ICO Research Project : Project Review

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 designing secure systems, it is essential to thoroughly comprehend the benefits and limitations of potential solutions, such as cryptography, authentication, access control, auditing, and others. 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 builds upon an existing collaboration among 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 postdoctoral researcher in the modeling group at CEA-Saclay (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 review

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

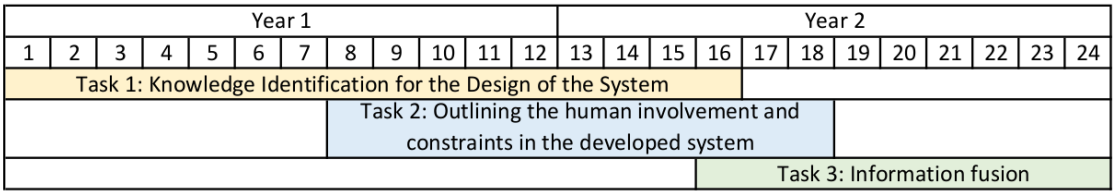

Figure 1: Project timeline.

3 Project review

Task 1: Identify the knowledge about the system to be designed. Our first step was to define the project's scope and the knowledge required for the system's design. We used the Global Positioning System (GPS) as a core use case to identify the specific system to be analyzed and the data to be collected. We then gathered all relevant information on the design of satellite systems and their orbital mechanics. The analysis modeled different system failures and external factors that negatively affect system performance.

Task 2: Outlining the human involvement and constraints in the developed system. Based on the use case, we have identified two teams whose purpose is to maintain the satellite system. Each team has a distinct set of skills and tasks. The on-orbit team is responsible for maintaining redundant satellites in orbit, sending update commands in the event of attacks or command manipulation, and relocating or replacing satellites. The on-the-ground team is responsible for checking the availability of satellites on the ground, building new ones, and launching them into orbit.

Task 3: Information fusion. The project began by collecting the knowledge base of the individuals involved in satellite maintenance. This process integrated knowledge about the system's design with the expertise of the maintenance personnel. The resulting formal composition, represented as a concurrent stochastic game, is then analyzed using probabilistic model checking. This analysis aims to evaluate the quality of maintenance tasks, for instance, in the case of attacks, by gauging the priority of each team's involvement. The model treats the system as a game and the maintenance teams as players, which allows us to assess which team is best equipped to maintain the satellite. This provides a crucial basis for making key decisions regarding security and performance during deployment.

4 Project results

The project has resulted in two papers: a conference paper and a journal paper. The conference paper highlights the team's skills in maintenance, with a focus on security issues and satellite maintenance, encompassing both in-orbit and on-the-ground operations.

- A. Baouya, B. Hamid, O. A. Mohamed and S. Bensalem, "Model-Based Reliability, Availability, and Maintainability Analysis for Satellite Systems with Collaborative Maneuvers via Stochastic Games," 2024 50th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Paris, France, 2024, pp. 27-34, doi: 10.1109/SEAA64295.2024.00014.

The conference paper was extended to include more failures and satellite features for submission to the Journal of Systems and Software.

- A. Baouya, B. Hamid, O. A. Mohamed and S. Bensalem, "Model-based dependability and performance analysis for satellite systems with collaborative maintenance maneuvers via stochastic games," Journal of Systems and Software, vol. 112610, pp. 1-10, 2025.

5 Future works

The work has been extended to map the team's knowledge and skills to specific tasks within a modeling tool, and to integrate teams specialized in heightened security concerns. This expanded model will be used to analyze a variety of teams and tasks for a specific private use case. The approach for assessing this composition is based on probabilistic model checking and game theory, which allows us to synthesize an optimal strategy.

6 One-Year Extension (Extension d'un an)

We are prepared to consider a one-year extension to expand the current research scope, implement additional features that require validation and experimentation, and fully validate the project's long-term viability. A detailed budget for this period will be communicated as needed to support these new objectives.

This extension will allow our team to complete research goals that require a longer-term investment and bring the project to a comprehensive conclusion.