Escuela Técnica Superior de
Ingeniería Informática

“Un marco de trabajo para evaluar la seguridad en el contexto de Sistemas de Sistemas”

TESIS DOCTORAL

Autor

D. Miguel Ángel Olivero González

Directores

Doctor D. Francisco José Domínguez Mayo

Doctora D.ª María José Escalona Cuaresma

Sevilla, XX de XXXX de 2020

"A framework for security assessment in the context of Systems of Systems"

DOCTORAL THESIS

Author

D. Miguel Ángel Olivero González

Supervisors

Ph.D. D. Francisco José Domínguez Mayo

Ph.D. Dª. María José Escalona Cuaresma

Seville, XXXX, xxth, 2020

A nice sentence.
A book without this
is not a real book


1491343
57195072341
0000-0002-6627-3699
Olivero:Miguel_Angel

PhD Thesis foreword

This study has been developed within two research groups, the *Web Engineering and Early Testing Group* (IWT2) from *University of Seville* and the *Software Engineering and Dependable Computing Research Laboratory* (SEDC lab) from the *Consiglio Nazionale delle Ricerche*. The influence of both have greatly contributed to the materialization of this PhD Thesis.

The IWT2 research group has worked in producing scientific and transference literature by identifying issues and defining and developing solution approaches.

The mission for IWT2 research group is to *bring together the scientific production obtained within the research group to the business fabric and public service*.

Research in IWT2 focuses on Software Engineering, Processes Engineering, Testing, and Software Quality.

Among the active research lines, researchers in IWT2 have combined Model-driven Engineering paradigm with information management in diverse areas on which they have demonstrated their success. The MDE paradigm allow to harmonize approaches in a way that the results of a research can be used as a base for the next.

The Italian National Research Council (CNR) is the main public research organization of Italy. The CNR consists of about 100 different research institutes that span from human sciences to engineering sciences.

Two research groups are involved within the conduction of this PhD Thesis: the Software Engineering and Dependable Computing (SEDC) and the Institute for informatics and telematics (IIT).

The Software Engineering and Dependable Computing (SEDC) research group, originated at the beginning of the year 2012 from the two previous laboratories of Software Engineering (SE) and Dependable Computing (DC), pursuing common goals from two different perspectives. Research in SEDC investigates on one side methods, techniques, and tools for predicting and reducing software development costs, focusing especially on quality and reliability from process definition, to testing, to validation of software products. On the other side calls for specialized methodologies, techniques and tools helping in designing and validating predictably dependable computing systems, while simultaneously assuring correctness and timeliness of critical applications.

The dynamism, heterogeneity, and pervasiveness of sophisticated computing systems pose unprecedented challenges to their design, analysis, and validation. SEDC pursues new development paradigms and in particular a holistic approach to the engineering of the required functional and non-functional properties to address such edgy challenges.

The mission of the SEDC lab is *to develop methodologies and practices for Engineering SW and critical systems*.

The research of SEDC focuses on two macro areas:

1. **Design Methodologies and Solutions**, suitable to address modern system challenges such as complexity and adaptation
2. **V&V Methodologies, Techniques, and Tools**, to analyze, assess and validate functional and non-functional properties such as QoS and dependability indicators.

The security group of the IIT is an internationally leading research group consisting of about 25 persons, ranging from researchers to Ph.D. students and software engineers. The security group has a significant expertise on **cyber security and crime**, **formal models for security and trust**, **secure software engineering**, **data sharing agreements**, **parental control technologies**, **language-based security**, **usage control monitoring and enforcement**, and **study of security metrics and risk**.

Overall the security group has been involved, in national and European projects: among the other, NESSoS, Aniketos, Coco- Cloud, CAMINO, Connect, Contrail, SESAMO, Consequence, Sensoria, S3MS, SPARTA, Cybersure, AEGIS, GridTrust. They are also active in EIT ICT Labs projects and leading some security activities.

The integration of the three different research cultures enhances the requirements for this research. The proximity of IWT2 research group to the industry promotes a practical research, scientific productions that could be used by the businesses. The SEDC group trusts that novel integrated methodologies rooted on the synergy between the two disciplines will be able to face the continuous evolution and rising criticality of software-intensive complex systems. The security group of the IIT provide their expertise on security, improving the quality of this PhD Thesis.

The influence of these three research groups allowed to adopt a wider perspective, that enriched the scientific production generated as a result of the development of this PhD Thesis. A framework that simultaneously provides value to the industry and the scientific areas within System of Systems context.

Abstract

The "*Systems of Systems"* (SoS) emerged as a new horizon with the predominant use of information systems. In this meaning, at the end of 20th century the Systems of Systems have been adopted to define a set of systems retaining operative and managerial independence. These systems temporary collaborate to reach a common goal in an organized way.

SoS are complex systems that are not managed by a single accountant, and its outcomes have not a single author or owner. Some shared resources, as functionalities and data are a compositional feature. It means, SoS functionalities and data is a sum of shared resources among the constituent systems.

SoS offer new challenges when defining general guidelines on its management, development or operative. Its dynamic composition involves additional complexity: constituent systems may join and disengage, affecting the SoS normal behavior. Diverse alternatives have been proposed with the aim of managing the SoS, analyze its functionalities or performance among others.

The security of each constituent system does not compose the SoS security. Despite each constituent system is secure by itself, it is only securing a SoS component, but not the SoS as a whole. An unexpected or mal-intentioned combination of functionalities may produce harmful results on the SoS.

SoS security is a complex feature to analyze, given the SoS evolutionary behavior and the no compositionality of security.

Since more than 20 years ago software engineering have been designing guidelines to unify routines and create standards as in the case of information system development in computer engineering. These routines include values, strategies, guidelines and methodologies that assist in the development and maintenance of software systems. The use of guides, methodologies and frameworks have evolved with the systems.

Technological advances in communication promoted the use of this kind of strategies, easing product and services control and management. However, these guidelines are usually designed for a single system. The use of these guidelines in complex systems as in Systems of Systems include additional challenges as progress and resources sharing.

This PhD Thesis study emergent behavior as the origin of SoS vulnerabilities and design a standard framework to assess the SoS security. This research work is motivated by the importance of security in this context. It is based on studies that analyze the security according to the SoS composition [1], and the potential impact of analyzing the vulnerabilities originated on such collaboration [2].

The general goal of this PhD Thesis is to research on a non-previously identify problem that arise when constituent systems are conducting a joint work. This goal

is: **to guarantee the security on data and functionalities that are shared on Systems of Systems.** This work is based on two main research hypotheses:

- Identify the effects of emergent behavior that may cause vulnerabilities.
- Define a framework to assess and guarantee security on Systems of Systems.

The literature review analyzed the current situation and detected a gap regarding strategies to manage SoS security. In particular those that could be applied by all the parties involved on the SoS. The gap is also confirmed by means a experts' judgment technique that bolster the first hypothesis. Experts' judgment provide knowledge to define the requirements for a solution approach. Therefore, this PhD Thesis contributes to the problem understanding, analyzing the initial hypothesis by applying a systematic literature review and a experts' judgment technique.

The solution approach for the identified problem is described as a framework that assist in the process of SoS security assessment by means of a organized set of stages. This approach is named TeSSoS *"Testing for Security in System of Systems"*. This framework has been communicated in Software Engineering for Systems-of-Systems conference and is inspired in agile methodologies, Deming cycle, Mitnick cycle and an attacker lifecycle. TeSSoS lifecycle is designed to be adapted with the use of other methodologies, guidelines or frameworks.

This proposal composed of five stages that iteratively and incrementally systematize security management in SoS. These stages start with **SoS Discovery**. Its objective is to model and analyze the SoS, defining the constituent systems and shared resources (data and functionalities). In the second phase, **Red Requirements**, this model is used to detect vulnerabilities by simulating the behavior of an attacker. After that, the third phase, **Blue Requirements**, focuses on jointly defining a set of alternatives that prevent an attacker from taking advantage of each of these vulnerabilities. The development of countermeasures that protect against these vulnerabilities is carried out in the fourth phase, **Development**. The fifth phase of TeSSoS is called **Evaluation**. This fifth stage uses the catalog of previously detected vulnerabilities. The vulnerabilities are used as a guide to simulated attacks that can verify whether the developed countermeasures have been affected to protect the system. Finally, the **Act** stage resumes the work done and a retrospective is carried out with the aim of optimizing the use of resources in the successive iterations of TeSSoS.

The thesis ends by presenting a case on which the TeSSoS framework is applied. This case study studying the resources and the vulnerabilities that may emerge on the SoS considering the Digital Persona as a virtual SoS. The constituent systems of this virtual SoS correspond to each one of the specific identities among the different systems. After analyzing the results, vulnerabilities were detected and countermeasures were proposed, improving the security on the Digital Personae.

Therefore, the scientific production of this thesis contributes to solving the problem with the design and use of a framework, which enabled the second hypothesis to be answered.

Table of contents

List of illustrations

List of tables

Chapter 1

Introduction

"*The beginning is the most important part of the work.*"

— Plato

Chapter 1. Introduction

This chapter initiates the PhD Thesis by introducing the topic of this research, the problem being addressed, the research strategy applied, and the original solutions proposed. The content of each chapter is described, and their scientific results are highlighted.

1. Context and objectives

From the dawn of time, every living being have been looking for their own survival. In a world full of perils and predators, living and conscious creatures have been developing natural capacities to avoid dangerous situations and prosper. Plants have developed toxins and spikes to avoid being eaten by the animals. Animals in contrast have learned to hide or use the environment on their favor. Looking for safety and security is a natural behavior also present in the human conduct. Instinctively people refuse risks and seek for controlled environments, where the predators do not represent a threat for their life.

This instinct for seeking secure environment has been evolving alongside the human culture. Once people started living in cities, the security was not only understood as to avoid predators, but also to avoid situations that could produce undesired consequences. At this point, humans perceived the security as a subjective welfare feeling that emerges in the absence of events unaligned with their interests [3]. The security is constrained to known hazards, and this makes security a double-edged sword. Asserting that something is secure may be self-defeating since unknown threats may jeopardize us. Security is a personal feeling that differs from one person to another. The more the people know, the more reliable their security feeling is.

The same occurs in computer science and computer engineering, where the systems are constantly facing new threats [4]. Security research that aims to provide a better understanding of current threats and provide a solution to avoid them to succeed. As for humans, in the case of the systems, the threats may focus on harming on their physical or logical structure or forcing the system to take inopportune decisions.

A system engineer is usually the responsible of securing the systems assets, which include the system development (i.e., the system structure and behaviors) and system operations (i.e., guarantee service provided by the system). The purpose of each system determines how much reliability is required on its security to guarantee the success of its goals. Systems handling sensitive data, or decision-taking responsibilities, demand much more security than others. Such systems require a deeper knowledge of their environment, their weak spots, countermeasures, and so on. This is one of the responsibilities of a system engineer.

Guaranteeing the security in a system is a complex task due to the huge number of existent alternatives to exploit the systems resources and how quickly new ones are discovered. The situation gets worse when the system management is distributed, and the resources are shared. This is the case of the Systems of Systems (SoS),

complex systems created as a result of systems that collaborate to achieve an objective that they could not get by themselves. SoS compositions have two main features, managerial independence and operational independence [5]. Thus, the people responsible of analyzing the security for SoS face additional challenges. In a SoS there is not one unique manager, each constituent is independently managed and can operate individually. Such level of decoupling requires a good communication among the parties to establish what goal to achieve and the resources to share to reach such objective. The responsibility of guaranteeing the security in a system typically resides in a single organization or individual. In contrast, in a System of Systems, this responsibility is distributed among the different individuals holding the product owner role. During the execution of their work, they do not only need to determine the level of security for a single constituent, but for the interaction of this constituent with any other and their emergent behavior. Considering that the security is a non-composable feature, the individuals responsible of guaranteeing the security in the SoS must not only determine the security in each single constituent, but also in the collaborations among them. Then, it is necessary to state mechanisms of consensus able to guarantee the security in a unanimous and standard way by defining the responsibilities among the parties. Not having a standard language to communicate the requirements or not having the same security concerns about the systems shared resources may generate vulnerabilities during the constituents' joint work. Recent studies [6] found that some teams were using their resources in an efficient and effective way as a consequence of involving security from early stages.

In this PhD Thesis a framework is proposed to assess and test the security of Systems of Systems from its design. This framework named TeSSoS is a management strategy to guarantee the security for a SoS during the development and its operations in an effective and efficient way. TeSSoS provides a wide perspective for the SoS, which eases the detection of vulnerabilities or security incompatibilities among the constituent systems. The lifecycle of this management process is based on a Deming cycle, including an additional stage for continuous improvement. The different stakeholders involved in the SoS can use TeSSoS to define their security requirements, detect security conflicts and define the division of responsibilities.

2. Research strategy

A methodological support helps researchers to ensure the quality of their results and organize the content of their findings. It also helps in structuring in a logical way and present the content in an understandable order.

During the execution of this PhD Thesis we have followed the *Design Science* method framework outlined in [7][8], a study describing an application of the Design Science methodology [9].

The framework is composed by four main components:

- Related activities with required artefacts and produced outcomes.
- General guidelines to conduct the activities.
- General guidelines to choose research strategies and methods to use in the activities.

- General guidelines to relate the research to an already existing knowledge base.

Design science method framework is not only about creating artefacts, but to provide questions and answers about them and their environment. The activities carried out following this method and their results must be related to an existing knowledge base to ensure that the produced research expresses valid and reliable knowledge. The method depicts five related activities that define the questions that the researcher needs to answer and the results that they need to produce. These activities begin by defining the problem and continue up to demonstrating and evaluating some produced artifacts that solve an already identified problem. Each activity is associated with guidelines offering practical advices that support and facilitate the research work. These guidelines help in assuring scientific rigor.

Six activities compose this framework:

1. **Explicate Problem.** The first activity formulates and justifies a problem.
2. **Define Requirements.** After detailing the problem, the second activity defines the requirement for a solution approach.
3. **Design and Develop Artefact.** This activity is the development of the solution approach.
4. **Demonstrate Artefact.** The artefact is used in a case to show that the artefact can solve the problem.
5. **Evaluate Artefact.** The last activity determines the effectiveness of the artefact to address the problem for which it was designed.

The relationship among these activities is shown in Figure 1-1 , as in a IDEF0 [10] diagram. These activities are not described as temporarily ordered but as logically related according to what they produce and require.

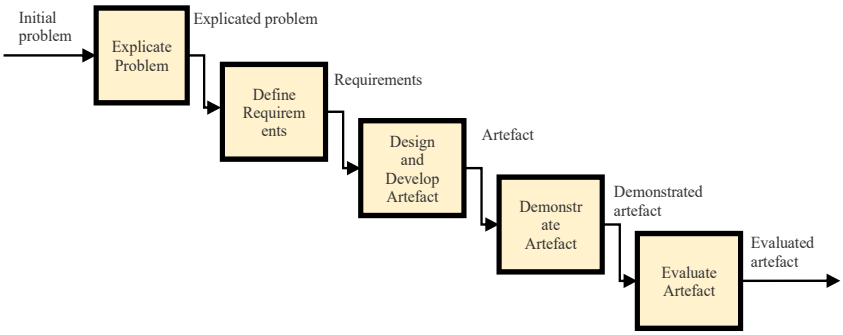

Figure 1-1. Design science research method overview

This research mainly focuses on the first activity, **Explicate Problem**. It focuses on precisely formulating and justifying a practical problem. This problem must be significant for some practice and not only relevant for one local practice. Explicating

problem activity studies the root causes of the problem, which may be identified and analyzed, and only outlines the design of the artifact. The goal of this activity is to provide an essential understanding of a problem. Once the problem has been identified, the design science proposes a solution outline in an activity named Define Requirements. It continues with the artefact designing and development, its demonstration and finally its evaluation.

The explicate problem activity focuses on providing answer to the question: *"What is the problem experienced by some stakeholders of a practice and why is it important?"*

The answer to this question is a description of the nature of the problem being addressed using descriptive knowledge. Sometimes even detailing the causes of such problem. In the design science a problem is defined as a gap between the current state and the desirable one. The problem being faced needs to be generalized to be considered a design science research. To accomplish this activity, it needs to be provided by knowledge in the research literature and information from relevant stakeholders.

Explicate Problem is composed of three sub-activities. (1) The first sub-activity is to define the problem. The problem should be precisely defined to ensure that different people will understand it in the same way. A common understanding help people to share the same view of a problem, and, helps to limit the scope of the research project. (2) Then, the problem needs to be justified. That means to describe its purpose, its environment, and its challenges in a way that people can agree that it is worthwhile to be addressed. (3) The latter is to find the root causes, which helps in defining a solution to mitigate the origin of the problem.

Explicate the problem has been addressed as follows:

- **Chapter 2.** The problem is described determining its environment in a precise, concise, and understandable way.
- **Chapter 3.** The importance of the problem is highlighted and points out the generalization of the addressed problem. This is made by describing the studies available on the literature that have previously identified or experienced the described problem. This chapter relates the results of applying the design science framework to an existing knowledge base.
- **Chapter 4.** Some stakeholders participate to ensure that the problem is solvable and to identify its root causes.

The second activity in design research, **Define Requirements,** deals with the question: *"What artefact can be a solution for the explicated problem and which requirements on this artifact are important for the stakeholders?"* This question has been addressed in Chapter 4. A potential solution to previously identified problem is described.

The third and last activity of design science covered in this thesis is **Design and Develop Artifact.** This activity provides a solution for the identified problem focusing on the root causes. **Chapter 5** and **Chapter 6** are elaborated by following the guidelines of this activity by using the results of preceding chapters.

Last stages of this design science framework focus on using the developed artefact in a real-life case and evaluating how well the produced artefact fulfills the

requirements according to the problem that motivated the research. However, the execution of these activities is out of the scope for this PhD Thesis.

3. Thesis objectives

The main objective for this PhD Thesis is to study the security issues in the context of Systems of Systems as emergent behaviors and its effects.

More particularly, to generate knowledge to ease analyzing the systems' security and help the systems stakeholders to document and specify the security test objectives, as well as systematize the generation of security test cases in the System of Systems context.

This objective has been divided in five subgoals to ease its accomplishment. The name of the subgoals pursued in this PhD thesis are inspired in the name of the stages described in the Design science research method. These subgoals lead the research starting by **(i) set a research scope**. Then, **(ii) formulating a problem** by means a gap in current state of the art. After identifying a novel issue, the third subgoal focuses on **(iii) define the requirements** for a solution approach. Considering these requirements, the fourth subgoal **(iv) generate an artefact for such solution.** The PhD Thesis would achieve all the subgoals after **(v) conducting an experiment** using the generated artefact for the identified issue. The thesis subgoals are described in Table 1-1.

Subgoal	Description
1. Explicate Problem	Determine a research hypothesis that would lead the research. It focuses on explaining and understanding an issue. This subgoal delimits the research scope, allowing to focus on a single topic.
2. Validate Problem	Identify a gap in the literature regarding the chosen topic on which concentrate the research studies. This subgoal validates the existence of the previous explained problem.
3. Define Requirements	Establish a set of requirements or characteristics that a solution approach would need to meet.
4. Generate an Artefact	Propose a solution approach according to solution requirements defined by means of previous subgoals.
5. Conduct a Case Study	Provide the results of using the solution approach for the formulated problem. Validate the artifact by means a Case Study.

Table 1-1. PhD thesis subgoals

4. Thesis outline

This PhD Thesis contributes to the science by describing a problem not previously identified in the Systems of Systems context and providing a solution approach. As a solution to this novel problem this PhD Thesis provides a framework to communicate security requirements and detect security issues among the constituent systems in a System of Systems environment.

The studies produced during the development of this PhD Thesis have been organized in seven chapters. The first chapters focus on identifying a problem (*Chapter 2, Chapter 3, Chapter 4*). The study begins by analyzing initial hypotheses and comparing them with the current state of the art. Then, the idea of a new type of vulnerability and its potential countermeasures was validated in a survey with a group of experts. By doing so, the existence of a problem in the security management in the Systems of Systems was validated.

The following ones describe an approach addressing the identified problem (*Chapter 5, Chapter 6*). This thesis proposes TeSSoS, a framework to mitigate such security problems. The framework has been applied in a real-case scenario with successful results.

The PhD Thesis finalizes highlighting conclusions and future work (*Chapter 7*). Figure 1-2 illustrates the value produced by each chapter and their relationship. Finally, two appendices complement the doctoral thesis.

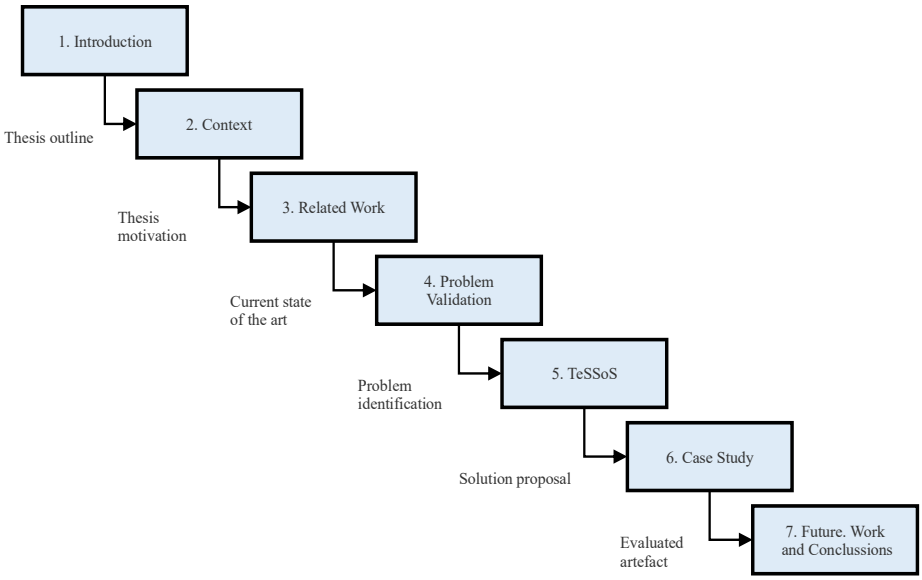

Figure 1-2. PhD. Thesis Outline

Chapter 2. Context describes the background related to this PhD Thesis research. It defines the scope of this research and the initial research hypotheses. In this chapter the different SoS architectures existing in the scientific literature are studied by distinguishing how the constituent systems organize themselves to achieve a common goal. It also discusses the particular security issues for each architecture and describes the identified challenges for each case. This chapter discusses about the depicted scenarios and relates about a problem not previously identified in scientific literature. As a solution, the second hypothesis briefly introduces the

TeSSoS approach to assess the security in SoS, by means a series of stages involving modelling and testing on its lifecycle. This chapter has been partially published in [1].

Key contributions of this chapter:

1. Identifying systems vulnerabilities that only exist because of a collaboration among constituent systems in a System of Systems.
2. Generates initial hypothesis.

Chapter 3. Related work details the current state of the art. This chapter presents the results of a Systematic Mapping Study. After analyzing 1405 papers, 87 were selected as related to SoS and Security, Trust, or Privacy. These papers allowed to identify the gaps in the current scientific literature. This chapter contributes the scientific knowledge by providing a review for the current state of the art.

Key contributions of this chapter:

1. A Systematic Mapping Study summarizes the current state of the art for security approaches in the System of Systems context.
2. Identifies numerous gaps in this research area.

Chapter 4. Problem Validation presents a Delphi questionnaire. A group of experts in security, Systems of Systems and standardization and good practices agreed in the existence of identified problems after reaching a consensus. After three rounds of survey using this technique, the experts agreed on the relevance of an orchestrated security and highlighted the key components that may affect in the quality of the security. This chapter validates the existence of the problems previously depicted in Chapter 2 and Chapter 3 and helps in defining the requirements for a solution approach.

Key contributions of this chapter:

1. A group of experts have been surveyed using a Delphi questionnaire to validate the existence of a problem not addressed before in the literature.
2. Experts identify the sources of the security issues and describe the nature for a potential solution.

Chapter 5. TeSSoS introduces a novel framework to assess the gap identified in the literature in Chapter 3. This chapter proposes a framework that systematizes the Systems of Systems security assessment and testing. The framework is organized in six stages and for each one it defines the expected input, outputs, and the involved roles. This proposal can be adapted to already existing agile development and management frameworks or methodologies even in heterogeneous composition. This chapter comprises another original contribution of this PhD Thesis, that has been partially published in [11].

Key contributions of this chapter:

1. Describes the TeSSoS framework to support security management and testing in a System of Systems context.
2. Contextualizes the roles and outcomes of this framework.

Chapter 6. Case Study introduces a case study on which TeSSoS has been applied. This case study considers the digital persona as a System of Systems with virtual architecture. After evaluating the digital persona of some participants by using TeSSoS some vulnerabilities were detected due to the constituent systems working together. This chapter has been partially published in [2]**.**

Key contributions of this chapter:

1. A real-scenario application of our solution proposal.
2. It shows the TeSSoS adaptability to improvised SoS architectures.
3. It introduces an instantiation of Knowledge Model and Security Model.
4. The term *Antimission* is introduced in the context of SoS.

Chapter 7. Conclusions a**nd Future Work** wrap up the PhD Thesis by discussing the results and points out some directions as a future work.

Annex A. Research activities gathers all the scientific production published within the development of this PhD Thesis, the projects on which I have been involved, grants, research stays, and research events on which I have been participating.

Annex B. Glossary of terms lists the terms used in this PhD Thesis and its definition.

Annex C. Bibliography lists all the knowledge base used that supports this PhD Thesis.

Part I.
Problem Identification

Chapter 2

Research context

"*Assume the enemy knows the system.*"
— Claude Shannon

Chapter 2. Research context

This chapter identifies the research area in which the PhD Thesis is developed. In particular, it describes the initial hypothesis that motivated this PhD Thesis and delimits the scope of the research. In addition to the context, this chapter points out the main factors that compromise the security in a system, and the security peculiarities that emerges in a SoS.

The context provided in this chapter offers a wide perspective of this research, providing motivations, and discussing relevant challenges. Some existing differences that arise when addressing the security on different SoS architectures are described, and how these challenges could be addressed.

After that the conclusions proposes a potential solution for those factors. Oncoming chapters continue shaping the described hypothetical problem and solution alternatives.

This chapter is censured as it has been published in [1].

In this chapter we have surveyed the security challenges over the four architectures of an SoS. Some examples are provided for each architecture, detailing how the joint work is managed by using an airport as a fil rogue.

Given their natures, each architecture has different security challenges and, according to their architecture, different approaches are identified to address them. The initial hypothesis of this research is based on the need of a SoS model to detect the potential vulnerabilities as well as to analyze and test its security.

The following chapters will focus on detailing the research conducted to validate the research hypothesis.

The first hypothesis is addressed in Chapter 3 and Chapter 4. These chapters deal with the existence of a problem regarding the combination of resources in the SoS. Given the variety of scenarios that can emerge from the systems compositions, it is needed to perform a Systematic Mapping Study to retrieve every study analyzing this issue and determine the current state of the art. The survey helps to understand the scientific progress conducted in this line to improve or enhance the security for SoS. After determining the existence of such issue, a survey with expert panels was conducted to validate the nature of the problems and define the requirements for a solution approach.

The second hypothesis is dealt with in Chapter 5 and Chapter 6. They detail a solution approach for such identified issue. A framework named TeSSoS that organizes a series of stages to orchestrate shared responsibilities when assessing the security on SoS. Chapter 5 identify the lifecycle of this framework, and how modeling and testing take part on it. TeSSoS is then used in a case study involving many constituent systems in a virtual SoS on a real scenario.

Chapter 3

Related Work

"If we knew what we were doing, it would not be called research, would it?"

— Albert Einstein.

Chapter 3. Related Work

A Systematic Mapping Study gathers research papers studying the issue faced in this PhD Thesis: the security on systems of systems. The current state of the art is analyzed to explore potential gaps in the literature and to motivate producing this PhD thesis based on the research hypothesis previously described in Chapter 2. The results of this chapter show that there is scope for action to provide new approaches in this line.

This chapter is censured as it is pending to be published.

Chapter 4

Problem Validation

"*It is better to change an opinion than to persist in a wrong one*"

—Socrates.

Chapter 4. Problem Validation

Previous chapters identify a security issue within the SoS context, and made a hypothesis about its existence and its scientific relevance. No evidences of previous publications have been found after conducting a survey in Chapter 3. This chapter surveys experts of the field to validate the scientific interest of this issue and define the requirements for an artifact solving it. The primary goal of this chapter is to assess how experts' judgment techniques, in particular the Delphi method, can be applied to validate the research value and identify the main properties for a solution approach.

This chapter describes a real case of application of Delphi method technique lasting three rounds involving fifteen experts. The results provided after analyzing the answers given by the experts offers a general understanding of the issue being studied allowing to design a solution approach according to a common issue definition and comprehension.

This chapter is censured as it is pending to be published.

Part II.
Solution Proposal

Chapter 5

TeSSoS

"If you know the enemy and know yourself,
you need not fear the result of a hundred battles.

If you know yourself but not the enemy,
for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself,
you will succumb in every battle."

—Sun Tzu

Chapter 5. TeSSoS

From the conclusions of previous chapters, the security in the Systems of Systems has been identified to be a question still not addressed in the scientific literature despite it has been proven to be a relevant issue. The lack of standard patterns or guidelines to define security assessment mechanisms, in a context of shared responsibilities, causes a detriment in the quality of such property. This chapter introduces TeSSoS. A framework that defines general guidelines to improve the management and handling regarding security properties for SoS with the aim of providing a solution to such matter.

This chapter is censured as it has been published in [11]

Chapter 6

Case Study: Digital Persona Portrayal

"*Well done is better than well said.*"
— Benjamin Franklin

Chapter 6. Case Study

The TeSSoS framework described in Chapter 5 is employed in this chapter by considering the digital persona as a System of Systems. The digital persona is characterized as a virtual SoS that originates from the interaction of people identities among the constituent systems. In this SoS, an attacker could execute personalized attacks by combining pieces of data and the resources from different constituents. Attack patterns that exploit this kind of vulnerabilities are described along this chapter. After that, some concepts are defined regarding the digital persona and define models that support the framework. This chapter shows that, after using TeSSoS, some vulnerabilities can be detected in virtual System of Systems compositions, validating the results from the application of the described framework. The results of applying the framework can be generalized to other SoS using any architecture. Communication among the parties and availability of resources would differ, nevertheless the use of the framework and the generated artefacts remains the same.

***This chapter is censured as it has been published in* [2]**

Chapter 7

Conclusions and Future Work

"*Don't adventures ever have an end? I suppose not.*
Someone else always has to carry on the story."
— J.R.R. Tolkien, The Fellowship of the Ring

Chapter 7. Conclusions and Future Work

This chapter concludes the thesis by describing the hypothesis on which this PhD Thesis is based, the scientific environment in which this work has been developed, the way in which the environment has influenced the obtained results and wrap up by proposing future work and research lines derived from this study.

1. Introduction

This thesis consists in a series of scientific results that define one of the security problems in the SoS and provide a solution approach that has been applied in a real scenario. More specifically this PhD thesis presents the validation of two research hypotheses within System of Systems security context. The first research hypothesis is addressed in Chapter 2, Chapter 3 and Chapter 4 and focuses on a non-previously identified problem and its definition. Then, a second research hypothesis, is addressed in Chapter 5 and Chapter 6, focusing on studying the causes and consequences of such potential SoS security issues and defining a solution approach.

The first hypothesis states that, systems doing joint work may give rise to vulnerabilities only existing when the systems are working together. More particularly, dissimilarities in a common security agreement for the SoS, and the complex organizational work to coordinate different parties are two key factors to generate vulnerabilities that may transform the SoS into a sitting duck. The hypothesis is defined in Chapter 2, where it is noticed that this vulnerability has not been previously identified for the SoS context. To verify such hypothesis, this study analyzes the state of the art regarding security and Systems of Systems. Such state-of-the-art study is conducted in Chapter 3 by means a Systematic Mapping Study. The results of such work however provided no relevant scientific productions regarding this research area. An expert's judgment was later employed to discover the real relevance of this issue in the scientific community. This study presented in Chapter 4 shows the importance of this topic despite not much previous work has been conducted in this line.

The second hypothesis states that a coordinated mechanism for assessing the SoS security improves its security. This hypothesis is firstly stated in Chapter 5. In this chapter a framework is defined as a solution to assess the security in SoS. Such framework organizes a series of stages and activities with the aim of unifying the process of security assessment for SoS. Such solution approach is later validated in a case study in Chapter 6. This chapter employs TeSSoS for security assessment by considering the Digital Persona and the identities of some individuals as virtual SoSs.

The results show that the problem identified in the first hypothesis is indeed a relevant issue for security in SoS. Then, the results on the second hypothesis show that a structured and organized mechanism for security assessment allows to detect SoS vulnerabilities.

2. Thesis contributions

The objective for this PhD Thesis is defined in **Chapter 1** and is composed of five subgoals: (i) *Explicate Problem*, (ii) *Validate Problem*, (iii) *Define Requirements*, (iv) *Generate an Artefact*, (v) *Conduct a Case Study*. These objectives are defined from the Design Science methodology [9]. Each one of the defined objectives is addressed in a different chapter. The scientific contributions produced during this PhD Thesis are closely related with the objectives defined in its beginning. This section lists the contribution provided in each chapter for accomplishing such identified objectives. A summary of the contributions is shown in Table 7-1

Subgoal 1. Explicate Problem

The thesis began with the definition of the starting hypothesis. This hypothesis is based on the existence of a problem that was not previously identified in the literature. After analyzing the characteristics of System Systems, it was theorized about the existence of a SoS security issue that has been not previously addressed. The hypothesis on the existence of this problem is developed in **Chapter 2** and was published in [1]. The research objective **Explicate Problem** was achieved with the definition of this research hypothesis.

Subgoal 2. Validate Problem

To discover the studies that have been developed in this line, a state-of-the-art study was carried out in which the published scientific productions addressing a security issue problem in the SoS context were analyzed. This review of the state of art classified the works found along nine dimensions:

1. Nature of the contribution.
2. Goals and means pursued.
3. Addressed non-functional requirement.
4. SoS nature
5. SoS dimension
6. Roles involves
7. Domain of application
8. SoS availability
9. Study validation

The results of this study show that most of the scientific progress was focusing on Descriptive and Prescriptive studies that focus on the SoS architecture, not providing a detailed description or implementation of a SoS either because it has been not validated or is using a synthetic case study. After analyzing the results of this survey, looking for a validation of the initial hypothesis, it was found that security on SoS is still an immature area of research that requires more effort. A main barrier to achieve such achievement is the lack of real scenarios for validations.

However, there are not scientific publications addressing the security assessment for SoS issue considering the combination of the resources available among the constituent systems.

Thus, this work, described in **Chapter 3** covers the research objective **Validate Problem**.

Subgoal 3. Define Requirements

A study based on a Delphi questionnaire was carried out due to the lack of contributions found from the scientific community in this area. The purpose of this questionnaire is to underline the validity and relevance of the issue not previously identified in the literature. An experts' judgment survey is developed in **Chapter 4** with participants from 8 countries. In this survey a series of questions were asked using a questionnaire on which three different SoS scenarios were described to identify the experts' criterion according to three dimensions:

1. Characteristics of described SoS.
2. The causes of the security vulnerability.
3. Identify the nature of a solution.

After three rounds of the Delphi questionnaire, the participants were able to reach consensus on 14 of 21 issues among the three dimensions. The results of this study allowed to identify the sources of the security issues, describe the nature for a potential solution and hence reach the research objective **Define Requirements**.

The **first hypothesis,** that detailed the issue regarding the combination of resources from the constituent systems, was validated after achieving Subgoal 1, Subgoal 2 and Subgoal 3,

Subgoal 4. Generate an Artefact

In **Chapter 5**, the TeSSoS framework [11] is described to provide a solution to the defined issue. This framework provides a guided process to ensure and assess the security for SoS. In particular, the focus of this approach resides in the coordination and cooperation among the parties. In this way people and organization constituting a SoS can follow a unified and homogeneous proceeding. This framework is strongly inspired in the Deming cycle, the cyber-attacks lifecycle, and includes artifacts that allow the integration of this framework with agile management or development methodologies. **¡Error! No se encuentra el origen de la referencia.** introduces a general overview of TeSSoS. This approach defines the roles for each participating actor and uses artifacts that define a common language among the parties in such a way to facilitate the reporting of vulnerabilities detected within the SoS. Each time a system joins or is modified in the SoS, the constituent systems may perform another cycle of TeSSoS framework to analyze the SoS to detect vulnerabilities, apply countermeasures and test its security.

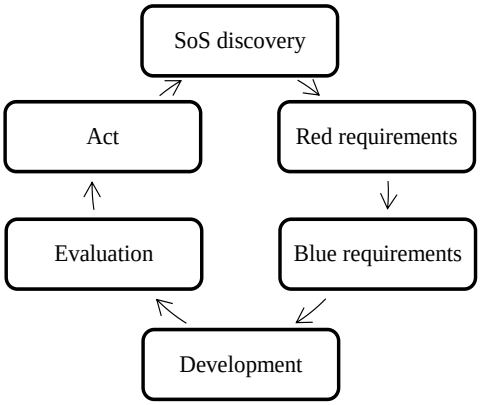

Figure 7-1. TeSSoS outline

The solution proposal to address the issue allows to achieve the research objective **Generate an Artefact**.

Subgoal 5. Conduct a Case Study

To evaluate the usability of TeSSoS, a security assessment on virtual SoS has been conducted in a real-scenario [2]. In **Chapter 6** it is detailed how Digital Personae are interpreted as virtual SoS, and how the combination of available resources among the constituents generate vulnerabilities that only exist after putting together the data and functionalities provided by these systems. After applying TeSSoS on 17 different SoS, this case study identified some vulnerabilities and eased countermeasures proposal to avoid attacks exploiting the vulnerabilities. This case study also shows the adaptability of TeSSoS to emerging SoS architectures.

Thus, the fifth subgoal **Conduct a Case Study** is achieved.

The **second hypothesis** defined for this PhD Thesis, regarding the analysis of causes and consequences of security issues in SoS is validated by means of the TeSSoS solution approach and the case study on which it has been used.

Having all the subgoals individually achieved, this PhD Thesis has achieved to generate knowledge to ease analyzing the systems' security and helps the systems stakeholders to document and specify the security test objectives, as well as systematize the generation of security test cases in the System of Systems context.

Subgoal	Scientific Result
1. Explicate Problem	The first subgoal is achieved by means of a descriptive scientific production describing the hypothesis that motivated this PhD Thesis. Addressed in Chapter 2, it shows the factors that compromise the security on SoS and the security peculiarities that emerges when constituent systems collaborate according to the SoS architecture. *Partially published in* [1]
2. Validate Problem	The second subgoal is achieved by means of a descriptive scientific production summarizing the state of the art. Addressed in Chapter 3, it shows the current state-of-the-art regarding security, trust, and privacy on the SoS context through a Systematic Mapping Study. The problem of security issues due to constituent systems collaboration has been not previously addressed in scientific publications. *Pending to be published.*
3. Define Requirements	The third subgoal is achieved by means of an explanatory scientific production. Addressed in Chapter 4, it provides the results of a experts' judgment survey regarding SoS security properties for three scenarios describing an attack on a SoS. *Pending to be published.*
4. Generate an Artefact	The fourth subgoal is achieved by means of a definitional scientific production. Addressed in Chapter 5, it defines the TeSSoS framework for assessing the SoS security. Using an ordered sequential process of 6 stages that orchestrates the SoS security assessment and testing. *Published in* [11]
5. Conduct a Case Study	The fifth subgoal is achieved by means of a descriptive and prescriptive scientific production. Addressed in Chapter 6, it provides the results of using the TeSSoS approach to a real-scenario case study. Using the framework using the Digital Persona as a virtual SoS. *Published in* [2]

Table 7-1. Scientific results

3. Future work and new research lines

This thesis leads not only to the contributions made during the development of this research, but it has also opened new research lines that promote further contributions for the SoS security. The future work derived from this PhD thesis is listed by considering the five sub-goals described in Chapter 1.

Explicate Problem. Explore other domains looking for similar addressed problems may provide original solutions that can be adapted to this one. SoS research area can benefit from the knowledge already generated in other areas if similar problems are

found and their solutions are adapted. On the other hand, another emerging research line focuses on an in-depth research to determine how the architecture and the constituent systems' nature affect SoS security assessment.

Future work derived from this subgoal is within this research line: explore other research areas, identify similar problems, adapt their solutions.

Validate Problem. New research lines in this context may provide better guidelines on how to categorize accepted papers on the review. To address this research line, it is needed to study common criteria for categorizing the systematic surveys. Then, propose a standard mechanism to identify what labels use to categorize accepted papers on systematic surveys.

From the results after achieving this subgoal, a future work is clear. As systematic surveys are temporary, it is required to launch regular updates. This help in keeping this area of knowledge updated and allows to timely discover research trends and niches. The systematic survey also allowed to identify some gaps regarding this method.

Define Requirements. As observed from this PhD Thesis, there is not a standard or widespread mechanism to communicate SoS properties among constituent accountants. Experts' judgment techniques can help in identifying the needs of such parties to design a fitting approach that could be used academically and industrially.

Generate an Artefact. One of the main flaws on the produced work is the inability to measure the degree of security of a SoS. The existence of such metric could help in determining the improvement on security a SoS achieves after developing the countermeasures. To mitigate such flaw, a future research focuses on defining a metric to assess and compare the degree of security of a SoS.

Additionally, this research can continue in two directions:

1. The development of a software tool to automatize partially or completely the usage of TeSSoS framework.
2. On the other hand, a second future work is scheduled to use this framework for SoS security assessment on industrial scenarios.

Conduct a Case Study. A research line emerges from this validation. This research line focuses on studying cases of attacks on SoS to determine common patterns or configuration on the constituent systems causing vulnerabilities.

Three validation works are scheduled from the results of this case study that have been conducted previously by other authors with satisfactory results as in [12][13]:

1. The first one is based on applying expert judgment methods to the modeling, security, and testing-related issues by using Delphi method [14].
2. Then, an industrial validation of this approach is intended to be performed in collaboration with some companies by studying the exposure of their employees by using this approach and evaluate if the overexposure could become a vulnerability not only for the employees but also for the organization as a SoS on which employees are considered as constituent systems. In this way the security team of the company can establish some metrics on how exposed the employees are and adjust the privileges of each individual or design defensive strategies.

3. A third validation is considered to study the feasibility of evolving a system by developing some vulnerabilities' countermeasures defined as Blue Requirements in those constituents' systems that allow it.

Table 7-2 points out the relation among the objectives described for this thesis, the solution proposed and new research lines that arise from them.

4. Conclusions

This thesis details the addressed problem regarding security on Systems of Systems and proposes a framework to help mitigate this issue. The problem has been defined and delimited within the context of SoS (Chapter 2). Then, a systematic literature survey was conducted to analyze the magnitude and better know the scope of the defined problem (Chapter 3). An experts' judgment was developed to validate the existence and relevance of this problem in this context after not identifying a remarkable number of scientific publications or a clear trend of increasing publishing in this area (Chapter 4).

After this issue was identified, described, and its relevance was evidenced according to the experts' judgment, this thesis proposes a framework to assess the security for SoS (Chapter 5). The TeSSoS framework details six cyclic stages that orchestrate the workflow to stablish common security criteria, detect vulnerabilities and develop countermeasures cooperatively among the parties that conforms the SoS.

This framework has been applied in a real scenario. TeSSoS evaluated the security of Digital Persona as SoS with virtual architecture (Chapter 6). In the case study some vulnerabilities were found as a result of combination of shared resources among the constituents.

This PhD Thesis has proposed an adapted environment to support security assessment for Systems of Systems continuously. The designed environment guarantees the security of constituent systems and as a result enhances the success ratio for the objective of the collaboration among the parties involved in the SoS.

Subgoal	Future Work – Research lines
1. Explicate Problem	**Research lines.** - Identify how SoS architecture and the constituent systems' nature affects to SoS security assessment. - Analyze other research areas to look for analogous problems and their solutions. **Future Work.** - Explore other research areas. - Identify similar problems to adopt their solutions. - Study the differences among different SoS according to their nature - Determine how the SoS's nature impacts on the security assessment.
2. Validate Problem	**Research lines.** - Define a standard process to define categorization for accepted papers in systematic surveys. **Future Work.** - Keep updated this kind of researches to avoid this becoming deprecated. - Study common criteria for categorizing systematic surveys - Propose a standard mechanism to identify categories to categorize accepted papers on systematic surveys.
3. Define Requirements	**Research lines.** - Proposing a standard mechanism to communicate SoS properties for security assessment among constituent systems accountants. **Future work.** - Use experts' judgment techniques to define a standard communication for SoS.
4. Generate an Artefact	**Research lines.** - Define metrics to assess and compare the degree of security of a SoS. **Future work.** - Develop a tool to automatize the framework usage. - Use this framework to assess the security in real scenarios.
5. Conduct a Case Study	**Research lines.** - Determine what common patterns causes vulnerabilities. **Future work.** - Develop a tool to automatize the security assessment for the Digital Persona. - Determine the feasibility of evolving a system according to the countermeasures defined as Blue Requirements.

Table 7-2. Thesis future work

Annex A

Research activities

Annex A. Research activities

This annex collects the research activity of the doctoral student in different sections. The research activities have been categorized in sections according to their nature:

- The **research stays** enumerate the periods of the research that have been conducted in external research centers and the scientific production published as a result of such stays.
- The **scientific outreach** events on which I have participated are listed chronographically in descendant order.
- The **publications** made have been classified as thesis related research or general research if the production is not closely related to the achievement of this thesis.
- The **projects and contracts** on which I have participated are grouped according to its nature and scope.
- **Pair review activities** as a reviewer for journals and conferences are listed and arranged by typology and year.

1. Acknowledgements

On the time this thesis has been developed I have been awarded with two stays grants. The first grant was conceded by **UDIMA university**, in Madrid, Spain, to conduct a research stay for six months on their offices as a predoctoral stay. Another research stay of seventeen months was carried out in the **Consiglio Nazionale delle Ricerche**, in Pisa, Italy after being awarded of a predoctoral stay grant.

This work has been partially supported by three main parties, each one for each research center on which this thesis has been developed.

In Spain the project POLOLAS, *TIN 2016-76956-C3-2-R*, sponsored by the **Ministry of Economy and Competitiveness.** Also, in Spain, in Madrid, the predoctoral stay was sponsored by the **Pre/Postdoctoral I+D+I UDIMA stays program.** In Italy the project GAUSS, MIUR, PRIN 2015, Contract *2015KWREMX*, sponsored by the **Ministero dell'Istruzione, dell'Università e della Ricerca.**

2. Research stays

Two stays have occurred during the time this PhD Thesis has been conducted.

The first stay was under the supervision of Dr. David Lizcano Casas in Escuela de Ingeniería y Ciencias Técnicas at the Universidad a Distancia de Madrid, UDIMA in Madrid, Spain. This grant had a duration of 6 months. During this stay a publication titled "*Una estrategia centrada en el usuario y guiada por modelos para el desarrollo sistemático de módulos ERP*" was made and presented in a conference.

A second stay have been supervised by research director Antonia Bertolino in the Istituto di Scienza e Tecnologie dell'Informazione in the Consiglio Nazionale delle

Ricerche in Pisa, Italy. This grant had a duration of 17 months. During this stay some studies have been produced and published in conferences and journals.

The produced research has been partially disseminated in topic-related events.

2.1. Universidad a Distancia de Madrid. UDIMA. 2018

Start date	03/2018
End date	09/2018
Place	EICT-UDIMA, Madrid, Spain
Research produced	[15] "Una estrategia centrada en el usuario y guiada por modelos para el Desarrollo sistemático de módulos ERP"

2.2. Consiglio Nazionale delle Ricerche. CNR. 2018 - 2020

Start date	10/2018
End date	02/2020
Place	ISTI-CNR, Pisa, Italy
Research produced	[1] "Addressing Security Properties in Systems of system: Challenges and Ideas [2] "Digital persona portrayal: Identifying Pluridentity vulnerabilities in digital life" [11] "Security Assessment of Systems of Systems"

3. Scientific Outreach events

During the period of this PhD Thesis, I have attended and participated in many scientific events, enumerated in Table A-1.

Period	Event name	Nature	Location
2020	GAUSS meeting	Project meeting	Brunico, Italy
2019	WEBIST 2019	Conference attendant	Vienna, Austria
	JISBD 2019	Conference attendant	Cáceres, Spain
	SERENE 2019	Conference attendant	Naples, Italy
	ICSE 2019	Conference attendant	Montreal, Canada
	ITASec 2019	Organizer committee	Pisa, Italy
	GAUSS meeting	Project meeting	L'Aquila, Italy
2017	WEBIST 2017	Conference attendant	Oporto, Portugal

Table A-1. Scientific Outreach Events

4. Publications

The list of studies published during the PhD Thesis considers works since the first day that officially started this research: May 10th, 2017. Such publications are sorted chronologically in descendant order. In addition, the publications have been categorized among thesis-related research and non-thesis-related research.

4.1. Thesis related

4.1.1. Journal publications

The content of Chapter 6 has been partially published in the following journal:

Contribution			
M. Olivero, A. Bertolino, F.J. Dominguez-Mayo, M.J. Escalona, I. Matteucci, "Digital Persona Portrayal: Identifying Pluridentity vulnerabilities in digital life" In: *Journal of Information Security and Applications*. 2020. Vol. 52. https://doi.org/10.1016/j.jisa.2020.102492			
Abstract: The increasing use of Internet for social purposes enriches the available data on the network about all of us and promotes the concept of the Digital Persona. In addition, this trend produces Digital Personae consisting of more than one identity, what we define as a Pluridentity. This trend also produces increased risks: the security of a Digital Persona can be exploited if its data and security are not managed properly. In this paper, we focus specifically on digital attacks that can be perpetrated by using pieces of data belonging to different identities of the same Digital Persona and combining them to profile their target. Some victims are so accurately depicted when looking at the Pluridentity that by using the gathered information attackers can execute very personalized social engineering attacks, or even bypass otherwise safe security mechanisms. This work describes a strategy to identify potential vulnerabilities caused by overexposure due to combining data from different identities of a Digital Persona. To this end, we introduce three Digital Persona Portrayal models that together support the process of architecting the data from different identities. These models can also be used to identify potential vulnerabilities. This proposal has been validated on seventeen chosen candidates from a data leak, retrieving the data of their Digital Personae, and matching them with their security. After analyzing the results several vulnerabilities were detected on some of the analyzed Digital Personae.			
Journal:	Journal of Information Security and Applications		
Volume:	Vol. 52. (2020)	**DOI:**	10.1016/j.jisa.2020.102492
Citations	0	**SJR:**	0,387 (2018)
JCR: (Scopus)	1,537 (2018)	**JCR 5 Years:**	n/a (2018)
JCR:	Computer Science; Information systems: 111/155 (Quartile Q3)		
SJR:	Computer Science; Software: (Quartile Q2) Computer Science; Computer Networks and Communications: (Quartile Q2) Engineering; Safety, Risk, Reliability and Quality: (Quartile Q2)		

4.1.2. Conference publications

Chapter 2 and Chapter 5 has been partially published in these conference publications:

Contribution			
M.A. Olivero, A. Bertolino, F.J. Dominguez-Mayo, M.J. Escalona, I. Matteucci "Addressing Security Properties in Systems of Systems: Challenges and Ideas" in 11th International Workshop on Software Engineering for Resilient Systems, 2019.			
Conference name:	11th International Workshop on Software Engineering for Resilient Systems. Co-located with the 15th European Dependable Computing Conference (EDCC)		
Held in:	Naples, Italy		
Geographic scope:	International	**Date:**	September, 2019
SCIE index:	Work in Progress	**CORE index:**	Core NC

Contribution			
M.A. Olivero, A. Bertolino, F.J. Dominguez-Mayo, M.J. Escalona, I. Matteucci "Security Assessment of Systems of Systems" in 7th International workshop on Software Engineering for Systems-of-Systems, 2019.			
Conference name:	SESoS-WDES '19: Proceedings of the 7th International Workshop on Software Engineering for Systems-of-Systems and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems Co-located with the ICSE '19: 41st International Conference on Software Engineering		
Held in:	Montreal, Canada		
Geographic scope:	International	**Date:**	May, 2019
SCIE index:	WiP (Class 1, Rating A++)	**CORE index:**	- (A++)

4.2. General research

During the time this PhD thesis have been being developed 13 non-thesis-related research papers have been published. Four of these papers have been published in journals, and nine in conferences.

4.2.1. Journal publications

Contribution			
Olivero, Miguel Ángel, Domínguez Mayo, Francisco José, Parra Calderón, Carlos Luis, Escalona Cuaresma, María José, Martínez García, Alicia. "Facilitating the design of HL7 domain models through a model-driven solution." BMC Medical Informatics and Decision Making. 2020			
Abstract: Background and goal. Health information systems are increasingly sophisticated and developing them is a challenge for software developers. Software engineers usually make use of UML as a standard model language that allows defining health information system entities and their relations. However, working with health system requires learning HL7 standards, that defines and manages standards related to health information systems. HL7 standards are varied, however this work focusses on v2 and v3 since these are the most used one on the area that this work is being conducted. This works aims to allow modeling HL7 standard by using UML. Methods. Several techniques based on the MDE (Model-Driven Engineering) paradigm have been used to cope with it. Results. A useful reference framework, reducing final users learning curve and allowing modeling maintainable and easy-going health information systems. Conclusions. By using this approach, a software engineer without any previous knowledge about HL7 would be able to solve the problem of modeling HL7-based health information systems. Reducing the learning curve when working in projects that need HL7 standards.			
Journal:	*BMC Medical Informatics and Decision Making*		
Volume:	Vol. 20 (2020)	**DOI:**	10.1186/s12911-020-1093-4
Citations	0	**SJR:**	0,908 (2019)
JCR: (Scopus)	2,067 (2018)	**JCR 5 Years:**	2,674
JCR:	Medical Informatics: 15/26 (Quartile Q3)		
SJR:	Health Informatics: 18/77 (Quartile Q1) Health Policy: 55/247 (Quartile Q1)		

Contribution			
M. Urbieta, S. Firmenich, G. Bosetti, P. Maglione, G. Rossi, M.A. Olivero "MDWA: a model-driven Web augmentation approach — coping with client- and server-side support," Softw. Syst. Model., 2020.			
Abstract: Web augmentation is a set of techniques allowing users to define and execute software which is dependent on the presentation layer of a concrete Web page. Through the use of specialized Web augmentation artifacts, the end users may satisfy several kinds of requirements that were not considered by the analysts, developers and stakeholders that built the application. Although some augmentation approaches are contemplating a server-side counterpart (to support aspects such as collaboration or crossbrowser session management), the augmentation artifacts are usually purely client-side. The server-side support increases the capabilities of the augmentations, since it may allow sharing information among users and devices. So far, this support is often defined and developed in an ad hoc way. Although it is clear that server-side support brings new possibilities, it is also true that developing and deploying server-side Web applications is a challenging task that end users hardly may handle. This work presents a novel approach for designing Web augmentation applications based on client-side and server-side components. We propose a model-driven approach that raises the abstraction level of both, client- and server-side developments. We provide a set of tools for designing the composition of the core application with new features on the back-end and the augmentation of pages in the front-end. The usability and the value of the produced augmentations have been evaluated through two experiments involving 30 people in total.			
Journal:	*Software and Systems Modeling (2020)*		
Volume:	TBD	**DOI:**	10.1007/s10270-020-00779-5
Citations	0	**SJR:**	0,575 (2019)
JCR: (Scopus)	2,66 (2020)	**JCR 5 Years:**	2,061
JCR:	Computer Science; Software Engineering: 24/107 (Quartile Q1)		
SJR:	Modeling and Simulation: 104/282 (Quartile Q2) Software: 123/349 (Quartile Q2)		

Contribution			
L. Morales Trujillo, Olivero, Miguel Ángel, Domínguez Mayo, Francisco José, García García, Julián Alberto, Mejías Risoto, Manuel: A testability and observability methodology to assure traceability requirements on System of Systems. Journal of Web Engineering. 2020			
Abstract: The advance in the digital world has caused a growth of complexity in innovation. Traditional approaches to innovation, based on reductionism, face greater difficulties. That is why we have witnessed the growth of those known as System of Systems (SoS). There is a wide variety of methodologies and domains of application in the literature to form framed solutions in the context of SoS, but there is no unified consensus for its use and even less when it comes to agile environments of continuous integration and deployment in which traceability requirements are critical. In recent years, the need to have traceability software that continuously records and monitors the trace of the entities that interact with it has become an essential feature. In addition, over the years there has been evidence of errors caused by poor traceability control. Therefore, this document presents an agile framework that aims to guarantee the traceability of a SoS from the early stages. This framework unifies the discovery, development and operations, providing full coverage in the conformation of the solution. Finally, we present a case study as future work, which is based on the application of our framework on smart laboratories for assisted reproduction.			
Journal:	*Journal of Web Engineering*		
Volume:	Vol 19. Num 2 (2020)	**DOI:**	10.13052/jwe1540-9589.1928
Citations	0	**SJR:**	0,199 (2019)
JCR: (Scopus)	0,854 (2018)	**JCR 5 Years:**	0,641
JCR:	Computer Science; Software Engineering: 87/107 (Quartile Q4) Computer Science; Theory & Methods: 76/105 (Quartile Q3)		
SJR:	Computer Networks and Communications 222/304 (Quartile Q3) Information Systems 232/301 (Quartile Q4) Software: 285/349 (Quartile Q4)		

Contribution			
J.G. Enríquez, Olivero, Miguel Ángel, Jiménez Ramírez, Andrés, Escalona Cuaresma, María José, Mejías Risoto, Manuel "MaRIA: A Process to Model Entity Reconciliation Problems". Journal of Web Engineering. 2018. Vol. 17. Núm. 3&4. Pag. 206-223			
Abstract: Within the development of software systems, the development of web applications may be one of the most widespread at present due to the great number of advantages they provide such as: multiplatform, speed of access or the not requiring extremely powerful hardware among others. The fact that so many web applications are being developed, makes enormous the volume of information that it is generated daily. In the management of all this information, the entity reconciliation (ER) problem occurs, which is to identify objects referring to the same real-world entity. This paper proposes to give a solution to this problem through a web perspective based on the Model-Driven Engineering paradigm. To this end, the Navigational Development Techniques (NDT) methodology, that provides a formal and complete set of processes that bring support to the software lifecycle management, has been taken as a reference and it has been extended adding new activities, artefacts and documents to cover the ER. All these elements are defined by a process named Model-Driven Entity ReconcilIAtion (MaRIA), that can be integrated in any software development methodology and allows one to define the ER problem from the early stages of the development. In addition, this proposal has been validated in a real-world case study helping companies to reduce costs when a software product that must give a solution to an ER problem has to be developed.			
Journal:	*Journal of Web Engineering*		
Volume:	Vol 17. Issue 3-4 (2018)	**ISSN:**	1540-9589
Citations	0	**SJR:**	0,199 (2019)
JCR: (Scopus)	0,854	**JCR 5 Years:**	0,641
JCR:	Computer Science; Software Engineering: 87/107 (Quartile Q4) Computer Science; Theory & Methods: 76/105 (Quartile Q3)		
SJR:	Computer Networks and Communications 222/304 (Quartile Q3) Information Systems 232/301 (Quartile Q4) Software: 285/349 (Quartile Q4)		

4.2.2. Conference publications

Contribution			
A. Bertolino, G. De Angelis, F. Lonetti, V. de Oliveira Neves, M.A. Olivero "EDUFYSoS: A Factory of Educational System of Systems Case Studies" Proc. – IEEE 15th International Conference on System of Systems Engineering (SoSE), 2020.			
Conference name:	IEEE 15th International Conference on System of Systems Engineering (SoSE)		
Published in:	IEEE (10.1109/SoSE50414.2020.9130551)		
Held in:	Budapest, Hungary		
Geographic scope:	International	**Date:**	June, 2020
SCIE index:	Work in Progress	**CORE index:**	-

Contribution			
C. Augusto, M.A. Olivero, J. Morán, L. Morales-Trujillo, C. De la Riva, J. Tuya "Test-Driven Anonymization in Health Data: A Case of Study on Assistive Reproduction," Proc. - 2020 IEEE Int. Conf. Artif. Intell. Testing, AITest 2020, 2020.			
Conference name:	IEEE 2nd International Conference on Artificial Intelligence Testing (AiTest)		
Published in:	TBD		
Held in:	Oxford, United Kingdom		
Geographic scope:	International	**Date:**	August, 2020
SCIE index:	Work in Progress	**CORE index:**	-

Contribution			
M.A. Olivero, L. Morales-Trujillo, F.J. Dominguez-Mayo, M. Mejías "Systematic development of ERP modules using a model-driven strategy focusing on the users" in 15th International Conference on Web Information Systems and Technologies, 2019.			
Conference name:	4th International Special Session on Advanced practices in Model-Driven Web Engineering (APMDWE) Co-located with 15th International Conference on Web Information Systems and Technologies (WEBIST)		
Published in:	TBD		
Held in:	Vienna, Austria		
Geographic scope:	International	**Date:**	September, 2019
SCIE index:	Work in Progress	**CORE index:**	Core C (2018)

Contribution			
M.A. Olivero, L Morales-Trujillo, D Lizcano, FJ Domínguez-Mayo "Una estrategia centrada en el usuario y guiada por modelos para el desarrollo sistemático de módulos ERP" in XXIV Jornadas de Ingeniería del Software y Bases de Datos			
Conference name:	XXIV Jornadas de Ingeniería del Software y Bases de Datos (JISBD)		
Held in:	Cáceres, Spain		
Geographic scope:	National	**Date:**	September, 2019
SCIE index:	Work in Progress	**CORE index:**	-

Contribution			
J.G. Enríquez, L. Morales Trujillo, Olivero, Miguel Ángel, Domínguez Mayo, Francisco José, Ramos Román, Isabel, et. al. "Hacia una metodología para el desarrollo guiado y sistemático de los Trabajos Fin de Grado". XXIV Jornadas sobre la Enseñanza Universitaria de la Informática. Barcelona, España. 2018			
Conference name:	XXIV Jornadas sobre la Enseñanza Universitaria de la Informática (JENUI)		
Held in:	Barcelona, Spain		
Geographic scope:	National	**Date:**	July, 2018
SCIE index:	Work in Progress	**CORE index:**	-

Contribution			
L. Morales Trujillo, Morena Leonardo, Sara, Olivero, Miguel Ángel, Jiménez Ramírez, Andrés, Mejías Risoto, Manuel: "Applying Model-Driven Web Engineering to the testing phase of the ADAGIO Project." 18th International Conference on Web Engineering. Cáceres, Spain. 2018			
Conference name:	18th International Conference on Web Engineering (ICWE)		
Held in:	Cáceres, Spain		
Geographic scope:	International	**Date:**	June, 2018
SCIE index:	Class 3, Rating B	**CORE index:**	Core B (2018)

Contribution			
Jiménez Ramírez, Andrés, García García, Julián Alberto, García García, Julián, Navarro Pando, Jose Manuel, Olivero, Miguel Ángel: "Imedea: Historia Clínica Centrada en el Paciente para la Reproducción Asistida." XXI Congreso Nacional de Informática de la Salud. Madrid. 2018			
Conference name:	XXI Congreso nacional de Informática de la Salud		
Held in:	Madrid, Spain		
Geographic scope:	National	**Date:**	March, 2018
SCIE index:	Work in Progress	**CORE index:**	-

Contribution			
Urbieta, Matias, Firmenich, Sergio, Maglione, Pedro, Rossi, Gustavo, Olivero, Miguel Ángel "A Model-driven Approach for Empowering Advance Web Augmentation - From Client-side to Server-side Support." 13th International Conference on Web Information Systems and Technologies. Oporto, Portugal. 2017			
Conference name:	2nd International Special Session on Advanced practices in Model-Driven Web Engineering Co-located with 13th International Conference on Web Information Systems and Technologies (WEBIST)		
Held in:	Porto, Portugal		
Geographic scope:	International	**Date:**	April, 2017
SCIE index:	Work in Progress	**CORE index:**	Core C

Contribution			
Martínez García, Alicia, Olivero, Miguel Ángel, Suarez, Almudena, Sánchez Begines, Juan Miguel, Domínguez Mayo, Francisco José, et. al. "A methodological proposal and tool support for the HL7 standards compliance in the development of health information systems.". 25th Annual International SQM Conference. 2017			
Conference name:	25th International Software Quality Management (SQM)		
Held in:	Solent, United Kingdom		
Geographic scope:	International	**Date:**	April, 2017
SCIE index:	Work in Progress	**CORE index:**	Core C

5. Projects and contracts

There are six projects and four contracts among national and international scope on which I have participated while the production of this PhD Thesis.

5.1. National projects

This research has been produced while collaborating with diverse national projects. Five national projects have taken part in the production of this research.

Title	NDT 4.0. Mecanismos para el diseño y gestión de software orientados al usuario
Code	US-1251532
Main Researcher	María José Escalona
Start date	02/2020
End date	01/2022

Title	SocietySoft-Transferencia de herramientas, políticas y principios para la creación de software de calidad para la sociedad digital
Code	AT17_5904_USE
Main Researcher	María José Escalona
Start date	02/2020
End date	01/2021

Title	Explorando Soluciones Guiadas para Sistematizar el Aseguramiento Temprano de la Calidad del Software
Code	TIN 2016-76956-C3-2-R
Main Researcher	María José Escalona
Start date	30/12/2016
End date	29/12/2019
Budget	181.200,00€

Title	Diseño de un marco de trabajo basado en herramientas para mejorar la gestión de guías clínicas y procesos asistenciales
Code	RTC-2016-5824-1
Main Researcher	María José Escalona
Start date	09/2016
End date	12/2019
Budget	824.881,60€

5.2. National contracts

This research has been produced while collaborating with diverse national contracts for transference projects.

Title	Jornadas de Difusión y Divulgación de la Investigación, Tecnología e Innovación: Estrategia para Fortalecer el Tejido Empresarial desde la Infancia hasta la empresa
Main Researcher	Julián Alberto García-García
Code	2017/950
Start date	09/2017
End date	12/2017
Budget	1.300,00€

Title	Prototipado Rápido de Aplicaciones mediante LEGO y Componentes Web
Code	P005-18/E09
Main Researcher	Javier Jesús Gutiérrez Rodríguez
Start date	01/2018
End date	12/2018
Budget	2.000,00€

Title	Puesta en marcha de la solución BIONAC Suite
Code	P027-17/E09
Main Researcher	Laura García Borgoñón
Start date	07/2017
End date	07/2018
Budget	15.840€

Title	ARIADNE – Value Chain: From IDMU to Lean Documentation for Assembly
Code	P054-15/E30
Main Researcher	María José Escalona
Start date	01/2016
End date	12/2017

5.3. International projects and contracts

In addition to national projects, this thesis has been partially developed during the participation in the following international research projects.

Title	GAUSS: Governing Adaptative and Unplanned Systems of Systems
Code	2015KWREMX
Main Researcher	Leonardo Mariani - Antonia Bertolino
Start date	01/2017
End date	12/2019
Budget	219.252,00€

6. Pair review process

Pair reviewing have been also part of the research process. I have participated in seven reviewing processes, six for conferences, and one for journal.

- **Conference related reviews.**
  - 16th International Conference on Web Information Systems and Technologies (WEBIST 2020)
  - 15th International Conference on Internet and Web Applications and Services (ICIW 2020)
  - 15th Conferencia Ibérica de Sistemas y Tecnologías de Información (CISTI 2020)

- 15th International Conference on Web Information Systems and Technologies (WEBIST 2019)
- XI Congreso Internacional de Computación y Telecomunicaciones (COMTEL 2019)
- X Congreso Internacional de Computación y Telecomunicaciones (COMTEL 2018)

- **Journal related reviews.**
  - Journal of Web Engineering (JWE 2019)

Annex B

Glossary of terms

Annex B. Glossary of terms

A.	
Authenticate	Use an identity to gain access to restricted resources.
B.	
Blue Product backlog	A catalog of Blue Requirements with responsibilities, cost estimation, and priorities assigned.
Blue Requirements	Requirements that defines the needed countermeasures to mitigate vulnerabilities.
Blue Team	Team that enforces the security by designing countermeasures.
C.	
Communicational capabilities	The communicational capabilities in mKAOS models represent the mechanisms that constituent systems use to share information to carry out the mission by using the functionalities described as operational capabilities.
D.	
Design Science	A research methodology that organizes the process of generating knowledge and solutions to identified problems.
Digital Persona	A record that is rich enough in data-items to provide an adequate image of the represented entity or identity.
Digital Persona Portrayal	See *Portrayal*.
DPKM	Acronym for “Digital Persona Knowledge Model”.
DPP	Acronym for “Digital Persona Portrayal”.
E.	
Emergent Behaviors	The emergent behaviors are those functionalities that do not belong to any constituent system in particular, but, arise because of the combination of partial results.
Entity	A being.
F.	
Framework	A structured set of activities that supports or guides something.
G.	
GDPR	Acronym for “General Data Protection Regulation”.
I.	
Identifier	A data-item whose purpose is to uniquely distinguish an entity given a context.

Identity	The virtual representation of an entity.
Ingeniería Web y Testing Temprano	Research group in *Universidad de Sevilla* located in Seville (Spain).
IWT2	Acronym for "Ingeniería Web y Testing Temprano".
M.	
mKAOS	A mission-level modeling language that allows specifying missions of SoS and defining relationships between missions and other aspects of the SoS.
Mission	A mission describes the common objective for all the constituent systems in the SoS. This represent the result of the collaboration.
Model-driven Engineering	A branch of computer science that focuses on creating and exploiting domain models, which are conceptual models of all the topics related to a specific problem.
MDE	Acronym for "Model-driven Engineering".
O.	
OMG	Acronym for "Object Management Group".
Operational capabilities	In mKAOS the operational capabilities are the set of resources that can perform activities. The operational capabilities usually are the functional requirements of the constituent systems.
P.	
PDCA	Acronym for "Plan Do Check Act".
Portrayal	The result of depicting a Digital Persona.
Privacy	The individual right to determine, when, how, and to what extent information is collected about them.
Product owner	A stakeholder representing the desires of good results.
R.	
Red Product Backlog	A catalog of Red Requirements with responsibilities, cost estimation, and priorities assigned.
Red Requirements	Behaviors that defines the needed steps to exploit identified vulnerabilities.
Red Team	Team that enforces the security by simulating attacks.
RSM	Acronym for "Relational Security Model".
S.	
Security	Concepts, beliefs, principles, policies, procedures, techniques, and measures that are required in order to protect the individual system assets as well as the system as a whole against any deliberate or accidental threats.
SEDC	Acronym for "Software Engineering and Dependable Computing".
SE	Acronym for "Software Engineering".
SLR	Acronym for "Systematic Literature Review".
SMS	Acronym for "Systematic Mapping Survey".

Software Engineering and Dependable Computing	Research group on the *Consiglio Nazionale delle Ricerche* in Pisa (Italy).
SoS	Acronym for "System of Systems".
SysML	Acronym for "Systems Modeling Language".
System of System	A system as a result of the combination of resources of constituent systems with shared responsibilities.
Systematic Literature Review	A structured replicable process to review the state-of-the-art on a particular science area with well-defined criteria.
Systems Modeling Language	A general-purpose modeling language for systems engineering applications.
Systematic Mapping Study	A more general SLR used when it is not clear how to categorize retrieved studies.
T.	
TeSSoS	Acronym for "Testing Security on System of Systems".
Trust	A belief that is influenced by the individual's opinion about certain critical system features.
U.	
UML	Acronym for "Unified Modeling Language"
V.	
V&V	Acronym for "Validation and Verification".

Annex C

Bibliography

Annex C. Bibliography

[1] M. A. Olivero, A. Bertolino, F. J. Dominguez-Mayo, M. J. Escalona, and I. Matteucci, '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)*, 2019, vol. 11732, no. Webist, pp. 138–146.

[2] M. A. Olivero, A. Bertolino, F. J. Domínguez-Mayo, M. J. Escalona, and I. Matteucci, 'Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life', *J. Inf. Secur. Appl.*, vol. 52, p. 102492, Jun. 2020.

[3] D. Gasper, 'Securing Humanity: Situating "Human Security" as Concept and Discourse', *J. Hum. Dev.*, 2005.

[4] S. B. Gould, 'Computers at risk: Safe computing in the information age', *Gov. Inf. Q.*, vol. 8, no. 4, pp. 404–405, 1991.

[5] M. W. Maier, 'Architecting Principles for Systems-of-Systems', *INCOSE Int. Symp.*, 1996.

[6] N. Forsgren, J. Humble, and G. Kim, *Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations*. 2018.

[7] P. Johannesson and E. Perjons, *An Introduction to Design Science*. Cham: Springer International Publishing, 2014.

[8] A. Dresch, D. P. Lacerda, and J. A. V. Antunes, *Design science research: A method for science and technology advancement*. 2015.

[9] R. J. Wieringa, *Design science methodology: For information systems and software engineering*. 2014.

[10] C. S. L. N. I. of S. and T. Director, 'Integration Definition for Function Modeling (Idef0)', *Draft Fed. Inf. Process. Stand. Publ. 183*, 1993.

[11] M. A. Olivero *et al.*, 'Security Assessment of Systems of Systems', *Proc. - 2019 IEEE/ACM 7th Int. Work. Softw. Eng. Syst. 13th Work. Distrib. Softw. Dev. Softw. Ecosyst. Syst. SESoS-WDES 2019*, pp. 62–65, May 2019.

[12] M. Urbieta, M. J. Escalona, E. Robles Luna, and G. Rossi, 'Detecting conflicts and inconsistencies in web application requirements', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012.

[13] M. J. Escalona, G. Lopez, S. Vegas, L. García-Borgoñon, J. A. García-García, and N. Juristo, 'A software engineering experiments to value MDE in testing. Learning lessons', in *Actas de las 21st Jornadas de Ingenier&#65533;a del Software y Bases de Datos, JISBD 2016*, 2016.

[14] N. Dalkey and O. Helmer, 'An Experimental Application of the DELPHI Method to the Use of Experts', *Manage. Sci.*, 1963.

[15] M. A. Olivero, L. Morales-Trujillo, D. Lizcano, and F. J. Dominguez-Mayo, 'Una estrategia centrada en el usuario y guiada por modelos para el desarrollo sistemático de módulos ERP', 2019.

■