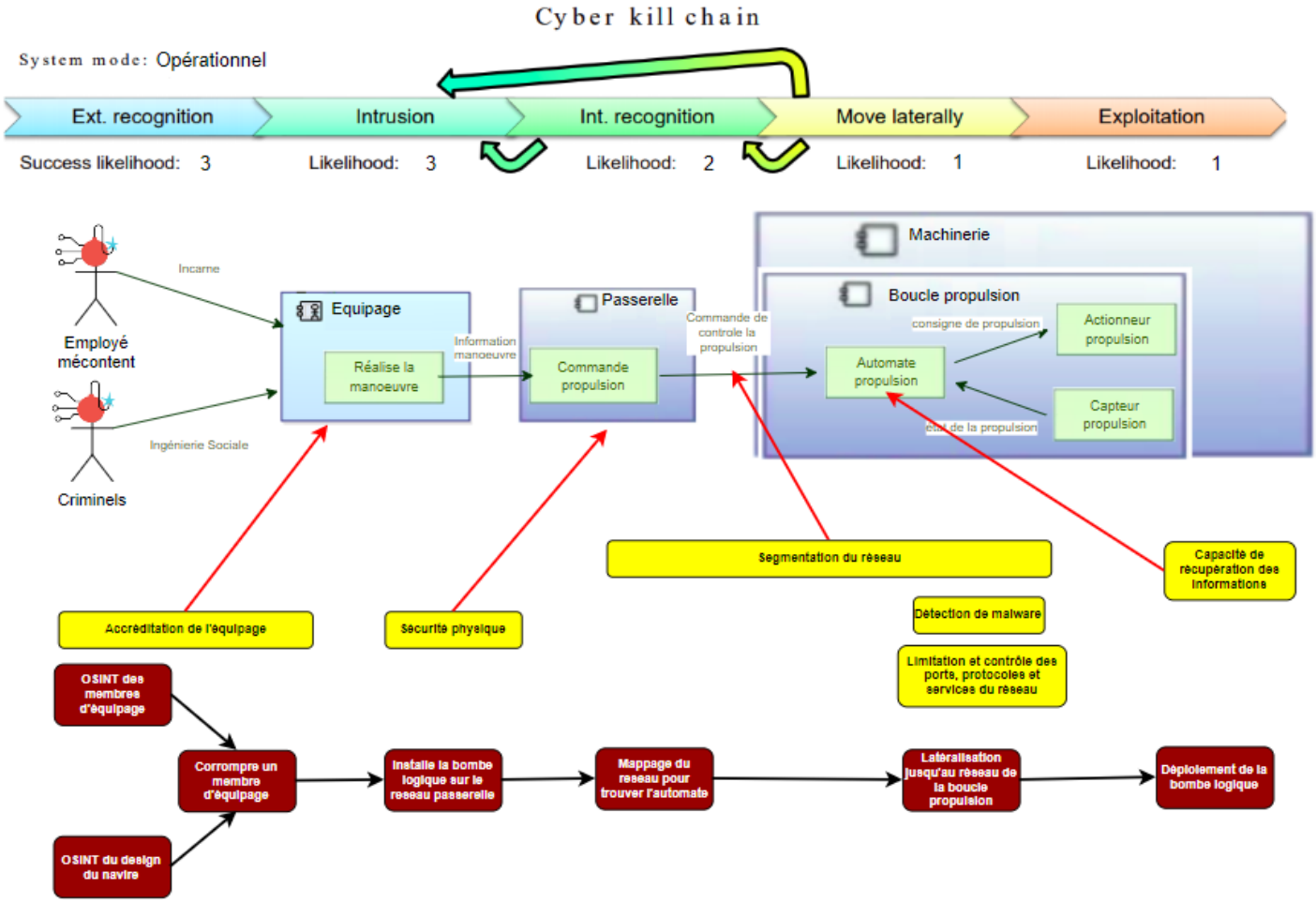


FIGURE IV.22: Définition de la cyber kill chain associée au scénario stratégique SS01

Pour le cas du scénario stratégique SS01, les équipes ont défini la cyber kill chain suivante :

- **Phase de reconnaissance extérieure :** Réalisation d'OSINT sur les membres d'équipage ainsi que sur le design du navire afin d'identifier et de corrompre un membre d'équipage ;
- **Phase d'intrusion :** Installation de la bombe logique sur le réseau passerelle ;
- **Phase de reconnaissance interne :** Mappage du réseau pour trouver le réseau des automates ;
- **Phase de latéralisation :** Latéralisation jusqu'au réseau de la boucle propulsion ;
- **Phase d'exploitation :** déploiement de la bombe logique ;

Suite à cette cyber kill chain les équipes on pu co-identifier et co-définir les mesures et exigences de sécurité à mettre en oeuvre dans le système notamment en se réfèrent à la

chaîne fonctionnelle du scénario.

IV.4 Discussion des résultats de l'utilisation de MoRiA pour la modélisation et l'analyse de risque du système naval

Les résultats de l'utilisation de notre méthode sur le cas d'étude de la plateforme navale ont été comparés avec les résultats d'une analyse de risque standard d'EBIOS RM réalisée sur cette même plateforme par les industriels à travers le projet Foresight [PNG21].

L'application de MoRiA implémentée avec EBIOS RM et Arcadia, a permis aux équipes systèmes et sécurité d'identifier des la première perspective les éléments structurels et fonctionnels du système nécessitant réellement un besoin de sécurité. Les grandes capacités du système identifiées à travers notre méthode sont donc identiques à celle de l'analyse standard cependant la précision et la réalisabilité de nos événements redoutés sont plus avancées et sont directement rattachées aux éléments concrets de modélisation.

Les diagrammes et éléments les composant ont permis une représentation et une traçabilité fonctionnelle claire des évènements redoutés ce qui a permis une meilleure compréhension et de meilleurs échanges lors des discussions sur les attaques possibles, les menaces et leur réalisation. Les équipes sécurité, ont notamment permis à travers l'expertise des équipes système à limiter l'explosion combinatoire des actifs à protéger ainsi que des événements redoutés réels pertinents en agrégeant les questionnements de sécurité similaire afin de concentrer les efforts d'analyse.

À travers ces efforts d'analyse, nous sommes arrivés sur les grands scénarios opérationnels de menace. La représentation des scénarios opérationnels sous forme de cyber kill chain a permis aux équipes de proposer de nombreuses actions élémentaires réalisables par l'attaquant ce qui a enrichi la pertinence et factualité des scénarios étudiés. Cette représentation a permis aux équipes d'identifier, éliciter clairement les mesures de sécurité en les rattachant aux éléments de modèles correspondants, ce qui n'est pas le cas dans l'approche standard de la méthode EBIOS RM. En supplément, l'apport des équipes systèmes et des modèles a permis l'identification, les éléments de modèles similaires et nécessitant les mêmes exigences de sécurité et a permis ainsi de tracer et reproduire les mesures et exigences de sécurité sur les éléments de modèles similaires ou identiques. La prise en compte

du contexte et de l'état du système à permis à travers l'expertise métier et sécurité de définir des profils de sécurité adaptée permettant ainsi des compromis d'architecture, de mesures de sécurité et de fonctionnalités.

IV.4.1 Limites du cas d'étude

Notre méthode MoRiA abordant la modélisation d'une analyse de sécurité complète à travers les modèles et les différentes perspectives est une méthode innovante, car il n'existe qu'un nombre très limité d'études, récemment publiées entre 2019 et 2021, qui abordent des défis similaires (voir section I.1.1).

En appliquant notre méthode MoRiA (langage MoRiAML et processus d'utilisation), sur l'étude de cas de la plateforme navale, nous avons montré l'opérabilité de la méthode et son potentiel pour répondre à nos questions de recherche. Cependant, il est impératif de mentionner que notre étude de cas présente certaines limites liées aux questions de validité. Tout d'abord, les données de l'étude de cas ont été recueillies lors de plusieurs réunions avec un nombre réduit de spécialistes. Nous n'avons pas discuté des détails profonds avec des experts spécifiques des divers systèmes constitutifs de la plateforme ainsi que les parties prenantes interagissant avec la plateforme. Cette étude de cas a été réalisée sur une durée de trois mois dans le cadre de ce doctorat, par conséquent, en raison des contraintes de temps et comme mentionné précédemment dans ce chapitre nous avons limité, simplifié le cas d'étude ainsi que ses résultats et réflexions pour qu'il ne ne reflète pas la situation opérationnelle des systèmes navals utilisés dans l'industrie.

Par conséquent, un travail supplémentaire devrait être mené pour assurer l'évolutivité de notre méthode MoRiA. Dans le même contexte, un travail supplémentaire est nécessaire pour étudier la capacité de MoRiA à passer à l'échelle en l'appliquant à des études de cas plus importantes avec des scénarios plus complexes. De plus, une analyse approfondie de la facilité d'utilisation de notre méthode MoRiA devrait être réalisée pour garantir sa facilité d'utilisation. Enfin, l'étude de cas et ses résultats ont été validés avec nos collaborateurs industriels système et les équipes plateforme, mais elle n'a pas été confrontée à des experts en sécurité. Par conséquent, l'évaluation de MoRiA doit être renforcée en validant les résultats avec des experts en sécurité. Cependant, l'étude de cas a été menée selon un protocole méthodique, qui a permis de capturer des informations importantes, y compris ses limitations, et qui a permis et permettra l'amélioration de notre méthode MoRiA.

IV.5 Conclusion

Dans ce chapitre, nous avons décrit en détail comment nous avons appliqué la méthode MoRiA lors de la définition et modélisation du système, en suivant son processus d'utilisation et sur l'étude de cas de la plateforme navale.

L'utilisation de MoRiA et de son processus d'utilisation a montré leur capacité à étudier, analyser et délimiter l'analyse. Permettant ainsi une analyse fidèle au système conçu et cohérent avec les préoccupations fonctionnelles des équipes système.

Les résultats de l'analyse montrent que les techniciens de maintenance ainsi que l'équipage sont les éléments pivots, point d'entrée de la majorité des scénarios identifiés et définis. La prise en compte de ces éléments des la phase de définition et modélisation du système permet de planifier et d'établir les exigences et mesures de sécurité à mettre en place pour réduire la vraisemblance de ces dits scénarios. Ainsi cela permet dès cette phase précoce de développement d'économiser des coûts et du temps de développement et de réduire les impacts et les dommages résiduels.

Pour l'étude de cas de la plateforme navale, l'équipe MoRiA a suggéré des exigences possibles pour améliorer la sécurité du système. Les collaborateurs industriels ainsi que l'équipe plateforme ont estimé que les résultats obtenus sont précieux et que la méthode MoRiA est très intéressante pour la modélisation et l'analyse sécurisée de systèmes.

Chapitre V

Conclusion générale et perspectives

Sommaire

V.1 Conclusion générale

Le paysage de la cyber-sécurité est en constante évolution et de nouvelles menaces apparaissent chaque jour, notamment une plus grande variété d'acteurs étatiques qui lancent des attaques à des fins politiques, stratégiques et économiques. À mesure que notre infrastructure numérique devient de plus en plus connectée et que nous commençons à compter davantage sur l'autonomie, la cybersécurité devient de plus en plus un principe majeur de la sécurité des systèmes.

D'ici 2035, la cybersécurité sera une perspective aussi fondamentale dans la conception des systèmes que le sont aujourd'hui la performance et la sûreté des systèmes [CD21]. La discipline de l'ingénierie des systèmes deviendra encore plus interdisciplinaire, intégrant l'expertise cybernétique dans l'équipe afin de garantir que la cybernétique est prise en compte tout au long du cycle de vie du système.

En outre, les outils de modélisation et de simulation permettant de tester et d'évaluer les aspects de cyber-sécurité du système seront de plus en plus répandus, ce qui donnera une image globale de la sécurité du système qui, trop souvent, n'est prise en compte que tardive-

ment dans le cycle de vie du développement. La conception de la cybersécurité s'étendra au-delà des composants du système pour inclure l'analyse de la chaîne d'approvisionnement,des pièces d'origine et de son écosystème afin d'éliminer tout point faible du système.

V.1.1 Objectifs réalisés et contributions

Dans cette thèse, nous avons abordé les défis de modélisation et de réalisation de l'analyse de risque dans l'ingénierie système, en nous basant sur les normes les constituant.

Nous avons proposé une méthode appelée MoRiA : **Mo**del-based Cyber **Ri**sk **A**nalysis pour surmonter ces défis dès les premières phases et perspectives d'ingénierie, afin d'identifier et d'évaluer la gravité des événements redoutés et leur impact, de modéliser les menaces, de réduire les coûts et les risques globaux du projet, et de permettre des compromis entre les préoccupations de cybersécurité et d'autres préoccupations fonctionnelles et non fonctionnelles. Nous avons suivi les lignes directrices de l'ingénierie dirigée par les modèles (IDM) pour développer notre méthode MoRiA, qui comprend un langage de modélisation, un outil de modélisation correspondant ainsi que leur processus d'utilisation décrivant comment le langage et son outil doivent être utilisés. Après avoir défini la méthode MoRiA, nous l'avons implémenté, en tant qu'extension de la méthode industrielle d'analyse de risque EBIOS RM et la méthode industrielle d'ingénierie système ARCADIA. Pour illustrer la méthode que nous proposons en termes de modélisation et de processus d'analyse amenant à une architecture sécurisée, nous avons mené une étude de cas sur une plateforme de simulation navale.

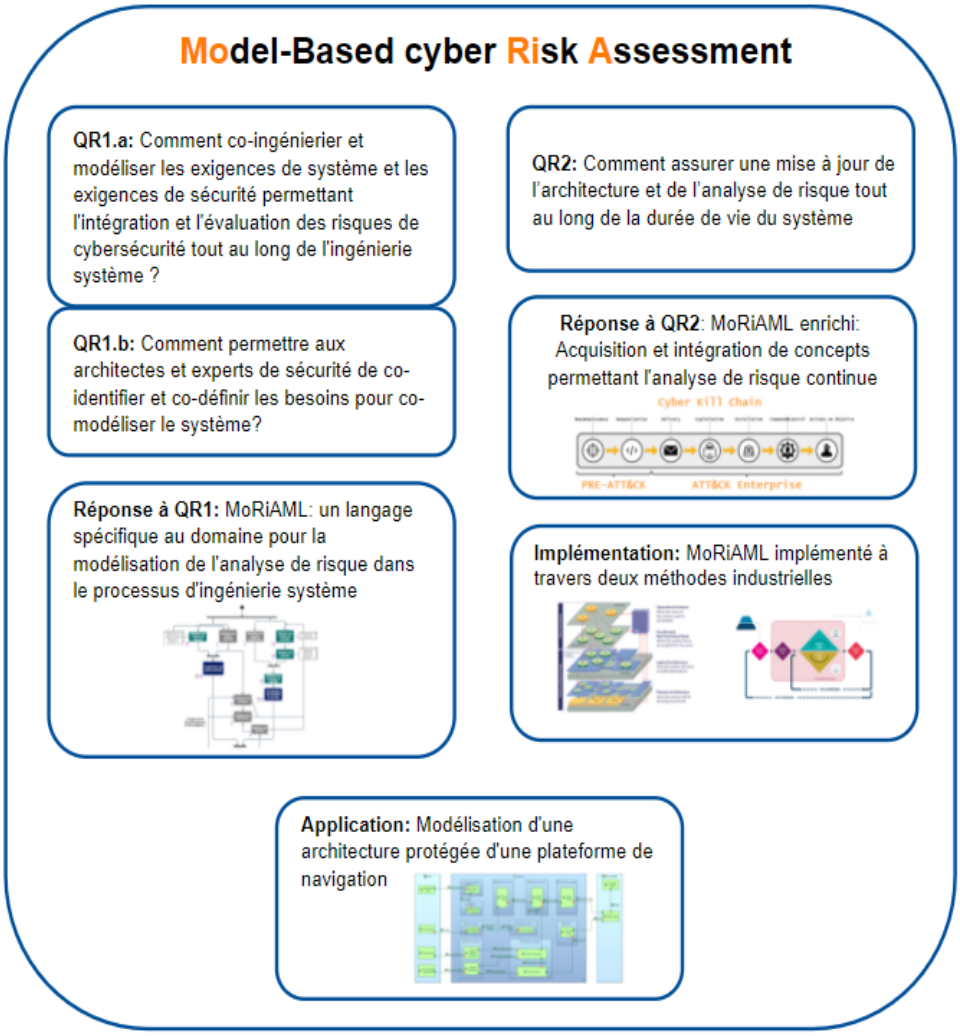


FIGURE V.1: Méthode MoRiA pour l'analyse et la modélisation de système sécurisé

Contributions à la modélisation de MoRiA :

Plus particulièrement, dans la partie modélisation des exigences de système et sécurité, pour répondre à notre première question de recherche QR1 "Comment co-ingénierier et modéliser les exigences de système et les exigences de sécurité permettant l'intégration et l'évaluation des risques de cybersécurité tout au long de l'ingénierie système" nous avons proposé un langage spécifique au domaine (DSL) appelé MoRiAML (MoRiA Modeling Language).

MoRiAML, étend le métamodèle de l'ingénierie système fonctionnelle issue des normes 15288 et 1220 tel que les concepts d'objectifs opérationnels, d'activités, d'interactions et de scénarios avec les concepts et des relations de sécurité de la famille des normes 27000 telles

que les actifs, les menaces, contrôle de sécurité et les incidents de sécurité. Ce métamodèle a été implémenté à travers deux méthodes industrielles ARCADIA et son outil Capella ainsi qu'EBIOS RM. Les extensions sont implémentées sous forme de profil en utilisant les mécanismes et les outils MDE. MoRiA a de nombreux points forts :

- Son langage est construit à partir des concepts de sécurité et de l'ingénierie système fonctionnelle issus de normes du domaine et permet l'implémentation du métamodèle à travers toutes méthodes elles aussi issues de ces mêmes normes ;
- Son langage et processus permet de guider les équipes d'architectures système et d'architectures cybersécurité dans leur démarche intellectuelle d'analyse afin d'assurer la cohérence à la fois de l'analyse de risque et de la définition et de l'architecture du système.
- Son langage réutilise les éléments de SysML qui est, d'après les études des travaux connexes, le langage le plus adapté et le plus activement utilisé et/ou étendu pour modéliser l'architecture de système ;
- MoRiA permet une analyse de risque et une modélisation de l'architecture sécurisée qui tient compte des préoccupations des équipes métiers, comme suit :
  - MoRiA permet le discernement et la compréhension des détails structurels et fonctionnels du système supportant ainsi une identification plus pertinente des éléments à protéger ainsi que des vulnérabilités et scénarios de menace ;
  - MoRiA permet de guider les équipes de cybersécurité dans leur démarche intellectuelle d'analyse ainsi que d'assurer la cohérence entre la vision des architectes système et les réflexions et résultats de l'analyse à travers son alignement sémantique, sa syntaxe et son processus d'utilisation ;
  - MoRiA permet une compréhension plus fine du système à travers à travers son analyse dans les modèles et cela à travers différentes perspectives/points de vue et sert de support de communication et d'échanges entre les équipes métiers et sécurité.
  - MoRiA propose des vues de synthèse ayant pour objectifs de regrouper le travail réalisé afin de brainstormer entre équipes techniques et communiquer, argumenter sur l'avancement et les choix à faire avec les équipes non techniques.
  - MoRiA couvre partiellement le développement évolutif puisqu'il s'inscrit dans la démarche d'ingénierie système sous plusieurs perspectives et de façon itérative ce

qui permet l'analyse de risque sous différents niveaux de précision et à chaque ajout, modification ou suppression dans le système.

- DSML extensible, portable et personnalisable du fait qu'il est développé en utilisant des mécanismes IDM (méta-modélisation, profil et mécanismes de transformation semi-automatiques) ;

Nous avons implémenté MoRiA, à travers deux méthodes industrielles implémentant les concepts issus des normes de notre modèle : ARCADIA et son outil Capella pour les concepts d'ingénierie des systèmes industriels et EBIOS RM et les concepts d'analyse des risques. Ces travaux ont été enrichis et validés à travers de nombreuses itérations avec nos collaborateurs industriels. Avec MoRiAML, il est possible d'implémenter l'éditeur graphique Capella basé sur Eclipse et open source. Nous pouvons bénéficier des mécanismes de transformation de MDE pour générer automatiquement notre outil offrant ainsi un outil avec les forces suivantes :

- Un outil qui étend l'outil open source Capella basé sur Eclipse, activement utilisé par la communauté du génie logiciel et correctement documenté et maintenu par Thales ;
- Non seulement un outil à base de modèles adapté au domaine spécifique l'ingénierie système sécurisée, mais aussi un outil personnalisable, réutilisable et extensible qui pourrait être adapté à d'autres domaines de modélisation connexes pour répondre aux besoins des architectes en étendant ou en filtrant la palette existante ou en intégrant des plug-ins Eclipse nouveaux/existants ;

Contributions à la continuité de l'analyse

En ce qui concerne la partie mise à jour de l'analyse dans le temps, pour répondre à notre deuxième question de recherche QR2 "Comment assurer une mise à jour de l'architecture et de l'analyse de risque tout au long de la durée de vie du système", la méthode MoRiA que nous proposons englobe une extension et une représentation de l'analyse des scénarios de menaces à travers la cyber kill chain ainsi que la prise en compte du contexte/comportement attendu et/ou subi amenant ainsi à des profils de sécurité contextuels créés, raffinés continuellement et itérativement dans le processus de définition du système. Cette proposition présente de nombreux points forts :

- Une vue permettant de regrouper tous les éléments d'analyse à travers un scénario de type cyber kill chain pour intégrer les préoccupations de chacun dans la réflexion de

l'attaque et des mesures et exigences de sécurité à mettre en place, soutenant ainsi la découverte précoce et l'anticipation de problèmes de sécurité imprévus (inconnus et connus) qui doivent être corrigés avant de modéliser les modèles d'architecture. Ce travail permet ainsi la production d'un Plan d'Amélioration Continue de la Sécurité (PACS) suivi et raffiné à travers les différentes perspectives d'ingénierie ;

- Une prise en compte du contexte/comportement attendu et/ou subi dans l'analyse permettant ainsi de définir en fonction de différents profils de sécurité. Ces différents profils nous permettent de réévaluer la vraisemblance et pertinence de la menace ainsi que l'impact et la faisabilité des incidents de sécurité en fonction du contexte d'utilisation choisi ou subi. Cela permettant aux équipes participant à l'analyse de produire des profils de sécurité contextuels et adaptés aux besoins de sécurité ainsi qu'aux besoins fonctionnels en fonction du contexte d'utilisation du système ainsi que de l'état de ces services ;
- Une méthode itérative permettant un lien entre les activités de modélisation d'analyse pour modifier/ajuster les exigences et besoins de sécurité afin de suivre un processus de ré-analyse jusqu'à atteindre un niveau de sécurité acceptable. En conséquence, notre processus MoRiA permet la prise en compte des préoccupations des équipes système et sécurité amenant à des compromis ainsi que la découverte de séquences de mauvaise utilisation ou de possibles vulnérabilités résultantes d'un évènement redouté.

En outre, nous avons défini un processus d'utilisation pour structurer et guider l'utilisation de MoRiAML. Le principal avantage de ce processus est de guider les architectes systèmes et les analystes de sécurité, à utiliser le langage et les outils MoRiA pour co-modéliser et co-analyser les risques, communiquer et justifier les choix ainsi que de produire une architecture sécurisée. Le processus décrit étape par étape, les acteurs et les ateliers nécessaires pour chaque activité de modélisation et d'analyse. Nous avons suivi ce processus d'utilisation pour modéliser un système industriel comme présenté dans le paragraphe suivant. De plus, nous avons mené une étude de cas sur un système industriel de plateforme navale. Nous avons suivi le processus MoRiA pour appliquer le DSML, les outils et le processus d'utilisation de MoRiA sur l'étude de cas. Nous avons modélisé les aspects fonctionnels du système, ainsi que les concepts de sécurité nécessaires à la réalisation d'une analyse de risque. Les résultats montrent :

- La capacité du langage proposé à modéliser un système à travers les quatre perspectives d'ingénierie permet dès les premiers éléments et réflexions fonctionnels de modélisation d'identifier et de tracer les actifs de façon plus précise et effective permettant ainsi une meilleure définition et appréhension des évènements redoutés, des points critiques ainsi

que des chemins d'attaques probables dans le système. De plus le langage permet de regrouper les travaux d'analyse à travers des vues de synthèse permettant aux acteurs métier d'échanger et de justifier les choix et résultats avec les équipes non métier ;

- La représentation sous forme de cyber kill chain permet aux différents acteurs de participer à la réflexion sur la vraisemblance et réalisation des différentes étapes d'attaques ainsi que des mesures de sécurité à mettre en place en fonction du contexte.
- La prise en compte du contexte permet d'ajuster les besoins de sécurité et la pertinence, impact de la menace en fonction du contexte d'utilisation du système et de l'état de ses services.
- La probabilité accrue d'adoption par d'autres utilisateurs, étant donné que le langage et l'outil sont accompagnés de documents d'orientation et de description des activités, montrant leur utilisation prévue.

Ces résultats ont été approuvés par nos collaborateurs industriels qui ont trouvé les résultats obtenus intéressants et la méthode MoRiA avantageuse quant à son utilisation comme support de collaboration et d'analyse de système industriel.

Comme on peut le constater, les contributions proposées ont plusieurs points forts, et répondent aux objectifs de cette thèse en répondant aux questions de recherche définies. Cependant, il est impératif de mentionner que notre méthode présente certaines limites qui pourraient être améliorées comme discuté dans la section suivante.

V.1.2 Perspectives

Sur la base de notre travail, nous présentons dans cette section de nombreuses perspectives et un certain nombre d'orientations futures possibles qui permettraient de faire progresser notre recherche. Certaines de ces perspectives sont motivées par des travaux en cours et des questions que notre étude a soulevées. Les autres sont définies dans l'intention d'étendre notre méthode MoRiA pour répondre à divers défis de modélisation et d'analyse.

Étendre la méthode MoRiA pour la prise en compte d'autres domaines non fonctionnels dans l'ingénierie système ou son outillage :

Dans ce travail, nous nous sommes focalisés sur l'intégration de la sécurité dans l'ingénierie système, sans prendre en compte dans les éléments de modèles les préoccupations de sûreté, performances et autres exigences non fonctionnelles. En ce qui concerne la sûreté,

même si les objectifs sont différents, l'approche de la détermination des risques se ressemble beaucoup. Il serait intéressant d'aligner les concepts de MoRiA avec ceux de la sûreté telle que la norme CEI 61508 afin d'identifier les éléments similaires, voire superposables, afin d'intégrer ces préoccupations et points de vue dans les différents ateliers et réflexions/choix d'architectures. Il est peut-être utile par la suite d'intégrer ces réflexions dans les documents d'homologation de sûreté telle que les Analyses des Modes de Défaillance, de leurs Effets, et de leur Criticité (AMDEC).

De plus, certaines extensions pourraient être envisagées pour renforcer l'analyse de risque dans l'ingénierie système :

1. Par l'accès à des bases de connaissances de scores, profils de menaces, vulnérabilités, et mesures de sécurité telle que ceux utilisés par les outils d'analyse de risque industriels : ALL4TEC - Cyber Architect [1], EGERIE-SOFTWARE [2], Risk'n Tic [3] afin d'automatiser et tenir à jour les éléments de sécurité ;
2. En utilisant les transformations de modèle afin de convertir les analyses et résultats de MoRiA en un format d'échange de données type XML ou JSON afin de les traiter et de les raffiner avec des outils d'analyse de risque industriels avant de les réintégrer dans l'outil d'ingénierie système basé sur les modèles ;
3. En raffinant l'analyse à travers la construction et sélection d'indicateurs plus aptes à servir les modèles et représentations à travers des métriques dites de "performance sécurité" afin d'approfondir les notions de sécurité et d'indicateurs en ne visant pas à servir une quête de conformité avec des modèles théoriques prédéfinis, mais plutôt à aider à analyser la réalité de ses pratiques et de ses représentations concernant la sécurité.

De manière cohérente, nous avons l'intention de mettre à jour les outils de modélisation et d'analyse pour répondre aux extensions de la méthode MoRiA. De plus, nous avons l'intention d'appliquer la méthode MoRiA (processus, langage de modélisation et outils) à plusieurs domaines d'application afin d'étudier sa facilité d'utilisation, son exhaustivité et de la valider par des architectes de système et de sécurité de l'industrie, ainsi que par des étudiants novices.

Enfin, il existe encore de nombreux défis et questions ouvertes à l'ingénierie des systèmes

1. https://www.all4tec.com/en/cyber-architect-en/
2. https://egerie-software.com/en/egerie-risk-manager/
3. https://www.riskntic.com/en/

qui doivent être abordés avant que celle-ci ne réalise tout son potentiel. Nous espérons que les contributions de cette thèse et les travaux futurs envisagés constituent un pas de plus dans cette direction.

Chapitre VI Annexes

Planning complet

L'étude de cas a été réalisée sur une période de 3 mois. Dans ce qui suit, nous décrivons le processus détaillé que nous avons suivi, par rapport aux étapes précédentes du protocole, pour réaliser notre étude de cas du système naval. Nous décrivons les acteurs/équipes et leurs rôles, ainsi que les différentes entrées et sorties de l'étude de cas en ce qui concerne les réunions et les échanges entre les équipes.

1. Lors de la première réunion VI.1, l'équipe MoRia a présenté la méthode MoRia (le langage, les processus) et a discuté avec l'équipe Thales et plateforme de la manière dont la méthode pourrait être utile pour la définition et la modélisation de l'analyse de risque dans l'architecture de la plateforme en tant que système naval. La réunion s'est terminée par une liste de questions de recherche auxquelles il faut répondre ;

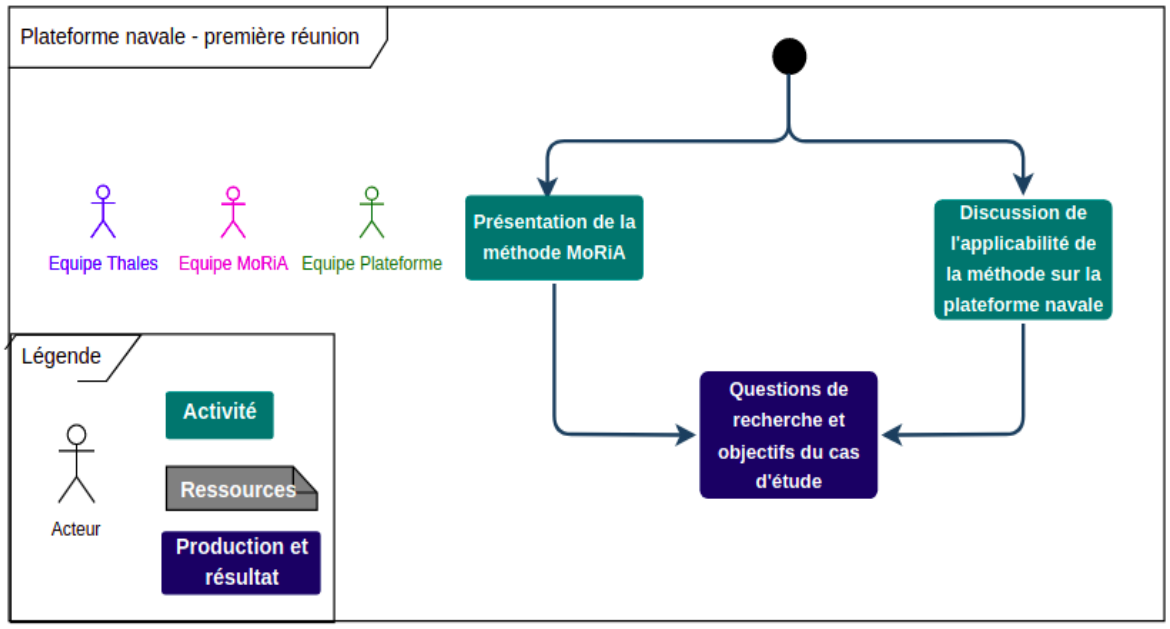


FIGURE VI.1: Protocole de planification - Première réunion

2. Lors d'une deuxième réunion VI.2, les deux équipes ont discuté plus en détail des objectifs globaux, du contexte et parties prenantes du système naval. Sur la base de ces informations et des directives de l'organisation maritime internationale (OMI), l'équipe MoRiA a proposé une définition de la perspective opérationnelle du système avec la méthode MoRiA. Cette perspective a été raffinée plusieurs fois, suite au retour de l'équipe Thales, jusqu'à la validation de celle-ci tant sur l'aspect modèle que sur les résultats de l'analyse de risque obtenus.

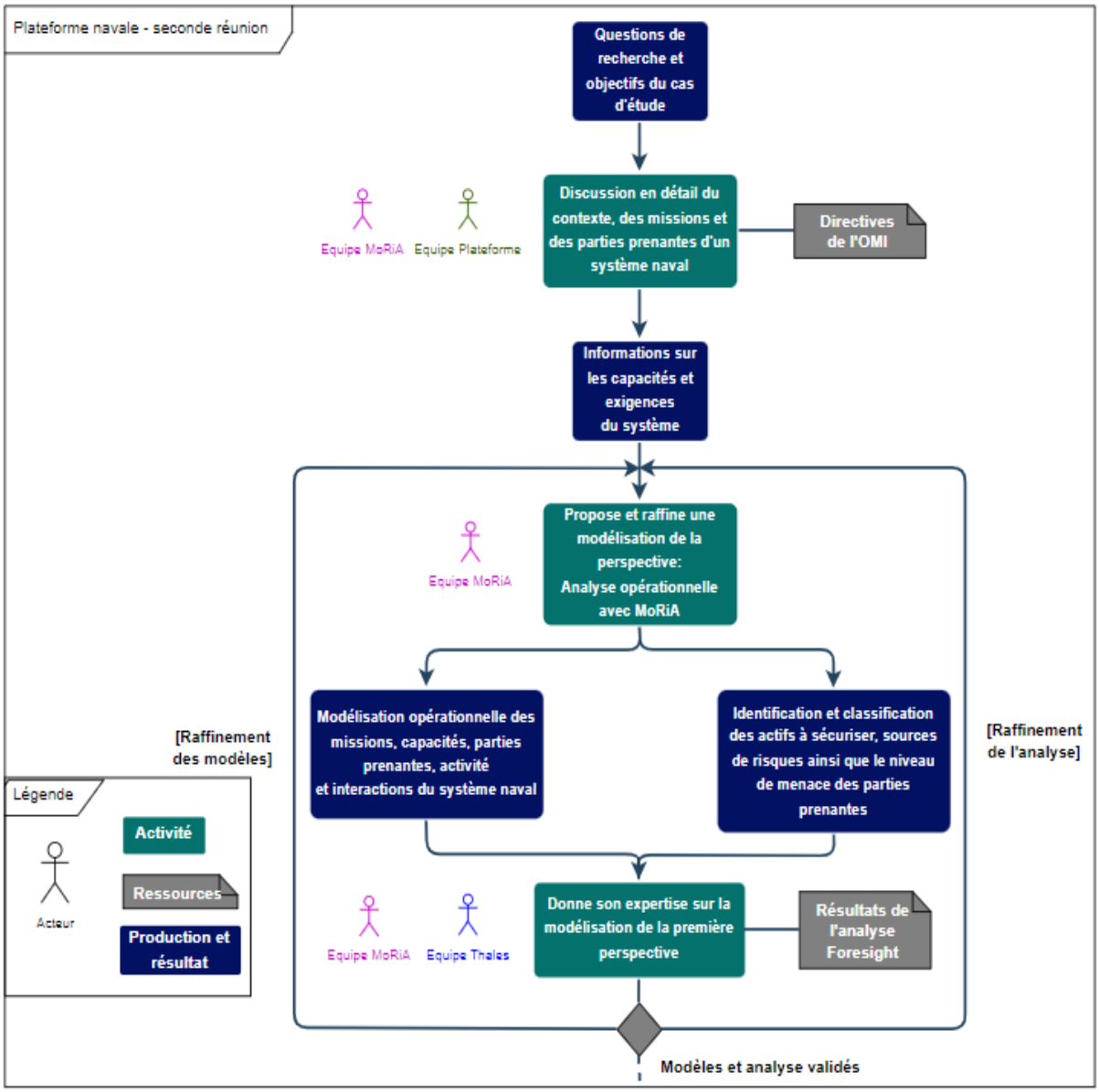


FIGURE VI.2: Protocole de planification - seconde réunion

Ayant la première perspective d'ingénierie, l'équipe MoRia modélise la seconde perspective (analyse système) amenant un raffinement des modèles et de l'analyse. Suite à cela les premiers scénarios stratégiques sont définis ainsi que les premières exigences de sécurité. Ensuite, l'équipe MoRia a présenté ses résultats et en discute avec l'équipe Thales lors de leur troisième réunion (figure VI.3). Plusieurs retours d'information et raffinements ont eu lieu jusqu'à ce que les scénarios stratégiques, les exigences et leurs détails soient validés ;

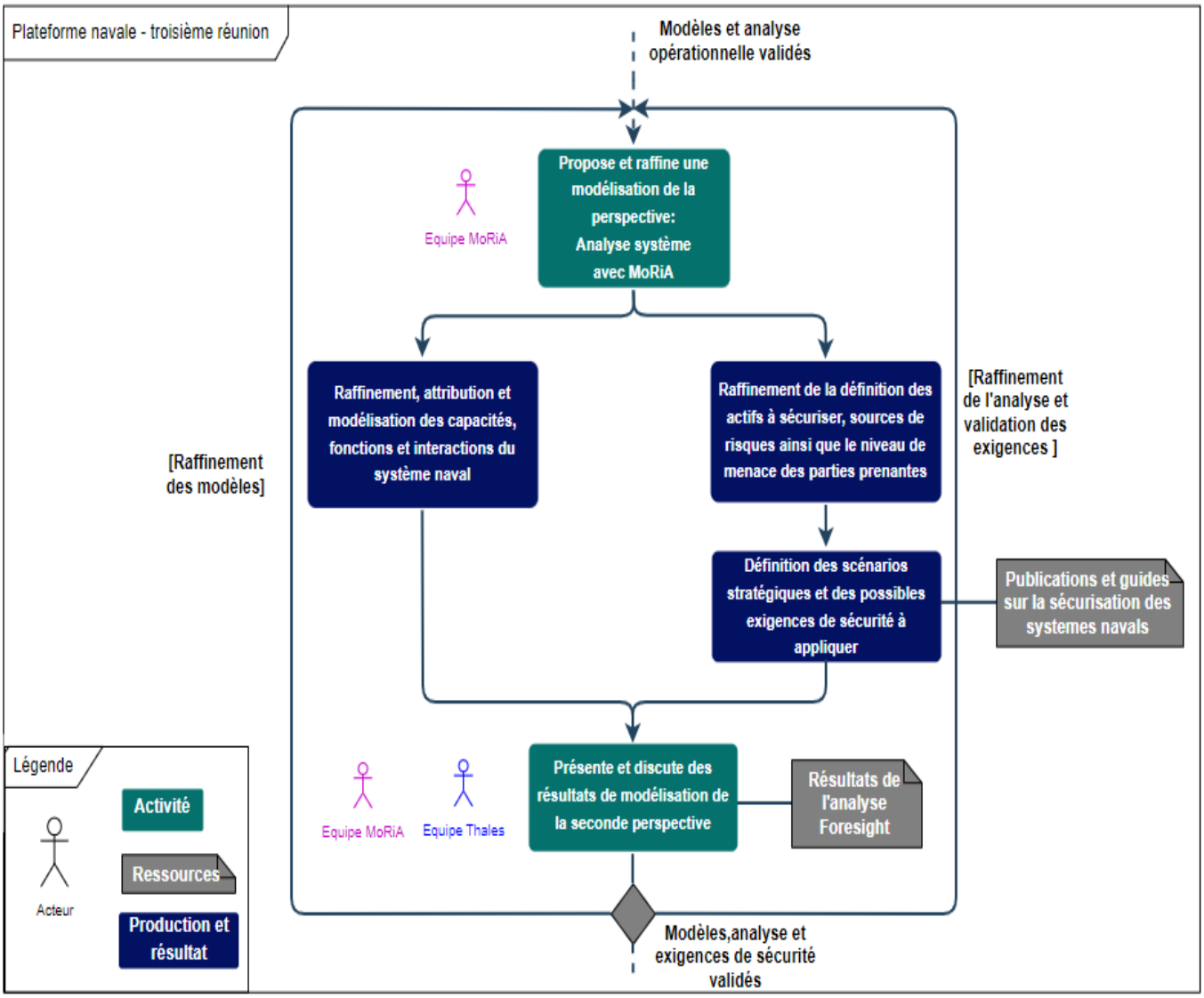


FIGURE VI.3: Protocole de planification - troisième réunion

Suite à la seconde perspective d'ingénierie, l'équipe MoRia applique les exigences de sécurité à travers des choix d'architecture amenant un raffinement des modèles. Suite à cela les premiers scénarios opérationnels sont définis ainsi que les premières vulnérabilités et mesures de sécurité associées. Pour finir, l'équipe MoRia présente ces résultats et en discute avec l'équipe Thales lors d'une quatrième réunion (figure VI.4). Plusieurs retours d'information et raffinements ont eu lieu jusqu'à ce que les bons choix d'architecture, les scénarios opérationnels, les mesures et leurs détails soient validés ;

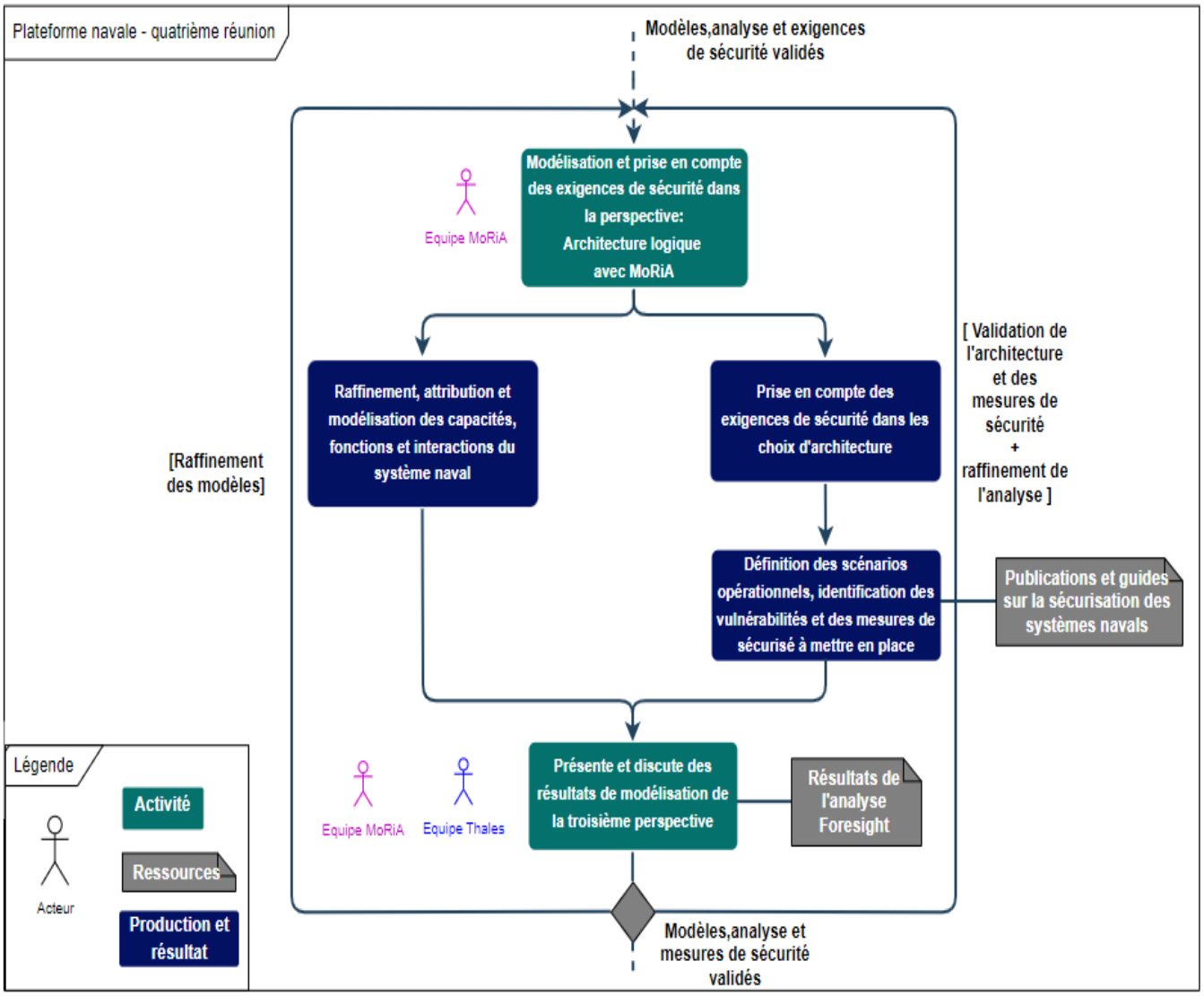


FIGURE VI.4: Protocole de planification - quatrième réunion

Après avoir appliqué les exigences de sécurité, l'équipe MoRiA modélise les mesures de sécurité remédiant aux vulnérabilités. Les résultats ont été présentés et discutés avec l'équipe Thales qui a trouvé le résultat valable et la méthode très intéressante pour la modélisation et l'analyse des futurs systèmes.

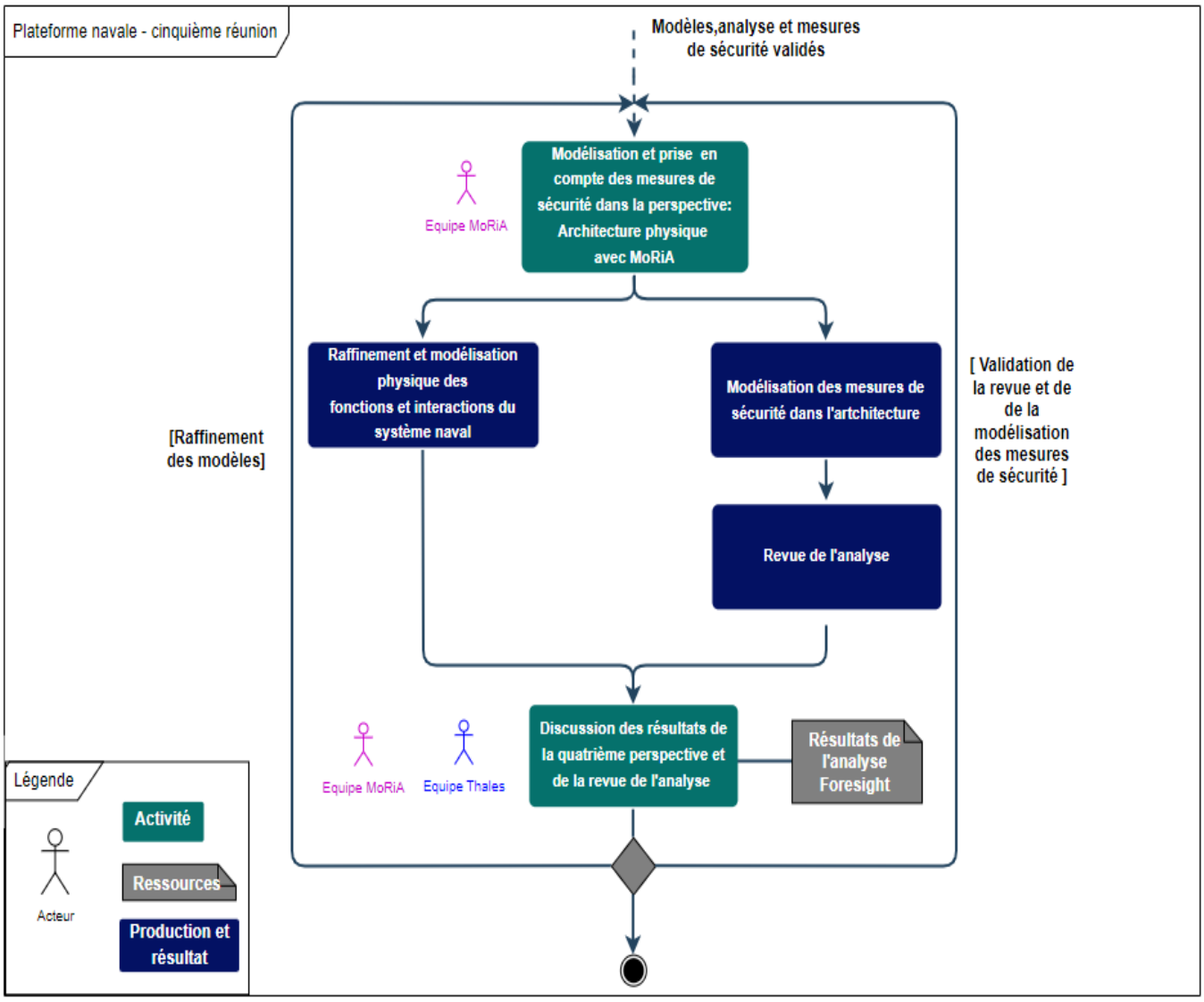


FIGURE VI.5: Protocole de planification - cinquième réunion

Il est important de mentionner que les données relatives aux composants du système naval ont été anonymisées pour des raisons de non-divulgation, et que toutes les informations relatives aux vulnérabilités réelles des composants du système naval ne sont pas présentées pour des raisons de sécurité. En effet, pour définir et modéliser les vulnérabilités de sécurité et pour définir les scénarios de menaces, nous avons suggéré quelques vulnérabilités possibles inspirées de notre étude des travaux relatifs à la sécurité des systèmes navals, y compris les nouvelles attaques, qui ont été validées par l'équipe de Thales et plateforme comme étant réalistes.

Liste de publications

VI.1 Articles de Conférences Internationales avec comité de relectures

[PNG21] Paul, S., Naouar, D., & Gureghian, E. (2021). Obérisk : Cybersecurity Requirements Elicitation through Agile Remote or Face-to-Face Risk Management Brainstorming Sessions. Information, 12(9), 349.

[NEHV+21] Naouar, D., El Hachem, J., Voirin, J. L., Foisil, J., Kermarrec, Y. (2021, September). Towards the Integration of Cybersecurity Risk Assessment into Model-based Requirements Engineering. In 2021 IEEE 29th International Requirements Engineering Conference (RE) (pp. 334-344). IEEE.

Bibliographie

[ABB15] Wissam Abbass, Amine Baina, and Mostafa Bellafkih. Using EBIOS for risk management in critical information infrastructure. In *2015 5th World Congress on Information and Communication Technologies (WICT)*, pages 107–112. IEEE, 2015.

[AG06] Yudistira Asnar and Paolo Giorgini. Modelling risk and identifying countermeasure in organizations. In *International Workshop on Critical Information Infrastructures Security*, pages 55–66. Springer, 2006.

[AGD18] Deniz Akdur, Vahid Garousi, and Onur Demirörs. A survey on modeling and model-driven engineering practices in the embedded software industry. *Journal of Systems Architecture*, 91 :62–82, 2018.

[AHA15] Mohammad Nazmul Alam, Sohrab Hossain, and Kazy Noor E Alam. Use case application in requirements analysis using Secure Tropos to UMLsec-security issues. *International Journal of Computer Applications*, 109(4), 2015.

[Ala19] Shashank P Alai. *Evaluating ARCADIA/CAPELLA vs. OOSEM/SYSML for system architecture development*. PhD thesis, Purdue University Graduate School, 2019.

[ALR16] Ludovic Apvrille, Letitia Li, and Yves Roudier. Model-driven engineering for designing safe and secure embedded systems. In *2016 Architecture-Centric Virtual Integration (ACVI)*, pages 4–7. IEEE, 2016.

[AM14] Naved Ahmed and Raimundas Matulevičius. Securing business processes using security risk-oriented patterns. *Computer Standards & Interfaces*, 36(4) :723–733, 2014.

[AMA12] Olga Altuhhova, Raimundas Matulevičius, and Naved Ahmed. Towards definition of secure business processes. In *International conference on advanced information systems engineering*, pages 1–15. Springer, 2012.

[AMSZ08] Yudistira Asnar, Rocco Moretti, Maurizio Sebastianis, and Nicola Zannone. Risk as dependability metrics for the evaluation of business solutions : a model-driven approach. In *2008 Third International Conference on Availability, Reliability and Security*, pages 1240–1247. IEEE, 2008.

[And16] Jack Sheldon Anderson. The fortress problem. *Homeland Security Affairs*, Vol. 12 :p1–19, 2016.

[andlsdsdA19] agence nationale de la sécurité des systèmes d'information ANSSI. EBIOS RM going further. Technical report, agence nationale de la sécurité des systèmes d'information - ANSSI, Novembre 2019.

[AR15] J Aracic and P Roques. Select and deploy a conceptual modelling language. some keys. *Crescendo Technologies*, Vol. 5, 2015.

[Asn06] Erika Asnina. The formal approach to problem domain modelling within model driven architecture. In *9th International Conference on Information Systems Implementation and Modelling*, pages 97–104, 2006.

[Auz09] Jean-Philippe Auzelle. *Proposition d'un cadre de modélisation multi-échelles d'un système d'information en entreprise centré sur le produit.* Theses, Université Henri Poincaré - Nancy I, March 2009.

[AYL15] Rouwaida Abdallah, Nataliya Yakymets, and Agnes Lanusse. Towards a model-driven based security framework. In *3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, pages 639–645. IEEE, 2015.

[BBI18] Marco Bertoni, Alessandro Bertoni, and Ola Isaksson. Evoke : A value-driven concept selection method for early system design. *Journal of Systems Science and Systems Engineering*, 27(1) :46–77, 2018.

[BCV11] Eduardo Blanco, Yudith Cardinale, and María-Esther Vidal. Aggregating functional and non-functional properties to identify service compositions. In *Engineering Reliable Service Oriented Architecture : Managing Complexity and Service Level Agreements*, pages 145–174. IGI Global, 2011.

[BCW17] Marco Brambilla, Jordi Cabot, and Manuel Wimmer. Model-driven software engineering in practice. *Synthesis lectures on software engineering*, 3(1) :1–207, 2017.

[Béz04] Jean Bézivin. In search of a basic principle for model driven engineering. *Novatica Journal, Special Issue*, 5(2) :21–24, 2004.

[BFM13] Sandro Bologna, Alessandro Fasani, and Maurizio Martellini. From fortress to resilience. In *Cyber Security*, pages 53–56. Springer, 2013.

[BHS91] Ferenc Belina, Dieter Hogrefe, and Amardeo Sarma. *SDL with applications from protocol specification*. Prentice-Hall, Inc., 1991.

[BKS10] Sabine Buckl, Sascha Krell, and Christian M Schweda. A formal approach to architectural descriptions–refining the iso standard 42010. In *International Workshop on Cooperation and Interoperability, Architecture and Ontology*, pages 77–91. Springer, 2010.

[BKV02] Stephan Bourduas, Ferhat Khendek, and Daniel Vincent. From MSC and UML to SDL. In *Proceedings 26th Annual International Computer Software and Applications*, pages 153–158. IEEE, 2002.

[BMP13] Simona Bernardi, José Merseguer, and Dorina Corina Petriu. *Model-driven dependability assessment of software systems*. Springer, 2013.

[BOF+14] Bruce Beihoff, Christopher Oster, Sanford Friedenthal, Christiaan Paredis, Duncan Kemp, Heinz Stoewer, David Nichols, and Jon Wade. World in motion-systems engineering vision 2025, international council on systems engineering, 2014.

[BPG+04] Paolo Bresciani, Anna Perini, Paolo Giorgini, Fausto Giunchiglia, and John Mylopoulos. Tropos : An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3) :203–236, 2004.

[bre]

[BSAN17] Ilhem Boussaïd, Patrick Siarry, and Mohamed Ahmed-Nacer. A survey on search-based model-driven engineering. *Automated Software Engineering*, 24(2) :233–294, 2017.

[BVEN16] Stéphane Bonnet, Jean-Luc Voirin, Daniel Exertier, and Véronique Normand. Not (strictly) relying on SysML for MBSE : Language, tooling and development perspectives : The ARCADIA/CAPELLA rationale. In *2016 Annual IEEE Systems Conference (SysCon)*, pages 1–6. IEEE, 2016.

[C+83] National Research Council et al. *Risk assessment in the federal government : managing the process*. National Academies Press, 1983.

[CAB+19] Bryan Carter, Stephen Adams, Georgios Bakirtzis, Tim Sherburne, Peter Beling, Barry Horowitz, and Cody Fleming. A preliminary design-phase security methodology for cyber–physical systems. *Systems*, 7(2), 2019.

[CBB+16] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, 56 :1–27, 2016.

[CD21] Paul Schreinemakers Sanford Friedenthal Sky Matthews David Nichols Christopher Oster Taylor Riethle Garry Roedler Emma Sparks Heinz Stoewer Christopher Davey, Paul Nielsen. Systems engineering vision 2035 - engineering solutions for a better world, 2021.

[Cer17] Cerema. Les 7èmes Assises du Port du futur. Technical report, Cerema, 2017.

[CH11] Paul D Collopy and Peter M Hollingsworth. Value-driven design. *Journal of aircraft*, 48(3) :749–759, 2011.

[Chi12] Vanea Chiprianov. *Collaborative construction of telecommunications services. an enterprise architecture and model driven engineering method*. PhD thesis, Télécom Bretagne, Université de Bretagne-Sud, 2012.

[CLU12] Lazaro PEJSACHOWICZ CLUSIF. CLUSIF-Conformite-AR-2012-Synthese. Technical report, CLUSIF, 2012.

[CM16] Edward Ralph Carroll and Robert Joseph Malins. *Systematic Literature Review : How is Model-Based Systems Engineering Justified ?*. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2016.

[Col12] KGJ Coleman. *Aggression in cyberspace conflict and cooperation in the global commons : a comprehensive approach for international security*. Georgetown University Press, Washington DC, 2012.

[Con05] Insight Consulting. *CRAMM Version 5.1 User Guide.* https ://pdfcoffee.com/cramm-version-51-userguide-pdf-free.html (accessed on 29 June 2021), 2005.

[CSG18] Mike Chapple, James Michael Stewart, and Darril Gibson. *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide.* John Wiley & Sons, 2018.

[CSYW07] Richard A Caralli, James F Stevens, Lisa R Young, and William R Wilson. Introducing OCTAVE ALLEGRO : Improving the information security risk assessment process. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2007.

[DCB+15] Thomas Degueule, Benoit Combemale, Arnaud Blouin, Olivier Barais, and Jean-Marc Jézéquel. Melange : A meta-language for modular and reusable development of dsls. In *Proceedings of the 2015 ACM SIGPLAN International Conference on Software Language Engineering*, pages 25–36, 2015.

[DHMM10] Éric Dubois, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering*, pages 289–306. Springer, 2010.

[dlsdlf10] CLUSIF Club de la sécurité de l'information français. *MEHARI - Méthode harmonisée d'analyse des risques.* https ://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/, 2010.

[DM17] Scott A DeLoach and Matthew Miller. A goal model for adaptive complex systems. *J. Adv. Comput. Res*, 2 :83–92, 2017.

[Dom20] Naval Dome. Security : Maritime Industry Sees 400% Increase in Attempted Cyberattacks Since February 2020. Technical report, Naval Dome, 2020.

[DPDC18] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton : The first ICS cyber attack on safety instrument systems. In *Proc. Black Hat USA*, volume 2018, pages 1–26, 2018.

[dSGB17] Marc Antoine Lefebvre de Saint Germain and Stéphanie Guénot Bresson. Un porte-avions 2.0 apte à relever les défis militaires du xxie siècle. *Revue Defense Nationale*, (3) :22–27, 2017.

[ebi18] *EBIOS RM - Expression des besoins et identification des objectifs de sécurité Risk Manager.* https ://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/, 2018.

[edap12] Ministère espagnol des administrations publiques. *Magerit - Methodology for Information Systems Risk Analysis and Management.* `https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html`, 2012.

[Edd20] Rhéa Eddé. Les entreprises à l'épreuve des cyberattaques. *Flux*, (3) :90–101, 2020.

[EG12] Joseph P Elm and Dennis R Goldenson. The business case for systems engineering study : Results of the systems engineering effectiveness survey. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2012.

[EH17] Jamal El Hachem. *A Model Driven Method to Design and Analyze Secure System-of-Systems Architectures : Application to Predict Cascading Attacks in Smart Buildings.* PhD thesis, Pau, 2017.

[EHPC+16] Jamal El Hachem, Zi Yang Pang, Vanea Chiprianov, Ali Babar, and Philippe Aniorte. Model driven software security architecture of systems-of-systems. In *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*, pages 89–96. IEEE, 2016.

[EM17] Thomas Edgar and David Manz. *Research methods for cyber security.* Syngress, 2017.

[Eng14] G Engel. Deconstructing the cyber kill chain. dark reading, 2014.

[EY07] Golnaz Elahi and Eric Yu. A goal oriented approach for modeling and analyzing security trade-offs. In *International conference on conceptual modeling*, pages 375–390. Springer, 2007.

[FDW16] Peter H Feiler, Julien Delange, and Lutz Wrage. A requirement specification language for aadl. Technical report, Carnegie-Mellon Univ Pittsburgh PA United States, 2016.

[FFC09] Robert W Ferguson, Summer C Fowler, and Rita C Creel. A method for assessing technical progress and quality throughout the system life cycle. Technical report, Carnegie-Mellon Univ Pittsburgh PA software engineering inst, 2009.

[FG12] Peter H Feiler and David P Gluch. *Model-based engineering with AADL : an introduction to the SAE architecture analysis & design language*. Addison-Wesley, 2012.

[Fis14] Eric A Fischer. Cybersecurity issues and challenges : In brief, 2014.

[Fla19] Jean-Marie Flaus. *Cybersécurité des systèmes industriels*. ISTE Group, 2019.

[FM84] F Frola and C Miller. System safety in aircraft management. *Logistics Management Institute, Washington DC*, 1984.

[FMC11] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. Stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6) :29, 2011.

[Fon14] Iris de Fontaines. *Pilotage des innovations d'ingénierie par la valeur : une voie d'amélioration pour l'ingénierie des aéronefs*. PhD thesis, Grenoble, 2014.

[G+03] DoD Architecture Framework Working Group et al. DoD architecture framework version 1.0. *Department of Defense*, 2003.

[GBT+20] Joe Gregory, Lucy Berthoud, Theo Tryfonas, Alain Rossignol, and Ludovic Faure. The long and winding road : MBSE adoption for functional avionics of spacecraft. *Journal of Systems and Software*, 160 :110453, 2020.

[GER12] Henrique M Gaspar, Stein Ove Erikstad, and Adam M Ross. Handling temporal complexity in the design of non-transport ships using epoch-era analysis. *Transactions of the Royal Institution of Naval Architects Part A : International Journal of Maritime Engineering*, 154(3) :109–120, 2012.

[GL07] Robin A Gandhi and Seok-Won Lee. Discovering and understanding multi-dimensional correlations among certification requirements with application to risk assessment. In *15th IEEE International Requirements Engineering Conference (RE 2007)*, pages 231–240. IEEE, 2007.

[GNB+15] Milena Guessi, Valdemar VG Neto, Thiago Bianchi, Katia R Felizardo, Flavio Oquendo, and Elisa Y Nakagawa. A systematic literature review on the description of software architectures for systems of systems. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, pages 1433–1440, 2015.

[Gra06] Rüdiger Grammes. Formalisation of the UML Profile for SDL-A Case Study. 2006.

[Gre98] Steven J Greenwald. Discussion topic : what is the old security paradigm ? In *Proceedings of the 1998 workshop on New security paradigms*, pages 107–118, 1998.

[Hara] M Hartley. The cyber threat kill chain part 2 of 2-isight partners. isight partners (2014).

[Harb] M Hartley. Strengthening cyber kill chain with cyber threat intelligence. isight partners (2014).

[HBF+18] Barry Horowitz, Peter Beling, Cody Fleming, Stephen Adams, Bryan Carter, Tim Sherburne, Carl Elks, Georgios Bakirtzis, Forrest Shull, and Nancy R Mead. Cyber security requirements methodology. Technical report, Stevens Institute of Technology Hoboken United States, 2018.

[HCA+11] Eric M Hutchins, Michael J Cloppert, Rohan M Amin, et al. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1) :80, 2011.

[HCB+20] Jamal EL Hachem, Vanea Chiprianov, Muhammad Ali Babar, Tarek AL Khalil, and Philippe Aniorte. Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems. *Journal of Systems and Software*, 162 :110484, 2020.

[HKS16] Romuald Hoffmann, Maciej Kiedrowicz, and Jerzy Stanik. Risk management system as the basic paradigm of the information security management system in an organization. In *MATEC Web of Conferences*, volume 76, page 04010. EDP Sciences, 2016.

[HNPS20] Romuald Hoffmann, Jarosław Napiórkowski, Tomasz Protasowicki, and Jerzy Stanik. Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, 44 :655–662, 2020.

[Hon13] Eric C Honour. *Systems engineering return on investment*. University of South Australia Adelaide, 2013.

[HS21] Kaitlin Henderson and Alejandro Salado. Value and benefits of model-based systems engineering (MBSE) : Evidence from the literature. *Systems Engineering*, 24(1) :51–66, 2021.

[HTLC15] Adam Hahn, Roshan K Thomas, Ivan Lozano, and Alvaro Cardenas. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 11 :39–50, 2015.

[HY16] Jennifer Horkoff and Eric Yu. Interactive goal model analysis for early requirements engineering. *Requirements Engineering*, 21(1) :29–61, 2016.

[Ins05] British Standards Institute. *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001 :2005)*. 2005.

[ISO08] ISO/IEC. *information technology security techniques information security risk management*. 2008.

[ISO15] ISO ISO. Iec/ieee 15288 : 2015. *Systems and software engineering-Content of systems and software life cycle process information products (Documentation), International Organization for Standardization/International Electrotechnical Commission : Geneva, Switzerland*, 2015.

[JFS08] Ivan J Jureta, Stéphane Faulkner, and Pierre-Yves Schobbens. Clear justification of modeling decisions for goal-oriented requirements engineering. *Requirements Engineering*, 13(2) :87–115, 2008.

[JP11] Erland Jonsson and Laleh Pirzadeh. A framework for security metrics based on operational system attributes. In *2011 Third International Workshop on Security Measurements and Metrics*, pages 58–65. IEEE, 2011.

[JS07] Jan Jürjens and Pasha Shabalin. Tools for secure systems development with UML. *International Journal on Software Tools for Technology Transfer*, 9(5) :527–544, 2007.

[JT19] JEAN-LUC ALLARD JEROME THEMEE. *EBIOS 2018 – Avantages et inconvénients*. PECB INSIGHTS CONFERENCE 2019, 2019.

[Jür02] Jan Jürjens. Umlsec : Extending uml for secure systems development. In *International Conference on The Unified Modeling Language*, pages 412–425. Springer, 2002.

[KBJV06] Ivan Kurtev, Jean Bézivin, Frédéric Jouault, and Patrick Valduriez. Model-based dsl frameworks. In *Companion to the 21st ACM SIGPLAN symposium on Object-oriented programming systems, languages, and applications*, pages 602–616, 2006.

[KG81] Stanley Kaplan and B John Garrick. On the quantitative definition of risk. *Risk analysis*, 1(1) :11–27, 1981.

[Kha20] Syed Munir Khasru. Digital age & cyberspace transiting to digital boom or digital doom ? *The Digital Age, Cyber Space, and Social Media The Challenges of Security & Radicalization*, page 1, 2020.

[KK19] Hans M Kristensen and Matt Korda. French nuclear forces, 2019. *Bulletin of the Atomic Scientists*, 75(1) :51–55, 2019.

[KPB+10] Barbara Kitchenham, Rialette Pretorius, David Budgen, O Pearl Brereton, Mark Turner, Mahmood Niazi, and Stephen Linkman. Systematic literature reviews in software engineering–a tertiary study. *Information and software technology*, 52(8) :792–805, 2010.

[KSF18] Muhammad Salman Khan, Sana Siddiqui, and Ken Ferens. A cognitive and concurrent cyber kill chain model. In *Computer and Network Security Essentials*, pages 585–602. Springer, 2018.

[KVKM21] Behnam Asadi Khashooei, Alexandr Vasenev, Hasan Alper Kocademir, and Roland Mathijssen. Architecting system of systems solutions with security and data-protection principles. In *16th International Conference of System of Systems Engineering (SoSE)*, pages 43–48, 2021.

[Laj17] Chokri Lajimi. *Évaluation dynamique du risque retard dans les flux opérationnels d'un système logistique : Application au cas d'une chaîne de distribution.* PhD thesis, 07 2017.

[LBD02] Torsten Lodderstedt, David Basin, and Jürgen Doser. SecureUML : A UML-based modeling language for model-driven security. In *International Conference on the Unified Modeling Language*, pages 426–441. Springer, 2002.

[LCS+09] Marcia Lucena, Jaelson Castro, Carla Silva, Fernanda Alencar, Emanuel Santos, and João Pimentel. A model transformation approach to derive architectural models from goal-oriented requirements models. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 370–380. Springer, 2009.

[LNIJ04] Luncheng Lin, Bashar Nuseibeh, Darrel Ince, and Michael Jackson. Using abuse frames to bound the scope of security problems. In *Proceedings. 12th IEEE International Requirements Engineering Conference, 2004.*, pages 354–355. IEEE, 2004.

[LO09] Simon Liu and Jerry Ormaner. From ancient fortress to modern cyberdefense. *IT professional*, 11(3) :22–29, 2009.

[Mat17] Raimundas Matulevičius. Secure system development. In *Fundamentals of Secure System Modelling*, pages 199–207. Springer, 2017.

[MB20a] Donatas Mažeika and Rimantas Butleris. Integrating security requirements engineering into MBSE : Profile and guidelines. *Security and Communication Networks*, 2020.

[MB20b] Donatas Mažeika and Rimantas Butleris. MBSEsec : Model-based systems engineering method for creating secure systems. *Applied Sciences*, 10(7) :2574, 2020.

[MBC+20] Nan Messe, Nicolas Belloir, Vanea Chiprianov, Jamal El-Hachem, Régis Fleurquin, and Salah Sadou. An asset-based assistance for secure by design. In *2020 27th Asia-Pacific Software Engineering Conference (APSEC)*, pages 178–187. IEEE, 2020.

[McN16] Michael McNicholas. *Maritime security : an introduction.* Butterworth-Heinemann, 2016.

[MDCM18] I May, J David, F Cohen, and M Marietta. One year after wannacry : Assessing the aftermath. *Network Security*, 2018(5) :1–2, 2018.

[MF99] John McDermott and Chris Fox. Using abuse case models for security requirements analysis. In *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)*, pages 55–64. IEEE, 1999.

[MFMP07] Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. A common criteria based security requirements engineering process for the development of secure information systems. *Computer standards & interfaces*, 29(2) :244–253, 2007.

[MFMP10] Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. Security requirements engineering framework for software product lines. *Information and Software Technology*, 52(10) :1094–1117, 2010.

[MG07] Haralambos Mouratidis and Paolo Giorgini. Secure Tropos : a security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(02) :285–309, 2007.

[MG10a] Danijel Milicevic and Matthias Goeken. Konzepte der informationssicherheit in standards am beispiel iso 27001. *INFORMATIK 2010. Service Science–Neue Perspektiven für die Informatik. Band 2*, 2010.

[MG10b] Danijel Milicevic and Matthias Goeken. Ontology-based evaluation of iso 27001. In Wojciech Cellary and Elsa Estevez, editors, *Software Services for e-World*, pages 93–102, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[MG11] Danijel Milicevic and Matthias Goeken. Model driven information security management-evaluating and applying the meta model of iso 27001. In *AMCIS*, 2011.

[MGA13] Denisse Muñante, Laurent Gallon, and Philippe Aniorté. An approach based on model-driven engineering to define security policies using OrBAC. In *2013 International Conference on Availability, Reliability and Security*, pages 324–332. IEEE, 2013.

[Mih12] Vladimir Lucian Mihailescu. Risk analysis and risk management using MEHARI. *J. Appl. Bus. Inf. Syst*, 3(4) :143–162, 2012.

[MJ10] Haralambos Mouratidis and Jan Jurjens. From goal-driven security requirements engineering to secure design. *International Journal of Intelligent Systems*, 25(8) :813–840, 2010.

[MMN+12] Raimundas Matulevicius, Haralambos Mouratidis, Mayer Nicolas, Dubois Eric, and Patrick Heymans. Syntactic and semantic extensions to Secure Tropos to support security risk management. *Journal of Universal Computer Science*, 18(6) :816–844, 2012.

[MNC21] Saoussen Mili, Nga Nguyen, and Rachid Chelouah. Model-driven architecture based security analysis. *Systems Engineering*, 2021.

[Mod06] Mohammad Modarres. *Risk analysis in engineering : techniques, tools, and trends*. CRC press, 2006.

[MUV+16] Abderrahman Mokni, Christelle Urtado, Sylvain Vauttier, Marianne Huchard, and Huaxi Yulin Zhang. A formal approach for managing component-based architecture evolution. *Science of Computer Programming*, 127 :24–49, 2016.

[NAY17] Phu H Nguyen, Shaukat Ali, and Tao Yue. Model-based security engineering for cyber-physical systems : A systematic mapping study. *Information and Software Technology*, 83 :116–135, 2017.

[ndlsdsdA10] Agence nationale de la sécurité des systèmes d'information (ANSSI). *EBIOS - Expression des besoins et identification des objectifs de sécurité*. https ://www.ssi.gouv.fr/entreprise/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/, 2010.

[NEHV+21] Douraïd Naouar, Jamal El Hachem, Jean-Luc Voirin, Jacques Foisil, and Yvon Kermarrec. Towards the integration of cybersecurity risk assessment into model-based requirements engineering. In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pages 334–344. IEEE, 2021.

[NGG+13] Elisa Y Nakagawa, Marcelo Gonçalves, Milena Guessi, Lucas BR Oliveira, and Flavio Oquendo. The state of the art and future perspectives in systems of systems software architectures. In *Proceedings of the First International Workshop on Software Engineering for Systems-of-Systems*, pages 13–20, 2013.

[NM10] Roy Nersesian and Subrina Mahmood. Baltic and international maritime council. In *Handbook of Transnational Economic Governance Regimes*, pages 747–754. Brill Nijhoff, 2010.

[NVPB19] Juan Navas, Jean-Luc Voirin, Stephane Paul, and Stephane Bonnet. Towards a model-based approach to systems and cyber security co-engineering. In *INCOSE International Symposium*, volume 29, pages 850–865. Wiley Online Library, 2019.

[OMG15a] Object Management Group OMG. *System modeling language specifications version 1.4*. http ://www.omg.org/spec/SysML/1.4/, 2015.

[OMG15b] Object Management Group OMG. *Unified modeling language specifications version 2.5*. http ://www.omg.org/spec/UML/2.5/, 2015.

[Org16] North Atlantic Treaty Organization. *NATO Architecture Framework v4.0 Documentation*. http ://nafdocs.org/, 2016.

[Pan10] RK Pandey. Architectural description languages (adls) vs uml : a review. *ACM SIGSOFT Software Engineering Notes*, 35(3) :1–5, 2010.

[Pap17] Barry L Papke. Enabling design of agile security in the IOT with MBSE. In *12th System of Systems Engineering Conference (SoSE)*, pages 1–6. IEEE, 2017.

[Pat19] Srikanta Patnaik. *New Paradigm of Industry 4.0 : Internet of Things, Big Data & Cyber Physical Systems*, volume 64. Springer Nature, 2019.

[PNG21] Stéphane Paul, Douraid Naouar, and Emmanuel Gureghian. Obérisk : Cybersecurity requirements elicitation through agile remote or face-to-face risk management brainstorming sessions. *Information*, 12(9) :349, 2021.

[PRRT14] Birgit Penzenstadler, Ankita Raturi, Debra Richardson, and Bill Tomlinson. Safety, security, now sustainability : the nonfunctional requirement for the 21st century. *IEEE software*, 31(3) :40–47, 2014.

[RAB+15] Stewart Robinson, Gilbert Arbez, Louis G. Birta, Andreas Tolk, and Gerd Wagner. Conceptual modeling : Definition, purpose and benefits. In *2015 Winter Simulation Conference (WSC)*, pages 2812–2826, 2015.

[RAC14] Lee Rainie, Janna Anderson, and Jennifer Connolly. Cyber attacks likely to increase. 2014.

[RB04] Ondrej Rysavy and Frantisek Bures. Formal abstract architecture for use case specifications. In *Proceedings. 11th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems, 2004.*, pages 203–210. IEEE, 2004.

[RFB10] Ana Luísa Ramos, José Vasconcelos Ferreira, and Jaume Barceló. Revisiting the similar process to engineer the contemporary systems. *Journal of Systems Science and Systems Engineering*, 19(3) :321–350, 2010.

[rob]

[Ros77] Douglas T Ross. Structured analysis (sa) : A language for communicating ideas. *IEEE Transactions on software engineering*, (1) :16–34, 1977.

[RR10a] Donna H Rhodes and Adam M Ross. Five aspects of engineering complex systems emerging constructs and methods. In *2010 IEEE International Systems Conference*, pages 190–195. IEEE, 2010.

[RR10b] Donna H Rhodes and Adam M Ross. Shaping socio-technical system innovation strategies using a five aspects taxonomy. *Proceedings, EuSEC May, Stockholm, Sweden*, 2010.

[Run20] Brian Runciman. Cybersecurity report 2020. *ITNOW*, 62(4) :28–29, 2020.

[Sag14] Tony Sager. Killing advanced threats in their tracks : An intelligent approach to attack prevention. *InfoSec Reading Room*, 2014.

[Sch17] Klaus Schwab. *The fourth industrial revolution*. Currency, 2017.

[SdBD+02] Ketil Stolen, Folker den Braber, Theo Dimitrakos, Rune Fredriksen, Bjørn Axel Gran, Siv-Hilde Houmb, Mass Soldal Lund, Y Stamatiou, and JO Aagedal. Model-based risk assessment–the coras approach. In *iTrust Workshop*, 2002.

[SDF16] Bastien Sultan, Fabien Dagnat, and Caroline Fontaine. Maîtrise des correctifs de sécurité pour les systèmes navals. In *CIEL 2016 : 5ème Conférence en Ingénierie du Logiciel*, pages 1–6, 2016.

[Sel09] Bran Selic. The theory and practice of modeling language design for model-based software engineering—a personal perspective. In *International Summer School on Generative and Transformational Techniques in Software Engineering*, pages 290–321. Springer, 2009.

[SG13] Bran Selic and Sébastien Gérard. *Modeling and analysis of real-time and embedded systems with UML and MARTE : Developing cyber-physical systems.* Elsevier, 2013.

[SGF02] Gary Stoneburner, Alice Y Goguen, and Alexis Feringa. *Sp 800-30. risk management guide for information technology systems.* National Institute of Standards & Technology, 2002.

[She19] SIPRI Fact Sheet. The sipri top 100 arms-producing and military services companies. 2019.

[SHJ+19] Shamika N Sirimanne, J Hoffman, W Juan, R Asariotis, M Assaf, G Ayala, H Benamara, D Chantrel, J Hoffmann, A Premti, et al. Review of maritime transport 2019. Technical report, tech. rep, 2019.

[Sil09] Hillary G Sillitto. 6.2. 4 on systems architects and systems architecting : some thoughts on explaining and improving the art and science of systems architecting. In *INCOSE International Symposium*, volume 19, pages 970–985. Wiley Online Library, 2009.

[Sin07] Guttorm Sindre. Mal-activity diagrams for capturing attacks on business processes. In *International working conference on requirements engineering : foundation for software quality*, pages 355–366. Springer, 2007.

[Slo02] Anthony M Sloane. Post-design domain-specific language embedding : A case study in the software engineering domain. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pages 3647–3655. IEEE, 2002.

[Smi17] Nathalie Smirnov. Refonte à mi-vie du charles-de-gaulle : aborder les enjeux militaires de demain. *Revue Défense Nationale*, (3) :28–33, 2017.

[SNMG08] Mohammad Saravi, Linda Newnes, Antony Roy Mileham, and Yee Mey Goh. Estimating cost at the conceptual design stage to optimize design in terms

of performance and cost. In *Collaborative product and service life cycle management for a sustainable world*, pages 123–130. Springer, 2008.

[SO05] Guttorm Sindre and Andreas L Opdahl. Eliciting security requirements with misuse cases. *Requirements engineering*, 10(1) :34–44, 2005.

[Sol02] IMO Solas. International convention for the safety of life at sea (solas). *International Maritime Organization, London*, 2002.

[SS04] Richard A Stephans and Joe Stephenson. *System safety for the 21st century*. Wiley Online Library, 2004.

[Sym17] S Symantec. What you need to know about the Wannacry ransomware. *Symantec Security Response*, 2017.

[THI03] André CHARDONNET-Dominique THIBAUDON. Le guide du pdca de deming. *Éditions d'Organisation*, 2003.

[Tur08] Skander Turki. *Ingénierie système guidée par les modèles : Application du standard IEEE 15288, de l'architecture MDA et du langage SysML à la conception des systèmes mécatroniques*. PhD thesis, Université du Sud Toulon Var, 2008.

[Ven19] Cybersecurity Ventures. 2019 official annual cybercrime report. 2019.

[VL01] Axel Van Lamsweerde. Goal-oriented requirements engineering : A guided tour. In *Proceedings fifth ieee international symposium on requirements engineering*, pages 249–262. IEEE, 2001.

[VL04] Axel Van Lamsweerde. Elaborating security requirements by construction of intentional anti-models. In *Proceedings. 26th International Conference on Software Engineering*, pages 148–157. IEEE, 2004.

[Voi17] Jean-Luc Voirin. *Model-based System and Architecture Engineering with the Arcadia Method*. Elsevier, 2017.

[Voi18] Jean-Luc Voirin. *Conception architecturale des systèmes basée sur les modèles avec la méthode Arcadia*, volume 3. ISTE Group, 2018.

[VVLPP05] Damien Vanderveken, Axel Van Lamsweerde, Dewayne E Perry, and Christophe Ponsard. Deriving architectural descriptions from goal-oriented requirements models, 2005.

[Whi04] Stephen A White. Introduction to BPMN. *Ibm Cooperation*, 2(0) :0, 2004.

[Wol10] Philippe Wolf. Les menaces numériques aujourd'hui. *Sécurité et stratégie*, 3(1) :44–46, 2010.

[YR15] Tarun Yadav and Arvind Mallari Rao. Technical aspects of cyber kill chain. In *International Symposium on Security in Computing and Communication*, pages 438–452. Springer, 2015.

[Yu97] Eric SK Yu. Towards modelling and reasoning support for early-phase requirements engineering. In *Proceedings of ISRE'97 : 3rd IEEE International Symposium on Requirements Engineering*, pages 226–235. IEEE, 1997.

[ZHLL18] Juntao Zhang, Cecilia Haskins, Yiliu Liu, and Mary Ann Lundteigen. A system engineering–based approach for framing reliability, availability, and maintainability : A case study for subsea design. *Systems Engineering*, 21(6) :576–592, 2018.

DOCTORAT BRETAGNE LOIRE / MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Titre : MoRiA : Une méthode basée sur les modèles pour l'analyse des risques de cybersécurité. Application à un système complexe de défense navale.

Mots clés : Ingénierie des systèmes basée sur les modèles, exigences de sécurité, évaluation des risques, co-ingénierie des systèmes et de la sécurité.

Résumé : L'analyse de risques et l'ingénierie système travaillent sur le même sujet (le système), mais avec des points de vue et objectifs différents. Une collaboration entre ces deux domaines permettrait de regrouper les points fort inhérents à ces domaines et de renforcer la définition du contexte de l'analyse, sa cohérence globale ainsi que la prise en compte des préoccupations et les enjeux de l'un et de l'autre. C'est ici que mes travaux s'inscrivent, ils ont pour objectif de combler le fossé entre l'analyse et la modélisation des exigences fonctionnelles et non fonctionnelles du système et l'analyse et la modélisation des risques de cybersécurité analogues et leurs maintien et mise à jour tout au long de la durée de vie du système à travers sa phase de définition et de modélisation. Pour cela nous proposons une méthode : MoRiA (Model-based Cyber Risk Analysis) qui étend les méthodes d'ingénierie dirigée par les modèles existants, adaptés et reposants sur des normes pour permettre l'identification, l'évaluation et le traitement des cyber-risques à travers les modèles. Cette méthode a été éprouvée sur un cas d'étude navale. De nombreuses perspectives émergent de ces travaux pour fournir une réponse globale à l'analyse et la maitrise des risques de cybersécurité tout au long de la vie d'un système.

Title : MoRiA: A model-based method for cybersecurity risk analysis. Application to a complex naval defense system

Keywords : Model-based systems engineering, security requirements, risk assessment, systems and security co-engineering.

Abstract : Risk analysis and systems engineering work on the same subject (the system), but with different points of view and objectives. A collaboration between these two domains would bring together the strong points inherent to these domains and reinforce the definition of the context of the analysis, its global coherence as well as the consideration of the concerns and stakes of both. This is where my work fits in, they aim to bridge the gap between the analysis and modeling of functional and non-functional requirements of the system and the analysis and modeling of cybersecurity risks and their maintenance and update throughout the life of the system through its definition and modeling phase. For this purpose, we propose a method: MoRiA (Model-based Cyber Risk Analysis) which extends existing model-driven engineering methods, adapted and based on standards, to allow the identification, evaluation and treatment of cyber risks through models.
This method has been proven on a naval case study. Many perspectives emerge from this work to provide a global answer to the analysis and control of cyber security risks throughout the life of a system.