Towards the Integration of Cybersecurity Risk Assessment into Model-based Requirements Engineering

Douraid Naouar, Jamal El Hachem, Jean-Luc Voirin, Jacques Foisil, Yvon Kermarrec

Towards the Integration of Cybersecurity Risk Assessment into Model-based Requirements Engineering

Douraïd Naouar*§, Jamal El Hachem†, Jean-Luc Voirin‡, Jacques Foisil‡, Yvon Kermarrec*§
*IMT Atlantique, Lab-STICC, F-29238 Brest, France, {name.lastname}@imt-atlantique.fr
†IRISA – UMR 6074, Univ. Bretagne-Sud, Vannes, France, jamal.el-hachem@irisa.fr
‡Thales Technical Directorate, SSI Systems Engineer, Brest, France, {name.lastname}@fr.thalesgroup.com
§Chair of Naval Cyber Defense, Brest, France, {name.lastname}@ecole-navale.fr

***Abstract*—Engineering projects requires to consider the increasingly significant needs and constraints regarding expected behaviors, services, quality and security. These requirements are introduced into system and software engineering projects as functional and non-functional properties. Satisfying such properties implies rigorous processes that steer the project, from the requirements identification and definition to the system deployment and maintenance. Model-Based System Engineering (MBSE) is an effective approach to address security requirements and risk assessment at the early stages of the development life cycle, which enables cost-efficient fixes. The aim of this work is to investigate how cybersecurity risk assessment could be integrated into model-based requirement engineering. We propose a Model-based Cyberisk Assessment (MBCA) method, that comprises: (1) A semantic alignment between risk assessment concepts and system modeling concepts and (2) A modeling language extension to represent security concepts and metrics throughout the system modeling life cycle. To illustrate our approach, validate its applicability and evaluate its expressiveness, we applied it to an industrial in-flight entertainment system.**

Keywords–Model-Based Systems Engineering, Security requirements, Risk assessment, System and security co-engineering

I. Introduction

Over the past few years, modern industrial systems such as automotive, medical, aerospace, and defense are becoming extremely complex due to the specificity of their services, behaviors, and requirements. Model-Based System Engineering (MBSE) has proven its efficiency to cope with the functional definition of the ever-growing system complexity [1] [2]. However, security features are more recent, and their integration in the system design phases raises new and specific challenges. The cybersecurity industry has grown exponentially over the past decade, vulnerabilities are identified on a daily basis, and new threats continue to emerge exploiting these vulnerabilities [3], making cybercrime one of the most significant risks faced by industries of all sizes and in all sectors [4]. Protecting an industrial system is becoming a very complex task. In addition to traditional problems, the complexity is amplified by Industry 4.0 [5], in which our dependency on services provided by cyber-physical systems is dramatically increasing.

It is essential to address these security challenges early at the requirement analysis and modeling phases to avoid time and cost wastage of later changes, prevent massive damages targeting the system functionalities, and impacting people's safety and security [6]. As a matter of fact, the INCOSE Vision 2025 [7], has included security, and particularly cybersecurity, as one of the eight key system characteristics desired by stakeholders. It hence proposes that system engineers should address cybersecurity as a fundamental system property that has to be understood, analyzed, and incorporated into system designs. In line with this, numerous methods guide users on how to benefit from MBSE when designing a system model, taking into account its security. However, a thorough review of these MBSE methodologies and frameworks[8][9] shows that none of the analyzed methods deals with the security risk assessment at the requirement and modeling phases of system development. Besides, communication between the system architect and security team, brought by a semantic alignment between risk analysis concepts and system modeling concepts, is barely addressed and capitalized. Therefore, our goal is to bridge the gap between system requirements modeling and analysis, and the analogous cybersecurity risks. To achieve this goal, we have to answer the research question *RQ: How to co-engineer system and security requirements allowing the integration of cybersecurity risk assessment into requirement engineering?*

MBSE is a key solution considering its ability to manipulate, create, manage and share models at a higher abstraction level, tailor generic modeling language (UML and SysML) with the security-related concepts, and perform security analysis with additional tools [10]. Nowadays, the design phase carried out by system architects and engineers remains an important aspect of MBSE activity, and it is used as a communication tool for monitoring progress throughout the project's lifetime. When developing complex systems, the security analysis is conducted upstream or in parallel with the design phase by security engineers and analysts. Even if efforts are made to consider each other's concerns, this activity remains a difficult task [11]. Similar to the approaches used for safety [12], quality [13], and other performance-based projects, cybersecurity should not be viewed as a one-time "project". It must be instead considered as functional elements and properties of the existing system elements, having a definition, representation, and impact on their surrounding environment to accommodate the emerging needs of risk representation and assessment at the requirement and modeling phases. Such process is an essential part of the so-called "security-by-design"[1] in which security concerns are considered at the very

[1]https://wiki.owasp.org/index.php/Security_by_Design_Principles

beginning of the system engineering effort, to prevent massive damages, to cut down the overall costs and risks of the project, and to permit trade-offs between cybersecurity concerns and other functional and non-functional concerns [14] [15] [16].

Consequently, we argue that MBSE and Risk Analysis approaches can be leveraged to identify, model, classify and analyze security risks. To answer our RQ, we propose the MBCA method as an extension of existing MBSE methods. MBCA encompasses: 1) A semantic and conceptual alignment between functional system modeling concepts and risk analysis concepts, these two notions often work on the same elements, but under different forms or vocabulary, therefore, an alignment is necessary to identify, couple and implement the shared concepts, as well as those not shared but necessary to perform a risk analysis; 2) A modeling language extension to represent security risk concepts and metrics, allowing by that an accurate risk modeling and later on assessment; 3) An implementation of our MBCA as an extension of the existing industrial MBSE Architecture Analysis and Design Integrated Approach (ARCADIA[2]) method and its modeling tool Capella, both developed by our industrial collaborator (Thales). We extended ARCADIA by incorporating the concepts from EBIOS Risk Manager[3], a method created by the French National Agency for Security and Information Systems (ANSSI) allowing the expression of needs and identification of security objectives.

This article's remainder is organized as follows: Section II introduces security requirements. In Section III, we investigate the related work for integrating cybersecurity risk analysis concepts at the system requirement and modeling phases. In sections IV,V and VI we present our proposed method, its implementation and application on an industrial example. Section VII discusses our results as well as the feedback from industrial system and security architects and experts. Section VIII concludes the article.

II. Background

A. Industrial needs in terms of security requirements

Mazeika [17] carried out a feasibility study to identify the cybersecurity needs and practices of industrial companies in many sectors, such as transportation, aerospace, defense, maritime, and health. In particular, results show that the answers to the question "Are the security requirements or other security artifacts represented (or linked) in your systems engineering models/documents?" were:

- No security artifacts produced. Security is approached as additional requirements on the system
- We currently only collaborate internally in our company
- Some system attributes that are relevant for security are modeled. Some model elements are also specifically created for security analysis purposes, mostly by linking security requirements with the elements model

These answers were very close to the needs identified during the discussions with our industrial collaborators: Thales, Naval Group and French Navy. They show that both systems and security engineers recognize the importance of co-engineering system and security, starting from the very early phases of the development life cycle. However, this co-engineering activity have not yet been formalized in practice by existing approaches.

B. Secure Systems Development Lifecycle

The Systems Development Life Cycle (SDLC) is a conceptual model used in project management to describe the stages of a system development project, from the initial feasibility study to the maintenance of the completed application. SDLC is used to define the phases and steps involved in the design of a system by giving a rigid structure and framework. It revolves mainly around five phases (requirements, design, development, testing, and deployment) where security procedures may be applied in each stage. In this work, to answer our RQ and properly integrate security at the very beginning of the project as suggested by the INCOSE, literature, and our industrial collaborators feedback, we will focus on the first and second phases of the SDLC process and their corresponding security activities.

- **Requirement phase:** In this phase, teams consider the project's functional requirements or solutions. The system analysis is conducted to study the system and to identify its objectives through structured analysis, allowing us to understand the system and its activities in a logical way. Moreover, it is also in this phase that the operational analysis is performed to ensure that the new system can meet its expectations by analyzing the needs.
- **Design phase:** This phase describes in details the specifications, features, and operations required to meet the functional requirements of the proposed system that will be implemented to bridge the gap between the problem area and the existing system. During this phase, the system development complex activity is divided into several smaller sub-activities, which coordinate to achieve the system's main objective through different types of system modeling such as Logical design, physical design, conceptual data modeling.

MBSE approaches, such as NATO Architecture Framework (NAF), SysML[18], ARCADIA [19], AADL[20] have been well known and used for years in the industry as system engineering frameworks that reinforce the application of detailed architecture modeling principles and best practices to system engineering activities throughout the development life cycle.

However, traditional development lifecycles do not mainly take security concerns into account. Therefore, there exist approaches that focus on security development techniques, methods, and tools such as the Secure System Development Life cycle SSDL [21]. Secure SSDL consists of a set of activities carried out to develop and deliver a system security solution. These activities are: risk assessment, threat modeling, static analysis, security testing, and security assessment. In our case, we will focus on the 1st and 2nd steps, that are correlated with the first two steps of the previously described SDLC process.

- **Requirement - Risk assessment:** This stage consists of activities to establish security requirements and to assess security needs. In this context, security risk assessment

[2]https://www.eclipse.org/capella/arcadia.html

[3]https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

[3]Figure modified form: https://www.checkmarx.com/glossary/a-secure-sdlc-with-static-source-code-analysis-tools/

allows the definition of functional system characteristics that might require a thorough security review.
- **Design - Threat modeling and design review:** Detailed system and architecture design are supported through security threat modeling with the aim of reducing the security attack surface.

A certain number of risk analysis methods have been developed to carry these steps: EBIOS 2010 [22] and EBIOS RM [23], MEHARI [24], OCTAVE [25], NIST SP 800-30 [26]. Most of these methods are conform to the security risk management process from the ISO 27005 standard and therefore have some similarities. They mostly consist first of all in proposing a systematic approach made up of simple steps, such as making an inventory of the system, representing it in one way or another, then identifying the risks based on the generic lists and assessing them using a well-defined scale. Moreover, conducting a risk analysis is a complex task requiring to be both precise and maintain an overview, covering all risks and situations while remaining homogeneous. However, SDLC and secure SDLC are currently two processes having their own life cycles and objectives while working with the same input elements. Conventional engineering captures a need, then declines it by progressively refining it in terms of a solution. It describes what stakeholders expect from the system, and how this latter achieves the requirements. In the security context, the approach is inverted: we must describe what the stakeholders fear from the system, and then how we manage to prevent the feared events from occurring. This inversion of the classic traceability pattern leads today to difficulties in identifying, estimating, and taking into account both system and security requirements. Besides, SDLC and Secure SDLC do not have common standards, methods, and frameworks for proper co-engineering activity.

In response to this challenge, in recent years, authorities and researchers have been proposing solutions to incorporate and represent security concepts directly in system models. To address co-modeling and risk co-assessment of both system and security, one of the most effective System Engineering (SE) approaches is Model-Based SE (MBSE). The fundamental advantage of MBSE is that it allows complexity management, risk and cost reduction, improved communication within multidisciplinary teams, and automated document generation. All these reasons justify the need to extend an existing MBSE language to model an industrial system considering security risk assessment specific properties. The extension should introduce security concepts to allow architectural level security requirement modeling and analysis.

III. Related Work

To answer our research question, we gain insight into the cybersecurity risk assessment's current status at the requirement and modeling phases. We reviewed existing approaches that jointly address MBSE and Risk analysis.

Researchers highlight in their investigations [27] the need to identify and address security risks during the system engineering life cycle, they do not cover the alignment or integration of all the elements and steps necessary to perform a risk assessment in the models.

In [28], the authors introduce an MBSEsec method aligned with the ISO/IEC 27001 consisting of a SysML/UML-based profile, security process definition, and recommendations, and how these security concepts based on the Unified Architecture Framework (UAF) could be defined with the SysML profile. This method has many benefits, in particular, the mapping of some security concepts into security modeling approaches and the fact that it is based on a common standard and profile. Nevertheless, this method has been designed to be used by security engineers and analysts and does not consider the benefits of co-defining these security concepts with system engineers.

In another work [29], the authors propose a model-driven based framework for security analysis by implementing the risk analysis method EBIOS and attack trees as UML profiles. This work aims to equip and help the security engineers without looking to collaborate with the systems teams, whose role is restrained from defining the system models' requirements.

Thales is currently working on security extension viewpoints. Thales teams have carried out a study in this direction to early identify possible threats, assets to be protected (information, capabilities, etc.), and some security measures to address the former [30]. This work lead to the first reflections on a real work of co-identification and co-definition of security elements through system engineering. However, this work is still at a very early stage, and it does not cover all the elements required to perform a risk analysis. Moreover, it does not take into account the dependency and impacts that these security concepts have on each other during the requirement and design phases of the system development life cycle.

The previously discussed studies lack a complete and applied approaches integrating all risk analysis concepts into the system engineering. None of them proposes a method (a language and its corresponding tool and processes), based on existing system modeling and risk analysis standards, for a co-engineering activity, not in a separate manner, but using a formalism understandable by both systems and security teams.

All these reasons justify the need to propose a modeling language or extending an existing one, such as SysML, to establish a more advanced formalization of the security requirements in the form of predominantly function-driven modeling as opposed to requirements-driven modeling usually employed. The security elements of the resulting models should then be considered, for engineering, as requirements carried by the model. These elements should be co-defined and co-modeled, and their dependencies, impacts, and treatment should be traced across all models and viewpoints. Moreover, the modeling language should allow the exchange and communication of results in a precise way with decision-makers.

IV. The proposed Model-Based Cyberisk Assessment (MBCA)

To address these challenges, we have worked on a semantic alignment of concepts from security risk analysis methodologies and model-based system engineering approaches. For this purpose, we studied worldwide approved norms and standards in both fields. Moreover, we traced their adaptations and implementations in different methods used in the industry. In addition, we aligned the two domains from both abstract and operational viewpoints in order to identify the specific security concepts to be implemented in the overall system modeling process.

A. System Modeling Basic Concepts

MBSE is a system engineering methodology that focuses on creating and exploiting domain models as the primary means of information exchange between, all teams involved in the engineering process rather than a method which relies on document-based information exchange. These models offer an effective means to explore, update, and communicate aspects of the system to stakeholders while significantly reducing or eliminating reliance on conventional documents. The ISO/IEC/IEEE 15288 and 1220 standard identifies a generic architecture development workflow composed of four processes to support SE.

- **Operational analysis:** Focuses on analyzing stakeholder needs and concerns and translating them into requirements specifications. Based on stakeholder needs, high-level business or mission objectives are identified and modeled using specific artifacts to create the most abstract formulation of requirements, called use cases;
- **System requirement analysis:** The stakeholder requirements are used to derive the system functional and non-functional requirements. They are used to identify the internal functions that the system should perform. Functional architecture of the system is subsequently described in functional terms independent of its technology;
- **Logical architecture definition:** A logical architecture is an abstract representation of the system components, independently from their technical solutions, in a way that every system function can be performed by a corresponding logical component;
- **Physical architecture definition:** This viewpoint defines the system's physical architecture, consisting of an arrangement of physical elements. The purpose of this architecture is to develop a technical solution to a logical architecture.

To be able to define and implement our method, we built a functional description of the concepts[4] and their relationships defined during these phases and implemented throughout the four modelling phases (figure 1).

- **Stakeholder:** Individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations;
- **Operational mission:** The specific task, duty, or function defined to be accomplished by a system;
- **Operational objective:** The ability of a system to execute a particular course of actions or achieve a desired effect under a specified set of conditions;
- **Scenario:** Description of an imagined sequence of events that includes the interaction of the product or service with its environment and users, as well as interactions among product or service components;
- **Activity:** Task or action performed to achieve the desired outcome;
- **Interactions:** Communications, cooperations, and collaborations among the different nodes (system, stakeholders,etc.) that act together, through performed functions and interactions, to solve both local and strategic problems;
- **Data:** A data must be taken in its broadest sense, it can represent a signal, an image, an information, a physical state, or a unit of magnitude.

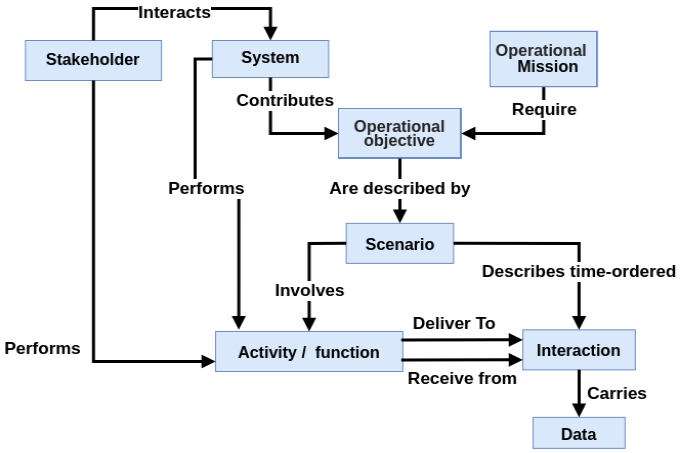

Figure 1. Functional description of the concepts and their relationships defined during the system definition

B. Risk Assessment Basic Concepts

In recent years, numerous standards and guidelines have been proposed in the field of information system security. In our MBCA method, we focus on the ISO 27000 series including standards that define good practices for information systems security management (in particular ISO 27001 represented in Figure 2) and the ISO 31000 series that describes the principles and guidelines for risk management at strategic and operational levels (in particular their implementation and representation in internationally recognized risk analysis methods such as EBIOS, EBIOS RM, OCTAVE ALLEGRO, and NIST SP-800-30) to ease the applicability of our method in industrial/operational environments. We summarized these concepts and their definitions in Table I.

C. Semantic alignments between system requirement and cybersecurity requirement concepts

After identifying the basic concepts from MBSE and cybersecurity requirements assessment domains, we defined a semantic alignment between the two domains. This alignment consists of lining up the entities (terms, concepts, roles) belonging to both domains in order to reach thereafter a common and shared vocabulary and semantics between these disciplines, as well as to define the cybersecurity concepts and properties to be attached to the model elements. As shown in the figure 3:

- Al.a: **Threat** is aligned with the **stakeholder** through the relationship ***constitutes***. In fact, a **threat** encompasses all potential causes of an incident. Consequently, from a functional point of view, the **stakeholder** of conventional engineering, conceived as legitimate, ***constitutes*** a part of the potential **threat** risks - sometimes unintentionally through their proximity and interactivity with the **system**
- Al.b: **Asset** is aligned with **Operational objective**, **activity/function**, **interaction**, and **data** through the relationship ***considered as***
- Al.c: **Control** is aligned to **activity/function**, **interaction**, and **data** through the relationship ***Applies to***. In fact,

[4]https://standards.ieee.org/standard/15288-2015.html

[5]https://www.iso.org/obp/ui/iso:std:iso-iec:27000:ed-5:v1:en

ISO 27001	EBIOS (2010)	EBIOS RM (2018)	OCTAVE allegro (2007)	NIST SP 800-30 (2012)	Definition[5]
Asset	Supporting, primary asset	Supporting, Business asset	Asset, Critical information asset, Asset container	Organizational operation, Asset, Individual and Stakeholder	Elements that can be considered as a subject for security analysis / Something in the system and/or its environment, to be protected from negative consequences
Role	Business, Depository manager, Owner	Business, Depository manager, Owner	Information asset owners, Information asset custodian	Information, System Owner	The asset owner, is responsible for the effective management of the asset over its whole lifecycle. It can be different from legal ownership, and it can be done at an individual level, department, or other entity
Requirement	Security criteria	Security criteria	Security requirement	Security requirement	A type of rule that captures a formal statement to define security laws, regulations, guidances, and policies
Threat	Threat source	Risk origin, Stakeholder	Actor	Threat Source	Potential cause of an unwanted incident, which can result in harm to a system or organization
Security incident	Feared event, Threat scenario	Feared event, Strategic and Operational scenario	Threat scenario, Threat tree	Threat tree	Single or a series of unwanted or unexpected information security events/exploit that have a significant probability of compromising business operations and threatening information security;
Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability, Predisposing Condition	A weakness of an asset or control that can be exploited as a threat
Exploit	Exploit	Elementary action	Access/means	Exploit	Is an identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security-relevant
Control	Security control	Security measure	Control	Security control	Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature
Control objective	Risk treatment	Risk treatment	Mitigation approach	Risk Mitigation	Statement describing what is to be achieved as a result of implementing controls

TABLE I. A summary of main security concepts used in risk assessment methods

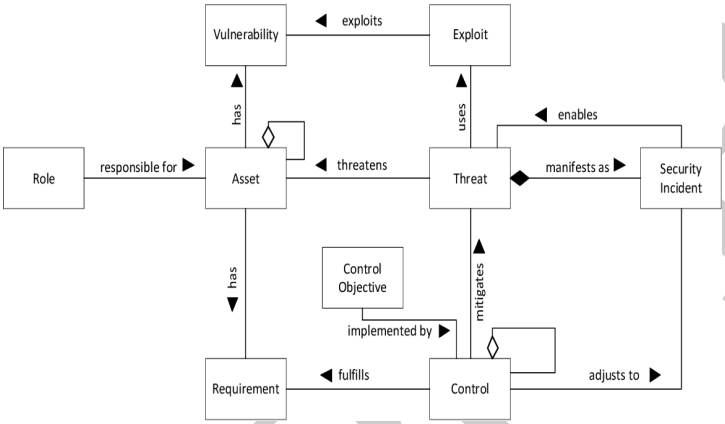

Figure 2. ISO 27001 metamodel from [31]

Control includes the means to manage a risk, and from a functional point of view, these measures will be ***applied to*** the system's elements, such as the tasks or performed actions and the **interaction** between them. The concept of **Asset** encompasses the key elements to be considered in the security analysis. From a functional point of view, the services and functionalities that the system performs, the necessary actions and tasks for their realization, the means of communication between these elements, and the information transmitted must be ***considered as*** **assets** (service-kind or information-kink) to be protected

- Al.d: **Security incident** is aligned to **scenario** through the relationship ***occurs as***. Both concepts rely on the notion of sequences of events, and both of them base their sequence on the previously aligned concepts **activity/function**, and **interaction**. A **Security incident** ***occurs as*** a specific scenario from the attacker's point of view, linking in such manner the sequences of events that the attacker will carry out or go through to achieve his objectives.

V. Implementation of the proposed MBCA method as an extension of an industrial modeling language and Workbench: ARCADIA

After defining the MBCA MetaModel, we implemented it, as an extension of the following risk analysis and system engineering industrial methods, conforming to the standards presented in the subsection IV-A and IV-B.

A. ARCADIA : An industrial system engineering method

To exhibit the proper MBSE values, Architecture Analysis Design Integrated Approach (ARCADIA) serves as an appropriate engineering method and modeling language choice, along with Capella, its corresponding modeling tool/graphical editor. ARCADIA and Capella are actively maintained with well-established documentation, and they are extensible and interoperable with existing SysML-based languages and tools. Indeed, ARCADIA, as well as Capella, are open-source, widely used around the world by manufacturers such Rolls Royce (UK), Virgin hyperloop (USA), Deutsche Bahn (GER), Comac (Chine) without forgetting the French industry, and particularly, their author Thales[6], a French multinational company that designs and builds mission-critical systems and provides services for space, aerospace, defense, transportation, and security markets. Thales is the 8th largest defense contractor in the world [32] and a European leader in cybersecurity[7].

ARCADIA is conform to the MBSE standards, particularly the ISO 15288 process that we used as a basis for our MBCA method, as detailed in section IV-A.

[6]https://www.thalesgroup.com/en

[7]https://www.thalesgroup.com/en/markets/defence-and-security/cyberdefence-solutions

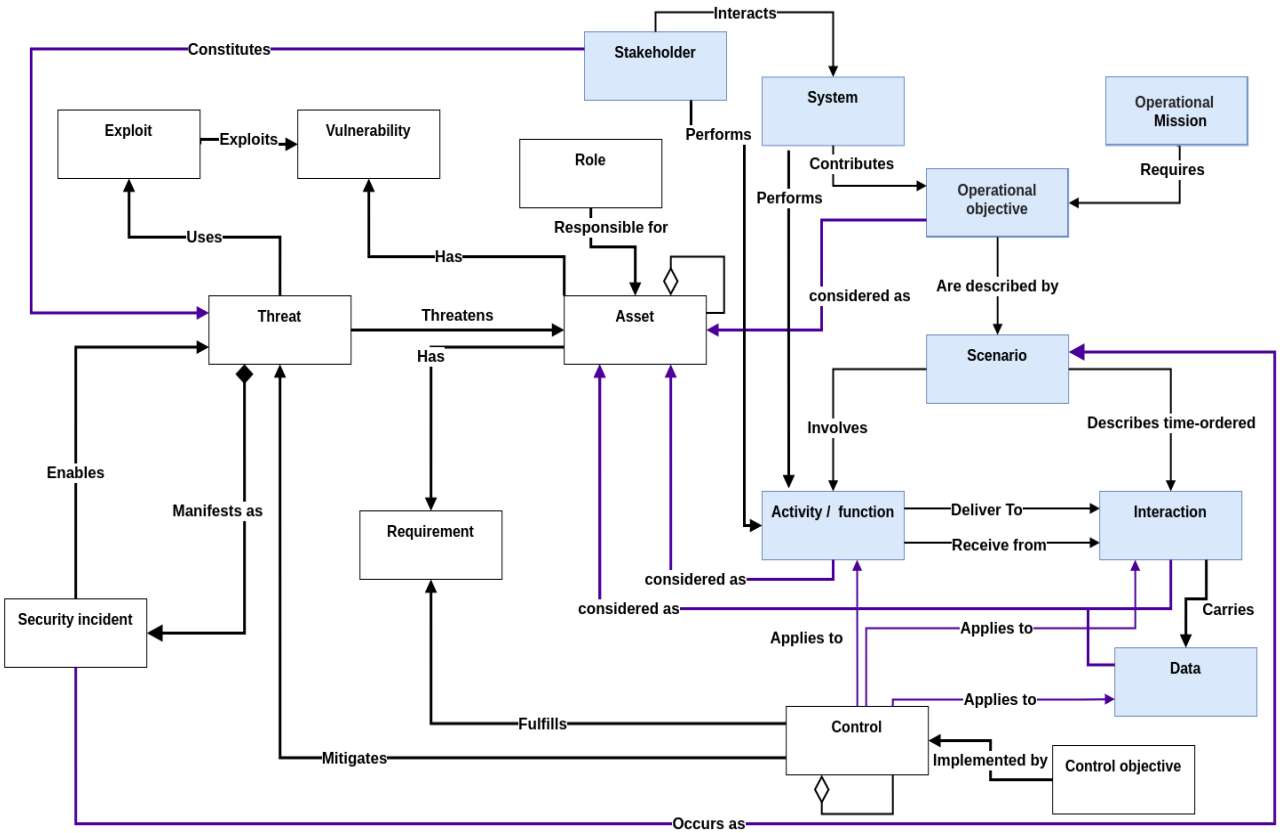

Figure 3. MBCA semantic alignment between System Modeling and Risk Analysis approaches

In this paper, we focus on the elements defined during the first and second viewpoints (Stakeholders, operational mission, operational objectives, scenario, activities, interactions and data). In fact, these elements cover a large part of the system concepts that have a strong impact on the subsequent system development activities [33]. Therefore, we implemented in ARCADIA the semantic alignments related to these elements as shown in columns 3 and 4 of Table II.

B. EBIOS RM : An industrial requirement analysis method

EBIOS Risk Manager (EBIOS RM) is a very well-known method for assessing and treating digital risks. EBIOS was born from a reflection and collaboration between the French National Agency for Security and Information Systems (ANSSI) and several major actors, embodied by the Club EBIOS. It comes from the experience accumulated over many years and from new industrial needs. Based on proven concepts, such as the notions of support assets and feared events, it has updated the risk analysis approach by taking into account the relationship with their ecosystem, ways to assess and validate the acceptable level of risk for a continuous improvement approach. Besides, it makes available resources and arguments that are useful for communication and decision-making within the organization and with regards to its partners. In this paper, we cover and represent the elements and objectives illustrated in the first two workshops, that represent the basis of any specific or advanced risk analysis.

- **Workshop 1 - Scope and security baseline:** This first workshop serves to lay the foundations of the analysis by listing the missions, business assets, and supporting assets, shareholders related to the studied object. We identify the feared events associated with the business assets and assess the severity of their impacts;
  - **Business asset:** Is an asset of high value and importance for the organization to accomplish its missions. This can be a service, a support function, a step in a project, and any related information or know-how;
  - **Feared event:** Is associated with a business asset and harms a security need or criterion of the business asset;
  - **Stakeholder:** Stakeholder of the ecosystem that is likely to form a privileged vector for attack, due for example, to their privileged digital access to the studied object, their vulnerability or their exposure to the risk;
- **Workshop 2 - risks origins:** The second workshop proposes a targeted study of the sources of risk and the intended high-level targets, called target objectives. The risk source-target pairs deemed the most relevant are selected at the end of this workshop. The results are formalized in a mapping of the risk origins;
  - **Risk origin:** Element, person, group of persons or an organization that can generate a risk;
  - **Target objectives:** End purpose targeted by a risk origin, according to its motivations.

C. Semantic alignment

Table II summarizes the main semantic alignments between the ISO 27001 cybersecurity concepts and their implementations in EBIOS on one side (columns 1 & 2); and the ISO

15288 SE concepts and their implementations in ARCADIA on the other (columns 3 & 4), along with the justification of these alignments (column 5). Moreover, figure 4 details the implementation of the semantic alignments (Al.a - Al.d defined in section IV and illustrated in figure 4) as an extension of ARCADIA and EBIOS RM (Al.1 - Al.4), as follows:

- Al.1: **Threat** is implemented through the **Stakeholder** and **Risk origin** concepts in the EBIOS RM method. The **Risk origin** represents all external element, person, group of persons or an organisation that can generate a risk. **Stakeholder** concept covers the elements that are part of the system's ecosystem and likely to form a privileged vector for attacks. Likewise, the SE concept **Stakeholder** is implemented through the concept **entity** in ARCADIA to represent the elements (person, information system, organization) that interacts directly or indirectly with the system and its users. Conforming to Al.a **Risk origin** was aligned to **Entity** using the ***constitutes*** relationship.
- Al.2: **Asset** concept is implemented through the **Business and Supporting asset** in the EBIOS RM method. The **business asset** includes all important components allowing an organisation to accomplish its missions through two forms: **Service-kind** and **information-kind**. The **supporting asset** covers the system components on which one or several **business assets** are based. Likewise, the SE concept of **Operational objective**, **Activity/Function**, **Interaction**, and **data** are implemented in ARCADIA through **capability**, **function/activity**, **interaction/exchange**, and **Data**. Consequently, conforming to Al.b Service-kind **Business assets**, are aligned with the system **Capability**, critical **Function/Activity**, and specific means of **Interaction** through the relationships ***Considered as***. Similarly, exchanged **Data** requiring particular requirements or vigilance are treated as an information-kind **Business assets**. As for the **Supporting assets** they will cover all the **Function/activity**, **Interactions/exchange** and **Data** allowing the realization of the **Capability** through the relationships ***Considered as***.
- Al.3: **Control** is implemented through the **Security measure** concept in the EBIOS RM method. **Security measure** represents means of dealing with a risk, first in the form of requirements and later in the form of security measures. Likewise, the SE concepts **Activity/Function**, **Interaction** and **Data** are implemented in ARCADIA through **Function/Activity**, **Interaction/Exchange**, and **Data**. Therefore, conforming to Al.c **Security measure** is aligned with **activity/function**, **interaction** and **data** concepts through the ***applied to***
- Al.4: **Security incident** is implemented through the **Feared event**, **Strategic scenario** and **Operational scenario** concepts in the EBIOS RM method. Indeed, the **Feared events *Based on* security criteria** and associated to the system's **Business asset**, represents a damaging attack to the system. The **strategic scenarios** with the evaluation of the ecosystem through the **Stakeholder**, defines the first scenarios starting from the **Risk origin** and evolving towards the **Targeted objective**, taking into account the entry point brought by the **Stakeholders**. Finally, **Operational scenario** is a chain of **Elementary actions** applying to the **Supporting asset** of the studied object. Likewise, the SE concept **scenario**, can be found in ARCADIA under the same name. Consequently, conforming to Al.d **Feared events, Strategic and Operational Scenario** were aligned with **Scenario** through the relationship ***Occurs as***

We benefit from our collaboration with Thales to collect the needed input and evaluate the outcome of this work, the validity of our method, and its usefulness for modeling and assessing security risks at the requirement level. We had numerous meetings with the Thales team. We exchanged with the different experts several emails and documents to certify the efficiency of the previously mentioned considerations, results, and the prominent potential of the MBCA method to improve the integration of cybersecurity risk assessment into requirement engineering. Several feedbacks and refinements took place, leading to the presented semantic alignments and their implementations.

VI. Application of MBCA on an industrial case

We present in this section an In-Flight entertainment System (IFE) as a study domain, on which we have applied our MBCA method to integrate cybersecurity concerns into systems engineering activities to improve security assessment and to assist decision making at the requirement level. Systems engineering emphasizes the analysis of the problem before jumping straight to the solution. The first step is to determine the **missions** - or more generally the motivations, expectations, goals, objectives, intentions, etc. - of the future users of the system, as well as the **capabilities**, **entities**, and **actors** required to fulfill these **missions**. In our IFE system, consists in entertaining passengers and transmitting imposed videos and announcements. This mission will have to fulfill three **capabilities**: "Entertain during flight", "Perform flight On-Board Announcement," and "Implement a commercial strategy."

A. Application of Al.2 alignment

Conforming to the **Al.2** alignment, the **Capabilities** are aligned with the **Business assets** and are handled as such. The system engineer defining the **Capability** will be able to participate in the definition of the security requirements, particularly due to his knowledge on the importance of this one in the global and functional realization of the project. The security engineer brings the evaluation matrix[8] and the **security criteria**, and the system engineer uses his expertise and knowledge of the system to evaluate it. The **capabilities** through exchanges between teams will be assigned a numerical value, usually between 0 and 4, depending on the completeness of the matrices and which allows evaluating the importance of each **security criteria**: confidentiality, integrity, availability, and traceability (CIAT). For instance, the notation [4301] is assigned to the **capability** "perform flight on-board announcement" which indicates that: 1) the integrity requirement is important without being critical, 2) the manipulated service must absolutely remain available, 3) the information used by this service is public, and 4) there is no specific need for access traceability. The **capability** with a **security criteria** considered "critical" or important enough to be taken into account will then be developed in the form of **feared events**. The **functions**, **interactions**, **data** defined later can, if judged critical (for example, a **data** requiring a certain level of

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

Cybersecurity concepts (ISO 27001)	Cybersecurity concepts (EBIOS RM)	Systems engineering concepts (ISO 15288)	Systems engineering concepts (ARCADIA)	Semantic Alignment
Threat	Risk origin, Stakeholder	Stakeholder	entity	Elements (person, information system, organization or source of risk) that interacts directly or indirectly with the system A threat can be internal or external to the organization to which the object of the study belongs.
Asset	Supporting and Business asset	Operational objective, activity / function, interaction, and data	capability, function / activity, interaction, and data	Those information resources, mission/business processes, and/or critical programs that are of particular interest to potential or actual adversaries. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation).
Control	Security measure	activity / function, interaction and data	function / activity, interaction, and data	The operational, and technical elements (its components, processes, data, safeguards or countermeasures) prescribed for a system to carry out its objectives or to protect the system.
Security incident	Feared event, Strategic and Operational scenario	scenario	scenario	How the system and its actors interact in the context of a system capability/service. These interactions often take the form of sequences of actions and in the case of an attacker their objective is to misuse these actions to achieve their own objective

TABLE II. Mapping between cybersecurity (EBIOS RM) and systems engineering (ARCADIA) concepts

classification (Defense or Confidential Secret ...)) modify the score of one or more **capability security criteria**, or at least be considered as specific **feared events** to the **capability**. If we take our previously noted **Capability** and its **Security criteria**, we may consider it appropriate to develop two feared events, one about its integrity: "Perform inaccurate flight on board announcement", and the other about its availability: "unavailability to perform flight on board announcement".

B. Application of Al.1 alignment

Once accomplished, **Risk origins** profiles will have to be defined from metrics such as motivation and resources as illustrated in the knowledge bases proposed in the ANSSI methodological sheets [8] to estimate the level of dangerousness, to subsequently associate the **risk origins** with the **feared events** they are likely to perform. In our context, we have identified three **risk origins**: "RO1: Dissatisfied employee", "RO2: spy" and "RO3: component subcontractor" that may have objectives related to our **feared events**. We have estimated that the "spy" and the "dissatisfied employee" will be more inclined to perform the feared integrity event, and the "component subcontractor" the feared availability event. Conforming to the **Al.1** alignment, the **stakeholder** concept is aligned with **entities** and **actors** and is handled as such. Stakeholders are assigned with metrics [8] (dependence, exposure, trust ...) to define their threatening level regarding the **capabilities**. These definitions are done in a unitary way in each corresponding diagram. Figure 5 illustrates a rough representation of what it could give if we apply this alignment to a specific **capability**. After defining, evaluating, and linking these concepts, "synthesis" views can be put forward to support the communications between different teams and stakeholders, the re-evaluation of elements, and to subsequently plan the flow of action with decision-makers. For example, at this point, the first outcome that we can illustrate is a general view of the alignments between the **feared events(FE)** and the **risk origins(RO)**, allowing a clear understanding of the critical couples, that should be treated in priority (figure 6). A representation in the form of radar could be chosen to select priority risk **RO/FE** pairs. A purple dotted area could visually represent the **RO/FE** pairs, the radial distance corresponds to the level of pertinence assessed for the element (the closer the circles are to the center, the more dangerous they are considered to be for the organization). Selecting **RO/FE** pairs is done by favoring pairs located near the center and sufficiently separated from one another to obtain a panel of risk origins and target objectives that are varied. A second outcome consists in a representation of the **actors** and **entities** rankings, according to their threatening level towards our system, or a ranking of our **business assets** according to their severity. In our application, we can see that the couples "dissatisfied employee / Perform inaccurate flight on board announcement" and "component subcontractor/unavailability to perform flight on board announcement" are the closest of the center, and therefore they will be treated in priority. The objective of these synthesis views is to support teams communications, to verify the coherence of our system "context and functionality" identification and evaluation.

C. Application of Al.3 and Al.4 alignment

Once this base of study is realized, we can subsequently unroll our analysis more deeply with the system analysis viewpoints, where we begin to distinguish between what will be realized by our **systems** and what will be treated by our **actors** and **entities**. Therefore, the **functions/activities** that will be performed by the **entities** and **actors** and those to be performed by our system, are identified. Conforming to the **Al.3** alignment, scenario concept is aligned with **feared events**, which together with its **Capability**, identify the impacted **functions/activities**, **interaction** and **data**. Afterward, the first **security measures** could be elicited. These measures should be respected and applied to the **stakeholders** or to the **system** in the form of security requirements. Through these scenarios of feared events, **strategic scenarios** could be defined, starting from the **risk origin** to reach its targeted objective (our **capability**), allowing the identification of the entry points to our system. Viewpoints 3 and 4 deal with the refinement of

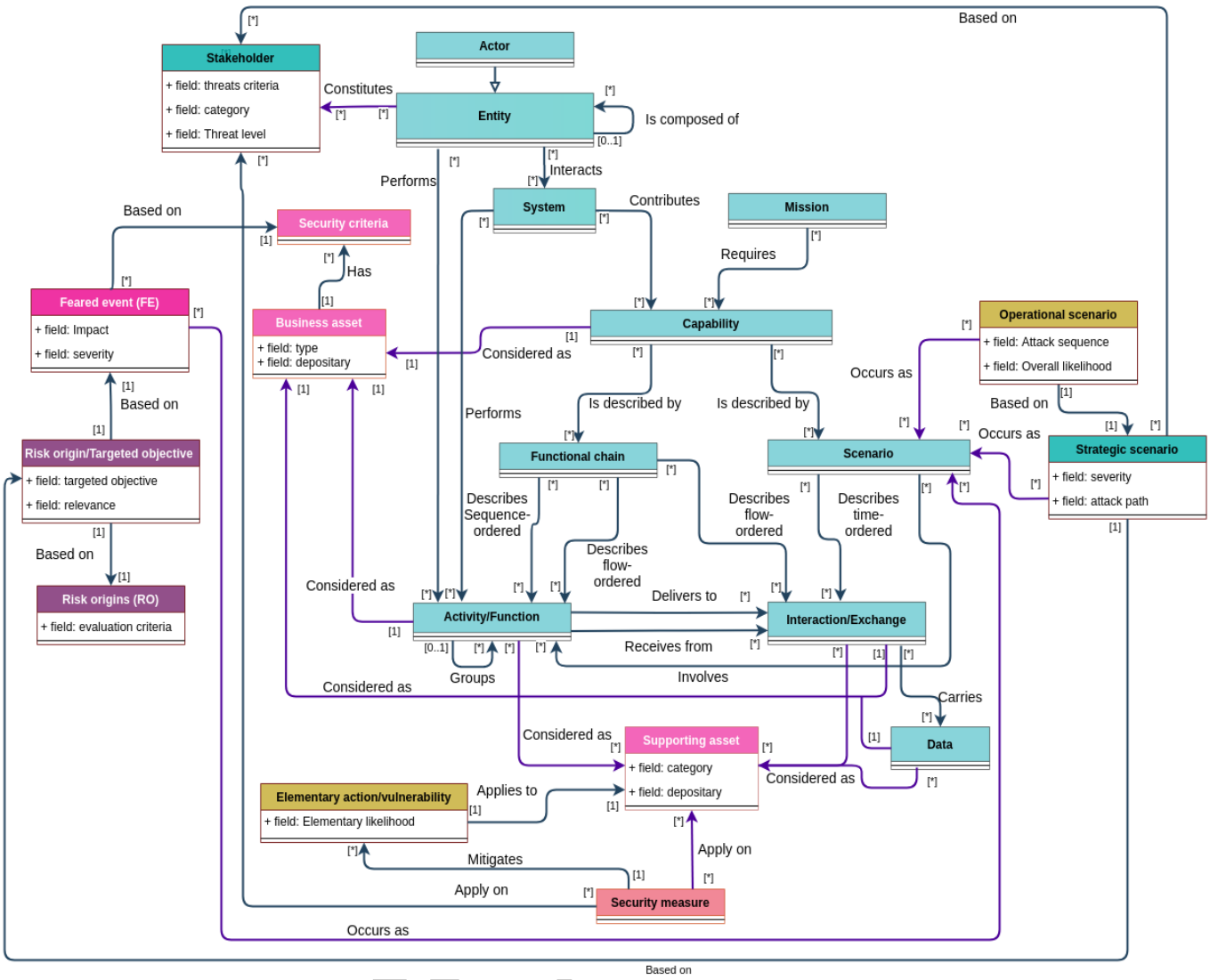

Figure 4. Implementation of the MBCA semantic alignment as an extension of ARCADIA

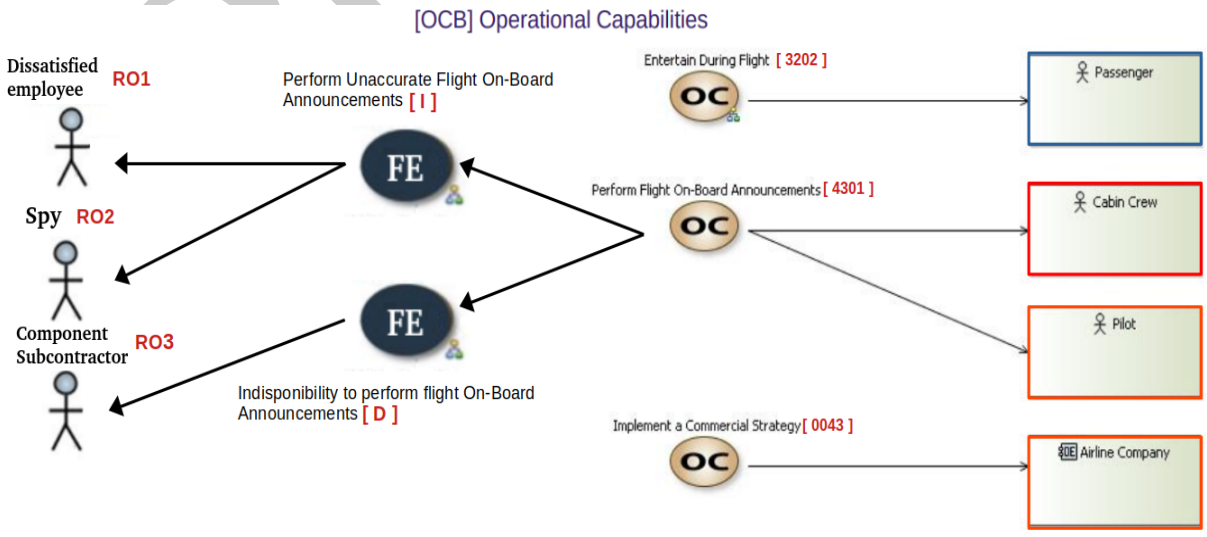

Figure 5. Operational Capabilities diagrams with security concepts

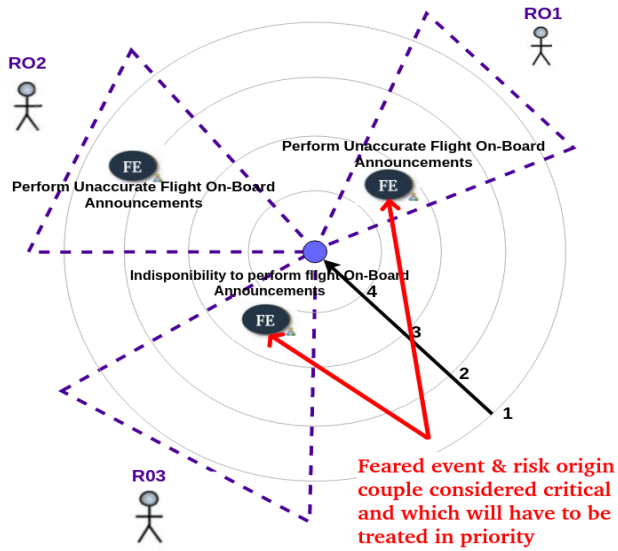

Figure 6. Synthesis view of the feared event / risk origin coupling

the system's **functions/activities**, **interaction**, and **data** from their logical architecture to their physical implementation. In these Viewpoints, conforming to the **AI.3** alignment, the attack scenarios will be realized, and the security requirements will take shape as **security measures** applied to operational elements. This alignment being part of the SE modeling method benefits from all the advantages concerning the traceability of the elements between each viewpoint, making it easier to trace and comprehend the security concepts impacts through the different viewpoints. In addition to being able to identify the problems that will occur or the measures to be implemented early, the advanced modeling elements designed will ease and structure the communication between the teams and decision-makers without needing knowledge or an understanding of the risk analysis concepts and used techniques.

VII. Discussion and Lessons Learned

Recently, new methods have emerged to introduce risk analysis at the system development design phase [34][35][36]. Most of them propose combining quantitative methods with the so-called qualitative risk analysis techniques generally carried out via attack trees. In particular, EBIOS RM encompasses operational and strategic scenarios concepts in the form of attack trees. It proposes a multi-step method going from the context definition to risks identification and assessment from an operational point of view, taking into account the ecosystem to identify the attacker's potential entry points into the system.

Other approaches such as ALL4TEC - Cyber Architect[9], EGERIE-SOFTWARE[10], Risk'n Tic[11], have tooled risk analysis methods, allowing the automation of some risk analysis steps through the use of online knowledge bases. This leads to a more accurate risk assessment, but the latter is mostly performed by the security teams. Few communications occur with the business teams, but the absence of a shared "model-centric" reference and common vocabulary leads to inconsistencies, and poor mastering of side-effect in case of evolution.

Therefore, even though recently proposed approaches and tools help consolidating the risk analysis process, they do not offer the means to co-engineer system and security requirements, and do not propose a structured and semantically justified process to integrate cybersecurity risk assessment into requirement engineering. Moreover, in those approaches, risk analysis is dissociated from system engineering (from a semantic, methodological, and life cycle point of view), and therefore when the risk analysis is modified/updated, the consideration of its impact on the system engineering remains very limited, and vice-versa. Consequently, the existing approaches and tools do not answer our research question, and accordingly do not fully satisfy the industrial need (as testified by our industrial collaborators).

Our MBCA method goes beyond existing work to integrate risk analysis into SE, based on standard-compatible concepts. MBCA proposes fundamental semantic alignment to facilitate the collaboration, communication, and knowledge sharing between system and security teams. Through our discussions with industrial collaborators, we were able to see the relevance of business expertise when carrying out a risk analysis. Therefore, we proposed a method built upon business expertise to identify in a precise way the critical elements, thus allowing a framed/focused evaluation without irrelevance caused by a lack of domain knowledge or a combinatorial explosion of non-essentiel risks and assets.

To capitalize on this work, we identified a number of possible perspectives that would advance our research. Some of them are motivated by ongoing work and others by the interest and need of our industrial collaborators. Firstly, we intend to improve/specify the definition of EBIOS RM security metrics, in particular those of the fourth workshop, for a better consideration of the system's element. Secondly, we plan to apply the MBCA method to a more representative large-scale case study illustrating a "complex naval-type defense system". Thirdly, it may be worthwhile to define alignments with safety processes to consider qualification and certification documents.

VIII. Conclusion

This paper proposes a Model-based method for cybersecurity risk assessment named (MBCA), conform to the ISO/IEC 27001 and 15288 standards. To illustrate our method, we implemented it as an extension of an industrial SysML-based method (ARCADIA) and we showed its applicability to an in-flight entertainment system. The results from this industrial example demonstrates that MBCA supports a co-engineering activity by combining expertise from both system and security teams. This allows the identification of the necessary system assets to be protected based on an analysis of the associated security risks/feared events, ensuring by that a valuable risk assessment. The results were validated with system and security engineers from Thales, who considered the MBCA as a promising solution for cybersecurity risk assessment at the requirement engineering phase. In the future, we plan to extend MBCA to ensure a continuous risk analysis build upon newly added vulnerabilities and cyber-attacker profile analysis. Moreover, we intend to apply the MBCA method on a large-scale industrial case study, and consequently refine it according to the experts feedback.

[9]https://www.all4tec.com/en/cyber-architect-en/
[10]https://egerie-software.com/en/egerie-risk-manager/
[11]https://www.riskntic.com/en/

REFERENCES

[1] S. Bernardi, J. Merseguer, and D. C. Petriu, *Model-driven dependability assessment of software systems*. Springer, 2013.

[2] B. Selic and S. Gérard, *Modeling and analysis of real-time and embedded systems with UML and MARTE: Developing cyber-physical systems*. Elsevier, 2013.

[3] B. Runciman, "Cybersecurity report 2020," *ITNOW*, vol. 62, no. 4, pp. 28–29, 2020.

[4] C. Ventures, "2019 official annual cybercrime report," 2019.

[5] K. Schwab, *The fourth industrial revolution*. Currency, 2017.

[6] J. E. Hachem, V. Chiprianov, M. A. Babar, T. A. Khalil, and P. Aniorte, "Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems," *Journal of Systems and Software*, vol. 162, p. 110484, 2020.

[7] B. Beihoff, C. Oster, S. Friedenthal, C. Paredis, D. Kemp, H. Stoewer, D. Nichols, and J. Wade, "world in motion-systems engineering vision 2025, international council on systems engineering," 2014.

[8] D. Mazeika, A. Morkevicius, and A. Aleksandraviciene, "Mbse driven approach for defining problem domain," in *11th System of Systems Engineering Conference (SoSE)*. IEEE, 2016, pp. 1–6.

[9] A. Morkevicius, L. Bisikirskiene, and N. Jankevicius, "We choose mbse: What's next?" in *Complex Systems Design & Management*, G. Auvray, J.-C. Bocquet, E. Bonjour, and D. Krob, Eds. Cham: Springer International Publishing, 2016.

[10] P. H. Nguyen, S. Ali, and T. Yue, "Model-based security engineering for cyber-physical systems: A systematic mapping study," *Information and Software Technology*, vol. 83, pp. 116–135, 2017.

[11] N. Messe, N. Belloir, V. Chiprianov, J. El-Hachem, R. Fleurquin, and S. Sadou, "An asset-based assistance for secure by design," in *27th Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, 2020, pp. 178–187.

[12] R. A. Stephans and J. Stephenson, *System safety for the 21st century*. Wiley Online Library, 2004.

[13] R. W. Ferguson, S. C. Fowler, and R. C. Creel, "A method for assessing technical progress and quality throughout the system life cycle," Carnegie-mellon univ pittsburgh pa software engineering inst, Tech. Rep., 2009.

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

[15] J. P. Elm and D. R. Goldenson, "The business case for systems engineering study: Results of the systems engineering effectiveness survey," Carnegie-mellon univ pittsburgh pa software engineering inst, Tech. Rep., 2012.

[16] B. L. Papke, "Enabling design of agile security in the iot with mbse," in *12th System of Systems Engineering Conference (SoSE)*. IEEE, 2017, pp. 1–6.

[17] D. Mažeika and R. Butleris, "Integrating security requirements engineering into MBSE: Profile and guidelines," *Security and Communication Networks*, 2020.

[18] J. Holt and S. Perry, *SysML for systems engineering*. IET, 2008, vol. 7.

[19] P. Roques, "MBSE with the arcadia method and the capella tool," in *8th European Congress on Embedded Real Time Software and Systems*, 2016.

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

[21] M. Howard and S. Lipner, "The security development lifecycle, vol. 8," *Redmond: Microsoft Press. Google Scholar Google Scholar Digital Library Digital Library*, 2006.

[22] A. 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.

[23] *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.

[24] C. C. 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.

[25] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, Tech. Rep., 2007.

[26] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Sp 800-30. risk management guide for information technology systems," 2002.

[27] J. Jürjens and P. Shabalin, "Tools for secure systems development with {UML}," *International Journal on Software Tools for Technology Transfer*, vol. 9, no. 5, pp. 527–544, 2007.

[28] D. Mažeika and R. Butleris, "Mbsesec: Model-based systems engineering method for creating secure systems," *Applied Sciences*, vol. 10, no. 7, p. 2574, 2020.

[29] R. Abdallah, N. Yakymets, and A. Lanusse, "Towards a model-driven based security framework," in *3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*. IEEE, 2015, pp. 639–645.

[30] J. Navas, J.-L. Voirin, S. Paul, and S. Bonnet, "Towards a model-based approach to systems and cyber security co-engineering," in *INCOSE International Symposium*, vol. 29, no. 1. Wiley Online Library, 2019, pp. 850–865.

[31] D. Milicevic and M. Goeken, "Model driven information security management - evaluating and applying the meta model of {ISO} 27001," in *AMCIS*, 2011.

[32] S. F. Sheet, "The sipri top 100 arms-producing and military services companies," 2019.

[33] J.-L. Voirin, *Conception architecturale des systèmes basée sur les modèles avec la méthode Arcadia*. ISTE Group, 2018, vol. 3.

[34] J. Martinez, J. Godot, A. Ruiz, A. Balbis, and R. Ruiz Nolasco, "Safety and security interference analysis in the design stage," in *Computer Safety, Reliability, and Security. SAFECOMP Workshops*, A. Casimiro, F. Ortmeier, E. Schoitsch, F. Bitsch, and P. Ferreira, Eds. Springer International Publishing, 2020.

[35] G. Pedroza, "Towards safety and security co-engineering," in *Security and Safety Interplay of Intelligent Software Systems*, B. Hamid, B. Gallina, A. Shabtai, Y. Elovici, and J. Garcia-Alfaro, Eds. Springer International Publishing, 2019.

[36] E. Rios, A. Rego, E. Iturbe, M. Higuero, and X. Larrucea, "Continuous quantitative risk management in smart grids using attack defense trees," *Sensors*, vol. 20, no. 16, p. 4404, 2020.