International Journal of Information Security (2024) 23:787–817
https://doi.org/10.1007/s10207-023-00757-0

SPECIAL ISSUE PAPER

A systematic mapping study on security for systems of systems

Miguel Angel Olivero[1] · Antonia Bertolino[2] · Francisco José Dominguez-Mayo[1] · María José Escalona[1] · Ilaria Matteucci[3]

Accepted: 2 September 2023 / Published online: 18 October 2023

Abstract

In the late twentieth century, the term "System of Systems" (SoS) became popular to describe a complex system made up of a combination of independent constituent systems. Since then, several studies have been conducted to support and assess SoS management, functionality, and performance. Due to the evolutionary nature of SoS and the non-composability of the security properties of its constituent systems, it is difficult to assess or evaluate SoS security. This paper provides an up-to-date survey on SoS security, aimed at stimulating and guiding further research efforts. This systematic mapping study (SMS) focuses on SoS security, privacy, and trust. Our SMS identified 1828 studies from 6 digital libraries, 87 of which were selected that presented approaches analyzing, evaluating, or improving security. We classified these studies using nine research questions that focused on the nature of the studies, the studied SoS, or the study validation. After examining the selected studies, we identified six gaps and as many future work directions. More precisely, we observed that few studies examine SoS problems and instead propose specific solutions, making it challenging to develop generalizable approaches. Furthermore, the lack of standardization has hindered the reuse of existing approaches, making it difficult for solutions to be generalized to other SoS. In addition, the lack of descriptions of industrial environments in the literature makes it difficult to design realistic validation environments. As a result, the validation of new SoS research remains a challenge in the field.

Keywords Human factor · Security · System of systems · Systematic mapping study · Privacy · Trust

1 Introduction

Security in computer systems has attracted increasing attention in recent years. This is undoubtedly due to the increasing number of systems and personal devices that are now being connected and which often contain sensitive information about matters like health, finances, or personal tastes. Consequently, people are becoming increasingly aware of security risks and concerned about attacks that may affect their private data.

The cloud is now also widely used to store or back up personal data. The use of cloud systems allows users to access their data from any device and at any time, as long as they have an Internet connection. However, this advantage comes at the cost of new privacy, security, and trust issues. Security, privacy, and trust become clearly related because when storing their personal data on different servers somewhere in the cloud, users necessarily have to trust that the provider organization will securely protect their data and defend their privacy.

This work was partially supported by the GAUSS national research project (MIUR, PRIN 2015, Contract 2015KWREMX), the NICO project (PID2019-105455 GB-C31) of the Spanish Ministry of Science, Economy and University and NDT4.0 (US-1251532) of the Andalusian Regional Government's Ministry of Economy and Knowledge.

✉ Miguel Angel Olivero
molivero@us.es

Antonia Bertolino
antonia.bertolino@isti.cnr.it

Francisco José Dominguez-Mayo
fjdominguez@us.es

María José Escalona
mjescalona@us.es

Ilaria Matteucci
ilaria.matteucci@iit.cnr.it

[1] Department of Computer Languages and Systems, University of Seville, Seville, Spain

[2] Institute of Information Science and Technologies, National Research Council, Pisa, Italy

[3] Institute of Informatics and Telematics, National Research Council, Pisa, Italy

Security, privacy, and trust assume even greater importance in the case of systems of systems (SoS) due to the evolutionary nature of such systems and the dynamic composition of their constituent systems. The SoS paradigm provides a strategy for coordinating the processes performed by independent systems working together to achieve global goals that a single system could not achieve on its own [1, 2]. Although it dates back to the mid-1990s [3], the SoS paradigm has attracted substantial interest only in recent years, thanks to the progress in connectivity capabilities and IoT technology.

Since a SoS connects individual systems in ways that may not have been planned in advance, it is evident that the interactions arising from a SoS arrangement may be vulnerable to new security threats and could also impact the privacy of the connected users or, indeed, any of the people whose data are saved in any of the constituent systems. Trust can also become a key concern in this scenario. The connections between the constituent systems of a SoS that were not foreseen could in fact undermine the preservation of pre-existing chains of trust among the different systems involved. Therefore, proper mechanisms are needed to control the transitivity of trust relationships across the emerging SoS.

In other words, as discussed by Petkovic and Jonker [4], security in our modern digital world is a multifaceted issue that cannot be analyzed without considering together privacy and trust concerns. On the other hand, the non-composability of security, privacy, and trust makes such properties more difficult to be determined in the context of SoS.

In a recent related study, we highlighted the challenges that arise when dealing with the security properties of SoS compositions [5], showing how the analysis of security properties is hindered by their non-composability. An unexpected combination of shared resources may generate emergent behaviors within the SoS, which may in turn introduce exploitable vulnerabilities that cannot be mitigated by examining the constituent systems individually. A well-described case in the literature is the exploited vulnerability of Mat Honan's digital life.[1] The different social systems Mr. Honan used were combined into a virtual SoS that suffered an attack exploiting an unplanned combination of the resources provided by the constituent systems.

Due to the dynamic composition of the SoS, the constituent systems may also connect or disconnect from the SoS in an uncontrolled manner. Studying the security, privacy, and trust properties of SoS is a complex task also because responsibilities and shared resources are handled in different ways depending on how the constituent systems are orchestrated, i.e., according to the SoS architecture.

Unsurprisingly, considerable research has been done in recent years to address security, privacy, and trust issues in SoS. Notwithstanding, to the best of our knowledge, no systematic collection and/or classification of that work has yet been undertaken.

In this work we aim at filling such a gap by providing a systematic survey of the existing literature. Since the seminal work by Kitchenham and Charters [6] providing Software Engineering researchers with guidelines for conducting systematic literature reviews (SLRs), secondary studies have become a major tool toward a rigorous analysis and categorization of results in a defined research field. Indeed, a systematic survey follows a standard method that facilitates the replicability of searches and reduces potential author bias by adhering to precise guidelines instead of the researcher's own assumptions [6].

While initially SLRs received the largest attention, another type of secondary study that has been broadly pursued in Software Engineering are Systematic Mapping Studies (SMSs) [7]. A SMS [7] is a method designed to provide a comprehensive overview of a field of interest (often a recently established one) by categorizing existing research results and also by identifying gaps that can properly direct more primary studies. SMSs are characterized as a complementary type of study to SLRs, from which they differ in goals and data collection breadth. Regarding goals, SMSs are considered a more appropriate tool when the study addresses a broad topic and the main goal is that of structuring the investigated research area (as opposed to SLRs that rather aim at synthesizing the existing evidence) [8]. Regarding data collection breadth, SMSs generally use less focused search strings and broader research questions [6], aiming at covering research trends [7].

As our goal here was that of identifying and categorizing existing research on security for SoS, encompassing security, privacy, and trust, in the absence of other secondary studies that cover the area, we hence opted for conducting a SMS.

Summarizing, this work offers a review of the state of the art, focusing on available and published work addressing security, privacy, and trust issues from a SoS perspective, and aims at identifying the gaps in current research. It is important to clarify that the scope of this SMS is limited to research on security, privacy, and trust specifically regarding the combination and cooperation of the constituent systems in a SoS. The study does not cover the vast amount of literature on security, privacy, and trust issues related to single systems, even if complex or distributed.

This SMS includes journal articles, conference papers, and workshop papers on systems of systems. A systematic search was carried out in the most important computer science digital libraries (namely ACM DL, IEEE Xplore, Science Direct, Scopus, Springer, and Web of Science). With the aim of finding as many relevant studies as possible, we used a comprehensive search string, covering security, privacy, and trust; as mentioned above, SoS security cannot really be addressed

[1] https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.

without also considering privacy- and trust-related aspects. After conducting the search and the defined selection process, 87 primary studies were finally identified as relevant to assess issues related to security, privacy, and trust in SoSs.

We categorized the selected studies using three perspectives, each consisting of three research questions (RQs). The first perspective delved into the nature of the study, including its goals, scope, and contribution. The second perspective examined the characteristics of the SoS being studied, such as its architecture and roles. The third perspective analyzed the application context of the approach or study, including its implementation, validation, and domain of application. In summary, this SMS sought to answer a set of nine related RQs through the three distinct perspectives we used to classify the selected studies.

Our SMS confirmed a growing interest in research into SoS security, with an increasing number of papers being published on just this topic that are the majority of the surveyed studies. A minor number of the works found focuses instead on security and privacy or security and trust, while we did not find works covering all three properties together. We identified though several major challenges, such as the lack of industrial cases and the absence of SoS details or material, which would allow results to be replicated.

The rest of the paper is organized as follows: Section II provides some background and summarizes some related work. Section III presents the SMS planning, Section IV describes the process of conducting the SMS, and Section V outlines the last stage of the SMS by providing a reporting of the findings. Finally, considering the current state of the art as reflected in the study, Section VI provides a set of conclusions and suggests some possible future research lines.

2 Related work

The "System of Systems" paradigm has been defined in different ways and domains by different authors since as far back as the 1950s [9]. In 1999, Maier [3] proposed a unifying definition of SoS in computer science, leveraging the features that characterize the concept in this domain. Years later, in 2005, the same author updated that early work by highlighting the research challenges that still needed to be addressed [10].

An SMS is a process for collecting and organizing existing studies in a research field to respond to a series of research questions [11]. The term "systematic" refers to the rigorous adoption of a well-defined search protocol to identify and evaluate the available literature so as to reduce the impact of author bias on the results found. This protocol guarantees that studies that do not match the initial hypotheses or expectations of the authors can be included as well.

Systematic literature reviews (SLRs) and SMSs share similar purposes and similar processes. SLRs focus on more specific RQs, seek more clearly defined details, and employ deeper analysis techniques, whereas SMSs are designed to consider more general RQs and provide broad coverage of a topic. The SMS has become a widely used approach for state-of-the-art research in emerging areas.

As explained in the introduction section, we conducted this paper as an SMS because such type of study enables us to capture a broader range of studies (including those that might not have been covered by a narrower search protocol of an SLR) and to draw a map of the research area, possibly identifying existing gaps.

In recent years, several surveys have been conducted in the area of SoS with different purposes, as we summarize in the following.

A systematic review in 2013 provided an overview of the SoS architecture [12]. The authors emphasized that this field was maturing at a slower pace than others. They also underlined that most of the approaches found developed solutions for specific SoS problems but did not provide a general perspective suitable for widespread adoption. In total, they analyzed 194 studies. However, in terms of quality attributes, only 14 papers focused on SoS security aspects.

Two years later, a review was published that classified SoS according to their purpose [13]. This work defined its own SoS characterization using already existing approaches for defining or classifying SoS. The authors concluded the study using the identified SoS characteristics to identify new research lines.

In 2015, a SMS was conducted to structure scientific developments in SoS [14]. From the results obtained, the author concluded that until 2015 the most researched areas were architecture, modeling, and simulation. The author also highlighted the immaturity of this area, the lack of citations of existing works, and the predominant participation of US researchers in this topic. This SMS says they studied nearly 3000 works, but the list of selected studies is not available.

Another review conducted in 2015 analyzed SoS according to their architecture and how they could be described [15]. Researchers reported a lack of consensus on how the SoS architecture is described and found that security was barely mentioned.

A third survey conducted in the same year addressed the quality attributes of SoS [2]. In this study, the three most relevant quality attributes identified in SoS were security, performance, and interoperability, and 14 articles referred to each attribute. This work highlighted the increasing difficulty of ensuring security in SoS given the dependencies, trade-offs, and relationships that existed between the different quality attributes.

Later, a systematic survey of SoS integration analyzed software engineering methods that can assist in the integration of constituent systems [16]. As in [12], the authors noticed that most of the studies were carried out by isolated groups to solve specific problems, making it difficult to generalize such approaches to wider SoS contexts.

A more recent systematic review of SoS was conducted by Daneva and Lazarov [17]. This study presented the results of an SLR that focuses on the SoS requirements of smart cities. The authors classified 32 selected papers according to the types of smart cities and the requirements addressed. Their results showed that requirements for architecture were the most discussed topic, and little was mentioned about security or privacy challenges.

According to this summary of previous literature reviews, SoS is an emerging research area with a growing community of researchers. Researchers have focused on functional and technical specifications, such as SoS architecture. Despite the concern regarding non-functional requirements (e.g., security, performance, interoperability) being raised, it seems the non-functional requirements have not been as much developed as the functional ones.

For instance, while previous studies have focused on specific areas within SoS research, such as architecture, modeling, and simulation, our study aims to provide a comprehensive overview of security for systems of systems. Our focus on security aligns with the growing concern regarding the security challenges posed by the shared resources and complex interactions in systems of systems.

Furthermore, while some previous studies have identified security as a significant non-functional requirement for SoS, they have not delved into the details of this issue as much as our study. For example, the 2015 review of SoS architecture and description noted that security was barely mentioned in the surveyed literature. In contrast, our study takes a deep dive into the security aspects of systems of systems, including issues related to trust and privacy.

With the aim of providing an overview and promoting the research on security, on SoS, the present systematic mapping study summarizes works that specifically address security, also including privacy and/or trust requirements and challenges in the context of a SoS and analyzes the current state of the art in this area. We aim at discovering if such properties have been developed, and the most relevant results so far. We ignore those SoS studies that do not focus on security, or privacy, or trust as their main concerns.

Additionally, our study also differs from most of previous works in its approach to conducting a systematic mapping study. As we have previously mentioned, an SMS provides a broader scope of coverage, including studies that might not have been captured by a narrower search protocol of an SLR. In addition, the use of generic keywords enabled us to capture a wide range of literature on security for systems of systems.

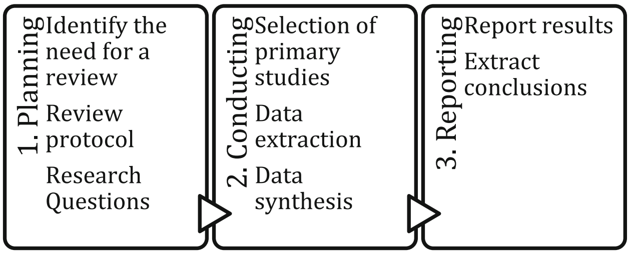

Fig. 1 SLR and SMS phases

This approach has allowed us to provide a comprehensive overview of the state of the art regarding security for systems of systems.

Since our objective is to provide comprehensive coverage of SoS security concerns, and not to answer specific RQs, the ultimate objective being to represent the current state of knowledge and research lines, this study was conducted using SMS guidelines. In particular, this SMS has been conducted following the guidelines proposed by Petersen et al. [7], which are similar to those provided by Kitchenham and Charters in their adaptation of systematic literature reviews (SLR) to computer science [6].

The following sections describe the activities we conducted in each of the three phases of the SMS as shown in Fig. 1: (1) planning, (2) conducting, and (3) reporting.

3 Planning

An accurate and rigorous planning is crucial to the quality of an SMS since the decisions taken in this phase will influence the results of the entire process. The planning phase was organized into three stages: (1) identifying the need for an SMS, (2) developing the review protocol, and (3) specifying the research questions.

3.1 Identify the need for a review

This SMS aims at identifying already existing solutions and relevant research lines and topics related to security, privacy, and trust issues in the SoS context.

The need for this review arises after finding that a recent study has identified some issues regarding the understanding of "*Security*." Such a study explores, particularly, the causes and consequences of vulnerabilities and the concept of homogeneity of security among the constituent systems [18]. After exploring the digital libraries, we did not find previous literature surveys addressing these concerns.

Consequently, the goal of this SMS is to explore the current state of the art with respect mostly to "*Security*," which is the property more widely studied. Notwithstanding, for

Table 1 Search keywords

Concept	Search keywords
System of systems	system of systems, systems of systems, system-of-systems, systems-of-systems
Security, privacy, trust	security, privacy, trust

the sake of broader coverage, we consider the trinity of *security*, *privacy*, and *trust* in the SoS context. As explained in the Introduction, privacy and trust are related to security as the shared resources within constituent systems composition are exposed to third parties that might affect the privacy of the resources and the chains of trust among the constituent systems.

In other words, we look forward to analyzing the characteristics of the SoS that in recent years researchers have been focusing on in their research when it comes to SoS security, privacy, and trust. The goal is to understand the current state of the art in this area.

3.2 Review protocol

The review protocol starts by defining the search strategy, which outlines how the search is performed in the main digital libraries, continues by stating the study selection criteria, and describes the applied snowballing effect.

3.2.1 Search strategy definition

At the beginning of the search strategy definition phase, a group of keywords was combined to perform a set of initial searches. The purpose of this was to analyze preliminary results and select the keywords that provided the most suitable results for our purpose. The used search keywords were in English, since this is the international language of research and because the search was going to be carried out in this language. Wildcards were avoided after some libraries showed incompatibilities with them, so we opted to use the most representative keywords. The keywords to be used during the searches had to be generic enough to provide a wide coverage of the need for this SMS. The finally chosen keywords for this review protocol are shown in Table 1, where each keyword is associated with its corresponding concept.

The first concept, "*System of Systems*," limited the papers to those with content related to this topic. The second concept, "*Security, Privacy Trust*," restricted the criteria, covering papers dealing with both "*Systems of Systems*" and "*Security*, *Privacy*, *Trust*."

The concept of "*Security*" included the terms "*Security*," "*Privacy*," and "*Trust*" to ensure complete coverage in the security context and in areas related to those concepts. Therefore, we included the terms *Privacy* and *Trust* in our search and analysis. The joint use of Security, Privacy, and Trust has been motivated by [4] and supported by their own definition in the National Institute of Standards and Technology (NIST). On the one hand, the term "*Privacy*" allows us to include studies focusing on new security threats that could also impact the privacy of connected users or, in general, of people whose data are saved in any of the constituent systems. Privacy has been defined as "Assurance that the confidentiality of, and access to, certain information about an entity is protected."[2] The confidentiality is one of the security properties; therefore, the assurance of the confidentiality would somehow benefit the privacy. On the other hand, the term "*Trust*" allows to include studies on the connection issues between constituent systems of a SoS, which may not have been foreseen and could cause problems about the preservation of pre-existing chains of trust between the different involved constituent systems. According to its definition,[3] trust is "A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly and impartially, along with assurance that the entity and its identifier are genuine." Consequently, it is related to security due to the need of preserving the integrity and authentication aspects.

Although our SMS study is motivated by our main concern with security in systems of systems, we identified that relevant literature on security may also be present in articles related to trust and privacy. Therefore, the inclusion of these concepts in our study allowed us to achieve a broader coverage of relevant studies while maintaining our focus on the security of systems of systems. The selection of general terms is common in an SMS as this type of study aims to map and categorize existing literature in a specific field. By using general terms, a wider set of relevant studies can be captured to achieve an overview of the available literature on the topic.

The decision of not including additional or more specific keywords is based on the fact that "security," "privacy," and "trust" are widely accepted and used in academia as well as in the industry presumably offering a considerable coverage. Also, constraining our search to these keywords helps in understanding the focus of this study and ease the analysis, comparison and contrast of our results. Despite we acknowledge that there are further concepts and keywords that are more specific but still relevant in the context of security and SoS, we decided to strategically limit the scope of the research to balance effort and results.

The search query finally used in the digital libraries is a combination of the keywords shown in Table 1. In the

[2] https://csrc.nist.gov/glossary/term/privacy.

[3] https://csrc.nist.gov/glossary/term/trust.

launched query, each concept was joined with the "AND" operator and every synonym of the concept was appended with the "OR" operator, as follows:

> ("system of systems" OR "systems of systems" OR "system-of-systems" OR "systems-of-systems") **AND** ("security" OR "trust" OR "privacy").

The search was executed in well-known computer science digital libraries, namely: *ACM* DL, *IEEE Xplore*, *Science Direct*, *Scopus*, *Springer*, and *Web of Science*.

The published proceedings and journals related to the subject of this SMS featured in two of the libraries: the "IEEE International Conference on System of Systems Engineering" and "International Workshop on Software Engineering for Systems-of-Systems," indexed in the IEEE Xplore Digital Library, and the "International Journal of System of Systems Engineering," indexed in Scopus.

Mendeley desktop software has been used to preserve the traceability of the articles found. The main advantages of this software are its ability to manage bibliographies to different standards and to import bibliographies in different formats.

3.2.2 Study selection criteria

A set of inclusion and exclusion criteria was defined to filter which studies would be chosen as relevant for the mapping study, and quality assessment parameters were established to guarantee the quality of the chosen studies. The study selection criteria were used to identify the studies that could provide useful answers to our RQs by specifying impartial inclusion and exclusion conditions. The study selection was designed to be conducted collaboratively by all authors. Therefore, the criteria used had to be clear to enable a standardized selection of primary studies. By defining the selection criteria before conducting the search, it was also possible to reduce author bias when selecting primary studies.

The inclusion criteria helped to establish the conditions that a primary study is required to meet to be considered relevant. On the contrary, the exclusion criteria determined the articles that would be considered out of the scope for this SMS.

The following conditions were considered as inclusion criteria (all of them had to be true for inclusion):

- The study was carried out in the System of Systems context.
- The study focuses on SoS security and/or trust and/or privacy: i.e., the constituent systems in joint operations.
- The study is written in English.
- The study was published after 2010. Starting from 2010 was considered sufficient, as according to Axelson [14] this is the year in which this field of research began to grow.
- The study describes a validation scenario or applies its contribution to a validation scenario.

The following conditions were considered as exclusion criteria (only one of them is sufficient for exclusion):

- The title or abstract is not within the scope of this literature research.
- The study was not peer reviewed.
- The systems of systems addressed are not computer-based systems.
- The study does not consider more than one system.
- The author(s) cannot be identified.
- The contribution of the paper is unclear.
- The full text of the study is not available.

Secondary or tertiary studies found in the search would not be selected or analyzed but would nonetheless be retained for discussion in the Related Work section.

3.2.3 Snowballing cycle

Snowballing backward and forward [19] was applied. Backward and forward snowballing is conducted with the selected primary studies to ensure that no important studies are missed. For backward snowballing, references in the chosen primary studies were examined. For forward snowballing, we used available online tools, mainly Google Scholar, to identify those studies that cite each chosen primary study. As our original search included all the main digital libraries, we considered one cycle of snowballing to be sufficient to pick up any study missed in the search.

3.2.4 Quality assessment

Our search process is carried out using the resources available in peer-reviewed scientific digital libraries. Therefore, the quality assessment is delegated to the peer review process of each journal.

3.3 Research questions

The research questions (RQs) guide the entire study, as the purpose of the SMS is precisely to generate answers to these questions.

Nine RQs were defined to help achieve the goal of this study. In order to derive an adequate set of RQs several meetings among all the authors were devoted first to identify the most important aspects to extract from the studies, and then to refine the RQs by going through a sample of the studies. We also compared our RQs against other similar reviews from close areas. Finally, to better organize the RQs, three perspectives are used to summarize them: *Nature of the studies*, *SoS under study*, and *Study validation*.

(1) Nature of the studies. This perspective groups RQ1.1, RQ1.2, and RQ1.3. The questions in this nature are designed to discover the nature of published studies by considering their goals, scope, and the purpose of the contributions. This perspective will provide us an insight to understand the focus of this area of research: the motivations, area of interests, and the status of maturation.

By understanding the existing context, we can assess the existing body of knowledge, identify potential limitations, and propose future directions for research that address the specific needs and challenges of the field. It helps researchers to align their investigations with the practical realities, identify relevant research questions, and contribute to the advancement of the field by addressing specific challenges and needs.

(**2) SoS under study.** This perspective deals with the SoS studied in each research. It is made up of RQ2.1, RQ2.2, and RQ2.3. These questions examine the SoS used in the contributions, in other words: its architecture, the SoS dimensions being studied, and the roles of the participating humans. These questions are designed to determine the characteristics of the SoS on which the researchers are focused. Not all SoS behaves in the same way, and not all approaches focus on the same characteristics from a SoS. In this sense, this perspective provides knowledge regarding the coverage of published studies.

By analyzing the characteristics of these SoS, we can identify the breadth and depth of knowledge available in the field. For example, we can assess whether certain types of SoS have received more attention or if there is a preference for investigating security in specific types of SoS. In addition, by studying the types of SoS used in studies, we can identify patterns, trends, and potential gaps in the research. For instance, if certain types of SoS are more prevalent in the literature, it prompts further investigation into why this may be the case. Is it due to their ubiquity in real-world applications, their complexity, or other factors? Understanding these aspects can provide valuable insights into the priorities and research directions within the field of SoS security.

(3) Study validation. The third perspective aims at identifying how other authors validated their research. This corresponds to RQ3.1, RQ3.2, and RQ3.3. The purpose of this third categorization is to determine the impact of the validation on the selected primary studies by analyzing their application domains, the validation of the study, and the description of the used SoS that it would allow to replicate the results.

Assessing the ease of finding suitable validation scenarios provides valuable information about the practicality of implementing and testing SoS security measures. It helps us understand whether there are readily available scenarios or if researchers need to create custom environments for validation purposes. This insight is crucial for determining the feasibility of implementing proposed security measures in real-world SoS contexts.

Table 2 Research questions

RQ	Textual question
RQ1.1	What is the nature of the contribution?
RQ1.2	What are the objectives of the study?
RQ1.3	What non-functional (NF) requirements does the study focus on?
RQ2.1	How are the constituent systems of the SoS to which the study is applied orchestrated?
RQ2.2	What SoS dimensions are being analyzed?
RQ2.3	What roles are involved in the SoS security domain?
RQ3.1	What is the domain to which the SoS security study is applied?
RQ3.2	What is the availability of the described SoS?
RQ3.3	What is the validation of the study?

The level of detail in describing the SoS used for validation is another essential aspect. It enables other researchers to replicate and verify the results of previous studies, fostering the advancement of knowledge in the field. If the level of detail is insufficient, it may hinder the reproducibility and comparability of research findings.

Additionally, studying the level of integration between academia and industry provides insights into the practicality and relevance of research in addressing real-world challenges. Understanding the degree of collaboration and interaction between academia and industry helps bridge the gap between theoretical advancements and practical implementations, fostering more effective solutions and their adoption in the industry. For the sake of readability, a summary of the nine RQs is shown in Table 2 and the potential answers used for categorizing the selected primary studies are provided in Table 3.

For some of the RQs, we already know what the potential categories to group the selected primary studies are (i.e., RQ1.1, RQ1.3, RQ2.1, RQ3.2, RQ3.3). However, in the rest of the RQs we do not know in advance the groups on which we might categorize the studies according to what we find. An advantage of using a systematic mapping study (SMS) instead of a systematic literature review (SLR) is that SMS allows for more flexibility in the grouping and categorization of the included studies. In fact, an SMS allows for more exploratory research, where the groupings and categorizations of the included studies can be adjusted and refined during the review process. This flexibility can lead to the discovery of new and unexpected groupings and insights,

Table 3 Research question purpose and expected categorization

RQ	Purpose	Expected categories
RQ1.1	Nature of the contribution	(“Definitional,” “Descriptive,” “Explanatory,” “Predictive,” “Prescriptive”)
RQ1.2	Research objectives	{open list}
RQ1.3	Non-functional requirements	(“Security,” “Privacy,” “Trust,” “Security & Trust,” “Security & Privacy,” “Privacy & Trust,” “All of them”)
RQ2.1	Discern SoS architecture	(“Directed SoS,” “Acknowledged SoS,” “Collaborative SoS,” “Virtual SoS,” “Any”)
RQ2.2	SoS dimensions	{open list}
RQ2.3	Roles involved	{open list}
RQ3.1	Domain of application	{open list}
RQ3.2	SoS availability	(“Unavailable,” “Partially,” “Completely”)
RQ3.3	Study validation	("Industrial/Survey," "Industrial/Case study," "Industrial/Experiment," "Academia/Survey," "Academia/Case study," "Academia/Experiment" "Not Validated," "Review")

which might be missed in a more rigid review process. Therefore, the use of an SMS in this study allows for a more open and iterative approach to the analysis, which may reveal new findings and contribute to the development of a more comprehensive understanding of the research field.

Research Question 1.1. Research Question 1.1 states: “What is the nature of the contribution?”. This question identifies the knowledge provided by each study.

According to a study’s contribution, its nature would be classified as: “*Definitional*,” “*Descriptive*,” “*Explanatory*,” “*Predictive*,” or “*Prescriptive*.”

These categories come from “An Introduction to Design Science” [20], a book that lists different levels of maturity in the output of scientific research. Each category is associated with a question that is answered with the original contribution to the categorized study. RQ1.1 helps to reveal the level of maturity of the research area as a reflection of the nature of the published studies. The nature of the existing research allows to assess the existing body of knowledge, identify potential limitations, and propose future directions for research that address the specific needs and challenges of the field. It helps researchers to align their investigations with the practical realities, identify relevant research questions for unexplored gaps, and contribute to the advancement of the field by addressing specific challenges and needs. Table 4 describes each one of the alternatives.

Research Question 1.2. Research Question 1.2 states: “*What are the objectives pursued by the study?*”. This question identifies the objective of each study. Two categorizations were defined to address this research question.

On the one hand, one was used to categorize the purpose of the study. This refers to the purpose of the research, the outcome of the work, or, in other words, to what the authors were aiming to achieve or improve with their contribution.

On the other hand, the other was used to categorize the means used when pursuing the goal. This represents the scientific resources used by the authors to achieve the goal. The categories represent the means used as an instrument which did not necessarily provide new knowledge or improvements to this topic. RQ1.2 reveals what the areas of interest of the researchers were according to the nature of their contributions.

By highlighting the goals and means, we can evaluate whether the study addresses specific research gaps, provides specific solutions, or contributes to theoretical and general advancements in the field of SoS security.

Neither the goal nor the means were known in advance. Their categorization was discovered during the execution of the SMS. The categorization is defined during the data synthesis stage, and it can be found in Section 4.2, where Table 9 identifies the goals and Table 10 identifies the means used to achieve the goals.

Research Question 1.3. Research Question 1.3 stated: “What *non-functional requirements (NF) requirements does the study focus on?*”. According to the scope of the SMS, three non-functional requirements were described, namely “*Security*,” “*Privacy*,” and “*Trust*,” and their combinations. Identifying the non-functional requirements that the study focuses on is significant as it allows us to understand the specific aspects of SoS security that the research aims to address. The selected studies were classified using these non-functional requirements as shown in Table 5.

Research Question 2.1. Research Question 2.1 stated: “*How are the constituent systems of the SoS to which the study is applied orchestrated?*”. The orchestration of the SoS determines how the constituent systems are configured. In the literature [21, 22], four types of orchestration are considered to categorize how the constituent systems are organized: “*Directed SoS*,” “*Acknowledged SoS*,” “*Collaborative SoS*,” and “*Virtual SoS*.” RQ2.1 helped us understand the type of

Table 4 Alternatives, purpose, and interpretation for RQ 1.1

Nature of the studies	Responds to	Interpretation
Definitional	What is defined in the paper?	The study defines concepts, constructs, terminologies, definitions, vocabularies, classifications, taxonomies, and other kinds of conceptual knowledge
Descriptive	What is being described?	The study describes and analyzes an existing or past reality. It describes, summarizes, generalizes, and classifies observations of phenomena or events
Explanatory	What cause/effect is being validated?	The study provides answers to questions of "how" and "why." It explains how objects behave and why events occur. It not only describes and analyzes, but also explains in order to offer understanding. These explanations often take the form of cause-and-effect chains, showing how events and outcomes are causally related to underlying mechanisms and factors
Predictive	What is affected by the predictions?	The study offers black-box predictions. The goal is accurate prediction, not understanding
Prescriptive	What are the benefits that are pursued with the artifact?	The study consists of prescriptive models and methods that help solve practical problems. Prescriptive models are understood as blueprints for developing artifacts, while methods are guidelines and procedures that help people work systematically when solving problems

Table 5 Alternatives and interpretation for RQ1.3

N.F. requirements	Interpretation
All of them	The study focuses on security, privacy, and trust in a SoS
Privacy	The study focuses only on privacy in a SoS
Privacy & Trust	The study focuses on both privacy and trust in a SoS
Security	The study focuses only on the security of a SoS
Security & Privacy	The study focuses on both security and privacy in a SoS
Security & Trust	The study focuses on both security and trust in a SoS
Trust	The study focuses only on trust in a SoS

orchestration used when studying SoS security as indicated by the SoS architecture.

The orchestration of constituent systems has a direct impact on the overall security and resilience of the SoS. Understanding this aspect provides insights into the mechanisms, protocols, and architectures employed to ensure secure operation and coordination within the SoS. Studies with contributions applicable to different architectures were considered as "*Undetermined*." The categories used according to the SoS architecture are shown in Table 6.

Table 6 Alternatives and interpretation for RQ2.1

SoS orchestration	Description
Directed SoS [21]	The study focuses on SoS with constituents that operate independently but are managed by a central system
Acknowledged SoS [21]	The study focuses on SoS with constituent systems that operate for a common goal, but that retain their own independence and control. Therefore, collaboration is needed between the constituent systems and the SoS
Collaborative SoS [21]	The study focuses on SoS with constituent systems that collaborate voluntarily and are not controlled by central management
Virtual SoS [22]	The study focuses on SoS with constituents that are not controlled by central management and do not share a purpose of collaboration. The behavior and outcomes of these SoS emerge dynamically
Undetermined	The study analyzes an issue in SoS without specifying or requiring a specific architecture

Research Question 2.2. Research Question 2.2 stated: "*What SoS dimensions are being analyzed?*". SoS are so complex that they can be studied from many different perspectives (e.g., researchers could examine the SoS composition, its interaction with humans, shared resource optimization, or how each constituent system accountant participates in the SoS). This question classifies which perspectives of the SoS the authors considered in their studies. Each of the different perspectives from which a SoS can be studied is denominated a dimension for such a SoS.

The *SoS under study* dimension could vary widely from one study to another. By identifying the dimensions, we can assess how these characteristics influence the security considerations and challenges within the SoS. The dimensions were not known in advance. Therefore, the list of categories was established during the execution of the SMS. The different dimensions used to organize the studies are shown in Table 11 in Section 4.2.

Research Question 2.3. Research Question 2.3 stated: "*What roles are involved in the SoS security domain?*". This focused on the stakeholders in the proposed approach, that is, if the study considers any roles for specific tasks or activities. As the development and use of a SoS may involve many different stakeholders, this question is included to help us understand which roles are primarily addressed in the approaches proposed to date. Discovering the roles involved in the SoS security domain helps us comprehend the various stakeholders, their responsibilities, and their interactions within the SoS. Understanding the roles is crucial for developing comprehensive security measures that address the specific needs and concerns of each stakeholder group.

Described roles could vary, and a complete list is not known in advance. The categorization is created during the data extraction stage and can be found in Section IV.B, where the identified roles are summarized in Table 12.

Research Question 2.3. Research Question 2.3 stated: "*What roles are involved in the SoS security domain?*". This focused on the stakeholders in the proposed approach, that is, if the study considers any roles for specific tasks or activities. As the development and use of a SoS may involve many different stakeholders, this question is included to help us understand which roles are primarily addressed in the approaches proposed to date. Discovering the roles involved in the SoS security domain helps us comprehend the various stakeholders, their responsibilities, and their interactions within the SoS. Understanding the roles is crucial for developing comprehensive security measures that address the specific needs and concerns of each stakeholder group.

Research Question 3.1. Research Question 3.1 stated: "*What is the domain to which the SoS security study is applied?*". The application domain of SoS contributions may vary widely from one primary study to another.

Table 7 Alternatives and interpretation for RQ3.2

Availability	Interpretation
Completely	The SoS described in the study is fully accessible and can be used to replicate the results
Partially	The SoS described in the study is partially described or available
Unavailable	The SoS described in the study is not available at all

Understanding the domain of application provides insights into the practical implications, challenges, and requirements of implementing secure SoS solutions in real-world settings.

The alternatives were not known in advance. The list of categories was generated during the execution of the SMS. The categorization is created during the data synthesis and can be found in Section IV.B, where Table 13 summarizes the studies that identified an application domain.

Research Question 3.2. Research Question 3.2 stated: "*What is the availability of the described SoS?*". This question helped identify whether the described SoS is available and/or can be used to replicate the study of its security. In many contexts, researchers are now requested or advised to make their experimentation constructs publicly available in order to facilitate further research and transition toward what is known as Open Science. To categorize availability, three alternatives were considered: "*Completely*," "*Partially*," and "*Unavailable*." They are shown in Table 7.

Research Question 3.3. Research Question 3.3 stated: "What is the validation of the study?". This categorization determines the validation of the selected studies.

The validation processes employed in the studies are crucial for evaluating the reliability and credibility of the research findings. Validation ensures that the proposed security measures have been rigorously tested and verified. It provides confidence in the effectiveness and correctness of the proposed solutions for SoS security.

To categorize the validation, three alternatives were considered: "Not validated," "Industrial validation," and "Academia validation." Validation has been considered as an inclusion criterion; however, there might be studies that, even though they do describe a validation, have not been conducted in that manuscript (e.g., the validation is described, is referenced, or is scheduled as a future work). For studies that conducted a validation, three different validations were considered: "Surveys," "Case Study," and "Experiment." The alternatives used to categorize the validation of the study are shown in Table 8. Some studies may describe a validation but may not have executed it. This question summarizes the

Table 8 Alternatives and interpretation for RQ3.3

Validation	Interpretation
Academia validation	The study presents a validation in academia. Such validation may be a Survey, a Case Study, or an Experiment
Industrial validation	The study presents an industrial validation. Such validation may be a Survey, a Case Study, or an Experiment
Not validated	The study may describe a validation scenario, but it has not been applied
Review	The study is a review. Validation is not applicable

levels of validation of the different approaches to SoS security.

4 Conducting

This SMS has been carried out by all authors according to the previously defined planning. The goal of this stage is to obtain a catalog of primary studies that would help answer the RQs. The data extracted from the selected primary studies allow us to generate a report on the current state of the art. A search in the digital libraries was conducted in October 2020 and was then updated in February 2022.

4.1 Selecting primary studies

The identification of the primary studies was divided into three milestones. (1) A pre-search was conducted prior to the systematic search. This pre-search was used as a sample for the quality of the findings. If the results were extremely poor in terms of providing adequate answers to the RQs or if very few results were found, the planning would be modified by using other keywords. (2) A systematic search was executed once the pre-search had returned relevant results. Finally, to provide better coverage, (3) the snowball effect was applied to the selected primary studies.

Following the pre-search to adjust the search criteria, some minor changes were needed in the keywords to bring them in line with the libraries' requirements. In particular, the acronym "SoS" was removed. In some cases, the acronym "SOS" was mistaken for, while in other cases the digital library assumed that our input was wrong and changed “SoS” to "so" or "os" in an attempt to correct the user input. Both options added excessive noise, resulting in some articles found that were not, in fact, about “SoS.”

The search string needed to be adapted to each different library. The results of applying each search string adaptation in its corresponding digital library are summarized in Fig. 2.

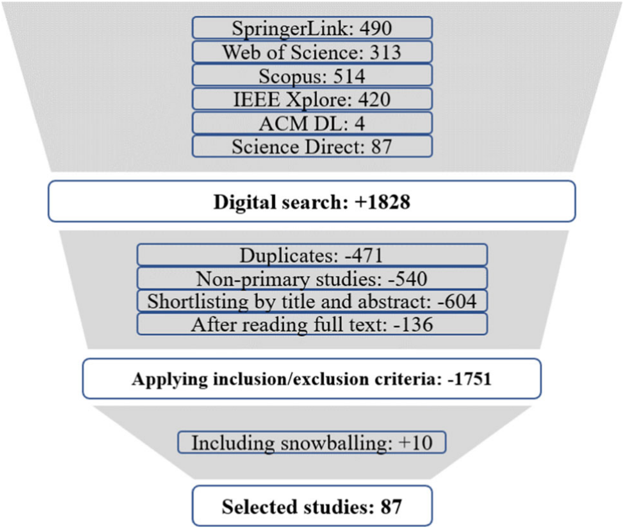
SpringerLink: 490
Web of Science: 313
Scopus: 514
IEEE Xplore: 420
ACM DL: 4
Science Direct: 87
Digital search: +1828
Duplicates: -471
Non-primary studies: -540
Shortlisting by title and abstract: -604
After reading full text: -136
Applying inclusion/exclusion criteria: -1751
Including snowballing: +10
Selected studies: 87

Fig. 2 SMS conducting summary

Automated filters such as the year of publication, language, and availability of full text were applied in those libraries that supported this filtering of the results. Also, area of knowledge filter was applied were possible restricting the discipline to computer science.

In total, among all consulted libraries, 1828 studies were found. A full list of papers was generated for each library using the tools available in each library. As mentioned in the Selection Criteria, only studies for which full articles were available were considered. The full list of papers was then imported into the Mendeley Desktop software.

The Mendeley software offers an automated tool to find potential duplicated studies. Using this mechanism, 471 articles were found to be included more than once in the catalog. Also 540 studies were found as non-primary.

The titles and abstracts of each of the remaining studies were read individually by a pair of authors, who were thus able to make a decision as to whether each study should be discarded or not. These decisions were later discussed in a plenary meeting of all authors, with the title and abstract of a work being read by a third author in the event of disagreement. A total of 604 articles were found to be not within the scope of this study. The last step in the systematic search was full reading of the remaining 210 selected articles by a pair of authors.

This full reading helped determine whether only the keywords were relevant or whether the context, too, was akin to the defined RQs. After full reading of the selected studies, some papers were found to describe systems of systems used to improve the security of a third party, rather than the application of SoS security by itself. In general terms, more than half of the works found used keywords in contexts outside the scope of our study (e.g., wars and crisis). Only 77 studies that were still relevant to our research remained.

The analysis and classification of each one of these 77 studies were assigned to a pair of authors. Each author read and classified their assigned chosen primary studies individually. The two classifications were then compared. If both authors agreed, the classification was confirmed; otherwise, discrepancies were discussed in a plenary meeting. If no agreement could be reached at the meeting, the first author was given the responsibility of analyzing the primary study in question and deciding the final classification after considering all points of view. This strategy contributed to ensuring the quality of the results and avoiding single-author bias.

Once the analysis of the studies found in the systematic search was complete, snowballing was applied. As a result, 10 more primary studies were found, which helped answer the RQs and detail the current state of the art. Then, these newly found studies were brought under the same selection criteria.

Eventually, a total of 87 studies were selected as primary studies. The results of this application of the systematic process are summarized in Fig. 2.

The 87 selected primary studies are listed in Table 25, organized as search papers and snowballing papers. Within each category, the articles are sorted alphabetically.

4.2 Data extraction

The data extraction process is a collaborative manual task that aims to categorize each selected primary study.

Analyzing data extracted from selected studies provides a general overview of trends in the area being surveyed and identifies gaps and tendencies. Here, the data were extracted considering the three perspectives previously defined while planning the SMS: *Nature of the studies*, *SoS under study*, and *Study validation*. The selected studies were tagged to organize them into the different RQs according to their content.

The categorization of each study during the *Data extraction process* was conducted in a similar way as it was during the *Selecting primary studies* stage. Each study was individually classified by a pair of authors. Furthermore, this stage is used to define a categorization for those RQs that initially did not have a well-defined categorization.

The pair of authors that read each full text proposed a categorization, and then all authors compared and discussed the two categorizations in plenary meetings, with the aim of agreeing on the most appropriate categorization. There were few cases in which an agreement was not reached, and the first author was responsible for rereading the full article and deciding on a classification for such a study.

The process of generating the classification criteria varied depending on the level of uncertainty associated with each question. As some questions had potential categories not constrained to a limited set of alternatives, we encountered challenges in determining the specific categories. In such cases, we had to rely on the information provided in the studies and use our best judgment to group them into relevant categories.

Table 9 Alternatives and interpretation for Goals RQ1.2

Goal—What?	Interpretation
Describe the state of the art	This is a descriptive study that does not provide a new approach or validation
Early detection	The study focuses on improving security, trust, or privacy through the early detection of vulnerabilities
Need for security	The study enforces or discusses the need for security in SoS
Risk management	The central topic of the study is risk management related to security, privacy, or trust
Security assessment/evaluation	The study provides knowledge about security assessment
Security controls	The study focuses on security controls and their impact on SoS security, privacy, or trust
Security engineering	The study provides knowledge about security engineering, it includes modeling and analysis
Security requirements	The study provides knowledge about security requirements and their impact on security, privacy, and trust
Trust among constituent systems	The study contributes to establishing or enhancing trust between the constituent systems of a SoS

The first perspective is the *Nature of the studies*. The combination of the research nature, goal, and means of each study allowed us to identify the nature of the contributions. When reading the full texts, some categories were required to group the selected primary studies according to their goals and means as proposed for RQ 1.2.

With the aim of developing a representative grouping, we classified the studies considering nine different goals, and 16 different means to be used to achieve such goals, as summarized in Tables 9 and 10, respectively.

This classification has been the most challenging one since not all studies explicitly described their goals and means in a way that could be easily summarized by a specific keyword. Therefore, the categorization in these cases involved a certain degree of interpretation based on the available text. Consequently, the classification of goals and means is as generic or specific as the text allowed us to classify them.

Table 10 Alternatives and interpretation for Means RQ1.2

Means—How?	Interpretation
Defense strategies	The study provides knowledge about security, trust, or privacy using defense strategies as their main vector
Domain-specific modeling language	The study achieves its goal using a domain-specific modeling language
Misbehavior analysis	The study focuses on analyzing the misbehavior between the constituent systems as a means of achieving the research goal
Model-driven engineering	The study uses the model-driven engineering paradigm to achieve the research goal
Patterns	The study uses patterns to achieve its research goal
Policy	The study describes how policies are used to achieve its goal
Process	The study provides a process as a set of activities and outcomes with which to achieve the goal
Security analysis	The study analyzes SoS security. This is used by some descriptive analysis to achieve its goals
Security challenges	The research focuses on examining security challenges to describe their novelty
Security controls	The study uses security controls as an instrument to achieve its goal
Security requirements	The study uses security requirements as an instrument to achieve its goal
Security validation/evaluation	The study uses security validation or security evaluation mechanisms to achieve its goal
SoS design	The study uses SoS modeling and SoS design as a resource to achieve its results
System interdependencies	The study uses interdependencies between systems to achieve the goal
Threat analysis	The study uses threat analysis as a mechanism or paradigm to achieve its goal
Undetermined	The study does not provide a well-defined means of achieving its stated goal

Table 11 Alternatives and interpretation for RQ2.2

SoS Dimension	Interpretation
Emergent behavior	The study analyzes the new behaviors emerging from the collaboration of the constituent systems
Human factor	The study analyzes how human involvement may impact SoS security
Multiple dimensions	The study simultaneously analyzes different dimensions but does not specifically focus on any of them
None in particular	The study does not clearly identify a SoS dimension
SoS Architecture	The study explores the technical details of what resources are shared and how the constituent systems share them
SoS Management	The study analyzes how the stakeholders of the constituent systems jointly manage the SoS
SoS Mission	The study analyzes the purpose of collaboration of the constituent systems

The goals and means were an open list, which has been created based on an interpretation made by the authors according to the primary studies read. We are aware that other groupings could have been identified using different keywords. Notwithstanding these categorizations have been used with the objective of showing the results and should not be considered as the unique alternative. For instance, some of the used means might be grouped into more generic categories (e.g., *Security analysis*, *Security challenges*, *Security controls*, and *Security requirements* could be a single category *Security*). An ontology of goals and means regarding security would improve the organization of these studies and make them reliable because even within the selected articles themselves, there may be semantic divergences in used words.

In order to organize the studies and provide an answer to RQ 2.2., five dimensions of SoS emerged from the analysis of the studies that could be relevant categories, namely: "*SoS Architecture*," "*SoS Mission*," "*SoS Management*," "*Emergent Behavior*" and "*Human Factor*." The dimensions used to organize the studies are described in Table 11. We also included additional criteria: *"None in particular,"* used to include generic studies that did not identify specific dimensions, and *"Multiple dimensions"*, for those studies that simultaneously covered different dimensions without focusing on a specific one.

Besides, the selected studies did not explicitly define the roles that participate, neither use the concept of "*role*" in their scientific contributions. Therefore, it was not possible to extract explicit information regarding RQ2.3. Nevertheless, two main roles are inferred from the full text of selected primary studies and described in Table 12.

Regarding the SoS application domain categories, 11 different scenarios were identified to categorize the selected primary studies and provide an answer to RQ3.1. Additionally, a "None" application domain is included as there are

Table 12 Alternatives and interpretation for RQ2.3

Identified roles	Interpretation
Not specified/not applicable	The study does not clearly identify any role
Security-related roles	The study describes a team responsible for assessing the security of a system
Systems related roles	The study describes a team responsible for studying the requirements of a system and setting up the environment for development

Table 13 RQ3.1 identified alternatives

Application domain	Interpretation
Automotive	Improving the way vehicles communicate and share information to provide a better experience for drivers or self-driven vehicles
Banking	The constituent systems serve the banking domain
Critical infrastructure	This is a general term for describing SoS related to safety–critical assets
Cyber-physical	The constituent systems include the internet of things and robots in their composition
Energy	Constituent systems are used in electricity companies
Industry 4.0	Some studies focus generically on Industry 4.0 but do not refer to any one specific application (e.g., Energy, Quarry, or Banking)
Maritime	The constituent systems are related to boats, lighthouses, and military (naval) systems
Military	Border control and cooperation in emergency operations are two recurrent application domains
None	No application domain is explicitly identified
Quarry	The constituent systems serve the quarrying industry
Smart {cities, grids, homes, …}	The SoS elaborates on the Smart concept, using different systems and connected information to improve the user experience
Social networking	The constituent systems are different social networks that share people’s data

some selected primary studies that did not describe any application domain (Table 13).

4.3 Data synthesis

The synthesis of the data collected from the selected primary studies and the categorization that organizes them are guided by the defined RQs. For each RQ, the studies were examined according to the defined criteria and following the procedure detailed in Section 3. Planning.

We have calculated the effect size of our results using Cohen’s*d* to provide a quantitative measure of the magnitude of differences or relationships among the study results. This method involves dividing the difference in means between two groups by the pooled standard deviation of the data. This approach allowed us to obtain an objective measure of the effect size of our findings, aiding in the interpretation of their practical significance.

The calculus to compare two groups has been achieved by calculating the effect size as (M1–M2)/SDp, where M1 is the mean of the first group, M2 is the mean of the second group, and SDp is the pooled standard deviation of the data. We determined the pooled standard deviation as $\sqrt{\left(\frac{((n1-1)*s1^2+(n2-1)*s2^2)}{(n1+n2-2)}\right)}$, where s1 and s2 are the standard deviations of the two groups, and n1 and n2 are the sample sizes of the two groups. To compare more than two groups, we used the Cohen’s *d* formula that provided a quantitative measure of the magnitude of differences or relationships among the means, allowing to identify statistically significant differences between groups.

Each one of the nine RQs identifies the selected primary studies and organizes those primary studies into tables, grouping them by their classification.

4.3.1 Nature of the studies

RQ1.1 stated: “*What is the nature of the contribution?*”. The selected studies were classified according to their nature, as shown in Table 14. It should be noted that each study was classified by considering only one nature.

According to this categorization, “*Descriptive*” and “*Prescriptive*” were by *far* the most common natures when addressing System of Systems security.

We applied Cohen’s *d* technique to compare the mean values of these five different groups and found significant differences between them, with effect sizes ranging from moderate to large.

Table 14 Classification of studies by nature

Nature	Selected primary studies ID	Number	*d*
5. Prescriptive	1, 2, 3, 4, 6, 7, 9, 11, 13, 14, 17, 23, 26, 27, 28, 29, 37, 41, 47, 48, 49, 51, 54, 56, 57, 58, 59, 61, 64, 67, 70, 72, 73, 75, 76, 83, 84	37	1.30
2. Descriptive	8, 10, 12, 18, 20, 21, 22, 24, 25, 31, 32, 34, 36, 38, 40, 42, 43, 46, 52, 62, 66, 69, 71, 74, 78, 81, 82, 86, 87	29	0.77
3. Explanatory	15, 30, 33, 39, 44, 55, 65, 77, 79, 80	10	− 0.49
1. Definitional	5, 16, 19, 35, 45, 50, 60, 63, 68, 85	10	− 0.49
4. Predictive	53	1	− 1.09

Table 15 Classification of studies by goal

Goal	Selected primary studies ID	Number	*d*
Need for security	1, 9, 10, 18, 19, 20, 21, 25, 29, 31, 46, 52, 55, 65, 86	15	1.75
Security controls	2, 3, 6, 7, 11, 12, 34, 37, 51, 53, 62, 84, 87	13	1.10
Security engineering	4, 23, 39, 41, 42, 47, 48, 56, 59, 70, 71	11	0.44
Describe state of the art	24, 33, 38, 43, 63, 68, 77, 79, 81, 82	10	0.11
Risk management	5, 26, 32, 35, 61, 67, 72, 74, 80	9	− 0.22
Early detection	13, 15, 36, 49, 50, 60, 66, 69, 85	9	− 0.22
Security assessment/evaluation	14, 17, 28, 44, 57, 64, 75, 78	8	− 0.55
Security requirements	16, 22, 30, 45, 59, 76, 83	7	− 0.88
Trust among constituent systems	8, 27, 40, 54, 73	5	− 1.53

4.3.2 Research objectives

RQ1.2 stated: “What are the objectives pursued by the study?”.

The classifications to RQ1.2 were discovered during the data extraction. Each study was classified according to its main objective and means. Therefore, each selected primary study was considered only once.

On the one hand, the classification of the studies according to their goal is summarized in Table 15. The most common objective pursued in the selected primary studies was to address the need for security, followed by security controls.

On the other hand, the means used in the selected primary studies are shown in Table 16. The most common means used to achieve such goals were security validation or evaluation and security controls.

In these tables is also included the Cohen’s *d* so that it is possible to compare the difference among each group by considering the numbers of studies included in each one of them.

4.3.3 Non-functional requirements

RQ1.3 stated: “Which non-functional (NF) requirements is the study focusing on?”.

To respond to this question, the papers were categorized according to the non-functional requirements being addressed.

Table 17 lists the primary studies according to their non-functional requirements. Each study has been classified into only one category. Security is the predominant topic, present in more than 97% of the primary studies selected.

We have separated those studies according to those focusing only in security (70 studies in a single group) and the rest of the studies (17 studies in 3 groups), Using Cohen’s formula, we calculated the effect size of our study to be 17.40. The large effect size suggests that there is a statistically significant difference between the means of the two groups. This value can be used to compare with future updates of the used queries, to determine whether there is an increase in the diversity of studied N.F. requirements or if security remains the most important N.F. requirement studied.

4.3.4 SoS orchestration

RQ2.1 stated: “How are the constituent systems of the SoS to which the study is applied orchestrated?”.

The studies were categorized according to the SoS orchestration being addressed. However, we found that most studies did not explicitly mention the targeted SoS orchestration. In those that defined the type of SoS orchestration, collaborative SoS was prevalent. Table 18 lists the primary studies according to the SoS orchestration.

The effect size of this RQ compares the studies with undetermined SoS orchestration (60) with those that stated their SoS (13, 6, 6, and 2). The value of Cohen’s *d* indicates that there is a significant difference between both groups with a magnitude of 5.43.

Table 16 Classification of studies by means

Means	Selected primary studies ID	Number	*d*
Security validation/evaluation	1, 18, 27, 32, 37, 38, 39, 48, 49, 57, 59, 65, 72, 75, 77	15	1.94
Security controls	3, 5, 6, 7, 11, 16, 21, 29, 31, 34, 53, 73, 83, 84	14	1.74
System interdependencies	17, 20, 24, 28, 36, 43, 45, 52, 62, 64, 69, 80	12	1.33
Security challenges	2, 8, 10, 25, 33, 55, 63, 81, 82, 87	10	0.93
Security requirements	4, 13, 22, 26, 30, 41, 46, 60, 61	9	0.72
Security analysis	14, 40, 56, 58, 70, 78	6	0.11
Defense strategies	12, 15, 35, 51	4	− 0.29
Undetermined	19, 66, 74, 79	4	− 0.29
Threat analysis	42, 67	2	− 0.70
Policy	54, 68	2	− 0.70
Domain-specific modeling language	47, 71	2	− 0.70
Patterns	9, 44	2	− 0.70
SoS design	23, 50	2	− 0.70
Model-driven engineering	76	1	− 0.90
Process	86	1	− 0.90
Misbehavior analysis	85	1	− 0.90

Table 17 Classification of studies by N.F. requirements

Non-functional requirements	Selected primary studies ID	Number
Security	1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25, 26, 28, 30, 33, 34, 35, 37, 38, 39, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, 55, 56, 57, 58, 59, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 76, 77, 78, 80, 81, 82, 83, 84, 85, 86, 87	70
Privacy & Security	23, 32, 53, 60, 61, 74, 75, 79	8
Security & Trust	8, 27, 29, 31, 43, 73	6
Trust	36, 40, 54	3
All of them	[]	0
Privacy	[]	0
Privacy & Trust	[]	0

Table 18 Classification of studies by SoS architecture

SoS orchestration	Selected primary studies ID	Number
Undetermined	1, 4, 5, 7, 8, 10, 11, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 25, 26, 27, 31, 33, 36, 38, 39, 40, 41, 43, 44, 46, 47, 48, 49, 50, 51, 53, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 67, 69, 70, 73, 78, 79, 80, 81, 82, 83, 84, 85, 87	60
Collaborative SoS	9, 12, 19, 24, 30, 34, 42, 45, 66, 68, 72, 74, 77	13
Acknowledged SoS	3, 29, 54, 71, 76, 86	6
Directed SoS	2, 6, 28, 32, 52, 75	6
Virtual SoS	35, 37	2

Table 19 Classification of studies by SoS dimension

SoS dimension	Selected primary studies ID	Number
SoS Architecture	1, 2, 3, 4, 5, 7, 8, 9, 16, 20, 22, 23, 25, 27, 28, 29, 30, 33, 34, 36, 38, 41, 42, 45, 47, 48, 50, 51, 52, 53, 54, 56, 58, 59, 62, 69, 70, 71, 72, 73, 75, 77, 78, 80, 83	45
Emergent behaviors	6, 14, 17, 18, 32, 39, 44, 55, 57, 60, 63, 67, 79, 84, 85	15
None in particular	10, 11, 12, 13, 15, 21, 31, 43, 65, 66, 68, 81	12
SoS Management	19, 26, 37, 46, 61, 64, 74, 87	8
Multiple dimensions	24, 76, 82, 86	4
Human factor	35, 49	2
SoS Mission	40	1

4.3.5 SoS dimensions

RQ2.2 stated: "What SoS dimensions are being analyzed?".

The selected studies were classified according to the SoS dimension on which they focused. This categorization started as an open list. From the analysis of the studies, five dimensions of SoS emerged that could be taken as relevant categories.

Table 19 lists the selected primary studies according to the SoS dimensions and the ratio for each dimension. Almost half of the primary studies selected focused on SoS architecture, while the second most researched SoS dimension was Emergent Behavior, with 15.52% of the studies.

When comparing the most populated group, SoS Architecture, to the other dimensions, the Cohen's *d* indicates a

Table 20 Classification of studies by roles

SoS role	Selected primary studies ID	Number
Not specified/not applicable	2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25, 26, 27, 30, 31, 32, 33, 35, 36, 38, 39, 40, 41, 42, 43, 44, 45, 46, 48, 49, 50, 51, 54, 55, 58, 59, 60, 63, 64, 65, 66, 67, 68, 70, 71, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 87	70
Systems related roles	1, 3, 23, 29, 34, 37, 52, 53, 56, 57, 61, 62, 69, 72	14
Security-related roles	28, 47, 86	3

smaller difference than in previous classifications, with a magnitude of 1.89.

4.3.6 Roles involved

RQ2.3 stated: “*What roles are involved in the SoS security domain?*” This categorization was left as an open list.

The selected studies did not explicitly define the roles that participate, neither use them on their scientific contributions. From our understanding, we could understand which role are participating on each study and classified them in Table 20.

This classification’s effect size reveals that there is a significant difference between studies that did not mention any role (70 studies) and those that stated any role (14 and 3), with a magnitude of 11.18.

4.3.7 Domain of application

RQ3.1 stated: “What is the domain to which the SoS security study is applied?”.

Almost half of the selected primary studies did not discuss the application domain of their scientific contribution. Table 21 shows the number of primary studies selected corresponding to each domain. Note that each study was classified only once, according to its principal application domain.

We categorized the studies based on their domain application and compared the group with a domain application to the group without any specific application domain. Using Cohen’s *d* formula, we calculated the effect size and found that the difference between these two groups was 1.98, indicating a moderate effect size.

4.3.8 SoS availability

RQ3.2 stated: “What is the availability of the described SoS?”.

Table 21 Classification of studies by application domain

Application domain	Selected primary studies ID	Number
None	2, 3, 4, 5, 7, 8, 10, 11, 12, 13, 15, 16, 18, 21, 26, 28, 33, 36, 39, 40, 42, 43, 44, 45, 46, 48, 53, 56, 57, 59, 63, 64, 65, 68, 69, 71, 79, 81, 82, 84, 87	41
Smart {cities, homes, …}	22, 47, 50, 58, 60, 61, 62, 66, 72	9
Military	19, 25, 49, 51, 80, 85, 86	7
Critical infrastructure	20, 24, 52, 73, 74, 77, 83	7
Automotive	1, 14, 23, 29, 34, 41	6
Cyber-physical	31, 38, 55, 78	4
Quarry	30, 75	2
Banking	17, 32	2
Social networking	35, 37	2
Industry 4.0	9, 27, 54	3
Maritime	70, 76	2
Energy	6, 67	2

Table 22 Classification of studies by SoS availability

SoS availability	Selected primary studies ID	Number
Not available	1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40, 41, 42, 43, 45, 46, 47, 48, 49, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87	78
Partially	2, 14, 21, 23, 24, 37, 44, 50, 77	9
Completely	[]	0

The availability of the SoS being studied in the primary selected studies was not high. Less than 8% of the primary studies selected described the SoS, and no single study fully described the SoS sufficiently to allow replication of the results obtained and support future research. Table 22 lists the primary studies according to SoS availability and the corresponding ratio.

To compare studies that specify their domain of application with those that do not, we grouped them into two categories. The Cohen’s *d* formula was used to calculate the difference between the means of these groups, which resulted in a magnitude of 16.33 apart.

Table 23 Classification of studies by validation

Research validation	Selected primary studies ID	Number
Not validated	1, 3, 4, 5, 7, 8, 10, 17, 20, 21, 22, 25, 29, 31, 32, 33, 34, 36, 38, 39, 40, 42, 44, 53, 55, 56, 61, 63, 68, 69, 71, 72, 78, 79, 81, 82, 86	37
Academia/Case study	9, 11, 12, 13, 14, 15, 16, 19, 23, 24, 26, 27, 28, 30, 37, 41, 43, 47, 48, 49, 50, 52, 57, 58, 59, 60, 62, 64, 66, 67, 70, 73, 75, 76, 83, 84	36
Academia/Experiment	2, 6, 35, 45, 80, 85	6
Academia/Survey	18, 46, 65, 87	4
Industrial/Case study	51, 54, 77	3
Industrial/Survey	74	1
Industrial/Experiment	[]	0

4.3.9 Study validation

RQ3.3 stated: "What is the validation of the study?".

Almost 57% of the selected primary studies did not present any kind of validation. Less than 5% of them described an industrial validation.

Table 23 lists the papers according to the types of validation offered.

The comparison between the studies showing validation and those without a specific validation resulted in a small effect size of 0.59, indicating a relatively small difference in the means between the two groups. Also, by applying the Cohen's d formula, to calculate the distance among those validated case study by the academia and the other validations we found a difference of 4.76 units, indicating a moderate effect size.

4.4 Threats to validity

Our identification of the threats to the validity of this work is based on those proposed in [23] and [24] and includes bias in the selection of the studies, inaccuracy in data extraction, and potential errors during the classification process. We also applied the mitigation strategies proposed by [24].

4.4.1 Study selection

Given the abundance of subscription libraries, gray literature, and continuous publication processes, it is impossible to achieve full coverage of every work on any given topic. To minimize this threat, we used multiple digital libraries and databases. Six digital resources (*ACM DL, IEEE Xplore, Science Direct, Scopus, Springer,* and *Web of Science*) were used, containing primary studies related to the System of Systems context. We considered the scopes of the libraries used in the searches in this SMS to be large enough to achieve a reasonable completeness.

As an additional challenge, some libraries list articles dealing with "Security" for "Systems of Systems," but some articles mention the same terms in reverse order, i.e., "Systems of Systems" applied to "Security," which is out of the scope of this SMS. Another threat is the lack of standard language, a potential source of confusion in the research process. To mitigate this threat, we held discussion meetings with all authors and some experts in the field of SoS security research.

Since research on SoS security is iterative and incremental, we expected to find the latest versions of each study, and thus detect a trend. However, not always being able to retrieve relevant studies, we established a protocol during the planning phase. This involved contacting the authors of inaccessible articles to obtain the missing texts. We also used multiple databases and tools that executed queries from different sources to reduce errors during the search phase.

A fair selection process is guaranteed because the research questions and inclusion and exclusion criteria were defined before the research was carried out. The selection of the studies involved all the authors who participated in this SMS.

Study duplication is a threat that was not found to exist after several verifications by the authors. Here, we applied the mitigation strategy proposed by [24], checking the articles twice to detect and remove duplicates. Irrelevant articles were excluded after reading the title, abstract, and conclusions.

4.4.2 Inaccuracy in data extraction

This research involved a detailed read of each selected primary study. This activity, carried out by all authors, was potentially susceptible to inaccuracy, with different parts of the studies incorrectly identified as relevant. To make our analysis of the primary studies as objective as possible and to reduce the bias of a single author, we organized it so that each article was read by at least two different authors. Therefore, bias in study selection was countered by a cross-check review to ensure the completeness of the searches and validate the suitability of each study for inclusion. Regular meetings of all authors were also used to reach agreement on the data to be extracted and the proposed classification.

4.4.3 Potential errors during the classification process

Potential errors in the categorization of some selected studies could not be ruled out. The incorrect classification of the extracted data could be attributed to a subjective interpretation of the data. We did our best to prevent this by establishing a meticulously shared process to read and classify each work at each step of the study. As previously described, both data extraction and classification were performed in pairs to reduce single-author bias. In other words, this threat was mitigated by having two authors perform data extraction and independently check the results of each review. As all results were evaluated collectively during the plenary meetings, this guaranteed additional perspectives and a more general, shared view of the results for each RQ.

4.4.4 Study reliability

The process of conducting this study has been documented to allow its replication. However, some differences may arise when compared with this SMS. For example, other researchers may interpret the selected studies differently during the classification process. This vulnerability is more relevant in those categories that were initially left open. While the semantics of the selected studies remain the same, the meaning of the same word may be understood differently among other groups of researchers. Furthermore, the depth of analysis may also vary, and therefore the answers to the RQs could be slightly different. To prevent this threat, we have detailed the process and reasoning of our decisions.

4.4.5 Study validity

The goal of the study is to provide a comprehensive understanding of the state of the art regarding security on systems of systems. For this purpose, we also included the terms privacy and trust while conducting the study. To guarantee the validity of this study, we stated a set of RQs organized on different perspectives according to their purpose. Consequently, giving an answer to these questions by using the results of the search provides validity to this research.

5 Reporting

In this SMS, 87 papers were selected, classified, and studied after conducting the systematic search strategy in six digital libraries.

As it can be seen in Fig. 2, a 4.81% (87/1828) of the found studies were selected as relevant in the SoS security, privacy, and trust context. The results were conditioned by the relatively low number of events and journals dedicated to this topic. Accordingly, IEEE-sponsored events represented near 60% of the articles found.

The vast majority of studies that were found while conducting SMS were discarded after noticing that the research was not about the security, privacy, and trust properties of SoS, but about using a SoS to improve such properties for third parties.

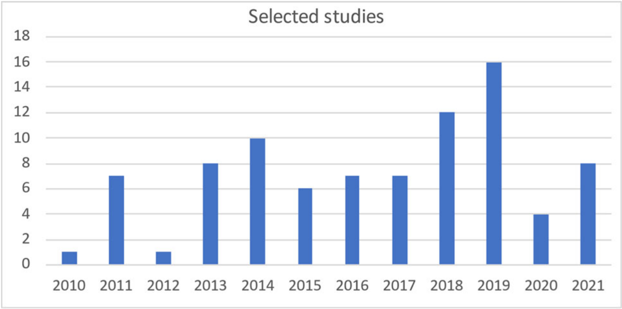

Fig. 3 Number of selected published primary studies papers

In the covered years, the number of primary studies published has increased slightly. This incremental trend in research into SoS security is attributable to the recent popularity of connected devices that collaborate to achieve shared goals; two of the most notable examples of SoS adoption are smart cities and smart grids.

To provide a graphical representation of the growing trend, Fig. 3 shows how the number of articles published has increased since 2010. If research in this area continues to grow at this same rate, nearly 10 new scientific contributions focusing on SoS security are expected to be published yearly.

The main findings of the selected primary studies are given below, divided according to the three perspectives used to organize the RQs, namely *the nature of the studies*, *the SoS under study*, and *the validation of the study*.

5.1 Nature of the studies

Regarding RQ1.1 "*What is the nature of the contribution?*", the most published contribution types were *Prescriptive* and *Descriptive* papers, with a total of 66 papers (75.86% of the total). The nature of these published studies indicates the beginning of a new area of research, and even recent studies are still *Definitional* and *Descriptive*, which define and describe the context of the SoS, namely the "*what*" question. Moreover, few of the selected primary studies are *Explanatory,* in other words, few are focusing on the "*how*" or the "*why*" questions. As this area of research keeps attracting more and more attention and motivates research and/or transference projects, the number of *Explanatory* articles will grow accordingly.

There is a noticeable difference between *Definitional* and *Prescriptive* primary studies. On the one hand, *Definitional* studies are intended to set out the basic knowledge, to establish a common understanding. This is in fact one of the natures with the fewest published manuscripts. *Prescriptive* contributions, which represent the last stage of research (i.e., saying why a solution is good to solve a problem), are the most common type. These results are counterintuitive as the authors are providing solutions to problems that (according to our findings) have not yet been defined or identified in depth.

To better guide the evolution of this area, more *Definitional* studies would be needed, setting up a standardized understanding before providing solutions to some particular issues. More precisely, this issue has already been identified by a set of experts in a recent study [18].

To identify the purpose of each selected primary study RQ1.2. stated "*What are the objectives pursued by the study?*". According to our findings, a huge number of selected primary studies aims at addressing the concepts of *need for security*, *security controls*, and *security engineering*. These three goals are pursued by 44.31% of the studies. The most used means to achieve such goals are the *security validation/evaluation*, the *security controls*, and the *interdependencies between systems,* which are used in 46.59% of the studies. As it has been already identified in related SoS SLRs, most of the research on security of SoS is intended to solve non-replicable problems. Not defining solution approaches able to be used in different contexts hinders their widespread adoption.

Among the used means, we found that most of the used means can be categorized as tactical processes rather than strategical ones. In other words, few selected primary studies have used a means that define planning. In contrast, most of the means are individual actions that help achieving their goal.

According to our findings, few works have focused on the need of establishing security standards for the constituent systems, an approach that could be categorized as a contribution to the establishment of common strategies [25–29]. Standardized security strategies among parties within the SoS would provide a common understanding of what security, privacy, or trust is, improving the efficiency and performance of security countermeasures.

The last question of this first dimension, RQ.1.3, states "*Which non-functional (NF) requirements is the study focusing on?*". This RQ aims to identify which one among security, privacy, and trust is studied the most. The results show that the largest part of the selected studies focuses on security (96.55%), being trust and privacy barely mentioned in the literature. This is contrary to our expectation and denotes a need for greater awareness of privacy and trust concerns.

Despite the high prevalence of security-related studies, security still seems to be considered a second-class feature by itself in SoS, with a relative scarce representation in scientific libraries. With the increasing interest in keeping the Internet and online data secure, it should constitute one of the most important issues that need to be addressed for the maturity of this research area and for the sake of successfully developing industrial scenarios with the ability of guaranteeing the security for such SoSs.

5.2 SoS under study

The second dimension explored in this SMS examines how SoS is being used in the selected studies. In this meaning RQ2.1. asks for "*How are the constituent systems of the SoS to which the study is applied orchestrated?*". The selected primary studies in the last eleven years did not reflect a clear trend in terms of how security is affected by specific SoS architecture. Authors are not focusing on any particular SoS architecture, and most importantly, studies are defining generic approaches, which seems to be applicable to any SoS architecture, or at least the opposite is not said. This might be motivated by one of these alternatives: (1) the approach is fairly general, (2) the authors are not aware of the architectural differences, or (3) the authors do not consider stating the SoS orchestration a relevant factor for their research. Notwithstanding, the applicability of the approaches of some studies is limited to Directed SoS and Acknowledged SoS. Such limitation is not explicitly described on the selected studies but can be inferred after reading the full text as the approaches assume the availability of certain restricted information that would not be generally available on Collaborative or Virtual SoS.

Regarding what the perspective has been used to examine the SoS, RQ2.2 poses "*What SoS dimensions are being analyzed?*". After complete reading of the selected primary studies, six different perspectives or dimensions were identified. On the one hand, the current literature mainly examines the SoS architecture (45/87). The relevance of SoS architecture, identified in a previous survey [12], continues to be the most studied dimension with respect to security-related work. The study of Emergent Behavior with 15/87 studies focusing on such a dimension denotes that there is concern regarding the vulnerabilities that emerges from the combination of shared resources. Emergent Behavior is one of the most difficult dimensions to analyze on SoSs considering the variability of SoS according to their architecture or sharing policies among other factors.

On the other hand, the human factor has not yet been properly considered, even though many security issues are known to be attributable to human misunderstanding or misbehavior. Although humans are well known to be the weakest link, only two studies [26, 30] explicitly considered and focused on the human being as a component of SoS security.

In contrast, after analyzing the SoS studied in the selected studies we find that there is still room for research into the SoS Mission [31]. In this meaning, an exploited vulnerability may produce an alteration on the workflow that leads the whole SoS to take unexpected or undesired actions which might compromise the purpose of the collaboration. Further research could design mechanisms to prevent SoS from responding to unexpected or fuzzy inputs.

Concerning the human factor, the results for RQ2.3 "*What roles are involved in the SoS security domain?*", shows that no roles were defined for the humans interacting with the constituent systems. There are, however, some approaches (e.g., [32]) that are intended to be automated, and roles are not applicable.

In this regard, social engineering seems to have been under-considered as a SoS vulnerability so far. Considering the human factor can allow for establishing role-based restrictions, so that only the allowed role might have access to certain resources within the SoS. Limiting the use of some resources may in fact serve as a mechanism to prevent Emergent Behavior. Therefore, research that focuses on role-based permissions may contribute to reduce unexpected or undesired emergent behaviors. In addition, more research is also needed on the inclusion of humans as constituent systems of SoS. This would not only help prevent social engineering attacks, but would also contribute to research on SoS privacy, the prevention of cascade attacks, and the definition of restrictions according to their role.

5.3 Study validation

The third analyzed dimension in this SMS is the validation of the selected primary studies. To this effect, the application domain is examined by means of RQ 3.1, "*What is the domain to which the SoS security study is applied?*". This question allows us to determine the context on which the described SoS is applied for each study. After analyzing the application domain described in the selected primary studies, 11 different domains have been found. Notwithstanding, quite many studies (47.12%) did not have an explicit application domain for their approaches. Among those that do describe an application domain, the most popular application domains for SoS security were the "*Smart*" environment (10.34% of studies), (e.g., smart cities, smart grids, smart homes, or smart things), and military applications.

Despite the different domains of applications used in the research of the selected primary studies, there is still room for improvement to bring the results of SoS research closer to society or industry. Further research may benefit from more detailed description of SoS scenarios. In this sense, a common SoS would help replicate research results when comparing different approaches. This will not only improve research results, but also increase confidence in the approaches, resulting in more industrial validation of research.

More precisely, RQ.3.2, "*What is the availability of the described SoS?*", addressed the amount of information available about the SoS being studied in the studies. The selected primary studies that describe a SoS barely provide sufficient information to allow their results to replicate. Among them, six studies partially described a SoS [33–38], and no study provides a full description of its constituent systems, shared resources, and purpose for such a joint work. One of the selected studies provides information regarding the SoS in an external web source [37].This fact limits researchers to replicate their results, to identify similar problems, or to design alternative solutions for those SoS or domains of applications.

Finally, the validation of the selected primary studies is examined in RQ3.3, "*What is the validation of the study?*". Validation is another identified gap among the selected studies. Most of the research presents theoretical contributions without any formal or empirical validation. The fact that SoS are still not widely adopted in the industrial or open-source domains restricts the chances of finding case studies or benchmarks where emerging SoS security approaches can be validated.

Few contributions considered data from real or industrial environments. In fact, we only found four during the execution of this SMS [27, 36, 39, 40]. This shortcoming is reflected in the lack of real-case validations and the high number of articles (42.52%) that do not explicitly report any validation. The scarce studies validation may be related to the relative novelty of this line of research. An area that keeps being mostly theoretical and that has been skimpily extended to industry.

5.4 Statistical analysis

Based on the Cohen's calculation used to compare the studies, it was observed that the top five significant impacts on the classification obtained from the results of RQs 1.3, 3.2, 2.3, 2.1, and 3.3. RQ 1.3 have the highest difference value (17.40), which clearly indicates a segmentation in the classification of the studies. The following magnitudes are summarized in Table 24 which also includes the ones with the lesser values. Based on the effect size values in the table, it is evident that there is a considerable variation in the significance of the effects. RQs 1.3 and 3.2 exhibit a significant difference between the groups, indicating that the variable being analyzed has a considerable impact on the classification of the studies. Conversely, other comparisons using the results on RQs 2.2 and 3.3 display a smaller effect size, which implies that the difference between the groups is less relevant.

A relevant comparison is the validation of studies. The effect size of those studies with an academic validation using a case study compared with those that used any other validation is 4.76, whereas the size effect of those not having any validation in contrast to those with any validation is 0.59. This highlights the necessity of having some form of validation in research before it can be published. Nevertheless, the challenges in designing a scenario to validate the approaches often result in researchers designing their own case studies.

Table 24 Summary of selected values of Cohen's *d*

RQ	Grouping by	Magnitude
1.3	Research focusing solely on security compared to research that also considers privacy or trust	17.40
3.2	Research without application domain compared with research with any application domain	16.33
2.3	Research without any role in contrast to research with any role	11.18
2.1	Research not declaring the orchestration of their SoS versus the research stating how the SoS is orchestrated	5.43
3.3	Research with academic case study as opposed to research with other validations	4.76
2.2	Research studying the SoS architecture in contrast to research studying other areas of the SoS	1.89
3.3	Research without validation compared to research with any validation	0.59

Overall, the effect size can aid in identifying variables that have a greater influence on the classification of studies, which can guide future research such as specific SLR focusing in a single area and facilitate the development of novel approaches in those areas that would take the higher impact.

6 Conclusions and future work

Systems of systems have been gaining popularity in recent years. As a research topic SoS is receiving increasing interest, and offers great opportunities for advancing the state of the art regarding interconnected systems. With an increasing number of devices that cooperate to reach a common goal, SoS needs to be adapted to meet the demands of current research requirements. On the other hand, digital security is today an area of paramount concern. In this sense, digital security also needs to be assessed in SoS contexts. The ability to analyze and assess the security, privacy, and trust of SoS would provide SoSs as a more suitable scenario to represent industrial SoS.

The objective of this SMS is to explore the state of the art in security, privacy, and trust in SoS to identify gaps and determine future work that would guide research in this area. To this end, we conducted a literature review for systems of systems using a systematic mapping study. As a result, 87 primary studies related to the topic were selected and analyzed.

Although several different papers have been published in the last decade, this SMS shows that little attention has been paid to the challenges imposed by the security in the SoS context where the resources are shared with the aim of achieving a common goal.

While our study aimed to provide a comprehensive overview of the literature on security for systems of systems using generic keywords, we acknowledge that our approach may have missed some relevant studies related to specific areas of security (e.g., risk management, cryptography, etc.). Therefore, we encourage future researchers to expand the search strategy with more specific keywords if they aim to focus on particular areas of security. This would enable a more focused analysis of the existing literature on the topic.

Regarding the data extraction process, it may be improved by defining a set of categories to organize the selected studies according to the area of security on which they are focusing and the means they are using to conduct such research.

In this work, we examined primary studies considering three main dimensions: (1) *the nature of the studies*, (2) *the SoS being studied*, and (3) *the validation of the studies*.

With regard to *the nature of the studies*, three gaps have been found, and correspondingly we give three hints for future work to fill them:

Gap 1 After analyzing the nature of the studies, we found that most of the primary studies selected were prescriptive. This means that most of them focused on providing a solution to problems. Whether definitional or descriptive studies are not considered in the same proportion, despite these are usually the initial steps in research according to [20]. This might be a sign of individual research that addresses an individual issue rather than a continuous research line that has studied a problem (or need) and then proposed a solution.

Future work 1. The next research work would benefit from a larger literature that focuses on standard constructs identified and described in definitional or descriptive studies. In this sense, approaches might address standardized concepts rather than those on particular SoS instances.

Gap 2. The *need for security* and *security control* have been the most frequent goals over the last 11 years and have been achieved mainly through security validation and evaluation, or by setting up specific security mechanisms protecting against particular vulnerabilities. In other words, currently most of the results are not easily reusable due to their nature. In contrast, very few selected primary studies have dealt with privacy or trust at the SoS level.

Future work 2. The design of next approaches and the validation of future work would benefit from security studies focusing on replicable processes rather than focusing on particular issues. Additionally, research on privacy and trust at all levels still has room for development.

Gap 3. Most of the pursued goals and means used by the authors so far can be interpreted as *tactical* approaches (i.e., a sort of construct that helps to achieve their research objective), rather than *strategical* ones. In our search no formal approaches have been found providing an outcome that could be appliable to any SoS. Nevertheless, SoS might benefit from adopting and applying strategical approaches being developed in akin contexts like cyber-physical or Industry 4.0 domains [41].

Future work 3. Future work must consider providing more *strategic* approaches. In other words, some kind of planning could be used to explore and understand the security on SoS providing a shared security approach for constituent systems. There are some questions that might arise on any SoS and have not been addressed so far: *Who is responsible for analyzing the security within a SoS? Who and how must develop counter measures to prevent the detected vulnerabilities? How might the security regarding the emergent behaviors be coordinated in a SoS?* Such questions require strategical studies to consider an overall consideration of each of the constituent parties.

The second dimension explored *the SoS being studied*, and two gaps have been found.

Gap 4. Most of the selected primary studies do not focus on describing the nature of the composition of the SoS (i.e., its architecture). It would be beneficial to differentiate the circumstances that allow each approach to fit some SoS. For instance, if the research result is applicable to a Directed or a Virtual composition, as the resources, and the coordination mechanisms are quite different from each other.

Future work 4. Future work shall consider explicitly depicting the SoS scenarios on which their results apply. Thus, replicability of studies would be easier to achieve, and case studies could be compared and contrasted. Additionally, a big research question arises from this gap: *How much information is required from the constituent systems to assess the security in the SoS? Which party should be responsible for gathering and analyzing such information?*

Gap 5. Regarding the perspective that has been analyzed to study the security on the SoS, the SoS architecture has been the most frequent one, whereas human factor has been barely studied, and the purpose of the collaboration has been ignored. On the one hand, humans are the weakest link and a vulnerable attack vector. On the other hand, SoS is a composition of independent systems (probably affected by the human factor), and as such it also composes different human factors, where each one may have a different culture concerning security, or even could participate with malicious intent and unpredictable behavior. In addition, constituent systems (or the human factor) not acting as expected could cause the SoS mission not to succeed. No primary study has been found that studies the security while considering the SoS mission.

Future work 5. Research must be carried out to clearly state the relevance of the human factor in SoS. Some of the research questions that arise are as follows: *How does the human factor impact the achievement of the SoS mission? May humans be a source of emergent behaviors? May a SoS become the target of social engineering attacks? Is role-based control access beneficial to secure shared resources in a SoS?*

Finally, the third analyzed perspective *validation of the studies* highlights another gap and future work.

Gap 6. Most of the studies did not provide a clear description of the SoS being studied, and many of them did not even define a clear application domain to explain how the SoS is deployed. The presence of scenarios based on industrial context could encourage the appearance of research contributions for the same scenario. Having a common scenario would promote standardized solutions for such issues. However, despite there being some initiatives that describe SoS scenarios using open-source resources, we were unable to identify any scenario fully described and used. Thus, the lack of a common scenario to apply research lines and general approaches is still an issue in SoS.

Future work 6. Researchers should consider defining their case studies or industrial scenarios used in a way that makes it possible to replicate their research, or at least better understand the circumstances under which it was developed.

Further and more complex challenges with respect to SoS security would include defining common metrics or mechanisms to share requirements and specifications between one system and another. Such metrics should, for instance, be asserted by constituent systems prior to establishing communication in a SoS context that may generate vulnerabilities between systems. It could be understood as cooperation agreement contracts that each one of the constituent systems signs when joining the SoS, i.e., a sort of SoS constitution that defines the rules and behaviors (Table 25).

Table 25 Selected studies

Search studies

Id	Title	Refs.
1	A knowledge-in-the-loop approach to integrated safety & security for cooperative system-of-systems	[42]
2	A Lightweight Architecture for Hardware-Based Security in the Emerging Era of Systems of Systems	[43]
3	A middleware framework to address security issues in integrated multisystem applications	[44]
4	A Model-Driven Method to Design and Analyze Secure Architectures of Systems-of-Systems	[45]
5	A modeling approach for interdependency in digital systems-of-systems security—Extended abstract	[46]
6	A Partition-Driven Integrated Security Architecture for Cyber-physical Systems	[47]
7	A Reasoning System for Composition Verification and Security Validation	[48]
8	A risk and threat assessment approaches overview in autonomous systems of systems	[29]
9	A security engineering process for systems of systems using security patterns	[49]
10	A Security Framework for Systems of Systems	[50]
11	A Security Framework for Systems-of-Systems	[51]
12	A security policy framework for enabled fleets and airports	[28]
13	A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis	[52]
14	A Security Scoring Framework to Quantify Security in Cyber-Physical Systems	[53]
15	A Sequential Game of Defense and Attack on an Interdependent System of Systems	[25]
16	A Systems-of-Systems Security Framework for Requirements Definition in Cloud Environment	[54]
17	Accounting Information Systems and System of Systems: Assessing Security with Attack Surface Methodology	[55]
18	Addressing Security Properties in Systems of Systems: Challenges and Ideas	[56]
19	An actionable framework for System of Systems and mission area security engineering	[57]
20	An operator-driven approach for modeling interdependencies in critical infrastructures based on critical services and sectors	[58]
21	Application of cybersecurity in emerging C4ISR systems	[33]
22	Applying model-based systems engineering approach to smart grid software systems security requirements	[59]
23	Architecting System of Systems Solutions with Security and Data-Protection Principles	[60]
24	Architectural Patterns for Self-Organizing Systems-of-Systems	[34]
25	Assessing Security Risk and Requirements for Systems of Systems	[61]
26	Assessing System of Systems Security Risk and Requirements with OASoSIS	[62]
27	Automated and Secure Onboarding for System of Systems	[32]
28	Autonomous Distributed Electronic Warfare System of Systems	[63]
29	Beyond connected cars: A systems of systems perspective	[64]
30	Clock synchronization considerations in security informed safety assurance of autonomous systems of systems	[65]
31	Context-Aware Security Solutions for Cyber Physical Systems	[66]
32	Cybersecurity as a centralized directed system of systems using SoS explorer as a tool	[67]
33	Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles	[68]
34	Cybersecurity Considerations for an Interconnected Self-Driving Car System of Systems	[69]
35	Defining "The Weakest Link": Comparative Security in Complex Systems of Systems	[26]
36	Dependable System of Systems Engineering: the COMPASS Project	[70]

Table 25 (continued)

Search studies

Id	Title	Refs.
37	Digital persona portrayal: Identifying Pluridentity vulnerabilities in digital life	[35]
38	Enhancing Security and Reliability for Smart-Systems' Architectures	[71]
39	Extending a Multi-Agent Systems Simulation Architecture for Systems-of-Systems Security Analysis	[72]
40	Goals within Trust-based Digital Ecosystems	[73]
41	Identification of Security Requirements in Systems of Systems by Functional Security Analysis	[74]
42	Incorporating Attacks Modeling into Safety Process	[75]
43	Introduction to Security and Quality Improvement in Complex Cyber-Physical Systems Engineering	[76]
44	Investigating Attack Propagation in a SoS via a Service Decomposition	[37]
45	IoTSAT: A formal framework for security analysis of the internet of things (IoT)	[77]
46	Managing runtime re-engineering of a System-of-Systems for cybersecurity	[78]
47	Model-Driven Software Security Architecture of Systems-of-Systems	[79]
48	Model-based Development of a System of Systems Using Unified Architecture Framework (UAF): A Case Study	[80]
49	Modeling human–technology interaction as a sociotechnical System of Systems	[30]
50	Modeling, analyzing, and predicting security cascading attacks in smart buildings systems-of-systems	[38]
51	Nncs: Randomization and informed search for novel naval cyber strategies	[27]
52	On Defense Strategies for Recursive System of Systems Using Aggregated Correlations	[81]
53	Predictive Control in the Era of Networked Control and Communication—a Perspective	[82]
54	Promoting trust in interoperability of systems-of-systems	[39]
55	Safety vs. Security-related trade-offs and emergent behaviors in cyber-physical systems	[83]
56	Securing System-of-Systems through a Game Theory Approach	[84]
57	Security and Autonomic Management in System of Systems	[85]
58	Security Assessment of Systems of Systems	[86]
59	Security Standard Compliance Verification in System of Systems	[87]
60	Smart City Security Issues: Depicting information security issues in the role of an urban environment	[88]
61	Strategic foresight and resilience through cyber-wargaming	[89]
62	System of Systems Characterization assisting Security Risk Assessment	[90]
63	System of Systems Composition Based on Decentralized Service-Oriented Architecture	[91]
64	System of Systems dependability—Theoretical models and applications examples	[92]
65	System of Systems Security	[93]
66	System security requirements analysis: A smart grid case study	[94]
67	Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach	[95]
68	Toward Attack Models in Autonomous Systems of Systems	[96]
69	Toward Methodological Support for Secure Architectures of Software-intensive Systems-of-systems	[97]
70	Toward Model-Driven Architecture and Analysis of System of Systems Access Control	[98]
71	Toward modeling and analyzing non-functional properties of systems of systems	[99]
72	Toward Security Software Engineering the Smart Grid as a System of Systems	[100]

Table 25 (continued)

Search studies		
Id	Title	Refs.
73	Trust Establishment in Cooperating Cyber-Physical Systems	[101]
74	Use case based approach for an integrated consideration of safety and security aspects for smart home applications	[40]
75	Using Bayesian Networks for a Cyberattacks Propagation Analysis in Systems-of-Systems	[102]
76	Using Relax Operators in an MDE Security Requirement Elicitation Process for Systems of Systems	[103]
77	Validating a European ATM Security System Architecture	[36]
Snowballing studies		
78	A Scoring System to efficiently measure Security in Cyber-Physical Systems	[104]
79	Challenges in security engineering of systems-of-systems	[105]
80	Communications, information, and cybersecurity in systems-of-systems: assessing the impact of attacks through interdependency analysis	[106]
81	Critical infrastructure protection: a twenty-first century challenge	[107]
82	Cyber-physical systems security: A survey	[108]
83	Development of Secure System of Systems Needing a Rapid Deployment	[109]
84	Misbehavior monitoring on system-of-systems components	[110]
85	Securing complex system-of-systems compositions	[111]
86	Security engineering in a system of systems environment	[112]
87	Systems of Systems with Security	[113]

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s10207-023-00757-0.

Author Contributions The authors confirm their compliance with ethical standards, and we are not aware of any conflict of interest. The work does not involve human participants and/or animals. Additionally, we confirm that the paper is not currently under submission at any conference/journal and that the paper covers our original work that has not been published/presented at any journal/conference.

Funding Funding for open access publishing: Universidad de Sevilla/CBUA. The funding for the research is acknowledged at the first page of the paper.

Data availability All data generated or analyzed during this study are included in this published article.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Graciano Neto, V. V., Guessi, M., Oliveira, L. B. R., Oquendo, F., Nakagawa, E. Y.: Investigating the model-driven development for systems-of-systems. In: Proceedings of the 2014 European Conference on Software Architecture Workshops - ECSAW '14, New York, New York, USA: ACM Press, 2007, pp. 1–8. https://doi.org/10.1145/2642803.2642825
2. Bianchi, T., Santos, D. S., Felizardo, K. R.: Quality attributes of systems-of-systems: a systematic literature review. In: Proceedings of the 3rd International Workshop on Software Engineering for Systems-of-Systems, SESoS 2015, pp. 23–30, (2015). https://doi.org/10.1109/SESoS.2015.12
3. Maier, M.W.: Architecting principles for systems-of-systems. Syst. Eng. **1**, 267–284 (1998). https://doi.org/10.1002/(SICI)1520-6858(1998)1:4%3C267::AID-SYS3%3E3.0.CO;2-D
4. Petković, M., Jonker, W.: Security, Privacy, and Trust in Modern Data Management. Springer, Berlin (2007). https://doi.org/10.1007/978-3-540-69861-6
5. Olivero, M. A., Bertolino, A., Dominguez-Mayo, F. J., Escalona, M. J., Matteucci, I.: Addressing security properties in systems of systems: challenges and ideas. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 11732 LNCS, pp. 138–146, (2019). https://doi.org/10.1007/978-3-030-30856-8_10
6. Kitchenham, B., Charters, S.: Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3.

Engineering **45**(4ve), 1051 (2007). https://doi.org/10.1145/1134285.1134500

7. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering. In: 12th International Conference on Evaluation and Assessment in Software Engineering, Vol. 17, p. 10, (2008). https://doi.org/10.1142/S0218194007003112
8. Petersen, K., Vakkalanka, S., Kuzniarz, L.: Guidelines for conducting systematic mapping studies in software engineering: an update. Inf. Softw. Technol. (2015). https://doi.org/10.1016/j.infsof.2015.03.007
9. Boulding, K.E.: General systems theory—the skeleton of science. Manage. Sci. **2**(3), 197–208 (1956)
10. Maier, M. W.: Research challenges for systems-of-systems context: collaborative systems. In: *Aerospace Corporation*, pp. 1–6, (2005). Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1571630&isnumber=33257
11. Budgen, D., Brereton, P.: Performing systematic literature reviews in software engineering. In: Proceeding of the 28th International Conference on Software Engineering—ICSE '06, sn, (2006), p. 1051. https://doi.org/10.1145/1134285.1134500
12. Klein, J., Van Vliet, H.: A systematic review of system-of-systems architecture. In: QoSA 2013 - Proceedings of the 9th International ACM Sigsoft Conference on the Quality of Software Architectures, pp. 13–21, (2013). https://doi.org/10.1145/2465478.2465490
13. Nielsen, C.B., Larsen, P.G., Fitzgerald, J., Woodcock, J., Peleska, J.: Systems of systems engineering: basic concepts, model-based techniques, and research directions. ACM Comput. Surv. **48**(2), 1–41 (2015). https://doi.org/10.1145/2794381
14. Axelsson, J.: A systematic mapping of the research literature on system-of-systems engineering. In: 2015 10th System of Systems Engineering Conference (SoSE), pp. 18–23 (2015)
15. Guessi, M., Neto, V. V. G., Bianchi, T., Felizardo, K. R., Oquendo, F., Nakagawa, E. Y.: A systematic literature review on the description of software architectures for systems of systems. In: Proceedings of the ACM Symposium on Applied Computing, Vol. 13–17-Apri, No. v, pp. 1433–1440, (2015). https://doi.org/10.1145/2695664.2695795
16. Vargas, I. G., Gottardi, T., Teresinha, R., Braga, V.: Approaches for integration in system of systems: A systematic review. In: Proceedings - 4th International Workshop on Software Engineering for Systems-of-Systems, SESoS 2016, pp. 32–38, (2016). https://doi.org/10.1145/2897829.2897835
17. Daneva, M., Lazarov, B.: Requirements for smart cities: results from a systematic review of literature. In: 2018 12th International Conference on Research Challenges in Information Science (RCIS), in International Conference on Research Challenges in Information Science, Vol. 2018- May. IEEE, May 2018, pp. 1–6. https://doi.org/10.1109/RCIS.2018.8406655
18. Olivero, M.A., Bertolino, A., Dominguez-Mayo, F.J., Matteucci, I., Escalona, M.J.: A delphi study to recognize and assess systems of systems vulnerabilities. Inf. Softw. Technol. **68**, 74 (2022). https://doi.org/10.1016/j.infsof.2022.106874
19. Wohlin, C.: Guidelines for snowballing in systematic literature studies and a replication in software engineering. ACM Int. Conf. Proc. Ser. (2014). https://doi.org/10.1145/2601248.2601268
20. Johannesson, P., Perjons, E.: An Introduction to Design Science. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10632-8
21. DoD: Chapter 4—Systems Engineering. In: DoD Defense Aquisition Guidebook, (2004)
22. Dahmann, J. S., Baldwin, K. J.: Understanding the current state of US defense systems of systems and the implications for systems engineering. In: 2008 IEEE International Systems Conference Proceedings, SysCon 2008, pp. 99–105 (2008). https://doi.org/10.1109/SYSTEMS.2008.4518994
23. Shull, F., Singer, J., Sjoberg, D. I. K.: Guide to Advanced Empirical Software Engineering, (2008). https://doi.org/10.1007/978-1-84800-044-5
24. Zhou, X., Jin, Y., Zhang, H., Li, S., Huang, X.: A map of threats to validity of systematic literature reviews in software engineering. In: Proceedings of the Asia-Pacific Software Engineering Conference, APSEC, (2016). https://doi.org/10.1109/APSEC.2016.031
25. He, F., Agwuegbo, C., Rao, N. S. V., Ma, C. Y. T.: A sequential game of defense and attack on an interdependent system of systems. In: 2018 21st International Conference on Information Fusion, FUSION 2018, pp. 2535–2541 (2018). https://doi.org/10.23919/ICIF.2018.8455314
26. Pieters, W.: Defining 'the weakest link': comparative security in complex systems of systems. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CLOUDCOM), Vol 2. International Conference on Cloud Computing Technology and Science, pp. 39–44 (2013). https://doi.org/10.1109/CloudCom.2013.101
27. Rubin, S.H., Bouabana-Tebibel, T.: Nncs: Randomization and informed search for novel naval cyber strategies. Stud. Comput. Intell. **621**, 193–223 (2015). https://doi.org/10.1007/978-3-319-26450-9_8
28. Montanari, M., Campbell, R. H., Sampigethaya, K., Li, M. : A security policy framework for eEnabled fleets and airports. In: 2011 Aerospace Conference, pp. 1–11 (2011). https://doi.org/10.1109/AERO.2011.5747379
29. Causevic, A.: A risk and threat assessment approaches overview in autonomous systems of systems. In: 2017 XXVI International conference on Information, Communication and Automation Technologies (ICAT), Institute of Electrical and Electronics Engineers Inc., pp. 1–6 (2017). https://doi.org/10.1109/ICAT.2017.8171624
30. Turnley, J., et al.: Modeling human-technology interaction as a sociotechnical system of systems. In: 2017 12th System of Systems Engineering Conference (SOSE), (2017)
31. Silva, E., Batista, T., Oquendo, F.: A mission-oriented approach for designing system-of-systems. In: 015 10th System of Systems Engineering Conference (SoSE), IEEE, pp. 346–351 (2015). https://doi.org/10.1109/SYSOSE.2015.7151951
32. Maksuti, S., et al.: Automated and secure onboarding for system of systems. IEEE Access **9**, 111095–111113 (2021). https://doi.org/10.1109/ACCESS.2021.3102280
33. Malik, A. A., Mahboob, A., Khan, A., Zubairi, J.: Application of cyber security in emerging C4ISR systems, (2011). https://doi.org/10.4018/978-1-60960-851-4.ch012
34. Nichols, C., Dove, R.: Architectural patterns for self-organizing systems-of-systems. In: 21st Annual International Symposium of the International Council on Systems Engineering, INCOSE 2011, pp. 851–862 (2011). https://doi.org/10.1002/j.2334-5837.2011.tb01246.x
35. Olivero, M.A., Bertolino, A., Domínguez-Mayo, F.J., Escalona, M.J., Matteucci, I.: Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life. J. Inf. Secur. Appl. **52**, 102492 (2020). https://doi.org/10.1016/j.jisa.2020.102492
36. Finke, M., de Waard, P., Recchilongo, P., Lahaije, R., Baumann, U.: Validating a European ATM security system architecture. In: 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC). IEEE-AIAA Digital Avionics Systems Conference. IEEE, pp. 27–35 (2018). https://doi.org/10.1109/DASC.2018.8569498
37. Lisova, E., El Hachem, J., Causevic, A.: Investigating attack propagation in a SoS via a service decomposition. In: G. M. O. K. R.-M. S. S. Y. W. S. W. Z. Chang C.K., Chen P. (Ed.), 2019 IEEE World Congress on Services (SERVICES), Institute of Electrical

and Electronics Engineers Inc., pp. 9–14 (2019). https://doi.org/10.1109/SERVICES.2019.00017
38. Hachem, J.E.L., et al.: Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems. J. Syst. Softw. **162**, 110484 (2020). https://doi.org/10.1016/j.jss.2019.110484
39. Allian, A. P., Paulo, S., Allian, A. P.: Promoting trust in interoperability of systems-of-systems. In: Proceedings of the 13th European Conference on Software Architecture—ECSA '19 - volume 2, vol. 2, pp. 67–70, (2019). https://doi.org/10.1145/3344948.3344953
40. Nicklas, J., Mamrot, M., Winzer, P., Lichte, D., Marchlewitz, S., Wolf, K.: Use case based approach for an integrated consideration of safety and security aspects for smart home applications. In: 2016 11th System of Systems Engineering Conference (SoSE), pp. 1–6 (2016). https://doi.org/10.1109/SYSOSE.2016.7542908
41. Corallo, A., Lazoi, M., Lezzi, M., Luperto, A.: Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. In: Computers in Industry, vol. 137. Elsevier B.V., (2022). https://doi.org/10.1016/j.compind.2022.103614
42. Chen, D., Meinke, K., Ostberg, K., Asplund, F., Baumann, C.: A knowledge-in-the-loop approach to integrated safety and security for cooperative system-of-systems. In: 2015 IEEE 7th International Conference on Intelligent Computing and Information Systems (ICICIS), pp. 13–20 (2015).
43. Mexis, N., Anagnostopoulos, N. A., Chen, S., Bambach, J., Arul, T., Katzenbeisser, S.: A lightweight architecture for hardware-based security in the emerging era of systems of systems. In: ACM J Emerg Technol Comput Syst, vol. 17, no. 3, (2021). https://doi.org/10.1145/3458824
44. Mohamed, N., Al-Jaroodi, J.: A middleware framework to address security issues in integrated multisystem applications. In: SysCon 2019—13th Annual IEEE International Systems Conference, Proceedings, (2019). https://doi.org/10.1109/SYSCON.2019.8836792
45. Hachem, J. E., Khalil, T. A., Chiprianov, V., Babar, A., Aniorte, P.: A model driven method to design and analyze secure architectures of systems-of-systems. In; Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS, Institute of Electrical and Electronics Engineers Inc., pp. 166–169 (2017). https://doi.org/10.1109/ICECCS.2017.31
46. Adetoye, A., Creese, S., Goldsmith, M., Hopkins, P.: A modelling approach for interdependency in digital systems-of-systems security—extended abstract. In: Xenakis, C., Wolthusen, S. (Eds.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Lecture Notes in Computer Science, vol. 6712 LNCS. Heidelberger platz 3, D-14197. Springer, Berlin, pp. 153–156 (2011). https://doi.org/10.1007/978-3-642-21694-7_13
47. Javed, Y., Felemban, M., Shawly, T., Kobes, J., Ghafoor, A.: A partition-driven integrated security architecture for cyberphysical systems. Computer (Long Beach Calif) **53**(3), 47–56 (2020). https://doi.org/10.1109/MC.2019.2914906
48. Hatzivasilis, G., Papaefstathiou, I., Manifavas, C., Papadakis, N.: A reasoning system for composition verification and security validation. In: 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–4 (2014). https://doi.org/10.1109/NTMS.2014.6814001
49. Ruiz, J. F., Rudolph, C., Mana, A., Arjona, M.: A security engineering process for systems of systems using security patterns. In: 2014 8th Annual IEEE Systems Conference (SYSCON). Annual IEEE Systems Conference, pp. 8–11 (2014)
50. Trivellato, D., Zannone, N., Etalle, S.: A security framework for systems of systems. In: 2011 IEEE International Symposium on Policies for Distributed Systems and Networks, Pisa, pp. 182–183 (2011). https://doi.org/10.1109/POLICY.2011.16
51. D. el D. I. Abou-Tair, Alouneh, S., Khalifeh, A., Obermaisser, R.: A security framework for systems-of-systems. In: Park, J.J., Loia, V., Yi, G., Sung, Y. (Eds.), Advances in Computer Science and Ubiquitous Computing. Lecture Notes in Electrical Engineering, vol. 474, pp. 427–432 (2018). https://doi.org/10.1007/978-981-10-7605-3_70
52. Feng, N., Wang, H.J., Li, M.: A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Inf. Sci. **256**, 57–73 (2014). https://doi.org/10.1016/j.ins.2013.02.036
53. Aigner, A., Khelil, A.: A security scoring framework to quantify security in cyber-physical systems. In: Proceedings of the 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems, ICPS 2021, Institute of Electrical and Electronics Engineers Inc., pp. 199–206 (2021). https://doi.org/10.1109/ICPS49255.2021.9468168
54. Carturan, S. B. O. G., Goya, D. H.: A systems-of-systems security framework for requirements definition in cloud environment. In: Proceedings of the 13th European Conference on Software Architecture - Volume 2, ECSA '19. New York, NY, USA: ACM, pp. 235–240 (2019). https://doi.org/10.1145/3344948.3344977
55. Petratos, P., Faccia, A.: Accounting information systems and system of systems: assessing security with attack surface methodology. In: Proceedings of 2019 3rd International Conference On Cloud And Big Data Computing (ICCBDC 2019). ICCBDC 2019. New York, USA: ACM, pp. 100–105 (2019). https://doi.org/10.1145/3358505.3358513
56. Olivero, M. A., Bertolino, A., Dominguez-Mayo, F. J., Escalona, M. J., Matteucci, I.: Addressing security properties in systems of systems: challenges and ideas. In: Calinescu, R., Di Giandomenico, F., (Eds.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Lecture Notes in Computer Science, vol. 11732.Springer, Cham, pp. 138–146 (2019). doi: https://doi.org/10.1007/978-3-030-30856-8_10.
57. Dahmann, J., Rebovich, G., Turner, G.: An actionable framework for system of systems and mission area security engineering. In: 2014 8th Annual IEEE Systems Conference (SYSCON), Annual IEEE Systems Conference, pp. 12–17 (2014). https://doi.org/10.1109/SysCon.2014.6819229
58. Canzani, E., Kaufmann, H., Lechner, U.: An operator-driven approach for modeling interdependencies in critical infrastructures based on critical services and sectors. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10242 LNCS, pp. 308–320, (2017). https://doi.org/10.1007/978-3-319-71368-7_27
59. Lakshminarayanan, S., Souvannarnarth, M.: Applying model based systems engineering approach to smart grid software systems security requirements. In: 22nd Annual International Symposium of the International Council on Systems Engineering, INCOSE 2012 and the 8th Biennial European Systems Engineering Conference 2012, EuSEC 2012, Rome, pp. 13–20 (2012). [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84883526951&partnerID=40&md5=d9694907fae25abf87b6ecf6aefec6a3
60. Khashooei, B. A., Vasenev, A., Kocademir, H. A., Mathijssen, R.: Architecting system of systems solutions with security and data-protection principles. In: 2021 16th International System of Systems Engineering Conference, SoSE 2021, Institute of Electrical and Electronics Engineers Inc., pp. 43–48 (2021). https://doi.org/10.1109/SOSE52739.2021.9497461
61. Ki-Aries, D.: Assessing security risk and requirements for systems of systems. In: 2018 IEEE 26th International Requirements

Engineering Conference (RE), pp. 454–459 (2018). https://doi.org/10.1109/RE.2018.00061

62. Ki-Aries, D., Faily, S., Dogan, H., Williams, C.: Assessing system of systems security risk and requirements with OASoSIS. In: B. K. L. S.-W. Faily S., Mead N. (Eds.), 2018 IEEE 5th International Workshop on Evolving Security Privacy Requirements Engineering (ESPRE). Institute of Electrical and Electronics Engineers Inc., pp. 14–20 (2018). https://doi.org/10.1109/ESPRE.2018.00009
63. Burton, I., Straub, J.: Autonomous distributed electronic warfare system of systems. In: 2019 14th Annual Conference System of Systems Engineering (SOSE), pp. 96–101 (2019)
64. Pelliccione, P., et al.: Beyond connected cars: a systems of systems perspective. Sci. Comput. Program. **191**, 102414 (2020). https://doi.org/10.1016/j.scico.2020.102414
65. Lisova, E., Čaušević, A., Uhlemann, E., Björkman, M.: Clock synchronization considerations in security informed safety assurance of autonomous systems of systems. In: IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, pp. 8385–8390 (2017). https://doi.org/10.1109/IECON.2017.8217473
66. Wan, K., Alagar, V.: Context-aware security solutions for cyber physical systems. In: Vinh, P.C., Hung, N.M., Tung, N.T., Suzuki, J. (Eds.), Context-Aware Systems and Applications, (ICCASA 2012). Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering, vol. 109, pp. 18–29 (2013)
67. Ashiku, L., Dagli, C.: Cybersecurity as a centralized directed system of systems using SoS explorer as a tool. In: 2019 14th Annual Conference System of Systems Engineering, SoSE 2019, pp. 140–145 (2019). https://doi.org/10.1109/SYSOSE.2019.8753872
68. Axelrod, C. W.: Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles. In: 2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT), pp. 1–6 (2017). https://doi.org/10.1109/CEWIT.2017.8263141
69. Straub, J., et al.: CyberSecurity considerations for an interconnected self-driving car system of systems. In: 2017 12th System of Systems Engineering Conference (SOSE), (2017)
70. Fitzgerald, J., Riddle, S., Casoto, P., Kristensen, K.: Dependable system of systems engineering: the COMPASS project. ERCIM NEWS **97**, 26–27 (2014)
71. Hofer, F.: Enhancing security and reliability for smart-systems' architectures. In: 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), pp. 150–153 (2018). https://doi.org/10.1109/ISSREW.2018.000-8
72. El Hachem, J., et al.: Extending a multi-agent systems simulation architecture for systems-of-systems security analysis to cite this version: HAL Id: hal-01908398 Extending a Multi-Agent Systems Simulation Architecture for Systems-of-Systems Security Analysis, (2018)
73. Cioroaica, E., Purohit, A., Buhnova, B., Schneider, D.: Goals within trust-based digital ecosystems. In: Proceedings - 2021 IEEE/ACM Joint 9th International Workshop on Software Engineering for Systems-of-Systems and 15th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems, SESoS/WDES 2021, Institute of Electrical and Electronics Engineers Inc., pp. 1–7 (2021). https://doi.org/10.1109/SESoS-WDES52566.2021.00006
74. Fuchs, A., Rieke, R.: Identification of security requirements in systems of systems by functional security analysis. In: Casimiro, A., DeLemos, R., Gacek, C. (Eds.), Architecting Dependable Systems VII. Lecture Notes in Computer Science, vol. 6420. Heidelberger platz 3, D-14197. Springer, Berlin, pp. 74–96 (2010). https://doi.org/10.1007/978-3-642-17245-8
75. Surkovic, A., et al.: Incorporating attacks modeling into safety process. In: Gallina, B., kavhaug, A., Schoitsch, E., Bitsch, F. (Eds.), Computer Safety, Reliability, and Security, SAFECOMP 2018. Lecture Notes in Computer Science, vol. 11094. Gewerbestrasse 11, Cham, CH-6330, Switzerland: Springer international publishing AG, pp. 31–41 (2018). https://doi.org/10.1007/978-3-319-99229-7_4
76. Biffl, S., Eckhart, M., Lüder, A., Weippl, E.L Introduction to security and quality improvement in complex cyber-physical systems engineering. In: Security and Quality in Cyber-Physical Systems Engineering. Springer, Cham, pp. 1–29 (2019). https://doi.org/10.1007/978-3-030-25312-7_1
77. Mohsin, M., Anwar, Z., Husari, G., Al-Shaer, E., Rahman, M. A.: IoTSAT: A formal framework for security analysis of the internet of things (IoT). In: 2016 IEEE Conference on Communications and Network Security, CNS 2016, IEEE Conference on Communications and Network Security. Institute of Electrical and Electronics Engineers Inc., pp. 180–188 (2017). https://doi.org/10.1109/CNS.2016.7860484
78. Waller, A., Craddock, R.: Managing runtime re-engineering of a System-of-Systems for cyber security. In: 2011 6th International Conference on System of Systems Engineering, Albuquerque, NM, pp. 13–18 (2011). https://doi.org/10.1109/SYSOSE.2011.5966566
79. El Hachem, J., et al.: Model driven software security architecture of systems-of-systems. In: R. S. D. J. Potanin A., Murphy G.C. (Eds.), Proceedings - Asia-Pacific Software Engineering Conference, APSEC, IEEE Computer Society, pp. 89–96 (2016). https://doi.org/10.1109/APSEC.2016.023
80. Eichmann, O. C., Melzer, S., God, R.: Model-based development of a system of systems using unified architecture framework (UAF): a case study. In: 2019 IEEE International Systems Conference (SysCon), Institute of Electrical and Electronics Engineers Inc., pp. 1–8 (2019). https://doi.org/10.1109/SYSCON.2019.8836749
81. Rao, N. S. V., Ma, C. Y. T., He, F.: On defense strategies for recursive system of systems using aggregated correlations. In: 2018 21st International Conference on Information Fusion (FUSION), pp. 507–514 (2018)
82. Lucia, S., Kögel, M., Zometa, P., Quevedo, D.E.E., Findeisen, R.: Predictive control in the era of networked control and communication—a perspective. IFAC-PapersOnLine **48**(23), 322–331 (2015). https://doi.org/10.1016/j.ifacol.2015.11.302
83. Schoitsch, E.: Safety versus security-related trade-offs and emergent behaviours in cyber-physical systems. In: IDIMT 2013—Information Technology Human Values, Innovation and Economy, 21st Interdisciplinary Information Management Talks, Prague, 2013, pp. 181–196. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84896816527&partnerID=40&md5=f86758a419963b0d4d3b535a4f142382
84. El Hachem, J., Lisova, E., Caušević, A.: Securing system-of-systems through a game theory approach. In: Proceedings of the ACM Symposium on Applied Computing, Association for Computing Machinery, pp. 1443–1446 (2021). https://doi.org/10.1145/3412841.3442125
85. Maksuti, S., Zsilak, M., Tauber, M., Delsing, J.: Security and autonomic management in system of systems. Infocommun. J. **13**(3), 66–75 (2021). https://doi.org/10.36244/ICJ.2021.3.7
86. Olivero, M. A., et al.: Security assessment of systems of systems. In: Proceedings of the 2019 IEEE/ACM 7th International Workshop on Software Engineering for Systems-of-Systems and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems, SESoS-WDES 2019, pp. 62–65, (2019). https://doi.org/10.1109/SESoS/WDES.2019.00017

87. Bicaku, A., Zsilak, M., Theiler, P., Tauber, M., Delsing, J.: Security standard compliance verification in system of systems. IEEE Syst. J. (2021). https://doi.org/10.1109/JSYST.2021.3064196
88. Ferraz, F. S., Guimaraes Ferraz, C. A.: Smart City Security Issues: Depicting information security issues in the role of a urban environment. In: 2014 IEEE/ACM 7th International Conference on Utility And Cloud Computing (UCC), International Conference on Utility and Cloud Computing, pp. 842–847 (2014)
89. Ormrod, D., Scott, K.: Strategic foresight and resilience through cyber-wargaming. In: European Conference on Information Warfare and Security, ECCWS, pp. 319–327 (2019). [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070015147&partnerID=40&md5=e27d26e902877268806c0a6ce2e2a103
90. Ki-Aries, D., Faily, S., Dogan, H., Williams, C.: System of systems characterisation assisting security risk assessment. In: 2018 13th Annual Conference On System of Systems Engineering (SOSE), pp. 485–492 (2018)
91. Derhamy, H., Eliasson, J., Delsing, J.: System of system composition based on decentralized service-oriented architecture. IEEE Syst. J. **13**(4), 3675–3686 (2019). https://doi.org/10.1109/JSYST.2019.2894649
92. Bukowski, L.: System of systems dependability—theoretical models and applications examples. Reliab. Eng. Syst. Saf. **151**, 76–92 (2016). https://doi.org/10.1016/j.ress.2015.10.014
93. Madan, B. B.: System of systems security. In: Rainey, L.B., Tolk, A (Eds.), Modeling and Simulation Support for System of Systems Engineering Applications, pp. 565–580 (2015). https://doi.org/10.1002/9781118501757.ch21
94. Zafar, N., Arnautovic, E., Diabat, A., Svetinovic, D.: System security requirements analysis: a smart grid case study. Syst. Eng. **17**(1), 77–88 (2014). https://doi.org/10.1002/sys.21252
95. Ceccarelli, A., et al.: Threat analysis in systems-of-systems: an emergence-oriented approach. ACM Trans. Cyber-Phys. Syst. **3**(2), 18:1-18:24 (2018). https://doi.org/10.1145/3234513
96. Surkovic, A., et al.: Towards attack models in autonomous systems of systems. In: 2018 13th System of Systems Engineering Conference, SoSE 2018, Institute of Electrical and Electronics Engineers Inc., pp. 583–585 (2018). https://doi.org/10.1109/SYSOSE.2018.8428701
97. El Hachem, J., Chiprianov, V., Babar, A., Aniorte, P.: Towards methodological support for secure architectures of software-intensive systems-of-systems. In: Proceedings of the International Colloquium on Software-intensive Systems-of-Systems at 10th European Conference on Software Architecture, SiSoS@ECSA '16. New York, NY, USA: ACM, pp. 9:1--9:6 (2016). https://doi.org/10.1145/3175731.3176178
98. El Hachem, J.: Towards model driven architecture and analysis of system of systems access control. In: 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Vol 2, pp. 867–870 (2015). https://doi.org/10.1109/ICSE.2015.280
99. Chiprianov, V., Falkner, K., Gallon, L., Munier, M.: Towards modelling and analysing non-functional properties of systems of systems. In: CooK, S., Ireland, V., Gorod, A., Ferris, T., Do, Q. (Eds.), Proceedings of the 9th International Conference on System of Systems Engineering: The Socio-Technical Perspective, SoSE 2014, pp. 289–294 (2014). https://doi.org/10.1109/SYSOSE.2014.6892503
100. Chiprianov, V., Gallon, L., Salameh, K., Munier, M., El Hachem, J., El Hachem, J.: Towards security software engineering the smart grid as a system of systems. In: 2015 10th System of Systems Engineering Conference (SOSE), IEEE, pp. 77–82 (2015). https://doi.org/10.1109/SYSOSE.2015.7151950
101. Rein, A., Rieke, R., Jaeger, M., Kuntze, N., Coppolino, L.: Trust establishment in cooperating cyber-physical systems. In: Becue, A., CuppensBoulahia, N., Cuppens, F., Katsikas, S., Lambrinoudakis, C (Eds.), Security of Industrial Control Systems and Cyber Physical Systems. Lecture Notes in Computer Science, vol. 9588. Gewerbestrasse 11, Cham, Ch-6330, Switzerland: Springer International Publishing AG, pp. 31–47 (2016). https://doi.org/10.1007/978-3-319-40385-4_3
102. El Hachem, J., Sedaghatbaf, A., Lisova, E., Causevic, A.: Using Bayesian networks for a cyberattacks propagation analysis in systems-of-systems. In: 2019 26th Asia-Pacific Software Engineering Conference (APSEC), in Asia-Pacific Software Engineering Conference, vol. 2019- Decem. IEEE, Dec. 2019, pp. 363–370. https://doi.org/10.1109/APSEC48747.2019.00056
103. Belloir, N., Chiprianov, V., Ahmad, M., Munier, M., Gallon, L., Bruel, J.-M. M.: Using relax operators into an MDE security requirement elicitation process for systems of systems. In: Proceedings of the 2014 European Conference on Software Architecture Workshops, in ECSAW '14. New York, NY, USA: ACM, pp. 32:1–32:4 (2014). https://doi.org/10.1145/2642803.2642835
104. Aigner, A., Khelil, A.: A scoring system to efficiently measure security in cyber-physical systems. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, pp. 1141–1145 (2020). https://doi.org/10.1109/TrustCom50675.2020.00151
105. Chiprianov, V., Gallon, L., Munier, M., Aniorte, P., Lalanne, V.: Challenges in security engineering of systems-of-systems. In: Troisiéme Conférence en Ingénierie du Logiciel, no. June, pp. 137–151, (2014). Available: http://munier.perso.univ-pau.fr/research/papers/2014/2014-CIEL/CIEL_2014_VC_LG_MM_PAn_VL_actes.pdf
106. Guariniello, C., DeLaurentis, D.: Communications, information, and cyber security in systems-of-systems: assessing the impact of attacks through interdependency analysis. Procedia Comput. Sci. **28**(Cser), 720–727 (2014). https://doi.org/10.1016/j.procs.2014.03.086
107. Merabti, M., Kennedy, M., Hurst, W.: Critical infrastructure protection: A 21st century challenge. In: 2011 International Conference on Communications and Information Technology, ICCIT 2011, pp. 1–6 (2011). https://doi.org/10.1109/ICCITECHNOL.2011.5762681
108. Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security—a survey. IEEE Internet Things J. (2017). https://doi.org/10.1109/JIOT.2017.2703172
109. Messe, N., Belloir, N., Chiprianov, V., Cherfa, I., Fleurquin, R., Sadou, S.: Development of secure system of systems needing a rapid deployment. In: 2019 14th Annual Conference System of Systems Engineering (SOSE), 345 E 47th St, New York, NY 10017 USA: IEEE, pp. 152–157 (2019)
110. Shone, N., Shi, Q., Merabti, M., Kifayat, K.: Misbehaviour monitoring on system-of-systems components. In: Crispo, B., Sandhu, R., CuppensBoulahia, N., Conti, M., Lanet, J.L., (eds.), 2013 International Conference on Risks and Security of Internet and Systems (CRISIS), in International Conference on Risks and Security of Internet and Systems (2013)
111. Shone, N., Shi, Q., Merabti, M., Kifayat, K.: Securing complex system-of-systems compositions. In: European Conference on Information Warfare and Security, ECCWS, pp. 370–379 (2013). [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84893433123&partnerID=40&md5=dc00401df5ee53497d159e63a6632059
112. Dahmann, J., Rebovich, G., McEvilley, M., Turner, G.: Security engineering in a system of systems environment. In: 2013 7th annual IEEE international systems conference (SYSCON 2013), in Annual IEEE Systems Conference, pp. 364–369 (2013). https://doi.org/10.1109/SysCon.2013.6549907
113. Lauritsen, R. W.: Systems of systems with security, p. 30,34, (2013)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Miguel Angel Olivero received the Ph.D. degree in Computer Science from the University of Seville, Spain, in November 2020. He has participated in various projects as a researcher as a member in the *University of Seville* and *Consiglio Nazionalle delle Ricerche*. He has been part of the organizing committee of different international conferences. He has made national and international stays and participated in both national and international projects. He is currently teaching at the Languages and Systems Department at the University of Seville. His current research interests are related to model-driven engineering, security, and the system of systems context.

Antonia Bertolino is a Research Director of the Italian National Research Council (CNR) at the Institute for Information Science and Technologies "Alessandro Faedo" (ISTI) in Pisa, Italy. Her research covers a broad range of topics and techniques within software testing. Bertolino has published more than 200 papers in international journals, conferences, and workshops. She has participated to several collaborative projects, including more recently the European projects ElasTest, Learn PAd, and CHOReOS. She currently serves as a Senior Associate Editor for the Elsevier Journal of Systems and Software, and as an Associate Editor of Wiley Journal of Software: Evolution and Process. She serves regularly in the Program Committee of top conferences in Software Engineering, such as ESEC-FSE and ICSE, and in Software Testing, as ISSTA and ICST.

Francisco José Dominguez-Mayo received the Ph.D. degree in Computer Science from the University of Seville, Seville, Spain, in July 2013. He is currently an Associate Professor with the Department of Computing Languages and Systems, *University of Seville*. He collaborates with public and private companies in software development quality and quality assurance. His lines of interesting research are plotted in the areas of continuous quality improvement and quality assurance on software products, and software development processes.

María José Escalona received her PhD in Computer Science from the University of Seville, Spain, in 2004. Currently, she is a Full Professor in the Department of Computer Languages and Systems at the University of Seville. Her current research interests include the areas of requirement engineering, web system development, model-driven engineering, early testing, and quality assurance. She manages the *web engineering and early testing* research group. She also collaborates with public companies like the Andalusian Regional Ministry of Culture and Andalusian Health Service in quality assurance issues.

received the bachelor's degree in information technology and the Bachelor of Computer Science degree (Hons.) from RMIT University, Melbourne, VIC, Australia, in 2013 and 2014, respectively, and the Ph.D. degree from the School of Science, RMIT, with data61, CSIRO, in 2018. He is a Research Fellow with the School of Computing Technologies, RMIT University. His research interests include cryptosystems, privacy preserving, and blockchain technology.

Ilaria Matteucci (M.Sc. 2003, Ph.D. 2008) is a researcher of the Trust, Security and Privacy group within the Institute of Informatics and Telematics of CNR. Her main research interests include formal methods for the synthesis of secure systems, analysis of data sharing, and policies on personal data privacy. Currently, the research interest is focused on automotive defensive and offensive cybersecurity, with particular reference to security properties of the CAN-bus protocol and possible vulnerabilities of in-vehicle network. She participates in national and European projects in the field of information security, such as FP6 EU S3MS, FP7 EU CONNECT, Consequence, Aniketos, NeSSoS, CocoCloud, Artemis EU SESAMO, H2020 C3ISP, NGI-Trust COSCA, PRIN TENACE, and GAUSS.