Towards Joint SoS and Threat Mission-based Modeling for Operational Impact Identification

Jesús Sánchez, Jérémy Buisson, Jamal El Hachem, Nicolas Belloir

Towards Joint SoS and Threat Mission-based Modeling for Operational Impact Identification

Jesús Sánchez*, Jérémy Buisson†, Jamal El Hachem‡* and Nicolas Belloir‡§
*Université Bretagne Sud, F-56000 Vannes, France
†École de l'Air et de l'Espace, CRéA, F-13300 Salon de Provence, France
‡UMR CNRS 6074, IRISA, F-56000 Vannes, France
§Académie Militaire de St Cyr Coëtquidan, CReC St Cyr, F-56380 Guer, France
sanchezr@univ-ubs.fr, jeremy.buisson@ecole-air.fr, first.last@irisa.fr

***Abstract*—Several application domains targeted by systems of systems (SoS), like defense, healthcare, transportation, are critical domains. So, securing such SoS is mandatory. Even if risk management frameworks root the analyses at the organizational, mission and business process levels, how to effectively integrate risk management and mission-based SoS engineering is not clear yet. In this paper, we explore how several SoS and cyber threat modeling approaches could be combined, both using a mission-based approach, and we illustrate it by a case study. Our ultimate goal is to enable the identification of the operational impact at the level of the SoS.**

***Index Terms*—System of systems, Security, Mission-based engineering, Operational impact, Mission impact**

I. Introduction

A system of systems (SoS) is a set of independent systems (or constituents) that interact to jointly fulfill a larger common global goal [13]. One of the main SoS engineering specificity is that the goal for which it is build (the SoS *mission*) prevails over the individual goals of its constituents and over the SoS structure, as highlighted by the mission-based SoS engineering approach [22]. Moreover, several typical SoS application domains are critical domains (defense, healthcare, transportation), therefore, there is a growing interest in their security [21]. SoS security should be considered at the SoS mission level, raising the challenge of the cyber attack *operational impact* identification at early engineering phases.

In this exploratory paper, we study how mission-based SoS engineering, threat modeling (for risk management), and mission impact assessment can be leveraged together in a single model-based engineering framework to deal with the previously mentioned challenge. The article structure is organized as follows: in section II, we review the current principles underpinning SoS engineering. In section III, we describe how cyber security is addressed in the context of SoS. In section IV, we describe how we propose to bridge the gap between the SoS mission and cyber security. In section V, we illustrate our ideas on a healthcare SoS and one of its cyber threats. Section VI reports related work. Section VII gives our final remarks and conclusions.

II. System of Systems Engineering

There exist different types of SoS (directed, acknowledged, collaborative and virtual) [5], depending on the level of centralized control that can be assumed. The first two types operate according to a central process in which SoS engineering methods are used, which are mostly inspired by those used to build monolithic systems. However, those methods must take into account the particularities of SoS, such as managerial independence. They are therefore concerned with specifying a global view of the SoS in the upstream phases, generally up to the definition of an architecture, with the aim of validating SoS operation during its constitution. In some cases, engineering choices at the SoS level may influence the development of the constituents, but this is not always the case. One of the main objectives of SoS engineering is to keep the emergence of SoS behaviors within the desired domain and to limit the emergence of undesired behaviors as much as possible. Abstraction is one of the key concepts allowing to deal with this complexity. Model-Based Systems Engineering (MBSE) is commonly used for this purpose, and is recognized as an area for widespread use in systems development [1].

One of the major differences between SoS and systems engineering is that the SoS architecture is no longer the guarantor of system stability as it is in systems engineering, because a constituent can be replaced by another one or by a combination of other ones [4]. In this context, the SoS specification must be based on another conceptual level, inter-medial between requirements elicitation and architecture definition. For this purpose, Cherfa *et al.* [4] propose to specify the SoS using the *mission* paradigm, inspired by mission engineering [22]. Cherfa *et al.* use the mission paradigm to balance the design and the end-to-end process using MBSE techniques, and SysML with specific extensions. A mission has a goal, which is achieved through a sequence of operational activities. It occurs in a specific context described by a set of contextual parameters. Activities are a set of actions handled by roles. Each role gathers the required competences (*capability* concept) to play the role needed to accomplish an action. Once the roles are described, an abstract architecture is generated. Constituents are assigned to play the roles, to constitute a concrete architecture. The advantage of this approach is that it models the system in a way that is agnostic with regard to the constituents that will ultimately make the effective SoS up. Grounding the SoS design on the concept of *mission* provides the mean to conceive and therefore deal

with the actions and operations expected to be carried out by the SoS.

This vision is not unique to mission engineering [22]. It can be found, for example, in the NATO Architecture Framework 4 (NAFv4)[1]. This framework is organized into viewpoints, each addressing a specific aspect or a specific concern of the architecture. The counterpart of the mission appears in:

- the *concepts* viewpoints, which are focused on the description of the capabilities and their relations;
- the *logical* viewpoints, which describe the operational entities (the roles in [4]) and the allocation of the capabilities to them.

Then, like in [4], the SoS constituents are allocated to implement the identified operational entities.

At a smaller system scale, the mission appears partly, for instance, in the so-named *operational analysis* phase of the Arcadia systems engineering method [24]. This phase is intended to make the engineer analyze the mission in order to identify the enabling capabilities in terms of activities to be executed, as well as operational entities (the roles in [4]) to which the activities are allocated. Then, similarly to NAFv4, in subsequent design phases of the life cycle, the activities are allocated to the system components.

III. Security in System of Systems

SoS particularity and characteristics, described in the previous section II, introduce many engineering challenges, in particular when considering SoS security as reported for example in [7], [21]. It is important to address these challenges early at the architecture phase to avoid time and cost wastage of later changes and to prevent massive damages targeting the SoS missions and operational aspects. A key approach to address SoS security challenges at early phases is MBSE [8], [16], [19]. MBSE allows to represent SoS security models at a higher level of abstraction, granting by that an early security analysis.

Many existing works address SoS security architecture modeling and analysis. The authors in [20] present a systematic mapping study on model-based approaches for security engineering in Cyber-Physical Systems (CPS). The results highlight the strength of modeling languages for security modeling and analysis. The work in [17] presents a model-based extension of the SysML to represent a smart grid scenario. They introduce the idea of defining a security viewpoint as a SysML profile covering SoS-independent security concepts with the aim of detecting, later on, security incidents and vulnerabilities. However, the solution is not fully explored, neither supported by tools. El Hachem *et al.* [8], [9] investigate the attack propagation in SoS. They study attacks composed of a sequence of vulnerabilities, which were initially judged as insignificant or low-impact for the individual constituents on which they were identified. The SoS particularities and constituent interactions induce a cascade between the vulnerabilities and intensify an attack impact.

A very recent systematic mapping study [21] identified 1828 studies covering SoS and Security/Trust/Privacy. They selected and examined 87 approaches dealing with SoS security analysis, evaluation or improvement. The study results display 6 research gaps and several future directions. Among others, the review highlights the need of SoS engineering to adapt to security concerns, as well as the importance of evaluating security in the context of SoS. One of the identified gaps reveals that most of the existing works address SoS security relying on tactical approaches (i.e. approaches for a specific SoS research problem), rather than strategical ones (i.e. formalized approaches that could be applicable to any SoS). In consequence, a key issue in existing approaches is the generalization and standardization allowing the reuse of existing work. The review concludes that, as a matter of fact, "*SoS might benefit from adopting and applying strategical approaches being developed in akin contexts like cyber-physical or Industry 4.0 domains. Future work must consider providing more strategic approaches*".

IV. Bridging Between Security and Missions

Given the above context, figure 1 summarizes the conceptual framework that we propose. The left part of this figure overviews the SoS engineering like it is described in section II, which is our first assumption. Namely, we assume that the SoS is built, and therefore designed to support a mission as defined by SoS stakeholders. Said otherwise, the goal is the mission, not the SoS itself. Fulfilling the mission requires some enabling capabilities, which are identified during the engineering process, in order to perform the operational activities underpinning the mission. Constituents specification describes what are the roles that each constituent is planned to play, providing the capabilities (see comments on [4] in section II). In the effective, deployed SoS, the actual constituents implement the planned specification.

The right part of figure 1 gives our second assumption, which comes from threat modeling as performed for the purpose of risk analysis, for instance by executing SP800-30[2] or EBIOS RM[3]. We mimic the same structure as for SoS engineering, where the adversary's intention describes the goal (the adversary's *mission*). Like the SoS mission, the adversary's intention is enabled by capabilities, which describe the operational activities the adversary has to perform to fulfill the intention. Enabling threat events are allocated to realize the required capabilities. These threat events may be, for instance, picked from MITRE CAPEC patterns and ATT&CK techniques[4], or from the anticipation of Common Weakness Enumeration (CWE) exploitation in relation with the constituents specification. In the *security-by-design* perspective, models describe how an anticipated adversary may realize each capabilities, despite the effective SoS is not (yet) known. The effective attack implements the planned attack specifically for the effective SoS. MITRE ATT&CK procedures and Common

[1] https://www.nato.int/cps/en/natohq/topics_157575.htm

[2] https://doi.org/10.6028/NIST.SP.800-30r1

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

[4] https://capec.mitre.org/about/attack_comparison.html

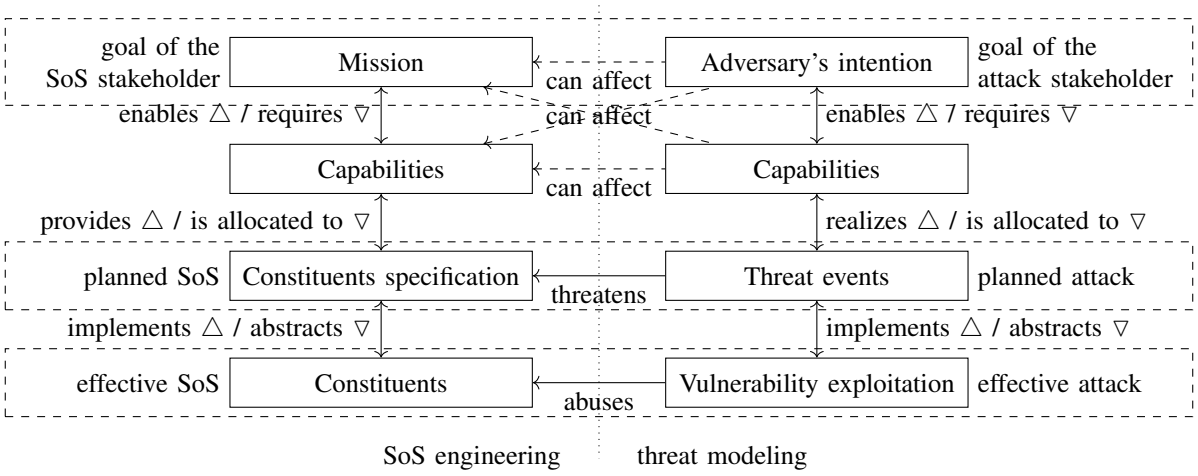

Fig. 1. Summary of the proposed conceptual framework

Vulnerability Enumeration (CVE) enumerate potential implementations of the threat events, which abuse the constituents of the SoS by exploiting their vulnerabilities.

As explained above, the two sides of figure 1, namely SoS engineering and threat modeling, are matched and the respective concepts are linked to entangle systems engineering and security engineering in an integrated process, see [16], [19] and SP800-160 vol. 1[5]. We leverage together complementary approaches, using here Arcadia, EBIOS RM and CAPEC to illustrate:

- *Capabilities*: as described in [19], the engineers would use, for instance, the Arcadia *capabilities* as EBIOS RM *business assets*. Then, as the Arcadia method proceeds, the Arcadia *components* can be used as EBIOS RM *supporting assets* [19].
- *Vulnerable domain asset*: as described in [16], the EBIOS RM *supporting assets* can be used as *domain assets*. CAPEC *patterns* can be used as *vulnerable assets*. When a *domain asset* matches with a *vulnerable asset*, this *vulnerable domain asset* can be involved when anticipating the EBIOS RM *operational scenarios*. So, it is an asset of interest for risk management.

From these combined analyses, system and security engineers can proceed with the introduction of controls, for instance taken from a knowledge base like SP800-53[6] or SP800-160 vol. 2[7], to mitigate the risks at the assets of interest. However, the above landscape poorly addresses the connection with feared events, risk origins and target objectives (EBIOS RM) or threat sources and threat events (SP800-30). At best, Naouar *et al.* [19] propose to model the EBIOS RM *strategic scenarios* as Arcadia *scenarios*. The link between the *target objectives* (the adversary's intention) and the *feared events* (the effect on the operation supported by the SoS, that is, the effect on the SoS mission and capabilities), appears implicitly in the strategic scenarios. It is up to the engineers to determine what capabilities (and therefore activities) implementing a target objective (adversary's intention) can cause a feared event (affect the SoS mission or capabilities).

Given the two above assumptions we summarize in figure 1, the security concern is the adversary ability to impede or deter[8] the SoS stakeholder's operations, that is, to produce an effect that impacts the SoS stakeholder's operation. This is how we define the *operational impact*. Such operational impact would enable earlier risk management in the context of SoS, as early as the elicitation of missions and capabilities even though few details are known about the actual systems.

V. Illustrative Case

To illustrate the proposed conceptual framework, we consider the SoS depicted in figure 2 in the healthcare domain for a patient's surgery. The SoS involves four organizations:

- At the neighborhood family medicine center, the patient's primary care physician coordinates the patient's health, achieving the initial diagnosis yielding to the surgery and supervising the post-surgery health cares. To this end, the primary care physician interacts with the medical laboratory to fulfill the diagnosis, directs the surgery to the surgery room, and prescribes medication for the post-surgery cares.
- The commercial pharmacy provides the medication according to the primary care physician's prescription, such as post-surgery antibiotic medication.
- At the hospital, the surgery room provides the capability to perform the surgery. It interacts with the pharmacy of the hospital for specific medication such as anesthetic drugs, and with the medical laboratory to access the patient's test results. It also interacts with the CT scan, for instance for the preparation of the surgery.

[5]https://doi.org/10.6028/NIST.SP.800-160v1r1
[6]https://doi.org/10.6028/NIST.SP.800-53r5
[7]https://doi.org/10.6028/NIST.SP.800-160v2r1

[8]We reuse the *effect* vocabulary from SP800-160 vol. 2, despite these effects are targeted at the feared events while we consider the SoS mission.

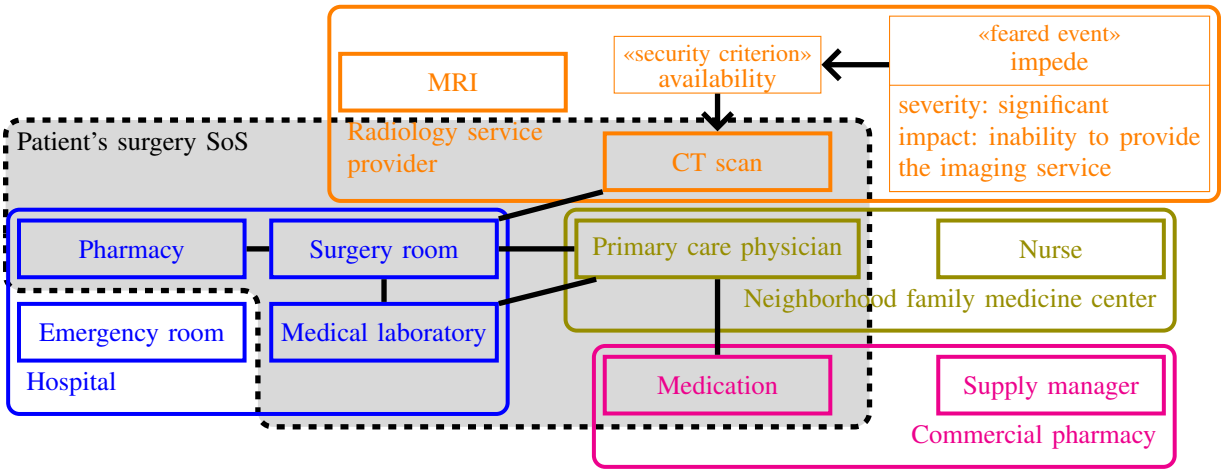

Fig. 2. An illustrative system of systems in the healthcare domain.

- At the radiology service provider, the CT scan provides the imaging service necessary to prepare the surgery.

The spread over the multiple organizations straightforwardly implies the managerial independence of the constituents. To emphasize the operational independence of the SoS constituents, we put additional constituents in each organization: each SoS constituent can interact with the other constituents belonging to the same organization, out of the scope of the SoS. The overall healthcare SoS is an *acknowledged* SoS [5].

By using the modeling approach of [19], we jointly model the result of the risk analysis in the top-right part of figure 2. In this paper, for the purpose of the illustration, we only attach the availability security criterion to the CT scan, and we attach the impede feared event to this security criterion. From the point of view of the radiology service provider, the impact of this feared event would be the inability to provide the service, with a *significant* severity (with the interpretation of the EBIOS RM scale: no impact on the safety of persons from the point of view of the radiology service provider, even if there is such impact for the point of view of the patient's surgery SoS).

The mission of this SoS is to perform a surgery on a patient. In the top of figure 3, we derive capabilities by decomposing the mission like explained in section II and in [4]. Table I shows the allocation between the capabilities identified in the top part of figure 3 and the constituents, leading to the interactions modeled by the connections in figure 2, according to the process describing the work-and-data flow (which is not depicted in the paper).

According to the US Department of Health and Human Services, ransom extortion is a credible intention for cyber attacks targeting the healthcare domain[9]: the attackers seize the opportunity offered by the sensitivity of medical data. Like noticed for instance by the CISA, a denial-of-service attack is often used to deflect attention of the security team

TABLE I
ALLOCATION OF THE CAPABILITIES TO THE CONSTITUENTS (SOS).

Capability	Constituent
prescribe the diagnosis test	Primary care physician
execute the diagnosis test	Medical laboratory
prescribe the surgery	Primary care physician
interpret the test result	Primary care physician Surgery room
administer the anesthesia drug	Pharmacy
construct the anatomical image	CT scan
execute the surgery	Surgery room
prescribe the antibiotic	Primary care physician
administer the antibiotic drug	Medication
supervise the recovery	Primary care physician

from secondary attacks[10]. Given this cyber threat intelligence, we anticipate a potential attack against the SoS of figure 2, starting with the mission breakout and identification of the capabilities in the bottom part of figure 3. For instance, the distracting maneuver could be targeted at the construction of the anatomical image, using `CVE-2020-25175`[11] to steal the credentials to gain access to the CT scan device after an initial access to network of the radiology service provider (e.g., by means of spearphishing), hence enabling the denial of service as the result of arbitrary code execution.

On the one hand, following the approach of [19], figure 4 outlines the operational scenario of this attack as a sequence of threat events, customizing the activity diagram notation, by referring to the ATT&CK tactics, techniques and procedures (TTP). We detail the threat event `T1563` *remote service session hijacking*[12]: by looking at security-related knowledge bases (here joining ATT&CK, CAPEC, CWE and NVD), and knowing candidate supporting assets to be targeted by this threat event, the engineers may identify the above-cited vulnerability (`CVE-2020-25175`) of the CT scan.

[9]https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html

[10]https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

[11]https://nvd.nist.gov/vuln/detail/CVE-2020-25175

[12]https://attack.mitre.org/techniques/T1563/

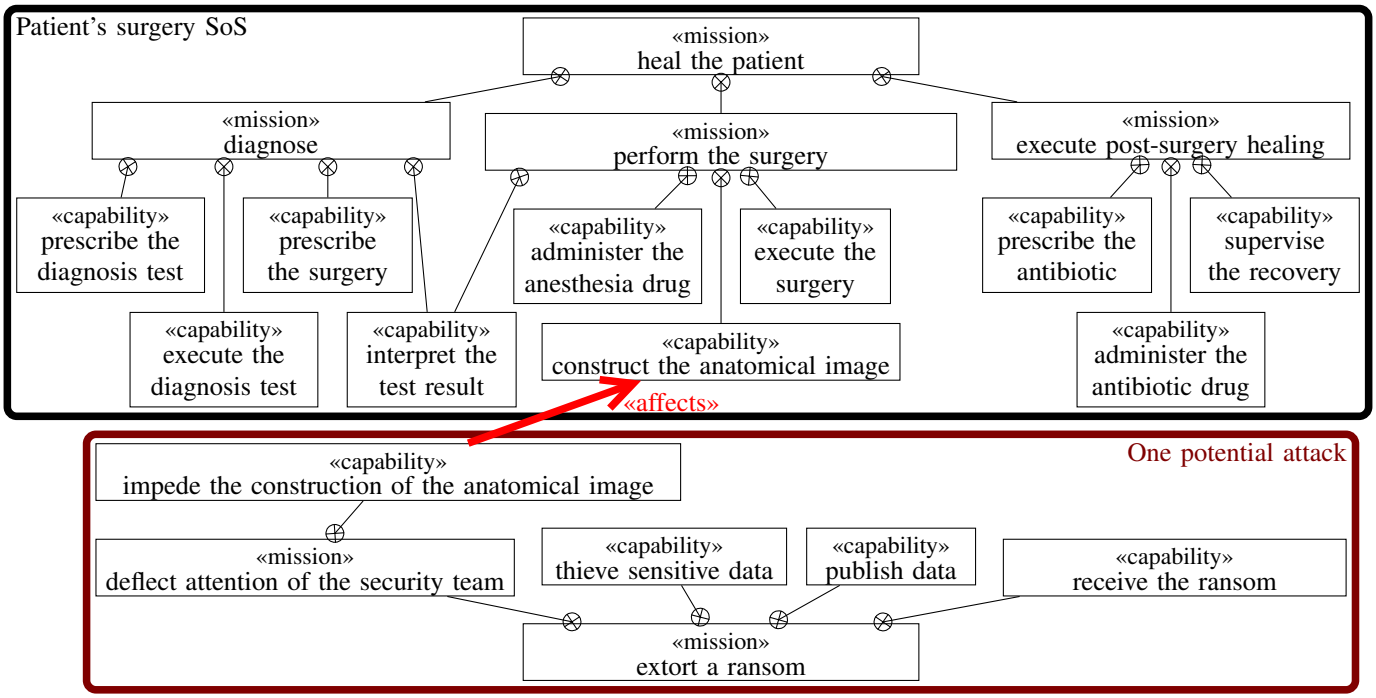

Fig. 3. Mission breakout and capabilities for the SoS and for one anticipated attack, according to [4]

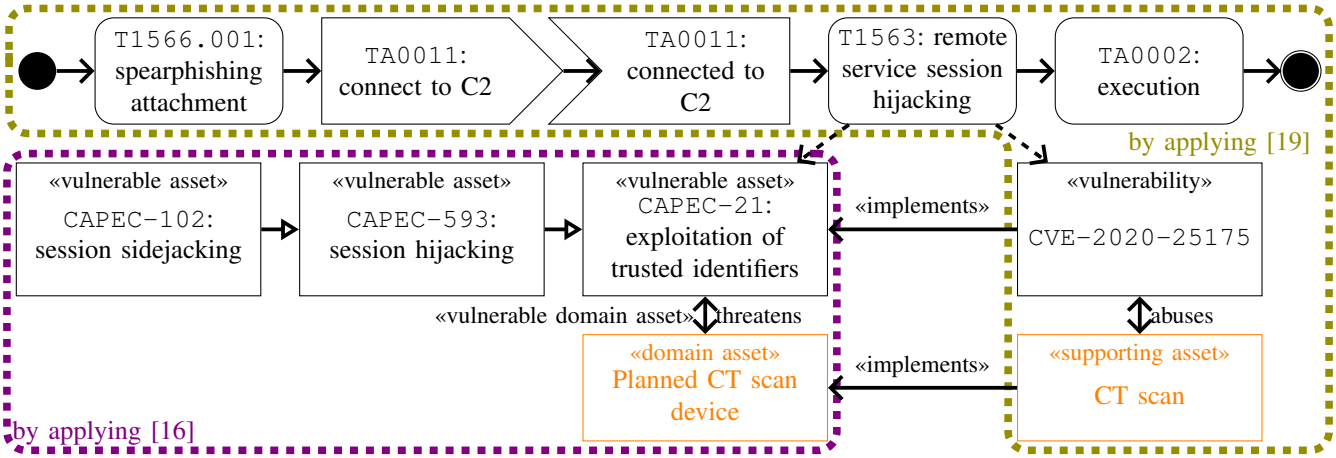

Fig. 4. Operational scenario of the attack, and links between [16] and [19].

On the other hand, following the approach of [16] and by looking at the same security-related knowledge bases, the hierarchy CAPEC-21 - CAPEC-593 - CAPEC-102 *session sidejacking*[13] can be found as an attack pattern to realize the T1563 threat event. Doing the analysis according to [16], the engineers can consider that this attack pattern threatens the planned CT scan device domain asset, yielding to a vulnerable domain asset, that is, a constituent of interest to secure the SoS.

The pattern CAPEC-21 - CAPEC-593 - CAPEC-102 (threatening the planned CT scan device) actually abstracts the CVE-2020-25175 vulnerability, which in turns is a vulnerability of the CT scan. So, the additional links we introduce in our conceptual framework of figure 1 effectively reconnects between the approaches of [16] and [19].

Last, the *operational impact* appears as the «affects» red arrow between the envisioned potential attack and the SoS in figure 3. By means of table I, we link the SoS constituents with the mission-engineering approach [4] in figure 3, which we extend with the mission analysis of the potential attack.

VI. Related Work

To assess vulnerabilities, CVSS[14] is based (among other criteria) on an evaluation of the impact of the vulnerability in terms of the usual security criteria: confidentiality, integrity,

[13]https://capec.mitre.org/data/definitions/102.html

[14]https://www.first.org/cvss/v4.0/specification-document

availability. However, these criteria are hardly meaningful to position with respect to the system mission [15]. To relate to the mission, *observability*, *controllability*, and *operability* could be more relevant criteria, as well as reduction of mission fulfillment and distance to the mission desired end state [15]. Putting the emphasis on operability lets reuse previous work on propagation analysis in dependency graphs [6], [10], [11], [18]. Layered modeling of the SoS and its mission appears to be the enabler to transpose propagation analysis to cyber threats [2], [3], [11], [14], [23], to ensure traceability across assets, infrastructure, capabilities, etc. to the mission. Besides, propagation analysis can also be transposed to study the propagation of confidentiality, integrity, and availability within the system [12].

In the above-paragraph, almost all of the previous work was based on the Jakobson's layered model [11] to describe the system, with the noticeable exception of [6]. This Jakobson's model mismatches the SoS engineering practices we summarized in section II. Such a model mismatch between SoS (or system or software) engineering and cyber security was the one of the motivation underpinning [16], [19], which do not consider the SoS mission. Actually, according to gap 5 in [21], the combination of security and mission were not studied in the context of SoS. In our paper, we make a step towards reconciling the work in the trend of propagation analysis with SoS engineering.

VII. Discussion and Conclusion

In this paper, we reviewed mission-based and security engineering in the context of system of systems (SoS). On top of these approaches and of previous efforts to join with threat modeling, we conducted an exploratory case study merging all these approaches in a single engineering process targeted at SoS. As expected, we observe mismatches between all the approaches we intend to combine. Among others, the join between MBSE and risk management [19] lacks the mission-orientation [4], [22]. Even if CIIA [3] adds threats to Jakobson's multi-layer framework [11] intended to adapt propagation analysis to cyber attacks, it needs a detailed description of the system down to the assets. Besides, it does not connect with SoS engineering. While Messe *et al.* linked threat intelligence and risk management [16], they do not support mission-based engineering nor propagation analysis. For our future work, we will better define the process we informally outlined in this paper. Adopting a model-based approach would provide a single source of truth to reconnect these engineering areas in a consistent framework. Doing so would enable to transpose analyses at earlier stages in the life cycle, at higher levels of abstraction.

References

[1] "A world in motion: systems engineering vision 2025," INCOSE, Tech. Rep., 2014.

[2] H. Bahşi, C. J. Udokwu, U. Tatar, and A. Norta, "Impact assessment of cyber actions on missions or business processes: A systematic literature review," in *International Conference on Cyber Warfare and Security*, Mar. 2018.

[3] O. Carvalho, F. Apolinário, N. Escravana, and C. Ribeiro, "CIIA: critical infrastructure impact assessment," in *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, May 2022.

[4] I. Cherfa, N. Belloir, S. Sadou, R. Fleurquin, and D. Bennouar, "Systems of systems: From mission definition to architecture description," *Systems Engineering*, vol. 22, no. 6, Nov. 2019.

[5] J. Dahmann and K. Baldwin, "Understanding the current state of US defense systems of systems and the implications for systems engineering," in *2nd Annual IEEE Systems Conference*, Apr. 2008.

[6] J. Dahmann, G. Rebovich, and G. Turner, "An actionable framework for system of systems and mission area security engineering," in *IEEE International Systems Conference*, Mar. 2014.

[7] J. El Hachem, T. A. Khalil, V. Chiprianov, A. Babar, and P. Aniorte, "A model driven method to design and analyze secure architectures of systems-of-systems," in *22nd International Conference on Engineering of Complex Computer Systems*, Nov. 2017.

[8] J. El 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, Apr. 2020.

[9] J. El Hachem, A. Sedaghatbaf, E. Lisova, and A. Causevic, "Using bayesian networks for a cyberattacks propagation analysis in systems-of-systems," in *Asia-Pacific Software Engineering Conference*, Dec. 2019.

[10] P. Garvey and A. Pinto, "Introduction to functional dependency network analysis," in *Second International Symposium on Engineering Systems*, Jun. 2009.

[11] G. Jakobson, "Mission cyber security situation assessment using impact dependency graphs," in *14th International Conference on Information Fusion*, Jul. 2011.

[12] O. Keskin, N. Gannon, B. Lopez, and U. Tatar, "Scoring cyber vulnerabilities based on their impact on organizational goals," in *Systems and Information Engineering Design Symposium*, Apr. 2021.

[13] J. Klein and H. Van Vliet, "A systematic review of system-of-systems architecture research," in *Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures*, Jun. 2013.

[14] A. Kott, J. Ludwig, and M. Lange, "Assessing mission impact of cyberattacks: Toward a model-driven paradigm," *IEEE Security & Privacy*, vol. 15, no. 5, 2017.

[15] A. Kott, N. Stoianov, N. Baykal, A. Moller, R. Sawilla, P. Jain, M. Lange, and C. Vidu, "Assessing mission impact of cyberattacks: Report of the NATO IST-128 workshop," Jan. 2016.

[16] N. Messe, V. Chiprianov, N. Belloir, J. El Hachem, R. Fleurquin, and S. Sadou, "Asset-oriented threat modeling," in *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications*, Dec. 2020.

[17] M. Mori, A. Ceccarelli, P. Lollini, B. Frömel, F. Brancati, and A. Bondavalli, "Systems-of-systems modeling using a comprehensive viewpoint-based SysML profile," *Journal of Software: Evolution and Process*, Apr. 2017.

[18] A. Motzek, R. Möller, M. Lange, and S. Dubus, "Probabilistic mission impact assessment based on widespread local events," in *Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks*, Jun. 2015.

[19] D. Naouar, J. El Hachem, J.-L. Voirin, J. Foisil, and Y. Kermarrec, "Towards the integration of cybersecurity risk assessment into model-based requirements engineering," in *IEEE 29th International Requirements Engineering Conference*, Sep. 2021.

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

[21] M. A. Olivero, A. Bertolino, F. J. Dominguez-Mayo, M. J. Escalona, and I. Matteucci, "A systematic mapping study on security for systems of systems," *International Journal of Information Security*, Oct. 2023.

[22] A. Sousa-Poza, "Mission engineering," *International Journal of System of Systems Engineering*, vol. 6, no. 3, Sep. 2015.

[23] J. Stanley, R. Mills, R. Raines, and R. Baldwin, "Correlating network services with operational mission impact," in *IEEE Military Communications Conference*, Oct. 2005.

[24] J.-L. Voirin, *Model-based system and architecture engineering with the Arcadia method*, 1st ed. Elsevier, Nov. 2017.