ICO Research Project

HERMES-Design: **H**uman-C**E**ntric Collabo**R**ative Architectural Decision-**M**aking for S**E**cure **S**ystem Design

Applicant: Abdelhakim Baouya

Contents

1 Brief summary of the project

The current state of tools and methods for collaborative architectural decision-making mainly emphasizes knowledge sharing, reuse, compromises, and seeking consensus among diverse stakeholders. However, our observation reveals a significant oversight in considering the decision-making constraints of various stakeholders in relation to human factors during the development process. For example, when dealing with the design of secure systems, it becomes essential to thoroughly comprehend the benefits and limitations of potential solutions like cryptography, authentication, access control, auditing, and more. The project aims to develop a *formal* modeling framework that takes into account human factors in architectural decision-making, particularly those related to the expertise and experience of team members involved in collaborative decision-making processes. More broadly, this research will enhance our understanding of how collaborative decisions are made and provide better traceability of decisions impacting system security. Consequently, it will increase confidence in the decisions made by a diverse team of members.

2 Detailed general information

The proposed project leverages an existing collaboration between the project participants.

2.1 Project participants

Abdelhakim Baouya is an Associate Professor of Computer Science at the University of Toulouse Jean-Jaurès and a member of the IRIT-ARGOS team. His primary research interests revolve around software language engineering for software and embedded systems. Notably, he specializes in software architectures with a particular emphasis on dependability, security, and AI.

Brahim HAMID is a professor in computer science at the University of Toulouse Jean-Jaurès and he is a member of the IRIT-ARGOS team. He got his Ph.D. degree in 2007 in the area of dependability in distributed computing systems from the University of Bordeaux (France). In addition, he has an M.Sc. in Theoretical Computer Science that provides him with a background on mathematical, logical and formal concepts. He has been an assistant professor (ATER) at ENSEIRB (Bordeaux, France) and a member of LaBRI (France). Then, he worked as a post-doc in the modeling group at the CEA-Saclay List (France). He was a visiting professor at Concordia University (August 2011), at the University of Florida (September 2014), and at the University of Vienna (April 2015). His main research topics are software language engineering at both the foundations and application levels, particularly for resource-constrained systems. He works on security, dependability, software architectures, formalization, validation, and verification, as well as supporting reconfiguration. Furthermore, he is an expert in model-driven development approaches both in research and teaching. The emphasis of his work lies on the development of tools to model and analyze secure and dependable software architecture of critical infrastructures such as railway and metrology systems.

2.2 Project timeline

The proposed project has a duration of 24 months, as depicted in Figure 1. The first two tasks (see Section 3.5) will be executed concurrently due to their inherent interdependence. The third task builds upon the stemming results obtained from the previous tasks. The information fusion provides a comprehensive approach towards automating the decision-making workflow.

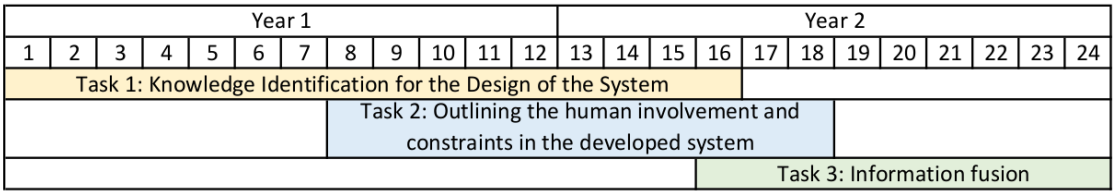

Figure 1: Project timeline.

3 Full description of the project

3.1 Context and Motivation

Successful product development relies heavily on the quality of continuous decision-making. Two primary factors significantly influence each decision. Firstly, the availability and reliability of system-relevant information play a crucial role. Throughout the development process, information about various aspects of the system evolves continuously, necessitating ongoing decision-making. The methods employed in this process are of paramount importance as they generate and refine system-related information. This raises a critical question: to what extent is information available and reliable at different stages, enabling accurate decision-making? Secondly, the individuals involved in the decision-making process, with their unique characteristics such as experience, emotional state, and knowledge, hold significant importance in shaping the outcome of the decision. Their expertise and perspectives contribute to the overall success of the decision-making process.

3.2 State-of-the-art

Numerous studies have been conducted to propose and develop models and methodologies for decision-making that heavily rely on human factors. In [1], authors present an overarching model that encompasses human and organizational factors crucial for developing safe and secure robotic systems. Through qualitative interviews with experts, the Prevent Model is derived, consisting of 17 individual factors and 13 organizational factors. The model serves as a roadmap for practitioners to implement tailored measures, focusing on personnel development programs, organizational structures, working environments, and other key aspects. The work done by [2] introduces a framework for (re)designing industrial work systems in the context of Industry 4.0, addressing socio-technical challenges and enhancing system performance and human well-being. The framework integrates human factors, ergonomics, work system modeling, and strategy design and has been validated through a collaborative workshop in an industrial setting. The research work in [3] focuses on designing and developing a practical solution called Sophos-MS, which integrates augmented reality, intelligent tutoring systems, and cutting-edge fruition technologies to support human operators in complex man-machine interactions within the Industry 4.0 paradigm. The proposed solution, based on a reference methodological framework for the smart operator concept, fulfills functional and non-functional requirements through a structured design strategy, resulting in a multi-layered modular solution. The research in [4] presents a comprehensive review of studies on the disaster resilience modeling of critical infrastructure systems (CISs) from a socio-technical systems perspective. The review identifies and classifies key human factors influencing CISs resilience, highlighting overlooked social aspects. The study also identifies knowledge and technical gaps, offering insights for possible solutions and future research directions. Application is made available in work in [5] where authors introduce a high-level architecture (HLA) based framework for co-simulating critical infrastructure systems (CISs) and human performance models to analyze dynamic human-system interactions. The framework demonstrates its efficacy through a case study, showcasing its ability to simulate complex feedback loops between

operator performance and system states. The proposed framework is valuable for CISs managers in identifying human-related failure points and making informed decisions to enhance system resilience. In the case of automotive systems manufacturing, the paper [6] reviews and analyzes existing research on human-machine interaction in the context of connected vehicles, focusing on messages conveyed through cooperative systems. It explores driver distraction levels, visual warning modalities, dimensions, and appropriate in-vehicle locations. These features are used to build an assisted driving system. For automation purposes, the research in [7] presents an experimental evaluation of human-machine cooperation on the decision level, focusing on cooperative decision-making situations. It introduces a novel experimental design that challenges conventional leader-follower approaches and compares them with automation designs based on cooperative decision-making models by relying on game theory. The results indicate the added value of the proposed automation designs in terms of objective cooperative performance, human trust, and satisfaction, emphasizing the benefit of designing machines as equal cooperation partners in line with models of emancipated human-machine cooperation. A similar approach to our proposed approach has been proposed by [8], where they introduced a meta-model for decision-making constraints, and a runtime enforcement tool called CoCoADvISE. However, the experimental tool focuses more on the human-centric aspect of proposing constraints for decision-making. Additionally, the absence of a system meta-model expands the scope of our research.

IEEE has developed two standards. The first document [9] provides guidance to diverse stakeholders engaged in nuclear facility design, including designers, applicants, licensees, architects/engineers, and regulators. The primary objective of this guidance is to establish a reasonable level of confidence in the safe and effective operation of a system by personnel, as validated by the validation team. The second document [10]outlines recommended practices for engineering personnel to develop integrated programs that apply human factors engineering to the design, operation, and maintenance of nuclear power facilities. The research work aims to automate system design, particularly in the design field, by integrating human factors into the decision-making process. However, there remain unanswered questions about the significance of human factors in ensuring the reliability of system design.

3.3 Problem statement

Throughout the lifecycle of a system, engineers encounter numerous decision-making scenarios. Given the complexity and substantial uncertainties surrounding the system and its environment, it is natural for engineers to have concerns about the quality of their decisions and the resulting consequences. However, it is common for many decisions to be made with limited and incomplete information. This can be attributed to various factors, including the unavailability or unreliability of information, as well as time constraints that hinder exhaustive data gathering and human knowledge acquisition. Consequently, the concept of belief becomes relevant when knowledge is incomplete, prompting a need to question the justification behind decisions. This is a common challenge faced in various decision-making scenarios. *In the realm of technical development, it becomes crucial to establish a clear understanding of what is known about the system, as it directly influences the role of human factors*. As depicted in the provided Figure 2, the level of knowledge about a technical system directly correlates with the extent to which belief factors into decision-making, thereby introducing an element of uncertainty.

3.4 Objectives of the research project

The objectives of this work are clearly outlined along three axes, which will serve as the projected dimensions. The first objective primarily revolves around acquiring a comprehensive understanding of the system to be designed and identifying its intended functionalities. The second objective focuses on gathering the expertise of the individuals involved in validating the system. Lastly, the third objective involves defining the structure of both knowledge and expertise to facilitate their assimilation and automation processes.

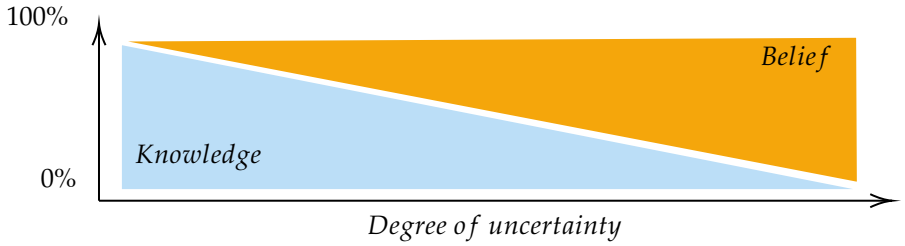

Figure 2: Relation of knowledge and belief for decision-making [11].

3.5 Scientific program and milestones

Achieving the project objectives will involve the following research activities and tasks:

Task 1: Identify the knowledge about the system to be designed. The primary task of the project is to identify the meta-structure of the system that the developers will construct, as well as to gather knowledge about attacks, threats, and countermeasures. This objective will be accomplished by creating a metamodel that facilitates building multiple system instances, along with the ability to model various attacks and defense measures. The system will be designed using the component-port-connector formalism, ensuring a comprehensive and robust architecture.

Task 2: Outlining the human involvement and constraints in the developed system. This task centers around the expertise of the developers or specialized individuals engaged in the development of the project. Each person brings their own distinct knowledge and perspectives to the table when it comes to constructing the system, mitigating potential threats in the form of *constraints*, and ensuring its robustness against performance and attacks. It is essential to *formally* model the realm of individual expertise to enable mathematical reasoning and evaluate the efficiency of each person's contributions in terms of the overall quality of the final project.

Task 3: Information fusion. This task encompasses the understanding of the meta-structure of the system to be realized, in addition to the knowledge of the individuals involved in the project's development. This process, referred to as *information fusion*, involves the integration of the knowledge pertaining to the system's construction and the expertise of the individuals. The resulting *formal composition* is then subjected to mathematical analysis to evaluate the quality of the generated system, serving as a criterion for *final system validation*. Learning approaches are also expected to evolve and develop models that effectively understand and incorporate human capabilities for refining decisions, addressing unexpected situations, and mitigating biases in the decision-making process that may arise from human beliefs.

3.6 Expected outcome

The expected outcomes encompass three dimensions: scientific, pedagogical, and industrial, as illustrated in Figure 3.

Scientific. The work resulting from this project will enable a significant advance in the state-of-the-art in tools and methods for achieving security-by-design and security assurance for critical software-dependent systems. Among other benefits, these methods and approaches will make it far more practical to address security concerns at the early stages of system development. This will provide substantial savings in terms of the costs associated with minimizing security vulnerabilities.

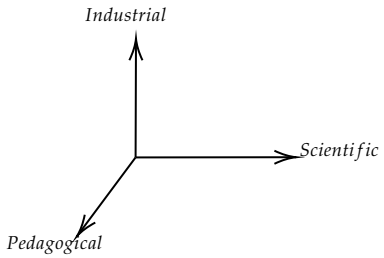

Figure 3: Project outcomes.

Pedagogical. The participants will integrate the findings into their ongoing teaching activities, which revolve around system engineering and validation for Master's Students at their respective universities. These results will be applied to enhance the educational experience and ensure the students gain a comprehensive understanding of the subject matter. Furthermore, there is a prospect for the outcomes to be embraced by external organizations and diverse audiences, extending the reach and impact of the research.

Industrial. The project aims to empower practitioners, including system designers, architects, and developers, by creating more accessible methods and tools. These resources will enable them to gain a deeper understanding of implicit interactions and offer support in evaluating and enhancing system designs during the early stages of development. As the project progresses, we will actively engage with our industrial partners who are involved in other collaborative initiatives. This collaboration will focus on validating the scientific outcomes through adoption and real-world use cases.

International. The proposed project involves an international collaboration with researchers in France and in Canada.

References

[1] C. Glasauer, "The prevent-model: Human and organizational factors fostering engineering of safe and secure robotic systems," *Journal of Systems and Software*, vol. 195, p. 111548, 2023.

[2] B. A. Kadir and O. Broberg, "Human-centered design of work systems in the transition to industry 4.0," *Applied Ergonomics*, vol. 92, p. 103334, 2021.

[3] F. Longo, L. Nicoletti, and A. Padovano, "Smart operators in industry 4.0: A human-centered approach to enhance operators' capabilities and competencies within the new smart factory context," *Computers & Industrial Engineering*, vol. 113, pp. 144–159, 2017.

[4] J. J. Magoua and N. Li, "The human factor in the disaster resilience modeling of critical infrastructure systems," *Reliability Engineering & System Safety*, vol. 232, p. 109073, 2023.

[5] J. J. Magoua, F. Wang, N. Li, and D. Fang, "Incorporating the human factor in modeling the operational resilience of interdependent infrastructure systems," *Automation in Construction*, vol. 149, p. 104789, 2023.

[6] C. Olaverri-Monreal and T. Jizba, "Human factors in the design of human–machine interaction: An overview emphasizing v2x communication," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 4, pp. 302–313, 2016.

[7] S. Rothfuß, M. Wörner, J. Inga, A. Kiesel, and S. Hohmann, "Human–machine cooperative decision making outperforms individualism and autonomy," *IEEE Transactions on Human-Machine Systems*, vol. 53, no. 4, pp. 761–770, 2023.

[8] P. Gaubatz, I. Lytra, and U. Zdun, "Automatic enforcement of constraints in real-time collaborative architectural decision making," *Journal of Systems and Software*, vol. 103, pp. 128–149, 2015.

[9] IEEE, "IEEE guide for human factors engineering for the validation of system designs and integrated systems operations at nuclear facilities," *IEEE Std 2411-2021*, pp. 1–38, 2022.

[10] IEEE, "IEEE recommended practice for the application of human factors engineering to systems, equipment, and facilities of nuclear power generating stations and other nuclear facilities," *IEEE 1023-2020 (Revision of IEEE Std 1023-2004)*, pp. 1–42, 2021.

[11] H. Hick, H.-F. Angel, P. Kranabitl, and J. Wagner-Skacel, *Decision-Making and the Influence of the Human Factor*, pp. 355–380. Cham: Springer International Publishing, 2021.

4 Detailed budget

We are requesting 15 000 euros to cover the following points:

- Conferences & workshops: 5000 euros
- Travel expenses between Canada and France: 3000 euros
- Research visit to IRIT for Concordia University Professors (1 month per year): 2*3500 euros