UMR IRISA

Activity Report 2024

Team SECREIZH

Security by Design

D4 – Language and Software Engineering

Université de Rennes | rennes | INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES | cnrs | Inria | Inserm | CentraleSupélec | IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom | Université Bretagne Sud ubs

1 Team composition

Researchers and faculty

Salah Sadou, Full Professor/PR 1ère classe, ENSIBS, UBS [1] (Team Leader)
Flavio Oquendo, Full Professor/PR classe exceptionnelle, UBS
Chouki Tibermacine, Full Professor/PR 2ème classe, UBS
Nicolas Belloir, Associate Professor/MCF hors cl., HDR, Académie de St-Cyr [2]
Jamal El Hachem, Assistant Professor/MCF cl. normale, UBS
Régis Fleurquin, Associate Professor/MCF cl. exceptionnelle, HDR, UBS

Associate members (IRISA/SEGULA Agreement)

Isabelle Borne, emeritus Full Professor, UBS
Elena Leroux, Assistant Professor/MCF hors cl., UBS
Paul Perrotin, Business Knowledge Dpt. head, DGA-MI
Soraya Mesli-Kesraoui, PhD, SEGULA Technologies - R&D Division

Research engineers, technical staff

Ph.D. students

Monica Buitrago (CDE, Dir Isabelle Borne)
Philippe Charton (CDI ENSIBS, Dir. Salah Sadou)
Ahmed Elmarkez (CIFRE SEGULA, Dir. Flavio Oquendo)

Mohamed Fendali
Mohamed Hamour (Cotutelle Univ. Luxembourg, Dir. Salah Sadou)
Etienne Lemonier (CDD chaire Saint Cyr, Dir. Nicolas Belloir)
Maykel Mattar (CDD CEA, Dir. Salah Sadou)
Jesus Antonio Sanchez-Ramos (CDE, Dir. Jérémy Buisson)
Lucas Tesson (CIFRE THALES, Dir. Jérémy Buisson)
Jeisson Andrés Vergara Vargas (Co-tutelle Univ. Nationale de Colombie, Salah Sadou)
Tales Viglioni (Co-tutelle UFPE Brésil, Dir. Flavio Oquendo)
Sidbewendin Angélique Yameogo (Bourse UBS, Dir. Régis Fleurquin)

Administrative assistant Anne Le Tohic (shared with all IRISA teams at Vannes).

External collaborator

Jérémy Buisson, Associate Professor/MCF hors cl., HDR, CRéA / Ecole de l'Air et de l'Espace.
Michel Bourdellès, Part-time associate professor, UBS.

1. Université Bretagne Sud
2. Académie militaire de Saint-Cyr Coëtquidan

2 Overall objectives

2.1 Overview

Modern society is critically dependent on a wide range of systems, and in particular software reliant systems (including systems of systems), i.e., systems that rely heavily on software to accomplish their goals.

Thereby, although it is fundamental to ensure that software reliant systems and systems of systems are developed to meet their functional requirements while ensuring correctness as well as safety, reliability, and performance, among other -ilities, it is equally fundamental to ensure their security.

However, traditionally security has only been considered after the design and more often after the implementation and even the deployment of software-reliant systems, meaning that security is fitted into pre-existing designs or code or executable. In practice, a fit-all solution is habitually assumed where security mechanisms are inserted into the system with very little consideration of the implications of inserting such mechanisms into the existing system design. As a result, security may conflict with the system requirements and this can raise problems, which most of the times translate into security vulnerabilities.

In contrast with those traditional security practices, in the last decade, has emerged a new vision on how to address security, in addition to functional correctness and other -ilities, that is the so called "security by design", thereby integrating security since the design of software reliant systems and systems of systems.

The SecReizh Research Team focuses on developing novel and sound languages, processes, and tools to address security by design, mainly driven by the software architecture for software-reliant systems and, in particular, systems of socio-technical systems.

2.2 Scientific foundations

Bellow we present some lines of research we address. These research lines cover manly the design and maintenance stages of the secure software development

2.2.1 Gaps Between Specification and Architecture Stages

The transition from the specification stage to the design stage involves several system security risks. The first risk concerns the means of expression in these two stages which are not always compatible to ensure a complete transfer of information. The second risk concerns the fact that in these two stages there are often three Stackholders (the application domain expert, the architect and the cybersecurity expert) who do not necessarily understand each other. Our approach to solving these problems consists in providing languages that allow each interlocutor to express themselves and thus break down the boundaries between these stages.

2.2.2 Architecture Security and Safety Verification

The architecture of a software system is conceived as a set of structures that allow reasoning about the system, through elements, relationships and properties. Thus, the system architecture design is a fundamental process to guarantee its quality and to withstand challenges in terms of size and complexity. In this way, one of the main issues on system architecture is the treatment of non-functional requirements, grouped into what are known as quality attributes. Among the most important quality attributes are performance, scalability, security, interoperability, availability, and usability. Particularly, security is a measure of a system's ability to protect data and information from unauthorized access while still providing access to people and systems that are authorized. From a system architectural point of view, security is one of the most representative quality attributes, and its foundation is based on the following three characteristics : confidentiality, integrity and availability (CIA).

There are different strategies to control security at the architectural level, on the one hand the architectural tactics and on the other hand the security patterns. Likewise, there are different security assurance techniques, some based on the use of architecture description languages and others based on traditional techniques used during the system life cycle and where there is no use of this type of language. However, it can be concluded that at the time of an evolutionary process in the architecture, there is no guarantee that the assurance generated by the application of these strategies will be maintained.

The objective of this research line is to make security a first-order entity in the architecture of systems. The architecture being the backbone of the system, the integration of the security properties sought will make it possible to preserve them throughout the life cycle of the system.

2.2.3 Humans as Constituents of an SoS

At the ECSA'22 conference, David Garlan gave an invited talk entitled "Humanizing Software Architecture". During this presentation he argues that humans were generally excluded from architectural design. However, according to his expertise there are advantages in integrating them as first-class entities in order to improve the human/system synergy required in current systems. This vision joins the one defended by our past work about human vulnerabilities in systems of socio-technical systems. The vision that carried in that work was that a human can be considered as a system like any other, from an architectural point of view. The objective is to promote a better synergy in order to lead to better design and to reduce the risk of poor consideration of human aspects and/or poor interaction between the two types of systems.

From an architectural design point of view, it is relevant to extend the human properties to go beyond the mere consideration of vulnerability. The idea is still not to be exhaustive in the human representation, the human complexity makes this impossible, but to propose a set of human properties covering various characteristics that the architect seeks to study and/or specify, according to several quality criteria. These quality criteria can be the traditional or more system-of-systems specific ones as summarized by. There is a first research question to be decided here : Which quality criteria are relevant to propose an architecture in which some subsystems are human ? Then, a second

question comes : What are the impacts in terms of architecture on this approach and what are the consequences on existing tools and methods ? Even if the questions are numerous the stakes are high.

2.3 Application domains

During our past research works, we have especially tackled the central characteristic of SoS, that is emergent behaviors, and smoothly shifted from software to software-reliant systems, where correctness and -ilities depend not only on the software itself but also on the related physical constituents and operational environment of the encompassing software-reliant system.

For example, landing aid software cannot be produced independently of the encompassing system, i.e. the aircraft. Thus, it is increasingly important to coordinate the work of the software architect with the work of the system architect.

Moreover, the interest of developing an SoS is to take advantage of emergent behaviors, as a result of the collaboration of the constituent systems. However, if it is already hard to master the intended emergent behavior of an SoS, it is yet harder to identify the emergent behaviors that are not sought and therefore, may be unwanted and often harmful. Indeed, unwanted emergent behaviors constitute a major threat to the security of software-reliant SoS, because they can create unknown vulnerabilities.

In this context, in addition to largely automated or autonomous SoS, the SecReizh research team also focus on sociotechnical SoS. In fact, humans have an important role in the successful achievement of the SoS mission in the case of sociotechnical SoS, and in particular of systems of sociotechnical systems (SoSTS).

3 Scientific achievements

3.1 Architecture Modeling for Security and Safety by Design

Keywords: Architecture Modeling, Executable Architecture Specifications, Secure Architecture Specifications, Digital Modeling for Software-intensive Systems-of-Systems.

Software architecture provides the right abstraction level to address the complexity of the design and development of Software-intensive Systems and Systems-of-Systems regarding, in particular regarding their extra-functional aspects, and in special security and safety.

This research line addresses the research challenges raised by architecture modeling based on the ISO SysML notation for both Security and Safety by Design.

The main research challenge is thereby to enforce correctness-by-design associating on the one hand a software architect-friendly notation with on the other hand formal representations for supporting formal analysis.

In the sequel, the main results of this research line produced in 2024 are presented.

3.1.1 A model-based approach for assessing the security of cyber-physical systems

Keywords: Risk Analysis Security, Privacy for Cyber-Physical Systems, Critical Infrastructures, Threats and Attack Modelling, Usable Security and Privacy, Security by Design.

Participants: Hugo Teixeira de Castro, Ahmed Hussain, Gregory Blanc, Jamal El Hachem, Dominique Blouin, Jean Leneutre, Panos Papadimitratos.

Cyber-Physical Systems (CPSs) complexity has been continuously increasing to support new life-impacting applications, such as Internet of Things (IoT) devices or Industrial Control Systems (ICSs). These characteristics introduce new critical security challenges to both industrial practitioners and academics. This work investigates how Model-Based System Engineering (MBSE) and attack graph approaches could be leveraged to model secure Cyber-Physical System solutions and identify high-impact attacks early in the system development life cycle. To achieve this, we propose a new framework that comprises (1) an easily adoptable modeling paradigm for Cyber-Physical System representation, (2) an attack-graph-based solution for Cyber-Physical System automatic quantitative security analysis, based on the MulVAL security tool, (3) a set of Model-To-Text (MTT) transformation rules to bridge the gap between SysML and MulVAL. We illustrated the validity of our proposed framework through an autonomous ventilation system example. A Denial of Service (DoS) attack targeting an industrial communication protocol was identified and displayed as attack graphs. In future work, we intend to connect the approach to dynamic security databases for automatic countermeasure selection.

The result of this work was published in [5].

3.1.2 Enforcing security by design of industrial systems in the industrial IoT

Keywords: Cybersecurity, Security by Design, SCADA, Industrial IoT (IIoT).

Participants: Flavio Oquendo, Ahmed Elmarkez, Soraya Mesli-Kesraoui, Pascal Berruet.

Security by design is rapidly becoming an essential approach in the rapid development of systems, in particular industrial control systems, in the Internet of Things (IoT), and especially in the Industrial IoT (IIoT) towards Industry 4.0. One of the major security challenges in industrial control systems deployed in the IIoT is that they involve both Operational Technology (OT) and Information and Communication Technology (ICT). Indeed, OT encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the

physical environment) while being increasingly distributed or accessible via the IoT in particular the IIoT.

In the reporting period, work was carried out on an automatic classification method for repository mitigations. Indeed, it is projected that cybercrimes will escalate to an alarming annual figure of 10.5 trillion USD. To counter this growing threat, cybersecurity repositories such as CVE, CWE, CAPEC, and Mitre Att&ck serve as crucial platforms for the exchange of threat intelligence and mitigations. These repositories play a pivotal role in the prevention of cyber threats. Yet, mitigations in these repositories are manually described by various experts, lacking standardized rules and often failing to reference widely accepted catalogs like NIST SP800-53.

To enhance the effectiveness and usability of mitigations within security repositories, this work was carried out to create an automatic classification method for repository mitigations, categorizing them into NIST SP800-53 classes. This classification relies on similarity approaches and introduces a novel algorithm aimed at refining and optimizing the accuracy of the classification results.

Results of this research work were published in [6].

3.1.3 Enhancing SysADL with an executable architecture viewpoint for supporting scenario-based simulations for safety-by-design

Keywords: Software Architecture, Executable Architecture, Simulation, Scenario Modeling, SysML.

Participants: Flavio Oquendo, Tales Viglioni, Thais Batista, Everton Cavalcante.

Executable software architecture descriptions enable architects to validate or verify the correctness of their designs early in the development process of software-intensive systems, reducing the risk of costly misconceptions. Executable architectures have been the subject of research for several decades, but there is no comprehensive panorama of the state of the art on this topic.

To fill this gap, we conducted, in this research line, a systematic mapping study that explores activities and approaches related to executable architecture descriptions for designing software-intensive systems. We have selected and analyzed 45 studies from the last 30 years to understand the activities related to executing architecture descriptions and identify the existing approaches. We also devised a taxonomy with key concepts related to executable architecture descriptions for software-intensive systems. The resulting insights from our study can help researchers pinpoint areas for further investigation.

Part of the results of this systematic mapping study were published in [12]. Complete results are planned to be published in a journal article to be submitted in 2025.

3.1.4 Roadmapping software engineering for systems of systems toward safety-by-design

Keywords: Systems of Systems, Software Engineering.

Participants: Flavio Oquendo, Thais Batista, Everton Cavalcante,.

Modern systems are increasingly connected and more integrated with other existing systems, giving rise to systems of systems (SoS). An SoS consists of a set of independent, heterogeneous systems that interact to provide new functionalities and accomplish global missions through emergent behavior manifested at runtime. The distinctive characteristics of SoS, when contrasted to traditional systems, pose significant research challenges within software engineering. These challenges motivate the need for a paradigm shift and the exploration of novel approaches for designing, developing, deploying, and evolving these systems. In this line of research, we carried out a study aimed at outlining the evolution and future trajectory of software engineering for SoS based on the examination of 57 papers spanning the 11 editions of the International Workshop on Software Engineering for Systems of Systems (SESoS). SESoS started in 2013 to fill a gap in scientific forums addressing SoS from the software engineering perspective, becoming the first venue for this purpose.

The study carried out combined scoping review and scientometric analysis methods to categorize and analyze the research contributions concerning temporal and geographic distribution, topics of interest, research methodologies employed, application domains, and research impact. Based on such a comprehensive overview, we identified and discussed current and future directions in software engineering for SoS in particular regarding safety-by-design.

Results of this research work were published in [2].

3.1.5 Knowledge Graph for Modeling Security Scenarios at the Software Architecture Level

Participants: Jeison Vergara, Salah Sadou, Chouki Tibermacine, Felipe Restrepo.

Security, as a software quality attribute, needs to be addressed from different perspectives and at different levels of the software lifecycle. One of these perspectives is the one that focuses on design decisions at the highest level, that is, at the architectural level. This paper presents a knowledge graph, called "Sarch-Knows", that models security scenarios based on the architectural design of a software system. The knowledge graph is based on different paths called scenarios, where each scenario covers the fundamental elements to meet a security property and the architectural elements on which the properties fall. This knowledge graph is being implemented as a Neo4J database on which queries can be issued to extract aggregated knowledge about security and architecture. This knowledge is scattered over many sources of documentation, like NIST, MITRE, databases, books and papers ; which is why this graph can be considered as a starting

option to establish an ordered scheme of this knowledge.

The result of this work was published in [10].

3.1.6 Sarch-Checks : A Method for Checking Software Architecture Security Properties Using a Knowledge Graph

Participants: Jeison Vergara, Salah Sadou, Chouki Tibermacine, Felipe Restrepo.

Checking the security properties of a software system during design is essential to enable the construction of a foundationally secure system. However, combining design tasks with security checks leads to a difficult and error-prone activity. This paper presents a checking method for security properties, called Sarch-Checks. This method allows analyzing the context of architectural elements in terms of an expected security property and identifying the presence of countermeasures and vulnerabilities. It uses an architectural description of the system to be analyzed, through the use of a modeling language. It also uses a knowledge graph, modeled and built from the elements of the software architecture, and cybersecurity elements taken from official information sources such as NIST and MITRE. This solution is an aide to the architect to design more secure architectures. Additionally, a validation process of the proposed method is presented through a case study based on a real report of a vulnerability in an open-source software system.

The result of this work was published in [11].

3.2 Data Centric Security

Keywords: Confidentiality, Integrity, Model Based System Engineering (MBSE), System Design Security Analysis, Automatic Security Code Generation, Initialisation and SetUp Platform Security Service.

The Industrial Product Development Flow of cyberphysical systems allows the production of artifacts from the capture of the functional requirements of the system to be produced. This highly automates the process that ultimately performs the validation of the system. These tooled processes do not take into account, or weakly, the security requirements resulting from a risk analysis.

This line of research proposes a certain number of security services to allow the validation of security requirements resulting from the risk analysis carried out upstream of the production of the cyberphysical system.

The research challenges are manyfold. The first aims to complete, in the modeling for the specification and system design, the current collaborative work mechanisms in order to protect access to sensitive elements of the model only to stakeholders who need to know. The second aims to enrich the models with information resulting from the security requirements. The third consists in allowing the exploitation of this information to verify the consistency of the design choices with regard to the security needs expressed. The fourth challenge is to automatically produce security code from these analyses. A fifth challenge is to offer a platform security service allowing the distribution of keys necessary

for securing sensitive data flows characterized during system analysis. Elements of these challenges and results were presented in an industrial dissemination action [3].

An aother aspect about data and security concerns data privacy regulation. As software systems get more operated for final users, personal data is collected and exploited more than ever before. This situation raises the issue of user privacy. Conforming to personal data protection regulations such as the European General Data Protection Regulation (GDPR) has thus become mandatory by law. Despite the legal obligations, there is no widely adopted solution for modeling and assessing the privacy of personal data. In order to help developers, our objective is to propose a tooled software engineering approach to add personal data protection capabilities into existing software, thus making software privacy-aware. The originality of our proposal is that it goes beyond a declarative description of the regulation by being concretely processable and actionable.

3.2.1 Confidentiality Management of Modellings

Keywords: Confidentiality Management of MBSE modellings, Access Control, Iterative Processing Compliancy, Confidentiality Protected Product Line Management.

Participants: Michel Bourdellès, Jamal El Hachem, Salah Sadou.

The use of modelling tools for the design of industrial systems is increasingly replacing the documentation production resulting from a classic system design process. One of the problems to be solved in order to fully succeed in this transition is information confidentiality management. It is also necessary to propose a system design process that allows an evolution through the whole design life cycle, and that guarantees a coherent design for a given level of confidentiality.

In [3] and [4], we propose a model based system design process to manage elements belonging to different levels of confidentiality. The process guarantees a plurality of confidentiality levels in line with Bell-Lapadula security policies for the secure management of system design and specification, as required for the protection of national and coalition defense information. It includes the separation into enclaves and adaptations guaranteeing the preservation of confidentiality and integrity to authorized users. We describe how this process can be leveraged for current modelling tools by exploiting existing multi-user functionality.

This confidentiality management can be extended to the variability management mechanisms of product line management by natively taking into account confidentiality constraints in a solution subject to the submission of an article in 2025.

3.2.2 Security Analysis and Security Code Generation of MBSE Modelling Designs

3. "MBSE Confidentiality Management and Security Analysis of Capella Designs", Michel Bourdellès, UBS, CapellaDays webinar 2024, 2024/11/21, https ://mbse-capella.org/capella_days_2024.html

Keywords: Confidentiality, Integrity, Model Based System Engineering (MBSE), System Design Security Analysis, Automatic Security Code Generation, Platform Security Service Initialisation and SetUp.

Participants: Michel Bourdellès, Jamal El Hachem, Salah Sadou.

Sensitive data confidentiality and integrity has critical impact on system's security. To handle the inherent complexity of securing sensitive data, protection measures are usually implemented after identifying potential system's vulnerabilities leading to security breaches. At early stages of the system development life cycle, this requires analyzing the various confidentiality levels within the system design, based on data flow representations, to assess and validate compliance with the system's specifications and security requirements.

Thus, in a patent [4] we propose a novel security-enhanced data-centric model to analyze vulnerabilities and reinforce sensitive date security at the system architecture level. Generally, it formalizes data flows and enrich them with essential security information knowledge. Specifically, to provide automation and preciseness, we propose a model and tool with two key improvements : (1) ability to confront the data security model with the system architecture to detect potential unsecure flaws within the latter, and (2) capability to automatically complement the code with signatures and ciphering security codes. The evaluation shows that the proposed approach outperforms state-of-the-art approaches, responding to the need of sensitive data protection required in CWE-311, CWE-312, CWE-319 and CWE-327, by offering automated and systematic integration of security controls to the system's design, at the requirement elicitation and architecture design stages.

This preliminary work gave rise to a contribution accepted in a conference (ICSA), to be published in 2025. This work focused on confidentiality requirements and is the subject of work for an extension to integrity requirements.

The proposed solution presupposes a prior distribution of keys to components of the platform. In a patent [5], we propose a mechanism for distributing such keys, allowing the protection in case of compromise of intermediate data transmission nodes.

3.2.3 Data Privacy Regulation Modeling and Assurance

Keywords: Data Privacy, GDPR (General Data Protection Regulation), Metamodelling, Domain-Specific Languages, Consent Management and Attribute-based Access Control.

Participants: Chouki Tibermacine, Selena Lamari (LIRMM, University of Montpellier), Christelle Urtado and Sylvain Vauttier (EuroMove and IMT Mines Ales)..

4. Michel Bourdellès, UBS, "Procédé logiciel permettant une analyse de sécurité à partir d'une conception système annotée d'informations issues d'une analyse de risque ", FR2313340, 5197

5. Michel Bourdellès, UBS, " Procédé d'échanges de clés pour sécuriser une transmission de données dans une plateforme informatique comprenant des processeurs interconnectés ", FR2409974, référence 5414.

In this work, we developed the PRIAM metamodel (PRIvacy Assessment Model) and its companion artifacts. PRIAM models the GDPR by capturing the concepts described in the regulation. This metamodel is the cornerstone of various artifacts that altogether model the regulation and how it adapts to a specific application that needs to become privacy-aware. It comprises a domain-specific language (DSL) derived from the PRIAM metamodel, generated user stories that need to be implemented in the context of a given application and a privacy enforcement database that stores application-specific as well as user-specific data that are needed to implement users' rights.The usefulness of the PRIAM metamodel and all its companion artifacts was showcased through the running example of a *Sport center management application* that needs to become privacy-aware. The extensivity of the PRIAM metamodel was evaluated in a qualitative manner by GDPR experts, through a questionnaire. The systematic process we followed to build these artifacts as well as this qualitative evaluation both contribute to assess the soundness of our proposal.

This work is under revision for a journal.

We leverage this metamodel and its artifacts in a software engineering process that we are developing in order to make it possible for engineers to make their applications compliant with GDPR. This process embeds in its core a micro-service architecture, which is under development. This architecture includes services for managing actors (final users/data subjects, processing holders, ...), data and processings, rights, consents, breaches and notifications. The software engineering process accompanies application developers in the integration of these services in her/his application in the most seamless and non-intrusive manner. For instance, consent management is handled in the micro-service architecture by a protocol that we have designed for access control including authentication, authorization management, and externalized consent management based on the ABAC (Attribute-Based Access Control) and the side-car architecture patterns.

This work has been published in [7].

3.2.4 Analysis of Access Control Mechanisms for a Dynamic and Decentralized Approach of Data-Centric Security

Participants: Jamal El Hachem, Lionel Touseau, Jérémy Buisson, Nicolas Belloir, Jean-François Wiorek.

Today, in many domains, stakeholders handle sensitive data that needs to be protected according to their confidentiality level. Among existing security paradigms, data-centric security (DCS) places security as close as possible to the data, to ensure confidentiality on any network, communication channel or storage server. To achieve this, DCS requirements are implemented through access control mechanisms. These mechanisms need to be (1) dynamic, to enable actors in a secure system to join it opportunistically and (2) decentralized, to guarantee data availability. However, existing approaches only partially address these challenges.

In [8], we illustrate these challenges using two examples and discuss the limitations of existing approaches in addressing them.

3.2.5 Creation of software to detect and characterize disinformation campaigns

Participants: Nicolas Belloir, Régis Fleurquin, Wassila Ouerdane (MICS, Centrale Supelec).

Keywords: Conceptual Modeling, Characterization, Fake News, Disinformation Campaigns, Explainable Artificial Intelligence.

The fight against misinformation is more necessary than ever. It comes up against the mass of fake news and the industrialization of manipulation by third parties in disinformation campaigns. Tools are needed to detect, characterize and combat this phenomenon. Current approaches use artificial intelligence to good effect, but fail to convince due to their lack of explicability. In this context, we propose an approach based on the development of ad-hoc software. Indeed, we propose to base these on a set of small, specific software bricks enabling semantics to be extracted and stored, based on a conceptual model designed to structure the universe of misinformation. Based on the data collected and enriched, we propose a high-level assistant for the analysis of disinformation campaigns [13].

3.2.6 Determining the operational impact of an attack on a system

Participants: Nicolas Belloir, Jamal El Hachem, Jérémy Buisson (Créa, École de l'Air et de l'Espace).

Keywords: Operational impact, Threat Modeling, SoS Analysis and Design.

In previous work, we have contributed to bringing risk analysis methods (such as EBIOS) closer to system-of-systems design methods (such as Capella) ; we have also proposed an approach aimed at bringing security experts closer to domain experts by reifying asset concepts. In this work, we use the two previous approaches upstream of the architecture analysis phases. To this end, we are developing an approach aimed at assessing the operational impact of a cyber-attack on the system as early as possible in a system-of-systems modeling process such as NAF. More specifically, we are assessing which of the system's operational functions will be impacted by a cyber attack, and what the consequences will be from an operational point of view [9].

4 Software development

4.1 Software development

Participants: Michel Bourdellès.

A software artifact [6] has been provided as an Open Research Object (ORO) in addition to the paper accepted to a conference as indicated in section 3.4.2. This de-

6. Michel Bourdellès, "Secured Functional Chain Analyzer", https ://zenodo.org/records/14508184

monstrator allows the computation of the directives and the production of code of the examples presented in the paper whose object is the definition of a Data-Centric Model for the analysis of architecture vulnerabilities.

5 Contracts and collaborations

5.1 National initiatives

— Public-private collaboration on the cybersecurity of large public events between the Université Bretagne Sud, Gendarmerie Nationale and GICAT (industrials in defense) in the domain of the cybersecurity of systems-of-systems. This ongoing collaboration is achieved through an industrial chair led by Salah Sadou. It aims to support the design and operation of large-scale sociotechnical systems-of-systems in open environments. It, in particular, aimed to support the 2024 Summer Olympics in Paris. The SecReizh team brings to this joint R&D project its expertise on security-by-design for mastering emergent behaviors in socio-technical SoS architectures.
In December 2024, we organised a ReTex in Paris on cybersecurity during the last Olympic Games. There were presentations on the organisation of cyber defence and the major events. The speakers were those directly involved in the cyber security of the games (ComCyber-MI, ATOS, etc.).
This work is helping to identify new challenges in the field of cyber security for socio-technical systems.

5.2 Bilateral industry grants

— SEGULA Engineering (Numéro de contrat Ouest Valorisation 2018-01307, renewed for 5 additional years as amendment 2022-01275) : Bilateral collaboration on cybersecurity in software architecture for industrial systems and systems-of-systems in the Industrial Internet-of-Things : Bilateral collaboration between ARCHWARE and the R&D division of SEGULA, a multinational systems engineering company developing large-scale systems and SoSs in different domains, including automotive, aeronautics, naval, and railway engineering. This ongoing collaboration aims to support the model-based engineering of critical systems-of-systems in the Industrial Internet-of-Things. The SecReizh team brings to this joint R&D project its expertise on formal approaches for the specification and verification of software architectures of SoSs. An additional PhD student has been funded by SEGULA under the scientific supervision of Flavio Oquendo, in this contract since November 2022 (for 3 years).
— Fondation St Cyr (Numéro de contrat Ouest Valorisation 2023_00971) : "Langage and infrastructure for data centric dynamic architecture", 3 years contract, lead by Nicolas Belloir.

5.3 Industrial partners in CIFRE grants

— SEGULA Engineering ;

— THALES.

5.4 Industrial academic chairs

— Chaire "Cybersécurité des Grands Evénements Publics", headed by Salah Sadou with ComCyber-MI and GICAT as partners. The aim of this industrial chaire is to anticipate future cyber threats related to grand events. An event is considered as a Systyme of Socio-Technical Systems.
— Chaire "Cyberdefense-Cybersécurité" St Cyr Thales (2023-2026), headed by Nicolas Belloir. The aim is to develop a software architecture supporting communications in collaborative warfare, with a data-centric security approach.

5.5 Academic research collaborations

Members of SecReizh actively participate in the following academic research collaborations.

National and international research networks :

— Salah Sadou, Isabelle Borne and Nicole Levy (CNAM Paris) leads the GT GL-Sec (working group on Software engineering and security) in the GDR GPL (Groupement de Recherche Génie de la Programmation et du Logiciel - INS2I-CNRS).
— Flavio Oquendo is a member of the INCOSE (International Council on Systems Engineering) System-of-Systems Working Group as well as a member of the AFIS (Association Française d'Ingénierie Système), French chapter of INCOSE, Technical Committee 3SAI (System-of-Systems & Services - Architecture & Engineering).

International research cooperation :

— Flavio Oquendo has a collaboration with UFRN in the framework of the DTArch research action on Digital Twins Architecture for Software-intensive Systems (Contract CNPq-MCTI).
— Salah Sadou has a collaboration with Univ. of Luxembourg (SnT) through a co-supervision of PhD thesis. The main subject concerns code vulnerability.
— Salah Sadou and Chouki Tibermacine have a collaboration with National University of Colombia throug a co-supervision of PhD thesis. The main subject concerns code vulnerability.

National collaborations with joint publications :

— Flavio Oquendo has a collaboration on systems-of-systems architectures with Khalil Drira (LAAS-CNRS) ;
— Salah Sadou has a collaboration with FramaC team, of the LIST Lab of CEA, through a co-supervision of a PhD thesis.

International collaborations with joint publications :

— Jamal El Hachem has the following international research collaborations :

  - Security vulnerabilities with an application on Big Data and IoT Systems with Faheem Ullah (University of Adelaide, Australia) and Mojtaba Shahin (RMIT University, Australia) ;
  - Attacks modeling and analysis via bayesian networks and game theory, with an application in the field of autonomous vehicles with Elena Lisova (University of Malardalen, Sweden) ;
  - Vulnerability knowledge bases evaluation with Mehdi Mirakhorli (University of Hawaii, New York) ;
  - Security risk governance with Yves Wautelet (KU Leuven, Belgium)
- Nicolas Belloir has a collaboration on the conceptual modeling of fake news with Oscar Pastor (Polytechnic University of Valencia, Spain) ;
- Flavio Oquendo has a collaboration on software architecture with Thais Batista and colleagues on software architecture modeling (UFRN - Federal University of Rio Grande do Norte, Natal, Brazil) ;
- Salah Sadou the following international research collaborations :
  - Architecture security with Felipe Restrepo-Calle (University National, Colombia) ;
  - Software engineering and cybersecurity with Mohamed Lamine Kerdoudi (Univ. Biskra, Algeria) ;
  - Code vulnerability Identification and automatic fixing with Tegawendé F. Bissyandé (SnT - Univ. of Luxembourg).

National collaborations with joint PhD supervision :

- Nicolas Belloir :
  - Centrale-Supelec, France, Ph.D. co-supervison with Wassila Ouerdane on the topic of improving understanding of misinformation campaigns using semantic analysis of Fake News.
- Jamal El Hachem has the following national collaborations :
  - Cybersecurity risk analysis with an application on SoS naval systems with Fabien Dagnat (IMT Atlantique, Lab-STICC, France) and Julien Franq (Naval group), in the context of the "Chaire de Cyberdéfense des Systèmes Navals" ;
  - Cyberattacks modeling and analysis, with an application on CPS, with Dominique Blouin, Gregory Blanc, Jean Leneutre and Vadim Malvon (Telecom Paris, France)
- Régis Fleurquin :
  - Centrale-Supelec, France, Ph.D. co-supervison with Wassila Ouerdane on the topic of improving understanding of misinformation campaigns using semantic analysis of Fake News.
- Flavio Oquendo :
  - Lab-STICC, France, Ph.D. co-supervison with Pascal Berruet on security-by-design of industrial control systems.
- Salah Sadou :
  - CEA, France, PhD supervision on machine learning to improve formal code verification.

International collaborations with joint PhD supervision :

- Salah Sadou :
  - University of Luxembourg : Ph.D. (Mohamed Hamour) co-supervision with

Tegawendé F. Bissyandé.
- Salah Sadou :
  - National University of Colombia : Ph.D. (Jeisson Vergara) co-supervision with Felipe Restrepo-Calle.
- Flavio Oquendo :
  - UFRN - Federal University of Rio Grande do Norte, Natal, Brazil : PhD co-supervision with Thais Batista on executable software architectures for software-intensive systems.

6 Dissemination

6.1 Promoting scientific activities

Research and Doctoral Supervising Awards (PEDR)
- Jamal El Hachem : PEDR (2021-2025) ;
- Flavio Oquendo : PEDR (2020-2024) ;
- Salah Sadou : RIPEC (2024-2027) ;
- Chouki Tibermacine : PEDR (2012-2024).

Chair/member of conference steering committees
- Flavio Oquendo :
  - European Conference on Software Architecture - ECSA (Steering Committee Member) ;
  - IEEE International Conference on Software Architecture - ICSA (Steering Committee Member) ;
  - Conférence francophone sur les architectures logicielles - CAL (Steering Committee Member) ;
  - ACM/IEEE International Workshop on Software Engineering for Systems-of-Systems and Software Ecosystems - SESoS (Steering Committee Member) ;
  - International Workshop on Digital Twin Architectures - TwinArch (Steering Committee Co-Chair).
- Chouki Tibermacine :
  - European Conference on Software Architecture - ECSA (Steering Committee Member) ;
  - Conférence francophone sur les architectures logicielles - CAL (Steering Committee Member) ;

Chair/member of conference program committees
- Jamal El Hachem :
  - DeMeSSA : Co-organizer of the 4th International Workshop on Designing and Measuring Security in Systems with AI co-located with the 10th IEEE European Symposium on Security and Privacy (EuroS&P 2025) ;
  - Member of the following confrences and journals PC : SoSE, ANSIM, FPS, SVM@ICSE, SESoS@ICSE, MoMMODELS, MPM4CPS@MODELS, EMSE-journal, JSS journal, EIS journal.

- Flavio Oquendo :
  - ICSA : IEEE International Conference on Software Architecture, 2024 ;
  - ECSA : European Conference on Software Architecture, 2024 ;
  - SoSE : IEEE International Conference on System-of-Systems Engineering, 2024 ;
  - ICSEA : International Conference on Software Engineering Advances, 2024 ;
  - ICAS : International Conference on Autonomic and Autonomous Systems, 2024 ;
  - TwinArch : International Workshop on Digital Twin Architecture at the IEEE International Conference on Software Architecture (Co-Chair), 2024
  - SESoS : ACM/IEEE International Workshop on Software Engineering for Systems-of-Systems and Software Ecosystems at the International Conference on Software Engineering, 2024 ;
  - FAACS : International Workshop on Formal Approaches for Advanced Computing Systems at the IEEE International Conference on Software Architecture (Co-Chair), 2024 ;
  - ICSE-SEET Track : International Conference on Software Engineering - Track on Software Engineering Education and Training, 2024 ;
  - ICSE-GE Track : International Conference on Software Engineering - Track on Gender Equality, Diversity, and Inclusion in Software Engineering, 2024.
- Salah Sadou :
  - ECSA : European Conference on Software Architecture, 2024 ;
  - SoSE : IEEE International Conference on System-of-Systems Engineering, 2024 ;
  - ICECCS : International Conference on Engineering of Complex Computer Systems, 2024 ;
  - SESoS : ACM/IEEE International Workshop on Software Engineering for Systems-of-Systems and Software Ecosystems, 2024 ;
  - International Conference on Emerging Security Information, Systems and Technologies 2024 ;
  - AISC : Australasian Information Security Conference, 2023 ;
  - ACSW : Australian Computer Science Week, 2023 ;
- Chouki Tibermacine :
  - ECSA : European Conference on Software Architecture, 2024 ;
  - ICSOC : International Conference on Service Oriented Computing, 2024 ;
  - WISE : International Web Information Systems Engineering conference, 2024 ;
  - ICSA (Software Architecture) and MODELS (Software Modeling) Satellite Events, 2024.

6.1.1 International conference keynotes

- Chouki Tibermacine : Keynote Speaker at the 6th International Conference on Advanced Aspects of Software Engineering, November 09-10, 2024, Constantine, Algeria : Software Engineering at the Service of Security : a Software Architecture Perspective.

6.1.2 International journal boards

Member of the Editorial Boards

- Flavio Oquendo :
  - Springer Journal of Software Engineering Research and Development (Member of the Editorial Board).

6.1.3 Scientific expertise

- Jamal El Hachem :
  - Scientific Expert acting as reviewer and evaluator of ANR JCJC ;
  - Scientific Expert acting as jury member and evaluator of Startups/Cyber Investor Day at the European Cyber Week 2024 ;
  - Scientific Expert acting as jury member for four Asscociate Professor recruitments ;
- Flavio Oquendo :
  - Scientific Expert acting as reviewer and evaluator of R&D Projects for the European Commission (Horizon Europe) ;
  - Scientific Expert acting as evaluator of R&D Proposals for the ESF European Science Foundation on Software Sciences and Engineering (Europe) ;
  - Scientific Expert acting as evaluator of R&D Proposals for the Swiss National Science Foundation (Switzerland) ;
  - Scientific Expert acting as evaluator of R&D Proposals for the FWO (Research Foundation Flanders) on Software Sciences and Engineering (Belgium) ;
  - Scientific Expert acting as evaluator of R&D Projects for the MESR-CIR on Software Engineering and Technologies ;
  - Distinguished Professor acting as evaluator of Scientific Standing and Achievements to Full Professorship for different universities in Europe on Computer Sciences and Software Engineering, e.g., for the Helmholtz Association of German Research Centers on Software Sciences and Engineering (Germany).
- Chouki Tibermacine :
  - Scientific Expert acting as reviewer and evaluator of R&D Projects for the Austrian Science Fund (FWF) ;
  - Scientific Expert acting as reviewer and evaluator of R&D Projects and research labs for the Quebec/Canadian Research Fund (FRQ).

6.1.4 Academic councils

- Salah Sadou : member of the administrative council (CA) of UBS.
- Isabelle Borne : Deputy director of the Doctoral School MathSTIC-Bretagne-Océane ;
- Régis Fleurquin : Member of the CAC (Commission recherche du conseil académique) of Université Bretagne Sud ;
- Jamal El Hachem : Member of the CL (Conseil du Laboratoire) of IRISA ;
- Chouki Tibermacine : Member of the Institute Council (conseil d'institut), IUT de Vannes, Université Bretagne Sud.

6.1.5 PhD supervision or co-supervision

— Monica Buitrago [?], UBS (since January 2021) by Isabelle Borne and Jérémy Buisson ;
— Philippe Charton, UBS (since March 2023) by Jamal El Hachem and Salah Sadou ;
— Ahmed Elmarkez, UBS (since November 2022) by Flavio Oquendo ;
— Mohamed Fendali, UBS/Badji Mokhtar-Annaba University (part-time, since September 2016) by Isabelle Borne ;
— Mohamed Hamour, UBS/Univ. Luxembourg (since 2024) by Salah Sadou
— Etienne Lemonier, UBS/Saint-Cyr (since October 2023) by Nicolas Belloir, Jérémy Buisson, and Jamal El Hachem ;
— Maykel Mattar, UBS/CEA (since December 2023) by Salah Sadou ;
— Jesus Ramos, UBS (since January 2023) by Nicolas Belloir, Jérémy Buisson, and Jamal El Hachem ;
— Lucas Tesson, UBS (since October 2023) by Jérémy Buisson and Jamal El Hachem ;
— Jeisson Vargas, UBS/National University of Colombia (since April 2022) by Salah Sadou and Chouki Tibermacine ;
— Tales Viglioni, UBS/UFRN (since October 2023) by Flavio Oquendo ;
— Sidbewendin Yameogo, UBS/CRéA (since December 2022) by Régis Fleurquin and Nicolas Belloir and Wassila Ouerdane (Centrale Supelec).

6.1.6 PhD juries

— Jamal El Hachem :
  — Examiner in Jury of Ph.D. defense by Ghazaleh Aghakhani, KU Leuven, Belgium ;
  — Examiner in Jury of Ph.D. defense by Paul Quentel at IMT Atlantique, France ;
  — Examiner in Jury of Ms. defense by Biplab Gautam, Universitè Libre de Bruxel, Belgium ;
— Flavio Oquendo :
  — *President* in Jury of PhD defense by Monica Buitrago [?] at Université Bretagne Sud, France ;
— Salah Sadou :
  — *Reviewer* in Jury of PhD defense by Mohammed El Amin Tebib at UniversitÃ© Grenoble Alpes, France ;
  — *Reviewer* in Jury of PhD defense by PriyadarshiniUniversitÃ© Grenoble Alpes, France ;
  — *Reviewer* in Jury of PhD defense by Aless Hosry at UniversitÃ© Lille, France ;
  — Examiner in Jury of HDR defense by Nicolas Belloir at Université Bretagne Sud, France.
— Chouki Tibermacine :
  — *President* in Jury of PhD defense by Hao XU, Sorbonne Université, LIP6 and Renault, France, December 2024 ;
  — *President* in Jury of PhD defense by Ali Benjilany, Nantes Université, LS2N,

France, December 2024.

7 diffusion

7.1 Teaching

— Academics of SecReizh teach at the Research Master on Computer Science of Université Bretagne Sud. Nicolas Belloir teachs at the Military Special Engineering School [7].

7.2 Teaching responsibility

— Nicolas Belloir : Head of mastere's (CGE) degree in cybersecurity and intangible fields (Military Academy of St Cyr Coëtquidan) ;
— Flavio Oquendo : Head of the Research Master on Computer Science of Université Bretagne ;
— Salah Sadou : Head of the Engineering Degree on Software Cybersecurity of ENSIBS School of Engineering ;
— Jamal El Hachem :
  — Responsible of the preparatory class of the ENSIBS Engineering School ;
  — Coordinator of a teaching unit and member of the Erasmus mundus joint master in cybersecurity consortium
— Chouki Tibermacine : Coordinator of International Relations at IUT de Vannes.

7.3 French "Habilitation à Diriger des Recherches"

— Nicolas Belloir : [1], 31/01/2024.

8 Bibliography

Doctoral dissertations and "Habilitation" theses

[1] N. Belloir, *Un voyage dans les modèles : du logiciel aux systèmes de systèmes socio-techniques*, Accreditation to supervise research, Université de Bretagne Sud, January 2024, https://hal.science/tel-04906029.

Articles in referred journals and book chapters

[2] E. Cavalcante, T. Batista, F. Oquendo, "Looking back and forward : A retrospective and future directions on software engineering for systems-of-systems", *Journal of Software : Evolution and Process 36*, 10, June 2024, https://hal.science/hal-04895251.

7. École Spéciale Militaire, Académie Militaire de St Cyr Coëtquidan : https://www.terre.defense.gouv.fr/amscc/devenir-officier/ecole-speciale-militaire

Publications in Conferences and Workshops

[3] M. Bourdellès, J. El Hachem, S. Sadou, "Ensuring Requirements Confidentiality during System Design Modelling", *in : Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, SAC '24*, p. 1178 â 1179, Avila, Spain, 2024, https://doi.org/10.1145/3605098.3636096.

[4] M. Bourdellès, J. El-Hachem, S. Sadou, ""Confidentiality Management in Complex Systems Design"", *in : 28th Intenational Engineering of Complex Computer Systems (ICECCS)*, G. "Bai, F. Ishikawa, Y. Ait-Ameur, G. A. Papadopoulos (editors), Springer Nature Switzerland, p. 303–322, Cham, 2025, https://hal.science/hal-04708770.

[5] H. T. D. Castro, A. Hussain, G. Blanc, J. E. Hachem, D. Blouin, J. Leneutre, P. Papadimitratos, "A Model-based Approach for Assessing the Security of Cyber-Physical Systems", *in : Proceedings of the 19th International Conference on Availability, Reliability and Security, ARES 2024, Vienna, Austria, 30 July 2024 - 2 August 2024*, ACM, p. 121 :1–121 :10, 2024.

[6] A. Elmarkez, S. Mesli-Kesraoui, F. Oquendo, P. Berruet, D. Kesraoui, "A Similarity Approach for the Classification of Mitigations in Public Cybersecurity Repositories into NIST-SP 800-53 Catalog", *in : 4th IFIP WG11.2 International Conference, WISTP 2024, Proceedings (LNCS, volume 14625)*, *Lecture Notes in Computer Science*, *14625*, Springer Nature Switzerland, p. 64–79, Paris, France, February 2024, https://hal.science/hal-04895280.

[7] S. Lamari, N. Benblidia, C. Tibermacine, C. Urtado, S. Vauttier, "Leveraging a Microservice Architecture, Access Control and Interoperability Patterns to Manage Privacy-related User Consents", *in : 22nd International Conference on Service-Oriented Computing (ICSOC'2024), December 3 - 6, 2024, Tunis, Tunisia*, Springer, 2024.

[8] E. Lemmonier, J. El Hachem, L. Touseau, J. Buisson, N. Belloir, J.-F. Wiorek, "Analysis of Access Control Mechanisms for a Dynamic and Decentralized Approach of Data-Centric Securit", *in : Proceedings of C&ESAR 2024, Rennes, France*, 2024.

[9] J. Sánchez, J. Buisson, J. El Hachem, N. Belloir, "Towards Joint SoS and Threat Mission-based Modeling for Operational Impact Identification", *in : 2024 19th Annual System of Systems Engineering Conference (SoSE)*, IEEE, p. 72–77, Tacoma, United States, June 2024, https://hal.science/hal-04674989.

[10] J. Vergara-Vargas, F. Restrepo-Calle, S. Sadou, C. Tibermacine, "SarchKnows : A Knowledge Graph for Modeling Security Scenarios at the Software Architecture Level", *in : Software Architecture. ECSA 2023 Tracks, Workshops, and Doctoral Symposium - Istanbul, Turkey, September 18-22, 2023, Revised Selected Papers*, B. Tekinerdogan, R. Spalazzese, H. Sözer, S. Bonfanti, D. Weyns (editors), *Lecture Notes in Computer Science*, *14590*, Springer, p. 107–119, 2023.

[11] J. Vergara-Vargas, S. Sadou, C. Tibermacine, F. Restrepo-Calle, "SarchChecks : A Method for Checking Software Architecture Security Properties Using a Knowledge Graph", *in : 21st IEEE International Conference on Software Architecture, ICSA 2024 - Companion, Hyderabad, India, June 4-8, 2024*, IEEE, p. 135–142, 2024.

[12] T. Viglioni, T. Batista, E. Cavalcante, F. Oquendo, "The Execution Perspective in Software Architecture Descriptions : A Systematic Mapping", *in : Software Architecture : 18th European Conference, ECSA 2024, Proceedings (LNCS, volume 14889)*, *Lecture Notes in Computer Science*, *14889*, Springer Nature Switzerland, p. 379–395, Luxembourg City, Luxembourg, September 2024, https://hal.science/hal-04895271.

[13] S. A. Yameogo, "Improving Understanding of Misinformation Campaigns with a Two-Stage Methodology Using Semantic Analysis of Fake News", *in : 18th Research Challenges in Information Science*, *Lecture Notes in Business Information Processing*, *514*, Springer

Nature Switzerland, p. 121–130, Guimarães, Portugal, France, May 2024, https://hal.science/hal-04905988.