Méta-modèle des concepts et processus d'analyse des risques selon les normes de cybersécurité

Christophe Ponsard [1], **Valery Ramon** [1], **Mounir Touzani** [2]

1. *CETIC - Centre de recherche, Gosselies, Belgique*
   {christophe.ponsard,valery.ramon}@cetic.be
2. *Chercheur indépendant, Toulouse, France*
   mounir.touzani@inrae.fr

RÉSUMÉ. *De nos jours, les systèmes d'information d'entreprise et de contrôle industriel sont fortement exposés aux menaces de cybersécurité. Dans de nombreux domaines, des mesures de protection sont activement déployées et encadrées par des normes ou standards. Il est fondamental de s'assurer que les risques de cybersécurité sont bien identifiés et contrôlés sur la base d'une analyse des menaces et d'une évaluation des risques. Cet article passe en revue les principales normes et permet de comparer des variantes dans différents domaines (systèmes d'information, systèmes industriels, automobile et aéronautique) afin de dégager un méta-modèle commun capturant tous les concepts manipulés durant une analyse des risques et le processus suivi pour la réalisation, éventuellement par itération et affinement. Enfin, nous illustrons et discutons son application sur un cas d'utilisation pour réaliser une analyse des risques dirigée par les modèles.*

ABSTRACT. *Today, corporate information systems and industrial control systems are highly exposed to cybersecurity threats. In many areas protective measures are actively deployed and supported by standards. A common foundation is to ensure that cybersecurity risks are properly identified and controlled based on a threat analysis and a risk assessment. This paper reviews and compares the different variants of standards in key domains (information systems, industrial systems, automotive and aeronautics) in order to derive a common meta-model capturing all the concepts required for a precise risk analysis as well as the process followed to perform it, possibly through iteration and refinement. We then illustrate and discuss how to deploy it for a model-driven risk analysis process.*

MOTS-CLÉS : *Cybersécurité, analyse de risques, modélisation, ISO 27000, EBIOS, IEC 62443, SAE 21434, DO-326, outillage*

KEYWORDS: *Cyber security, risk analysis, modelling, ISO 27000, EBIOS, IEC 62443, SAE 21434, DO-326, tool support*

---

1. Introduction

De nombreux secteurs d'activité sont devenus tributaires de systèmes d'information ou de contrôles industriels pour leur fonctionnement quotidien. Si cela contribue à les rendre plus réactifs, automatisés et compétitifs, la quantité de plus en plus importante de logiciels, combinée à un haut degré de complexité des systèmes et de leurs interconnexions accroît leur exposition aux menaces de cybersécurité. De récents rapports sur les menaces confirment les principaux fils conducteurs (logiciels malveillants, attaques en ligne, phishing) et leur évolution vers des attaques plus fréquentes et plus ciblées (ENISA, 2020). Les technologies numériques s'étant installées au coeur de toutes nos infrastructures critiques, en assurer la cybersécurité devient une préoccupation essentielle dans de nombreux secteurs industriels afin de les garder opérationnelles, voire d'en préserver la sûreté de fonctionnement. De plus, l'Europe a pris des actions en la matière pour imposer la directive NIS (Network Information System) dans une série de domaines de services essentiels (transport, énergie, traitement de l'eau, etc.) (EU, 2016), d'ailleurs en voie d'élargissement (services postaux, secteur alimentaire, fabrication des dispositifs médicaux...).

Les exigences principales de chaque secteur peuvent être remplies en mettant en place des mesures de protection capables d'assurer des propriétés clefs de ses services généralement en termes de disponibilité, intégrité et confidentialité. Pour ce dernier point, lorsque des données personnelles sont concernées, les exigences sont renforcées par le RGPD (Règlement Général de Protection des Données) (European Commission, 2016). De telles mesures se déclinent sur plusieurs lignes de défense (protection, réaction, récupération) et s'appuient sur une démarche de gestion des risques qui doit au préalable identifier les risques, les évaluer avant de décider des mesures qui permettent de les traiter, par exemple, en les réduisant à un niveau acceptable. Pour atteindre ces objectifs, cette démarche doit englober toutes les activités coordonnées et nécessaires afin de diriger et contrôler une organisation en matière de risque (ISO, 2009).

La mise en place d'une telle démarche requiert des normes dont le degré d'aboutissement et d'adoption varie selon les domaines. Ainsi, si le secteur des technologies de l'information (TI) dispose de la série intégrée des normes ISO27K depuis 2005 (ISO, 2013), d'autres secteurs ont été plus tardifs à se doter des normes : les systèmes industriels et l'aéronautique vers 2010 et l'automobile en 2021. Cette évolution est positive et cette adoption par domaine est adéquate car chaque domaine a ses spécificités en termes de biens à protéger et technologies mises en oeuvre, de type IT (Information Technology) et/ou OT (Operation Technology) (BSI, 2020). Cependant, la diversité des normes peut aussi constituer un obstacle à leur mise en oeuvre notamment quand il s'agit d'en considérer plusieurs ou encore par rapport à la disponibilité de plateformes outillées soutenant efficacement le travail d'analyse des risques.

Notre objectif consiste à dégager un socle commun suffisamment riche pour permettre la mise en place d'approches efficaces basées sur des modèles et assurer un bon niveau de précision de l'analyse, plutôt que des approches documentaires qualitatives encore fréquemment de mise. Cela est envisageable car toutes les méthodes partagent

de nombreux concepts et processus issus d'une norme générale de gestion des risques (ISO, 2009), s'appuyant sur des notations et outils similaires comme des diagrammes de contexte, (mis)use cases, des descriptions d'infrastructures et parfois des arbres de menaces. Ceux-ci étant mis en oeuvre en fonction des spécificités d'un secteur et du degré de maturité de l'organisation. La contribution centrale est de réaliser un méta-modèle riche en concepts et processus qui permettent de capturer, comprendre et manipuler les analyses des risques prescrites par les différentes normes. Notre approche procède par enrichissement plutôt que par abstraction : nous essayons, d'une part, de mettre en évidence le socle commun, d'autre part, de capturer des variantes plus riches qui ajoutent de la précision, l'expressivité et la modularité dans la démarche. Ceci contraste avec d'autres approches déjà réalisées, ce qui nous a inspiré en partie.

La structure de cet article reflète la méthodologie suivie. La section 2 passe en revue les diverses normes concernées et en fait une synthèse dans quatre secteurs clefs. La section 3 dégage un méta-modèle qui donne une vision globale en termes de concepts manipulés : notions de biens, risques, menaces, mesures... et d'un processus de conduite d'une analyse des risques qui peut être plus ou moins élaborée selon les cas. Ensuite, la section 4 illustre et discute la mise en oeuvre de ces abstractions sur plusieurs scénarios. Enfin, nous concluons et présentons nos travaux futurs.

2. État de l'art

Cette section passe en revue des processus d'analyse des risques prescrits par plusieurs normes. Après la présentation du cadre générique de l'ISO 31000, nous décrivons des normes spécifiques à la (cyber) sécurité dans quatre secteurs clefs : les systèmes d'information purs (ISO27K), les systèmes industriels mixant de l'IT et de l'OT (IEC 63443), l'automobile (SAE 21434) et l'aéronautique (DO-236). Nous nous concentrons ici uniquement sur des normes protégeant des organisations et non pas des produits spécifiques qui sont pris en charge par d'autres types de normes, notamment les critères communs.

2.1. Cadre de gestion des risques : ISO 31000

Un processus générique d'analyse des risques est spécifié par la norme ISO 31000 (ISO, 2018) qui structure les autres normes présentées. Voici les principales étapes identifiables dans la Figure 1:

– **identification des risques**, identifie, permet de comprendre et décrire les risques. Elle prend en compte à la fois ce qui peut entraver mais aussi aider à l'atteinte des objectifs.

– **analyse des risques**, vise à comprendre la nature des risques et leur caractéristiques : type d'incertitude, sources, conséquences, probabilité, scénarios, contrôles existants et leur efficacité. Les risques sont souvent difficiles à quantifier avec précision. Une approche qualitative est souvent adoptée.

– **évaluation des risques**, soutient le processus de décision selon les critères de l'entreprise pour décider de mesures complémentaires. Elle s'appuie sur l'analyse des risques qui est souvent résumée à l'aide d'une matrice des risques telle que celle de la figure 3. Les risques nécessitant des mesures sont identifiés et priorisés.

– **traitement des risques**, sélectionne et met en œuvre les actions résultant du processus de décision. Il doit également prendre en compte les aspects de coût, d'efforts et de délais. Pour chaque risque, les options possibles sont : ne rien faire (accepter), envisager des actions supplémentaires (atténuation), partager les conséquences (transfert), supprimer la source (évitement). Comme il n'est pas réaliste d'éliminer totalement les risques et que les actions peuvent en introduire de nouveaux, le degré de risque résiduel doit être évalué. Un plan d'actions est alors préparé et exécuté.

– **surveillance des risques**, le processus suit une boucle globale avec des réévaluations régulières (complètes ou incrémentales), suite à l'évolution de l'organisation et de son exposition aux risques.

2.2. Systèmes d'information : cadre ISO 27005

La norme ISO 27000 (ou « ISO27K » en abrégé) est une famille des normes relatives au déploiement d'un système de gestion des risques de sécurité de l'information. Elle définit le vocabulaire (27000), les exigences du système de gestion (27001), les contrôles (27002) et une approche de gestion orientée sur le risque (27005).

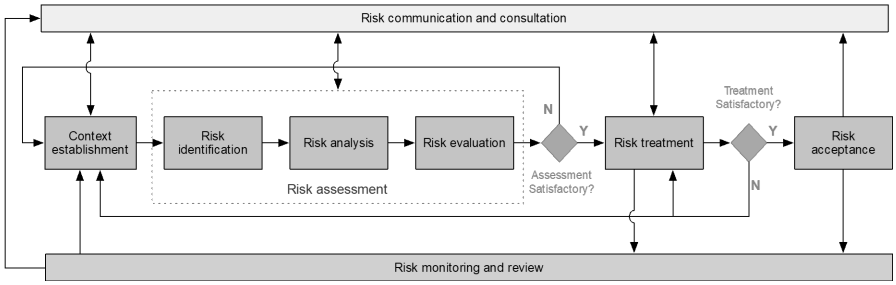

FIGURE 1. *ISO 27005 Analyse des menaces et évaluation des risques*

Le processus d'analyse des risques de sécurité de l'information est une spécialisation de la norme ISO 31000, comme le montre la figure 1. La norme ISO 27005 n'impose pas de méthodologie, mais un ensemble d'exigences à atteindre :

– **Établissement du contexte**, définit la portée, les limites, rôles, responsabilités.

– **Identification des risques**, explicite les principaux actifs à protéger et les actifs de soutien (logiciels, matériels, infrastructure physique, personnel...), de même que les sources de menaces (internes, externes) et les contrôles existants.

– **Estimation des risques**, fournit une estimation, généralement qualitative, de chaque risque en termes de probabilité et de conséquence en fonction de l'impact sur les propriétés de confidentialité, d'intégrité ou de disponibilité.

– **Évaluation des risques**, produit une liste des risques classés par ordre de priorité selon les critères d'évaluation des risques de sécurité.

Le processus comprend deux portes de décision explicites contrôlant respectivement le niveau de qualité de l'évaluation des risques et du plan de traitement des risques. De nombreuses implémentations de la norme ISO27005 sont disponibles, par exemple, EBIOS , MEHARI ou OCTAVE. Dans le cadre de cet article, nous nous limitons à EBIOS (ANSSI, 2010).

2.3. Systèmes d'information : EBIOS

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode française développée par la communauté EBIOS et soutenue par l'ANSSI, l'autorité française de défense des systèmes d'information. Elle est conforme à la norme ISO27005. Malgré l'évolution vers un schéma plus agile, nous prenons en compte la version 2010 dont la structure est représentée dans la Figure 2.

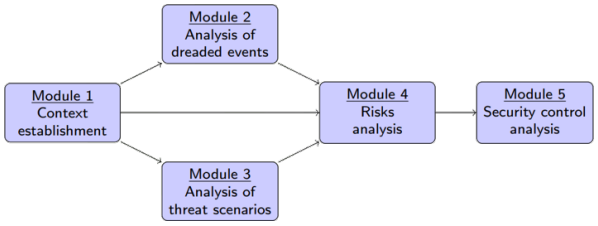

FIGURE 2. *Activités EBIOS*

Globalement, voici la correspondance avec la norme ISO 27005 et les spécificités de mise en œuvre :

– **L'établissement du contexte** nécessite d'énoncer les objectifs de l'organisation, le périmètre considéré, les échelles qualitatives de mesure de la confidentialité, la disponibilité et l'intégrité. Cela couvre aussi l'identification des actifs « primaires » (données et processus métier) et « secondaires » (infrastructure informatique et personnes). Le niveau de complexité de l'attaque est également identifié.

– **L'analyse des événements** redoutés est la première partie de l'estimation des risques. Il s'agit d'une approche descendante axée sur l'impact au niveau du métier. Elle estime les conséquences de la perte de confidentialité, d'intégrité et de disponibilité sur les différents actifs primaires. Les sources de menaces sont aussi identifiées.

– **L'analyse des scénarios de menace** est la deuxième partie de l'estimation des risques, réalisée en parallèle avec l'analyse des événements redoutés. Elle fonctionne de manière ascendante en considérant les scénarios de menace affectant les ressources de support. La probabilité est estimée sur une échelle qualitative contextuelle, avant et après l'application des mesures existantes.

– **L'analyse des risques** combine les résultats des deux étapes précédentes pour estimer chaque risque et produire une matrice des risques telle que décrite dans la

figure 3. Le processus peut combiner plusieurs scénarios (cas le plus défavorable). Une hiérarchisation est effectuée et le type d'action est décidé parmi les options proposées dans la norme ISO 31000 (éviter, accepter, atténuer, transférer).

– **L'analyse des contrôles de sécurité** détermine les mesures nécessaires pour traiter les risques. Ces contrôles peuvent être organisés sur plusieurs lignes de défense de prévention, de protection et de récupération. Les conseils sont fournis à l'aide d'une base de connaissances en lien avec la liste des contrôles ISO 27002.

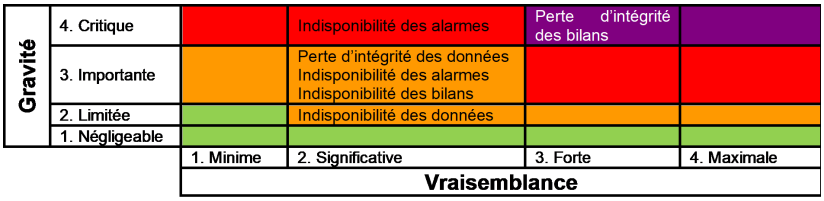

FIGURE 3. *Matrice des risques*

2.4. Système industriels : IEC/ISA 62443

La norme CEI/ISA 62443 a été développée par les comités ISA99 et CEI pour améliorer la sécurité des composants ou des systèmes utilisés dans l'automatisation et le contrôle industriel (IACS) (IEC, 2010a). Elle est le double de la norme CEI 61508 (IEC, 2010b) qui vise la sûreté de fonctionnement. Son périmètre est plus large que la norme ISO27K car il couvre non seulement l'IT mais aussi l'OT pour assurer le contrôle et la supervision de systèmes industriels ou de transport (par exemple ferroviaire). Elle est divisée en plusieurs parties couvrant les généralités, les politiques, les systèmes et les composants. L'évaluation des risques de sécurité (SRA) est couverte par la partie 62443-3-2. Sa classification des exigences de sécurité est également plus riche et avec 7 catégories qui couvrent les classiques : intégrité (FR3), confidentialité (FR4) et disponibilité (FR7) mais aussi 4 autres caractéristiques : le contrôle d'identification et d'authentification (FR1) de tous les utilisateurs. Puis, le contrôle de l'utilisation pour s'assurer du respect des privilèges requis (FR2), la restriction des flux sur les zones et conduits (FR5) ainsi que la réaction aux violations de sécurité (FR6). Elle introduit aussi quatre niveaux de sécurité (SL) afin de classifier et raisonner sur les risques en fonction de la criticité avec une progression en termes d'intentionnalité, sophistication et ressources mises en oeuvre.

Voici les étapes de l'évaluation des risques de sécurité (SRA) :

– ZCR1 : identification du système (cf. établissement du contexte dans l'ISO27K).

– ZCR2 : analyse des risques de haut niveau pour identifier les risques de cybersécurité liés aux opérations critiques. Elle peut se baser sur une analyse HAZOP.

– ZCR3 : partition en zones et conduits. Il s'agit d'une forme plus spécialisée de modélisation du système afin de fournir une isolation et organiser les lignes de défense.

– ZCR4 : évaluation de l'acceptabilité du risque au vu des mesures existantes.

– ZCR5 : en cas de risque non acceptable, une évaluation détaillée est effectuée au niveau des zones et des conduits. Des mesures supplémentaires sont identifiées et ZCR4 est réévaluée jusqu'à atteindre un niveau acceptable.

– ZCR6 : documentation des exigences/hypothèses/contraintes de cybersécurité.

– ZCR7 : approbation du rapport d'analyse par le propriétaire du bien.

2.5. Automobile : ISO 21434

Cette norme récente (2021), vise à établir un consensus sur les principaux problèmes de cybersécurité dans le domaine automobile (ISO, 2020). Elle remplace les bonnes pratiques J3061 (SAE, 2016) par des recommandations plus structurées. Son champ d'application concerne les véhicules routiers (voitures, camions, bus) et couvre leurs sous-systèmes, composants, connexions et logiciels. Son objectif est de garantir que les constructeurs et tous les participants de la chaîne d'approvisionnement disposent de processus structurés dès la phase de conception.

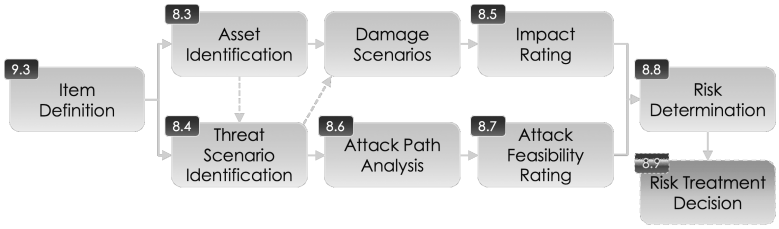

FIGURE 4. *ISO 21434 Analyse des menaces et évaluation des risques*

La norme est structurée en 10 sections et 15 clauses. Elle commence par définir (1) le champ d'application, (2) la référence normative, (3) le glossaire, (4) les considérations générales et (5/clauses 5-6-7) l'approche de gestion. Ensuite, (6/clause 8) se concentre sur l'évaluation des risques. Elle est suivie de trois sections couvrant respectivement (7/clause 9) la phase de conception, (8/clauses 10-11) le développement du produit et (9/clauses 12-13-14) le produit, l'exploitation et la maintenance. La dernière section (10/clause 15) traite des processus de soutien.

La norme n'impose aucune méthode d'évaluation des risques mais sa clause 8 rappelle les étapes requises, dans le même esprit que l'ISO 27005. La figure 4 détaille ses activités qui suivent un processus composé d'une branche métier identifiant les actifs (8.3) et évaluant les impacts (8.5), ainsi qu'une branche technique se concentrant sur l'analyse des menaces (8.4), l'identification du chemin d'attaque (8.6) et l'évaluation de la faisabilité (8.7). Les deux branches sont utilisées pour déterminer (8.8) et traiter les risques (8.9). Elle introduit aussi des niveaux d'assurance sur 4 niveaux CAL (Cybersecurity Assurance Level) totalisant 27 activités classées en 7 catégories. La norme ne décrit pas de technologies ou de solutions spécifiques et ne donne pas de recommandations sur les contre-mesures.

2.6. Aéronautique : DO-326/ED202

Si l'aéronautique disposait depuis longtemps de normes strictes en matière de sûreté de fonctionnement (DO-178), elle ne s'est dotée de normes de cybersécurité que vers 2010 avec la DO-326/ED-202, largement inspirée de l'ISO 27K et du standard de facto plus général SAE ARP 4754 (David, 2019). Elle aborde les considérations essentielles/de guidance et est complétée par d'autres documents pour les aspects services, systèmes sols et de plus haut niveau qui relèvent aussi des responsabilités externes (équipementiers). Elle ne spécifie aucune mesure de sécurité ou technique ni méthode mais donne plutôt des stratégies/tactiques applicables au domaine et recommande l'utilisation d'autres normes telle que l'ISO27K pour la mise en oeuvre.

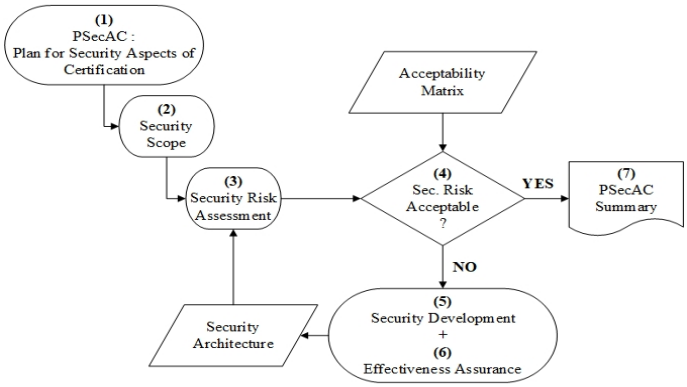

FIGURE 5. *Analyse des risques selon la norme aéronautique DO-326*

Cette norme détaille un processus de sécurité de la navigation aérienne (en anglais Airworthiness Security Process - AWSP) qui comporte 7 activités dont une analyse des risques qui comprend des étapes de définition de périmètre, d'identification des menaces, de leur caractérisation et évaluation de leur niveau. Les activités sont plus précisément représentées dans la figure 5, en parallèle avec les activités relatives au développement et à la sûreté de fonctionnement. On note la décomposition en trois étapes : préliminaire, système, spécifique à l'appareil lui-même. Les activités d'assurance sont réparties sur 4 niveaux SAL (Security Assurance Level) et sont au nombre de 118 classées en 13 sections.

2.7. Synthèse

La table 1 donne une synthèse comparative des différentes normes présentées en résumant leur domaine, le périmètre, le type d'exigence de sécurité, éventuellement le mécanisme de décomposition, le processus associé, la présence de listes d'exigences ou de contrôles ainsi que la présence de niveaux de sécurité/maturité (notamment en référence au modèle CMMI - Capability Maturity Model Integration).

Globalement, on constate plusieurs convergences qui permettent d'envisager la suite du travail de rapprochement des concepts et processus. EBIOS (ISO 27005) ap-

TABLEAU 1. *Synthèse comparative des différentes normes*

Sujet	EBIOS (ISO27K)	IEC 62443	ISO 21434	DO-326
Domaine	Systèmes d'information	Systèmes industriels	Automobile	Aéronautique
Périmètre	IT	IT/OT	IT/OT	IT/OT
Exigences clefs	3 (CID)	7 (FR1-FR7)	3 (CID)	3 (CID)
Décomposition	non	oui préliminaire puis détaillée (zones/conduits)	notion de sous-système et de chemin d'attaque	oui (préliminaire, système, bord)
Processus	ISO 31000 avec branche métier et infra	ISO 31000 avec niveau global et niveau détaillé	ISO 31000 avec branche métier et infra	ISO31000 (via inspiration ISO27005)
Liste d'exigences ou contrôles	basés sur l'ISO 27002 2013: 14 chap., 114 mesures 2022: 4 chap., 93 mesures	8 catégories (7 FR+1) 72 exigences	pas de liste	via norme externe
Niveaux de sécurité	Prioritisation libre	Niveaux SL0 à SL4 (cible/réalisé)	–	–
Niveau d'assurance	hors scope	4 niveaux de maturité basé sur CMMI 8 pratiques, 45 exigences	CAL 1 à 4 (informative) 7 catégories, 27 activités	SAL 0 à 3 13 sections, 29 exigences, 118 activités

paraît plus léger et moins capable de traiter des systèmes par approche de décomposition. IEC62443 est très complète. L'ISO 21434 en automobile reste assez monolithique mais plus détaillée qu'EBIOS, tandis que la DO-326 est structurée mais est essentiellement une norme chapeau qui défère sa mise en oeuvre à d'autres.

3. Méta-modèle des concepts et processus de gestion des risques

Cette section décrit un référentiel de gestion des risques indépendamment de normes spécifiques sous la forme de méta-modèles couvrant à la fois les concepts manipulés par ces normes mais aussi le processus de conduite de l'analyse des risques. Avant de décrire ces méta-modèles, le paragraphe suivant présente la finalité et la démarche.

3.1. Finalité et démarche de construction du méta-modèle

La synthèse des normes a montré de fortes similitudes notamment dans la démarche sous-jacente de gestion des risques. On constate bien sûr des différences mais qui relèvent plus de la variante ou du raffinement. Ceci permet d'envisager des bases communes de conceptualisation. Le point fondamental est de permettre une démarche explicitement orientée modèle en évolution de démarche basée sur des processus documentaires. Plus précisément, la modélisation explicite des concepts et des processus permettant de :

– disposer d'un référentiel unique pour ensuite appréhender un domaine plus spécifique, par exemple, l'automobile ou un système industriel de contrôle.

– faciliter le processus de passage à une autre norme, à partir d'un domaine soumis à une norme spécifique, combiner plusieurs normes pour des domaines hybrides ou si un domaine s'appuie explicitement sur une autre norme (cas de la DO-326).

– favoriser la transposition des menaces de nature similaire entre domaines, par exemple, une attaque de mise à jour de firmwares industriels vers l'automobile avec notamment Uptane comme mesure spécialisée (Kuppusamy *et al.*, 2018).

– développer un outillage d'analyse des risques, capable de capturer les concepts essentiels en utilisant les conventions spécifiques à des domaines pour leur capture et documentation, que cela soit en termes de liste de contrôles, de niveau d'assurance ou encore de la manière de dérouler le processus d'analyse.

La démarche suivie se base sur l'identification d'un tronc commun, en premier lieu, l'ISO31000 et la norme ISO27005 plus ancienne qui a été inspirante pour les autres. Ensuite, nous procédons par enrichissement en capturant des concepts qui ont été introduits pour combler des lacunes identifiées lors de notre état de l'art. Par exemple, les notions de zones et de conduits de la norme IEC 62434 rendent possible une analyse plus modulaire en contrôlant le niveau de granularité. Ces concepts raffinent la modélisation de l'infrastructure d'EBIOS, mais avec des concepts plus forts, prenant en compte la criticité des actifs, la fonction opérationnelle, l'emplacement physique ou logique, l'accès requis ou l'organisation responsable. En termes de processus, la norme automobile ISO 21434 introduit une démarche plus fine sur les étapes d'identification des chemins d'attaque permettant de mieux quantifier le risque. Notre démarche n'est donc pas réductrice : elle vise à capturer un maximum de contributions des normes en unifiant les concepts similaires tout en prenant en compte des mécanismes et spécificités réutilisables. Ce travail ne prétend pas être parfait car il à dû réaliser certaines concessions et arbitrages.

Au niveau plus technique, le méta-modèle conceptuel est spécifié à l'aide de diagrammes de classes UML reprenant les concepts apparaissant dans les descriptions de la section 2 de l'état de l'art. Sa formalisation s'appuie aussi sur plusieurs méta-modèles déjà documentés dans des cadres spécifiques telle qu'une norme t.q. ISO 27K (Akoka *et al.*, 2018), un outil t.q. Capella (Naouar *et al.*, 2021) ou plus général comme la co-ingénierie (Bakirtzis *et al.*, 2022) ou la gestion des risques projets (Sienou *et al.*, 2009). Ces méta-modèles ne sont pas reproduits ici et notre travail se démarque (1) par son ancrage dans la cybersécurité sans être spécifique à un domaine applicatif, (2) une vision unifiant le vocabulaire des normes, (3) la prise en compte d'un contexte élargi capturant des buts de l'entreprise et les motivations de l'attaquant.

3.2. Méta-modèle des concepts d'analyse des risques

La figure 6 structure les biens métier et de support suivant la classification proposée par EBIOS ainsi que la structuration en zones et conduits de l'ISO 62443. La figure 7 décrit l'articulation entre les biens de l'entreprise, les propriétés de sécurité à garantir, les risques et les mesures de contrôle. Voici les caractéristiques principales :

– la partie relative à l'organisation permet la modélisation structurée des objectifs via des arbres de buts. Cela permet de relier des propriétés de sécurité aux autres buts du système et d'employer des notations et méthodes d'ingénierie des exigences orientées buts telles que KAOS (van Lamsweerde, 2009) ou i* (Yu, Mylopoulos, 1997).

– de manière duale, la notion d'attaquant est explicitée et ses motivations sont capturées par des anti-buts appelés ici événements redoutés (terme EBIOS) qui se matérialisent via des scénarios d'attaque. Cette partie liée à la modélisation de l'attaquant

est représentée dans un ton plus foncé dans la figure 7.

– le risque lui-même est capturé selon ses dimensions d'impact (en lien avec les biens et propriétés métier) et de faisabilité (en lien avec les biens de support qui sont ceux qui peuvent contenir des vulnérabilités exploitables par des scénarios d'attaque).

– enfin, les risques de sécurité sont traités par des stratégies qui mettent en oeuvre des contrôles. Ceux-ci se situent sur différentes lignes de défense spécifiées à l'aide du framework NIST CSF (NIST, 2014).

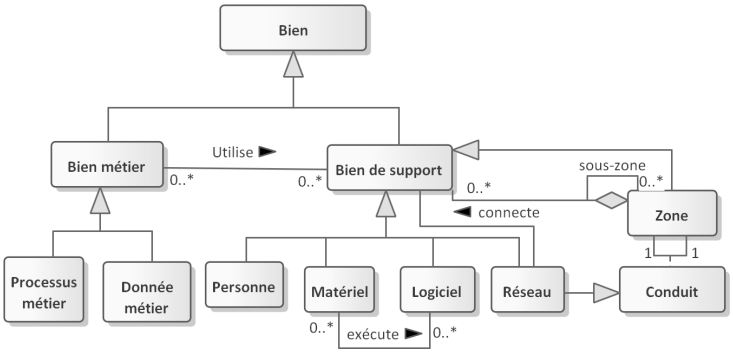

FIGURE 6. *Méta-modèle de la classification des biens métier et de support*

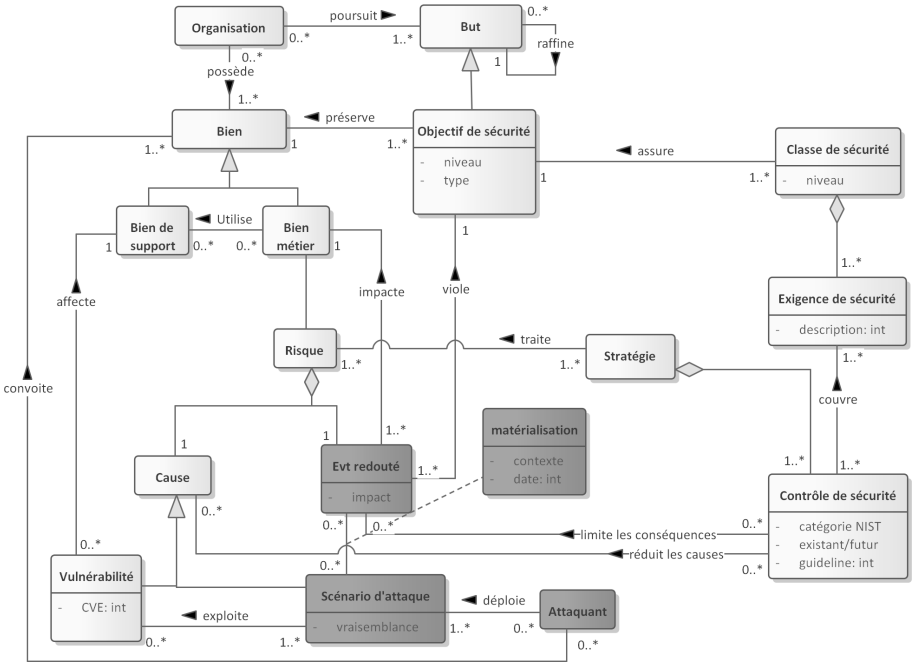

FIGURE 7. *Méta-modèle des concepts de gestion des risques*

3.3. Processus généralisé d'analyse des risques

La figure 8 représente une généralisation des processus d'analyse des risques décrits dans la section 2 à l'aide des notations BPMN. La partie gauche de la figure représente les étapes standards de l'ISO 31000.

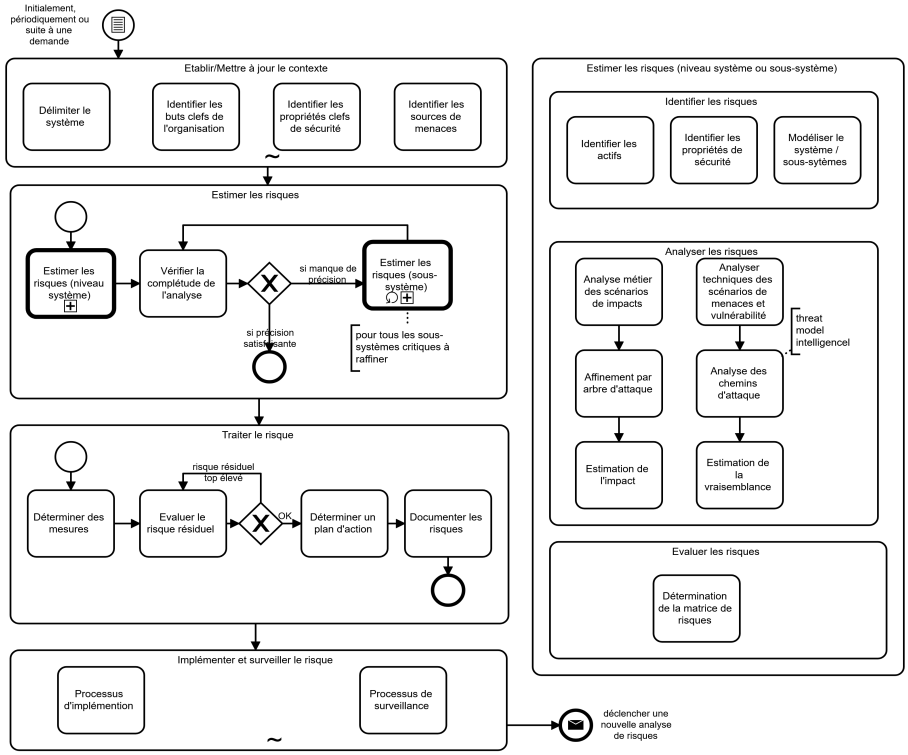

FIGURE 8. *Processus d'analyse des risques*

– l'étape d'établissement du contexte couvre aussi sa mise à jour lors d'une itération ultérieure. Elle comprend des activités d'identification du périmètre, des buts de l'organisation, des propriétés de sécurité et des sources de menaces.

– l'étape d'estimation des risques procède par raffinements, d'abord au niveau système, ensuite dans des sous-systèmes (ou zones) jusqu'au niveau de précision souhaité. L'étape clef (au niveau système ou sous-système) est modélisée via une « call activity » détaillée dans la partie droite de la figure 8. Elle traite séparément les aspects métier et d'infrastructure via des diagrammes spécifiques.

– l'étape de traitement des risques identifie des mesures réduisant le risque à un niveau résiduel acceptable, en plusieurs itérations si nécessaire. Les mesures sont ensuite documentées et priorisées au sein d'un planning.

– l'étape finale de mise en oeuvre et surveillance sort de la portée de l'analyse des risques mais permet d'initier une mise à jour quand c'est nécessaire.

4. Discussion sur un cas d'analyse des risques dirigée par les modèles

Les méta-modèles riches proposés offrent bien sûr un cadre conceptuel clair, utile à un apprentissage de l'analyse des risques et pour faire une transposition des notions similaires entre différentes normes à faire coexister. **Cependant l'apport principal que nous illustrons ici concerne la transition vers une approche d'analyse des risques dirigée par les modèles plus précise et automatisée** que les approches manuelles basées sur des tables et documents textuels qui montrent rapidement leurs limites sur des systèmes complexes (Ponsard, Massonet, 2022). A cette fin, nous analysons un service public de traitement des eaux usées, composé d'un système de surveillance (réseau de capteurs OT) qui transmet les informations et des alarmes à une salle de contrôle informatique (IT) (qui traite les alarmes) et génère des rapports quotidiens. Atteindre les objectifs de sécurité consiste à assurer la disponibilité (éviter des pollutions et être conforme aux réglementations environnementales) et la sécurité opérationnelle (intégrité). La confidentialité n'est pas pertinente car les données sont publiques. Afin de préparer l'analyse des risques, notre diagramme de processus unifié (figure 8) indique la nécessité de modéliser le contexte, d'identifier des biens, les risques, des propriétés et de réaliser des analyses métier et techniques.

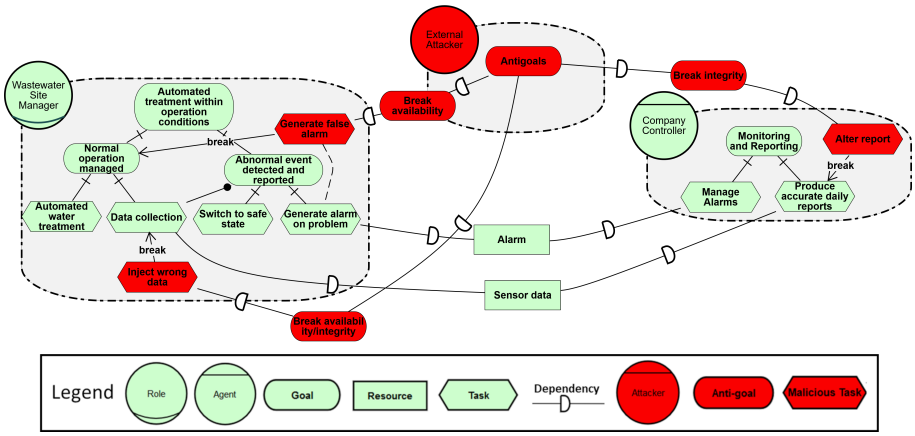

FIGURE 9. *Modèle stratégique*

Concernant l'analyse métier pour estimer les impacts, La figure 9 montre une modélisation dans les notations i*. L'examen de sa légende permet immédiatement d'identifier des concepts du méta-modèle liés aux biens métier : buts, agents (zones), dépendances (conduits), attaquant, biens (ressources), événements redoutés (anti-buts) et tâches malicieuses (scénarios d'attaque). Ainsi, l'utilisation d'un outil i* tel que piStar (Pimentel, 2018) permet immédiatement de modéliser ces concepts, les liens établis de nos modèles avec les différentes normes permettant ensuite de les transposer directement dans la norme souhaitée. Au niveau de notre modèle de processus, ceci permet de couvrir les étapes initiales liées au contexte et plus détaillées de l'analyse métier, arbre d'attaque et de l'estimation d'impact. En effet, ce modèle stratégique capture les principaux objectifs fonctionnels du système ainsi que l'intentionnalité d'un atta-

quant. Ainsi, ce raisonnement permet d'identifier les propriétés de sécurité à assurer sur des données (intégrité) et des services (disponibilité). Une analyse plus spécifique d'un sous-système (par exemple OT) peut être réalisée en fonction de sa criticité. Par exemple, un système de potabilisation soumise à la directive NIS nécessiterait une telle analyse.

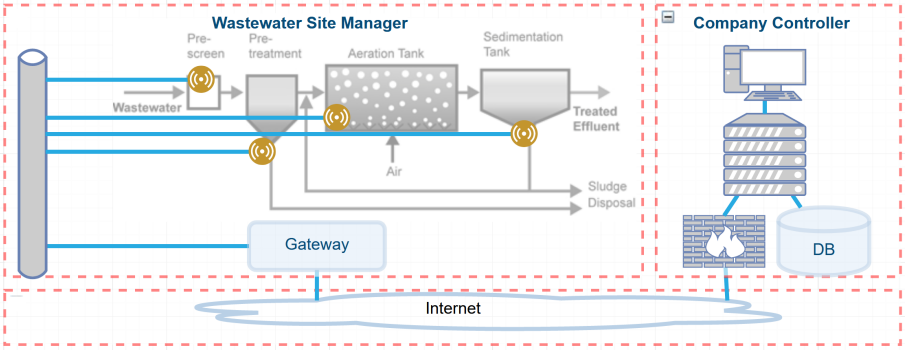

FIGURE 10. *Modèle d'infrastructure réalisé avec Irius Risk*

Concernant l'analyse technique menant à l'estimation de la vraisemblance, la figure 10 décrit l'infrastructure à l'aide de notations graphiques correspondant ici à des concepts de notre méta-modèle centré sur les biens de support. On y voit deux zones de nature différente : une zone OT avec des capteurs et un réseau IoT ainsi qu'une IT avec des serveurs et une base de données. Elles sont reliées par un conduit représenté par un réseau de communication. Cette modélisation permet des analyses automatisées, par exemple, pour identifier des vulnérabilités sur base de CVE (Common Vulnerability Enumeration) connus et des chemins d'attaques possibles, deux concepts clés du méta-modèle qui permettent d'estimer les vraisemblances des risques.

L'étape suivante du processus est d'évaluer le risque. Grâce aux concepts communs du méta-modèle, les modèles précédents peuvent être mis en correspondance notamment les acteurs du système avec les zones de l'infrastructure. Les informations respectives d'impact et de vraisemblance peuvent alors être combinées pour estimer les risques en prenant en compte des menaces multiples, la présence de mesures, etc. En manipulant les représentations des modèles (JSon, XML, EMF...) et en les transformant, il est possible d'automatiser la production de la matrice (figure 3 selon EBIOS) (Ponsard *et al.*, 2021). De cette analyse découle une série de contre-mesures. Des rapports dans des formats spécifiques à la norme cible peuvent aussi être automatisés.

Notre travail s'apparente à certains travaux, notamment UML a été étendu pour capturer les propriétés de sécurité, par exemple UMLSec (Jürjens, 2002). Les méthodes d'ingénierie des exigences dirigées par les objectifs déjà citées ont aussi été appliquées plus spécifiquement. i* dispose d'extensions de sécurité pour les analyses de vulnérabilité (Elahi *et al.*, 2010), Secure Tropos permet de traiter les systèmes socio-techniques (Paja *et al.*, 2013) et une ontologie spécifique à la sécurité a aussi été proposée (Sales *et al.*, 2018). Notre méta-modèle s'appuie sur une série de méta-

modèles et d'ontologies déjà publiés mais pourrait être consolidé sur base d'une revue plus systématique et approfondie de tels travaux.

5. Conclusion et perspectives

Dans cet article, nous avons proposé un méta-modèle de concepts et de processus donnant une synthèse unifiée de la démarche d'analyse des risques en passant en revue différentes normes de cybersécurité. Nous avons illustré les bénéfices liés à une modélisation plus précise et automatisée des risques à l'aide d'un système industriel. Nos travaux sont alignés avec d'autres propositions et permettent de combiner diverses techniques et outils, en s'affranchissant du cadre spécifique imposé par une norme.

Nos travaux futurs porteront sur l'affinement de notre méta-modèle et la mise en place d'un outillage permettant d'intégrer plus facilement divers formalismes dans notre référentiel pour y appliquer des analyses de risques. Cette approche s'inscrit aussi dans une intégration au sein d'une démarche de type DevSecOps alimentée en amont par des bases de connaissances issues de la surveillance opérationnelle, en élaborant plus cette partie de notre modèle générique de processus. En aval, les modèles produits peuvent être également exploités plus systématiquement pour alimenter des démarches de conception, de développement et de tests axés sur la sécurité.

Remerciements

Ces travaux ont été en partie financés par les projets CYRUS (8227) et CyberExcellence (2110186). Nous remercions les partenaires industriels pour avoir partagé leurs expériences en matière d'analyse des risques.

Bibliographie

Akoka J., Laoufi N., Lammari N. (2018, mai). Méta modèle de la sécurité des systèmes d'information : enrichissement par le contexte. In *INFORSID 2018.* Nantes, France.

ANSSI. (2010). *Expression des Besoins et Identification des Objectifs de Sécurité.* https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf.

Bakirtzis G. *et al. (2022). An ontological metamodel for cyber-physical system safety, security, and resilience coengineering.* Softw. Syst. Model.*, vol. 21, n° 1, p. 113–137.*

BSI. (2020). ICS Cybersecurity Assessment Framework - Suitable standards supporting a hybrid approach to risk management. *White paper.*

David A. (2019). An Introduction to DO-326A/ED-202A – Aviation Cyber-Security Set for Engineers and Managers. *https://afuzion.com/do-326a-ed-202a-aviation-cyber-security.*

Elahi G., Yu E., Zannone N. (2010, mars). A vulnerability-centric requirements engineering framework. Requir. Eng.*, vol. 15, n° 1.*

ENISA. (2020). Threat Landscape 2020 - List of top 15 threats .

EU. (2016). Dir. 1148 concerning measures for a high common level of security of network and information systems across the Union. *http://data.europa.eu/eli/dir/2016/1148/oj.*

European Commission. (2016). Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.*

IEC. (2010a). 61508 - functional safety of electrical/electronic/programmable electronic safety-related systems. *http://www.iec.ch/functionalsafety.*

IEC. (2010b). IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems. *http://www.iec.ch/functionalsafety.*

ISO. (2009). Risk management – vocabulary. *ISO Guide 73.*

ISO. (2013). ISO/IEC 27000 Family - Information Security Management Systems. *https://www.iso.org/isoiec-27001-information-security.html.*

ISO. (2018). ISO 31000, Risk management - Guidelines, provides principles, framework. *https://www.iso.org/iso-31000-risk-management.html.*

ISO. (2020). ISO/SAE FDIS 21434 Road vehicles — Cybersecurity engineering (draft). *https://www.iso.org/standard/70918.html.*

Jürjens J. (2002). UMLsec: Extending UML for Secure Systems Development. In Uml - the unified modeling language.

Kuppusamy T. K., DeLong L. A., Cappos J. (2018). Uptane: Security and customizability of software updates for vehicles. IEEE Vehicular Technology Magazine*, vol. 13, n^o 1.*

Naouar D. et al. (2021). Towards the integration of cybersecurity risk assessment into model-based requirements engineering. In *29th int. requirements engineering conference.*

NIST. (2014). *Cybersecurity Framework.* https://www.nist.gov/cyberframework.

Paja E. *et al. (2013). Sts-tool: Specifying and reasoning over socio-technical security requirements. In* Proc. of the 6th international *i** workshop 2013, valencia, spain, june 17-18.

Pimentel J. (2018). pistar tool for i* 2.0. *https://www.cin.ufpe.br/~jhcp/pistar.*

Ponsard C., Massonet P. (2022). Survey and Guidelines about Learning Cyber Security Risk Assessment. *8th Int. Conf. on Information Systems Security and Privacy, online, Feb 9-11.*

Ponsard C., Ramon V., Touzani M. (2021). Improving Cyber Security Risk Assessment by Combined Use of i* and Infrastructure Models. *Proc. of the 14th Int. iStar Workshop.*

SAE. (2016). Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - J3061_201601. *https://www.sae.org/standards/content/j3061_201601.*

Sales T. P. et al. (2018). The common ontology of value and risk. In *Conceptual modeling - 37th int. conf., ER 2018, xi'an, china, october 22-25.*

Sienou A., Lamine E., Pingaud H. (2009, 08). A method for integrated management of process-risk. , vol. 339.

van Lamsweerde A. (2009). *Requirements engineering - from system goals to UML models to software specifications*. Wiley.

Yu E., Mylopoulos J. (1997, avril). Enterprise modelling for business redesign: The i* framework. *SIGGROUP Bull.*, vol. 18, n^o 1.