Security Management: An Opportunity for Adopting the MBSE Approach in Critical Complex System Designs

Author[1]

[1]Author Entity, Town, Country (author@email.address)

Keywords: MBSE; Security; Critical Systems

1 Introduction

Although modelling tools for specification and design in systems engineering have existed for several years, they are not yet widely exploited, particularly for the specification and design of complex critical systems. This is due to the fact that complex critical systems have their product process strongly constrained by the protection of the confidentiality of sensitive assets of the specification as the most critical requirement in the decision choices of the product design flows. This leads to a documentation-driven process compared to the modelling-driven process flow, due to a more controlled user access to confidential information. In addition, the capture of security requirements and their exploitation are poorly taken into account by model-based specification and design tools. This complicates the global and automatic assessment of the security requirements of the product system. However, the share of security requirements in the specification of these systems and their integration into the product life cycle and their evaluation in the validation phase is becoming increasingly significant. Their very late consideration may require a complete redesign.

Here we present a set of security services that not only allow these locks to be lifted, but also provide analysis and automatic production capabilities for security code, making the validation of security requirements more systematic and more secure in a process equipped with MBSE tools for the creation of critical complex systems. This presentation first presents a confidentiality management of models that keeps confidential the sensitive information of unique designs only to people who have the right to know. This presentation then proposes a capture of information from a risk analysis, and their exploitation for the production of security directives and automatic generation of integrity and confidentiality protection code.

2 Methods

The global flow of system design is presented in Figure 1.1. Figure 1.1 describes in blue the operational product development flow, and in red the service complements added to perform the validation of security requirements. These complements do not impact the existing process flow of the system design related to the validation of operational requirements.

This process enrichment with security services applies on MBSE tools the problem solution of multi-user management of a system engineering design model as described in (Bourdellès et all (2024)) applying Bell and Lapadulla's rules on models containing information of different confidentiality levels. The model information enriched with information for a given confidentiality level is stored in a specific enclave with access control to this enclave for people having a need to know. Figure 1.2 depicts this implementation.

This problem solved, the capture of system specification information in its modelling has to be tackled. For this the description of data flows by deployment information is extended, allowing to identify on the one hand the type of processing on the data carried out on the function and on the other hand the available platform services of integrity and confidentiality calculation capacity (encryption, hashing). We then use this information to verify that the system architecture choices meet the initial security requirements. This exploitation also makes it possible to automatically generate security code (hash calculation, encryption) allowing the security requirements to be validated on the product system. Figure 1.3 specifies this functional chain with the calculation of security directives and production of security code as a proxy completing the software code of the operational part.

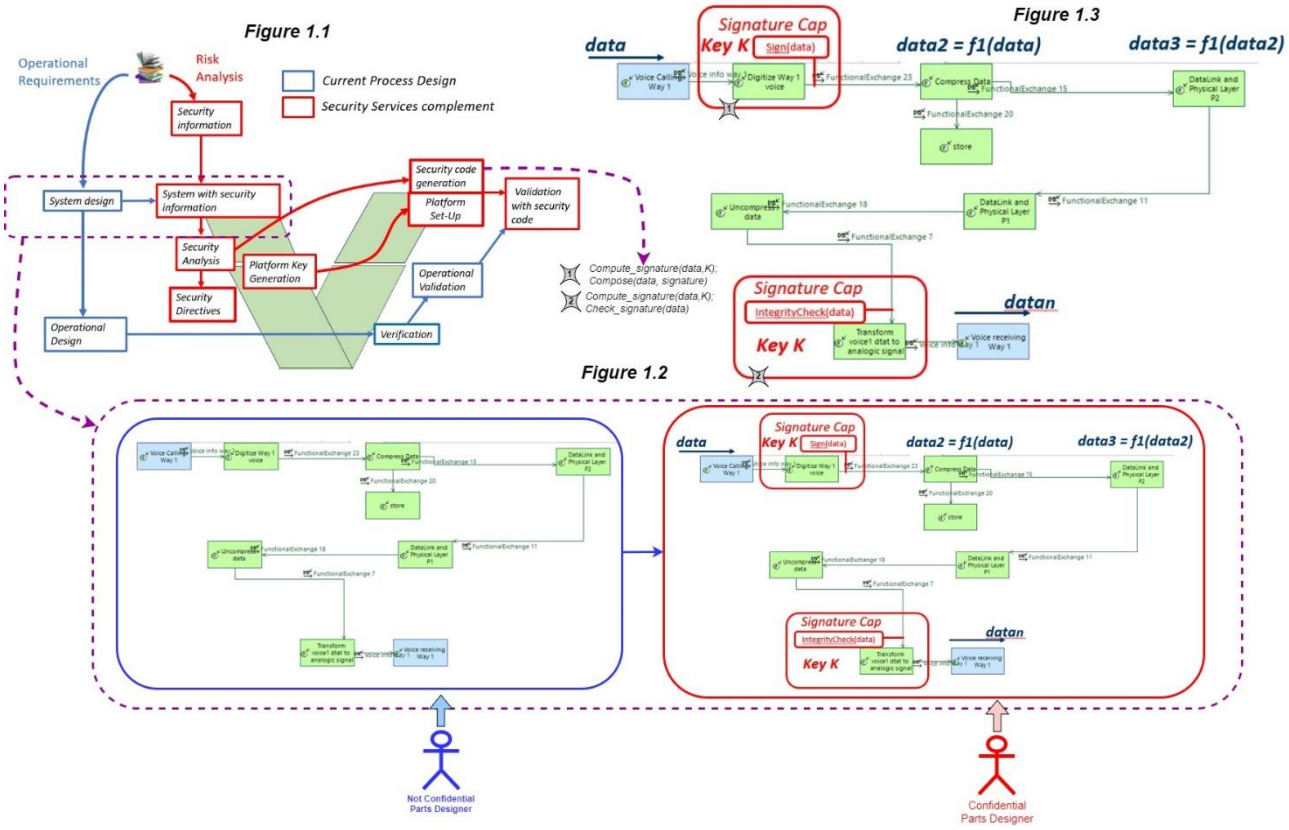

Figure 1: Figure caption

3 Results

The annotation of security information to be completed by a modelling by MBSE (here by the Capella tool) and their analysis has been implemented in a software tool and makes it possible to verify that the system architecture respects security requirements resulting from a risk analysis and produces security codes in integrity and confidentiality protection.

4 Discussion

The methodology described allows, in transparency of the process of realization of the operational part of the system to be produced, to integrate and automatically generate the code allowing the validation of the security requirements. This analysis and automatic generation of security code promotes the securing of these systems and facilitates the audit of the security controls to be carried out. The need for securing systems being increasingly important, the integration of these services exploiting system design modelling enriched with security information allows a better control of the validation of security requirements and can act as a powerful lever for the choice of MBSE-based processes for the design of critical systems.

References

Bourdellès, M., El-Hachem, J., Sadou, S. (2024). Confidentiality Management in Complex Systems Design. ICECCS 2024. Lecture Notes in Computer Science, vol 14784. Springer. https://doi.org/10.1007/978-3-031-66456-4_17