Confidentiality Management in Complex Systems Design

Michel Bourdellès, Jamal El Hachem, Salah Sadou

Confidentiality Management in Complex Systems Design

Michel Bourdellès
Université Bretagne Sud
F-56000 Vannes, France
michel.bourdelles@univ-ubs.fr

Jamal El Hachem
IRISA – UMR 6074 , Univ. Bretagne Sud
F-56000 Vannes, France
jamal.el-hachem@irisa.fr

Salah Sadou
IRISA – UMR 6074 , Univ. Bretagne Sud
F-56000 Vannes, France
salah.sadou@univ-ubs.fr

***Abstract*—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. To the best of our knowledge, neither current Model Based System Engineering (MBSE) tools, nor academic research propose solutions to this specific issue. In this paper, 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.**

***Index Terms*—Security of complex systems, System modelling, Product life cycle**

I. Introduction

System specification and design documents for sensitive projects often consist of two separate parts: confidential and non-confidential. Among confidential documents, there are security annexes which state the rules to correctly use the whole documents. Thus, identifying data classification levels becomes the first step an organization should consider when developing a data sensitivity program. Then, the organization should apply an access control on data with respect to the level of sensitivity. This corresponds to the "Information Flow Enforcement" access control in the SP800-53 report from the National Institute Standards and Technologies (NIST) [1].

Indeed, to be protected against system attacks, the design of these systems should include a prior security analysis. More precisely, a first security analysis consists in identifying critical assets, performing a risk assessment and taking decisions regarding the security controls to be applied. The latter information being sensitive and impacting the system design, it is important to propose solutions allowing, in a system modelling, to take this information into account and to restrict its access to only authorized persons.

Prospective analysis [2] foresee a greater use of modelling approaches for system design. This is known as Model-Based System Engineering (MBSE). These designs respect normed industrial processes such as ISO/IEC/IEEE 12207 and capture information from initially separate documents (Technical Requirements Specification, System/Subsystem Specification, System/Subsystem Design Description, Security Annexes, Product Breakdown Structure, Interface Control Document). Yet the confidentiality is ensured by a unique level of separation in sensitive documents. However, the information from security analysis documents impacts the overall design and is an integral part of its modelling. In case of sensitive systems, modeling involves adding mechanisms to manage different levels of confidentiality and authorization within the models. It is therefore necessary to extend all the design constraints based on an MBSE approach to introduce a management process considering the confidentiality and the access authorization rules.

Many recent works (UAF [3], SysMLSec [4], MBSEsec [5], Capella Cyber Security viewpoint [6], MBCA [7], SMSA [8], SoSSEC [9]) make it possible to integrate security elements into system modelling designs to secure requirements. However, those approaches, as well as their corresponding modelling tools (Cameo System Modeller, Modelio, Capella/Arcadia, and other SysML modelling tools) work with a "flat" view on the information, which means without managing the confidentiality protection need of specification parts design nor managing access in line with an authorization policy.

To the best of our knowledge, related works not or only partially cover these needs, in particular works based on Model Driven Development [10], [11], data obfuscation and filtering [12], enclave partitioning [13], works on database confidentiality management [14], [15] and [16], or industrial processes [17] do not, or only partially address the previously mentioned challenges.

Thus, in this paper we propose an approach, based on the security enclaves concept, to manage different levels of confidentiality in an MBSE process. This approach is built on top of several years of expertise in design in sensitive systems within a large company in the defense area.

The remainder of the paper is organized as follows: in the next section we provide an example illustrating the research problem of mixing elements of several confidentiality levels in MBSE modelling and an analysis of confidentiality man-

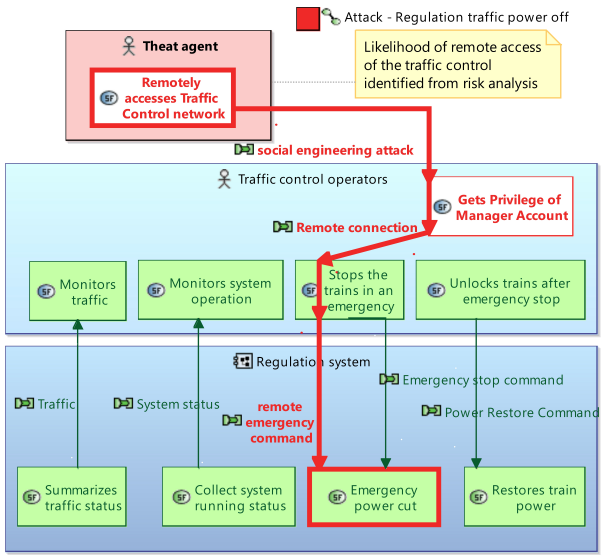

Fig. 1. System modelling design including a remote attack vulnerability identification.

agement choices done in the Galileo modelling system design. In section 3, we list a set of criteria derived from industrial experience in a sensitive domain, to which our approach comply. Section 4 details our approach. We show how our approach complies to the criteria in this section 5. We present the application of the proposed approach on the illustrative example in section 6, as well as its integration in current MBSE tools. Before concluding in section 9, a comparison with related work is given in section 7, and a discussion on the integration in MBSE tools in section 8.

II. Illustrative Example and Industrial Solutions Proposal

In this section, we illustrate the problem using a simple example. We then emphasize the limits of the solutions proposed on a complex industrial project, before presenting our approach in the rest of the paper.

A. Illustrative Example

In order to illustrate the problem and the need to distinguish the elements of an MBSE modelling according to the level of confidentiality and to allow a differentiated access in integrity, we present in Figure 1 a view of the design of a Level-Crossing Control System carried out with the Capella tool[1]. We are amending this design and adding a remote attack vulnerability identified on one of these design elements. This information is issued from a risk analysis and is considered as a sensitive security information.

Consequently, such information should only be accessible by a limited number of authorized users. Further, it should not be visible to the system engineers in charge of designing the operational part of the Level-Crossing Control System. In addition, to prevent this information from leaking, it should not be stored in the same memory space as the rest of the system design when it is defined. Moreover, designers in charge of modelling the risk analysis elements must not be able to modify the elements of the operational part.

Thereupon, our approach deals with the latter requirements among others. It aims to ensure the non-disclosure of confidential information from global system design models to unauthorized persons.

B. Proposed solutions in the Galileo Complex System

Morlet and all [17] present a feedback from the use of MBSE tools in the system design of the Galileo satellite navigation system. Among all the issues stated is this need for confidentiality management and protection. The two solutions proposed are to first completely validate a design for a given confidentiality level in order to carry out the system design at the higher confidentiality level. The solution proposed in a second step consists of working in parallel on all levels based on the unclassified reference model. A modification to a security level impacting this model is reported to it.

These two solutions have strong drawbacks. The first is the safest but does not allow agile, iterative and parallel operation according to the confidentiality levels of the system design. The second partially allows such operation, but allows working on the same model element at different design levels, and postpones modifications from a given confidentiality level to a lower confidentiality level, with a high risk of data disclosure sensitive.

The solution proposed in this paper aims to propose a solution as secure as the first solution, but offering iterative production capabilities in a collaborative environment specific to the needs of product development in a real industrial context.

More specifically contributions of this paper are as follow: **(1)** A design process for MBSE modelling with confidentiality inter-enclave management, **(2)** an implementation of this process based on read/write access to modelling elements carrying confidentiality and integrity information, **(3)** an application of the proposed approach on a case study, **(4)** a process allowing the integration of the solution in current MBSE tools, and a concrete integration in the Capella tool as a real proof of concept.

III. Assessment Criteria

As previously mentioned, according to our industrial experience in a sensitive area, regardless of the proposed approach to multi-level confidentiality management, the criteria below must be met. These criteria respond to the changing needs, according to the evolution of the risks of a major European industrial player in the defence and cybersecurity sector in designing its systems. As a former designer in that company, one of this paper's authors has managed these criteria for several years. The first three relate to security requirements, derived from security controls as defined in the NIST SP800-53 framework. The fourth criterion results from the control and

[1]https://www.eclipse.org/capella/getstarted.html(access September 2023)

handling of accountable information as indicated in the NATO note [18], the latter links a confidential data creation to the level of protection of the physical resource to be processed and stored. The fifth criterion concerns iterative and agile process flow application and the last one assesses the generalisation of the proposal to any kind of models.

- **Confidentiality, Consistency, Integrity assessment (AC1):** The solution should assess the access to authorized people with a strict access in reading and writing. The design at one given confidentiality level should be consistent. By consistency we mean in the one hand the complete design of the system related to requirements up to a confidentiality level, and in the other hand without inconsistencies between the models regardless their level of confidentiality of modelling design.
- **No leak assessment (AC2):** A model element being designed at a given confidentiality level can't be accessed from the lower confidentiality levels of system modelling design.
- **Storage confidentiality assessment (AC3):** A model element being set at a given confidentiality level can't be stored in the same memory space where lower confidentiality levels system modelling designs are stored.
- **No manual labelling assessment (AC4):** The user should work with modelling design tool without being worried on confidentiality labelling. The confidentiality level set of a model element is at the liability of the design process environment.
- **Iterative and adaptive assessment of process flow compliance (AC5):** The solution should be adaptable to any life cycle, with a separation of the specification, design, development, test and validation stages with respect to the confidentiality levels of the system.
- **Genericity of the solution assessment (AC6):** The solution should be generic according to the metamodels and models to which it is applied, and to their number of confidentiality levels.

These criteria are the result of extensive expertise in the construction of sensitive systems that have to withstand real attacks.

IV. A Design Process to Ensure Requirements Confidentiality During System Design Modelling

The approach we are proposing consists of a process aimed at satisfying these criteria. This approach ensures the management of a system design combining information from several levels of confidentiality at the design modelling stage.

A. Inter-Enclave Behavior Justification

The capture of attack scenarios such as the one presented in section 2 comes from a risk analysis. It is clearly stated in the ISO 31000:2018 [19] standard relating to risk management that the creation, storage and processing of documented information resulting from this analysis should take into account the sensitive nature of the information. It is therefore necessary to adapt the access to this information and its processing only

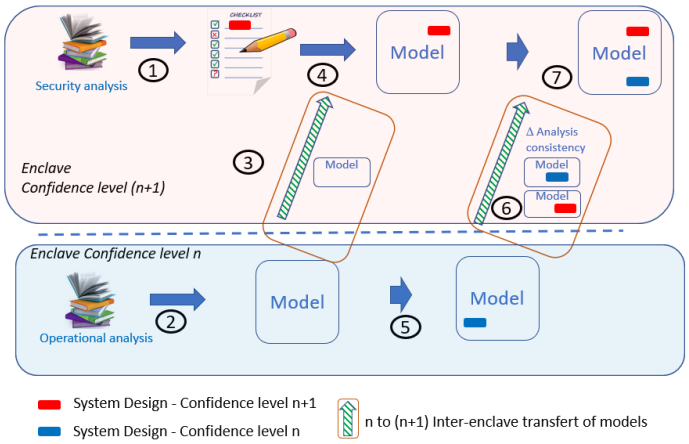

Fig. 2. Process including confidentiality management

to users identified as authorized to access it. This need of protection is even more significant when it comes to systems in the field of defense and whose information (e.g. encryption key, sensitive algorithms, information on the physical characteristics of the secret information transmission) comes under a level of confidentiality (secret, top secret, coalition defense secret) imposing clearance and strict rules regarding the access to information.

The application of this risk management therefore imposes a separation in terms of access and storage of the elements described in the form of requirements. These requirements are the entry documents of the system analysis, and propagate a need for differentiated management in access and storage of the result of the design of these requirements.

It is therefore essential, in the modelling approach used for the systems design considering a risk analysis, to offer the management capacity in separate enclaves for elements from different sensitivity. Although the elements are in different enclaves they still form the same system design.

The first task will take place at the upstream of the system design to properly classify the information on the input requirements provided to the various involved actors in the system design. Indeed, in the example of section 2, it is likely that the information on the potential system vulnerabilities should be hidden from the system engineers in charge of the operational design part. On the other hand, they will surely have information on the identification of the sensitive assets to be protected, as well as their life cycle (creation, storage, transmission and processing). This information is used to apply generic security controls as described in the NIST 800-53 standard [1].

B. The Proposed Design Process

This classification of requirements related to their level of confidentiality supposes that the system design is carried out in parallel on separate parts handled by different people. In the long term these parts compose a global design verifying all the input requirements of the system design. We will therefore have an operating mode such as described in Figure 2, with

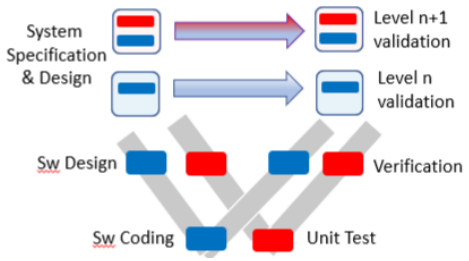

Fig. 3. Validation with multi-levels of confidentiality

the following steps:
(1) At the end of the risk analysis, we include an identification of the elements to be injected into the modelling for the system design and their level of confidentiality. These elements are listed to be traced in their injection into a design by MBSE. **(2)** The system analysis excluding security analysis is carried out in the enclave of lower level of confidentiality, with capture of the design by MBSE. **(3)** This model with level n of confidentiality is transferred to the n+1 confidence level enclave. **(4)** Security analysis information (e.g. an attack scenario or the sensitivity level of a system asset) is integrated into the model. Elements of confidence level n can't be modified. **(5)** In an iterative behavior, the confidentiality level n enclave model evolves. **(6)** This model is transmitted to the level n+1 enclave in the same way as in step 3. It is possible to identify by comparison the delta between these two models and the impact of the injection of level information confidentiality (n+1). **(7)** In the same way as in step 4, this model can be completed with confidentiality level information (n+1).

In this management, it is not mandatory to give people authorized to write in the confidence level enclave (n+1), to have this right in the confidence level n enclave.

This iterative process applies the no read-up and no write down Bell-Lapadula rules [21]. It forbids storage in an enclave of information of higher confidentiality level. It also provides a strong write integrity rule of limiting write capability in the exact enclave of confidence level of the model element.

C. Inter-Enclave Designs Inconsistency Mitigation

Note that between 2 iterations of design model feedback (step 6), from confidentiality level n, it is necessary to integrate again and adapt the design information of confidentiality level n+1. This implies a potential redesign work which can be quite expensive. This can also lead to choices that do not allow satisfactory consideration of security requirements.

This situation can however be strongly attenuated by a coarse grain structure of the design model with the prior definition of the interfaces making it possible to work on fixed architectural elements. In addition, the system engineers have part of the design security information, which makes it possible to direct the design towards choices that facilitate the integration of elements resulting from higher level confidentiality requirements. However, the need to modify the lower privacy level design cannot be ruled out.

A restrictive industrial process involving security and product managers must then be provided for adapting the input requirements of this design to the next iteration, without disclosing higher confidentiality level requirement information.

D. Validation of Systems with Multi-Levels of Confidentiality

The purpose of validation is to demonstrate that a product or product component fulfills its intended use when placed in its intended environment. In the previous example of Level-Crossing Control System, we might wanted to mitigate the remote threat identification by the addition of a specific endpoint detection and response (EDR) proxy, which will be described in the physical refinement view of the system view presented in Figure 1.

In enclave of confidence level n, the requirements related to this design will be validated. In enclave of confidence level n+1, the validation of specific requirements, as the test of mitigation procedures assessment related to remote attack in the example, should be done.

As shown in Figure 3, this may be considered as a particular integration test suite mixing elements of level of confidentiality at most n+1.

E. Impact on Modelling

Subsection 4.1 justifies the global process based on enclave partitioning. We express here its refinement at modelling level to ensure confidentiality, consistency and integrity. The solution is applied on cases of potential confidential elements in MBSE, reported in Table 1.

We state here our proposal of constraints for multi-enclave management of MBSE designs. Metamodels and models used

TABLE I
CONFIDENTIAL INFORMATION IN SYSTEM MODELLING DESIGNS

	Confidential information	Example
1.	Metamodel element	Part of the metamodel describing the capture of instances of the risk analysis part, or certain parts such as the list of encryption algorithms offered.
2.	Instances of metamodel element	Instance of this metamodel describing an attack scenario.
3.	Attribute	The annotation following the risk analysis as an asset to be secured of a model element
4.	Information broadcast by metamodel transformation	Application in the Capella metamodel of confidential information report actions between operational, system, logical and physical views as proposed in the ARCADIA methodology [20].
5.	Element inconsistent with deletion of confidential elements	A proxy that is only traversed by higher confidential information. Maintaining this element can be considered as a disclosure of confidential information.

in a given enclave carry information confidentiality by read-only or read/write access. Any metamodel and model element from lower level enclave is **read-only**. All element created within an enclave has **read and write access** in that enclave. Access Enclave Elements in reading and writing and potential relations towards the elements of models and metamodels from enclaves of the level of less privacy **are stored in the current enclave**.

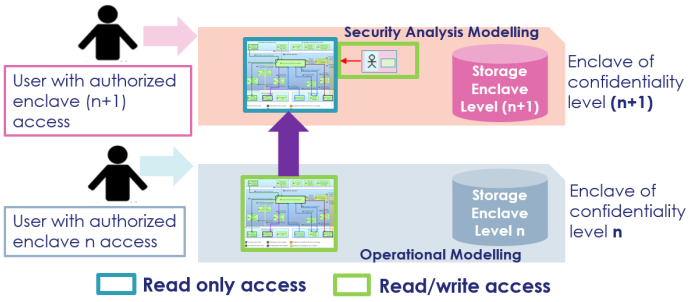

Fig. 4. User data access of multi layered modeling designs.

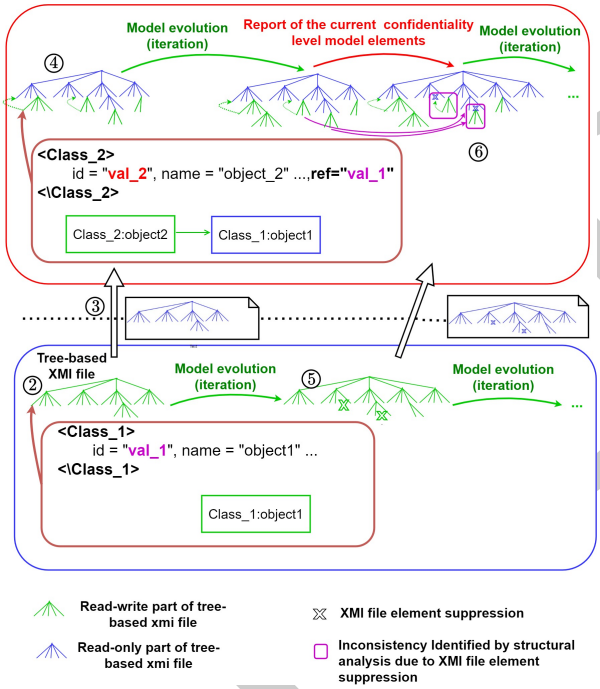

Fig. 5. Figure 2 steps impact at modelling level

Figure 4 presents the application of the proposed solution on the example from section 2. Access to the enclaves will be done with a secure access policy of the Mandatory Access Control (MAC) type, and restrictions conforming to the role of the users.

F. Modifying the Model Between Iterations

In this section we provide the elements allowing a transfer of design model information to be carried out when receiving a new model of the enclave with a lower sensitivity level. The underlying model for these models is an XMI file which has a tree structure and cannot be modified in higher sensitivity level enclaves. The design complements therefore appear in the XMI file at the extremity of the trees. Frequently, capturing relationships between model elements results in memorizing identifiers of other elements. Each element is stored in an XMI tag and has an attribute carrying a unique identifier distinguishing it from other elements. Linking two elements means either containing in this element description attributes memorizing the identifiers of other elements, or including the beacon of one element inner another element, as defined in the tree-based structure of these files.

Figure 5 presents the impacts of the models in their representation in the form of XMI files in their use in the process described in Figure 2. The steps ② and ⑤ report the evolutions of the model in the lowest confidentiality enclave. Each node of the tree structure corresponds to an XML beacon.

A copy of the elements between two models received will consist of ensuring the presence of the leaf nodes on which the design elements have been added, as well as the referenced beacons.

At one iteration of the model, it is transmitted to the higher level ③ which completes it ④ and enriched with superior confidentiality elements without modifying the model received.

In the next iteration, the model evolved with the addition and removal of ⑤ elements. If the deleted elements are not elements in which elements to be integrated from the higher level enclave, or referenced elements, are nested, then the extension is carried out without difficulty with a guarantee of respect for the grammar of the model. Otherwise, it is easy to identify situations of loss of consistency ⑥. Either the higher level privacy model is modified to allow the extension, or a process under the responsibility of security managers is applied to modify the lower level model.

V. Evaluation of the Proposed Solution

To evaluate the proposed solution, we analyse its compliance to the verification criteria defined in section 3. Table 2 presents the results on rules corresponding to criteria refinements.

For each rule, explanatory elements are provided and prove this compliance. The proposed design process, integrating modeling system design tools, covers all the needs expressed.

The proposed process processes and stores data at a confidentiality level in a dedicated enclave accessible only to people authorized to access. This data can only be transmitted to enclaves with higher confidentiality levels. Confidentiality protection is well assured.

Maintaining consistency is also well integrated and illustrated in Figure 5, which allows validation of the system for a given level of confidentiality.

Integrity is also guaranteed because the modification of an element for a given confidentiality level is only possible in the enclave allocated to this confidentiality level. Users of the

TABLE II
ASSESSMENT CRITERIA VERIFICATION

	Rule assessment	Verification
AC1.R1.	Confidentiality	Each element can be annotated with the level of that of the enclave in which it was added, but it is not mandatory with access read-only privacy level items inferior. Implicitly writable elements of the enclave are of the enclave level of confidentiality, the others are of a lower level.
AC1.R2.	Consistency	Lower enclave-level consistency and higher level model elements addition consistency guarantee the consistency of the model at any level of confidentiality.
AC1.R3.	Integrity	Enclave access control and read-only protection of level-n model elements reported at level (n+1) guarantee the integrity criterion assessment.
AC2.R1.	No leak to lower level	It is not possible to add elements with a level of confidentiality higher than that of the enclave.
AC2.R2	No miss from lower level	Steps 3 and 6 in Figure 2 reflect the provision of the level n models in the level enclaves confidentiality (n+1).
AC3.R1	Storage confidentiality	In Figure 4, we see that at each enclave can only be stored elements up to the compliance level of the enclave.
AC4.R1	No labelling error	By construction, any added element is of level of privacy of the enclave.
AC5.R1	Iterative process flow	The process presented in Figure 2 provides such iterative steps.
AC5.R2	Multi-levels modification impacts	A comparison between 2 iterations of n-level enclave models helps to identify differences.
AC5.R3	Dynamic metamodel modifications impacts	As the level enclave metamodel (n+1) includes the level n enclave metamodel, it can be modified dynamically independently of the treatments lower enclave level. On the other hand, it will be necessary to postpone these metamodel changes to the level enclaves of superior confidentiality.
AC5.R4	Validation at a given confidentiality level	The confidentiality level of each system element is defined, and the system is consistent for each confidentiality level. We deduce the validation of the system at a given confidentiality level.
AC6.R1	Genericity	The solution is applicable to multi layers designs independent to the models.
AC6.R2	Multi-layer management	The solution is applicable to multi layers designs, with no prerequisites to the number of layers.

template at a higher privacy level have read-only access to this item.

The description of the impacts on the product development process is presented in Figure 2 and refined in Figure 5 to describe the impacts in terms of manipulation of system design models. Figure 3 shows the variation in the other stages of the life cycle, allowing confidentiality protection at each of them. The iterative process applies to any life cycle, notably allowing its application in agile processes [22]. This process also offers a sharing of design work according to the confidentiality levels of the product to be produced. This sharing makes it possible to work in parallel on these different enclaves.

We have not made any presuppositions about the metamodels and models on which the process applies. The proposed solution does not require annotating the elements of specific security information models and metamodels. Our proposed approach is therefore generic and applies to any metamodel for which the identification of the level of confidentiality has not been carried out beforehand, this can be carried out in the upstream phase for the production of a product by those responsible. of security. For the same metamodel used, this choice of division into confidentiality levels may vary depending on the project.

In the following section we show how to represent in a hierarchical form a model described on a single level and mixing information from different confidentiality levels. We then discuss in section 8 how the additional capabilities necessary for this hierarchical representation are already present in modeling tools offering multi-user functionality.

VI. APPLICATION ON THE MBCA METAMODEL

We rely on the metamodel elements described in a very recent existing work on the integration of cybersecurity risk assessment into requirement engineering [7] to illustrate the application of the approach. These elements are reported in Figure 5. In blue we present classes of the metamodel describing the operational features, and in white the classes added to specify features related to security management. We extracted from the metamodel description the part dedicated to capture scenario description information. These scenarios can be either operational scenarios or scenarios describing feared events. These elements are highlighted in purple in the initial MBCA metamodel.

Conforming to the proposed process, we will therefore consider that the part of the metamodel describing the operational scenarios of a confidentiality level n, and the part of the metamodel describing the scenarios of feared events with a level of confidentiality (n+1). We deduce in Figure 6 the corresponding metamodel parts and an instance example of it for the enclaves of privacy level n and (n+1) for the purple part of the initial metamodel presented in Figure 5.

In accordance with the principle set out in subsection 4.5, the elements of confidentiality level n are read/write accessible in the privacy level n enclave and are accessible read-only in privacy level enclave (n+1). The confidentiality level elements

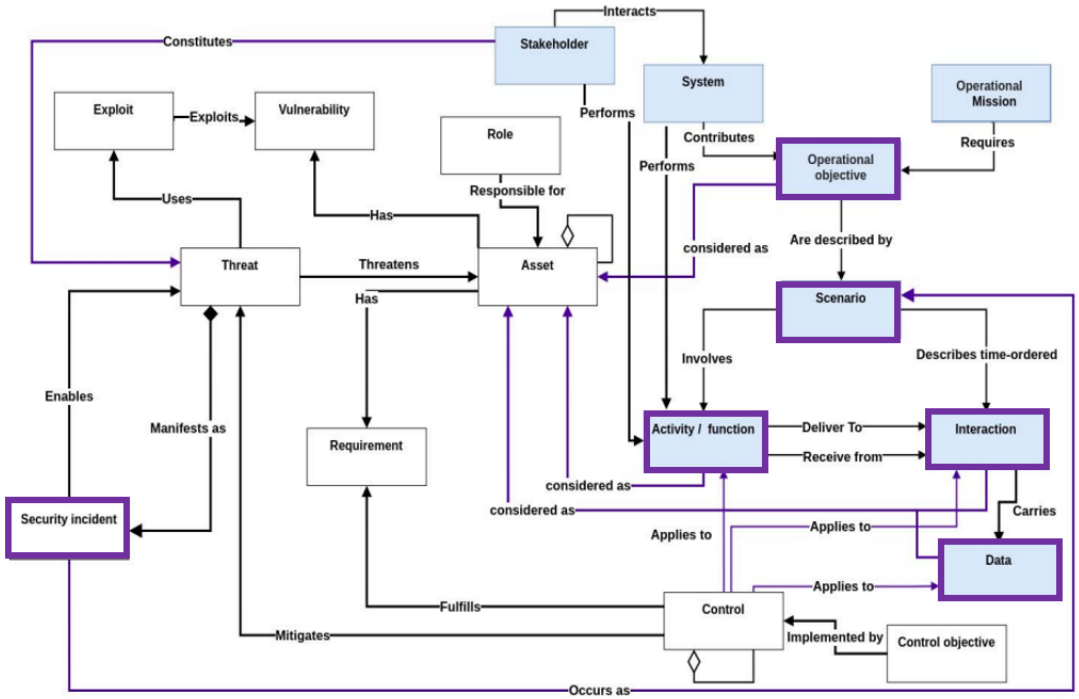

Fig. 6. "Flat" view of the MBCA metamodel from [7]

(n+1) are accessible in read and write in the level enclave of confidentiality (n+1), and are not present in the enclave of confidentiality level n.

VII. Related work

Recent work deals with the capture of security information ([3], [4], [5], [6], [7], [8], [9]) in models. However the multi-level confidentiality of the model is not addressed in these works. The specific problem of managing the confidentiality of information in multi-level confidentiality models is therefore new and, to the best of our knowledge, there are no proposals that specifically address the problem explained in section 3.

Therefore, we analyze different approaches for managing confidentiality or existing masking and see to what extent it is possible to adapt them. We are guided in this by constraints such as those defined by state bodies, for example French Inter-ministerial General Instruction No. 1300 [23] on the protection of national defense secrets.

In a different modelling descriptions as the security models already mentioned, an overview of Model-Driven Developments [10] list several proposals with particularly rich security information stored and processed. But they do not apprehend access right and storage constraints issues of specific modelling elements. It is also the case of Hu et all model [11], which proposes a UML security model but with no separation in enclaves.

As indicated in [12], obfuscation is known as being a good data confidentiality protection. In our case, obfuscation does not obfuscate elements of the metamodel, which may be necessary. Moreover, obfuscation keeps the structure of the model, which can already be considered as a disclosure of confidential information.

Filtering tools would allow confidential elements to be hidden. However, it will be necessary to ensure that the filtering information is not present in the underlying formats of the filtered model displayed. It will also be necessary to ensure a distinct memory storage of the models of different level of confidentiality for their modification in writing. Finally, it is necessary to ensure that the data of a given level of confidentiality resulting from a security analysis is considered, which may be different from the instances of a predefined set of classes of the metamodel.

Johnson and Stevens [13] propose a model confidentiality management between two companies with a common part and specific confidential parts managed either by a two-way transformation relationship, or with specific access to certain parts of the model. There is not in their work a conformity of confidentiality order relationship present in the management of enclaves respecting the rules defined by Bell and Lapadula.

We present in the following security management on databases with similarities with the current work. Denning, Lunt, and all [14] annotated database table entries with items of privacy levels, and views restricted to those levels by anonymization. Their work of defining a multi-level relational data model (MDB) focuses on the impact of these anonymizations in the inter-table inference rules and maintaining consistency with anonymized inputs. These works differ because they are not based on a description of metamodels and consistency rules that benefit MBSE-type solutions, and do not address multi-enclave storage. The modification of access

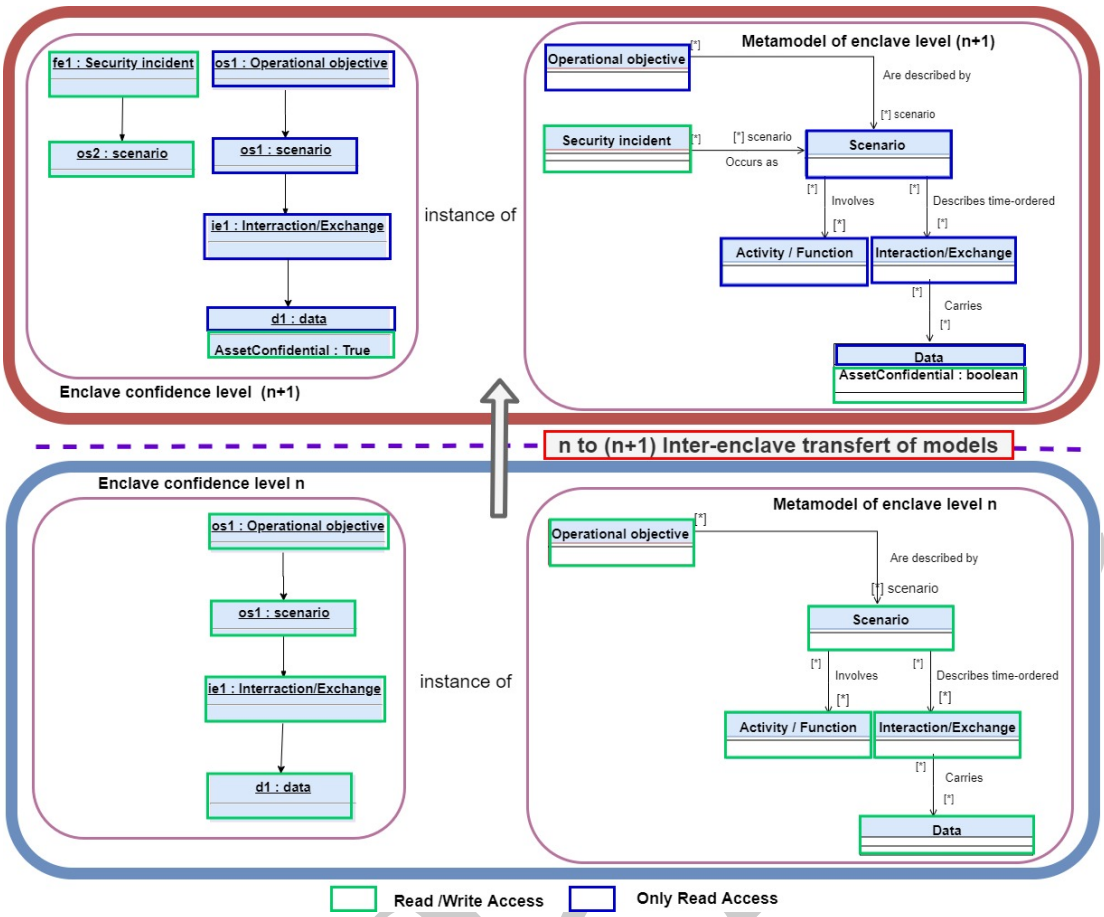

Fig. 7. Hierarchic view of the purple metamodel part of Figure 6, and of a system design instance

to data according to the level of confidentiality authorized for access has been studied mainly on databases and characterized under the term polyinstantiation. Among these works, [15] analyzes the management of the same database with different levels of confidentiality. In their proposal, the access management with respect of integrity respects the rules of Bell-Lapadula, but with the level of confidentiality carried by the database and not by the storage enclave. These works differ also by information duplication.

Brodsky and all [16] propose to process queries with respect to confidentiality to a database via a Disclosure Inference Engine (DIE). In this proposal the level of confidentiality of the information is explicit by annotation, there is no mention of the modification of this data, nor of the storage in enclaves of different level of confidentiality.

VIII. Discussion

A. Application by Current Modelling Tools

We have presented in section 4 an approach allowing to process models with elements of several levels of confidentiality, ensuring confidentiality of access and storage. This solution applies to any model managing information with a plurality of confidentiality levels. This was barely addressed by the previous work described in section 7.

The application of this solution requires on the one hand the possibility to determine the read-only or read/write access of elements of models and metamodels, and on the other hand the ability to compare two models. These functionalities exist in several modelling tools for systems design. In particular to allow multi-user use which obliges to make accessible only in read-only mode (locker) the elements being modified by a stakeholder. Thus well known tools such as EMFStore [24], ModelCSV [25], Modelio Constellation [26], or even Team for Capella [27] offer such multi-user capabilities.

Let us take the example of Capella. Capella is an open-source MBSE modelling tool and a graphical editor provided with an appropriate engineering method called “Architecture Analysis Design Integrated Approach” (ARCADIA). Capella and ARCADIA are designed by THALES, a European leader in cybersecurity.

Capella offers a multi-user capability called Team4Capella. In this capacity, users must authenticate before accessing the model. An item that is modified by one user is not writable by other users until that modification is complete. The Capella tool also allows you to add additional design capabilities that are included in the form of plugins called viewpoints. These viewpoints are extensions of the basic meta-model in order to enrich the model. Among these viewpoints a security

viewpoint, called DARC, notably makes it possible to qualify the assets in terms of level and type of vulnerability, as well as the addition of attack scenarios.

To ensure access to model elements only to authorized persons with guaranteed respect for read/write or read-only rights, and in accordance with the proposed approach we define two memory enclaves. In one of these enclaves, in charge of the system design of the operational part of the application, we do not integrate the DARC viewpoint.

At a given deadline, this model is transferred to the other enclave, via its xmi description file. In this enclave the DARC viewpoint is added to the basic Capella metamodel.

This approach is illustrated in Figure 7, on the crowd surveillance drone case study provided for download with the DARC view point. To allow the reproducibility and replicability of the proposed solution, Team4Capella and DARC are available for download.[2]

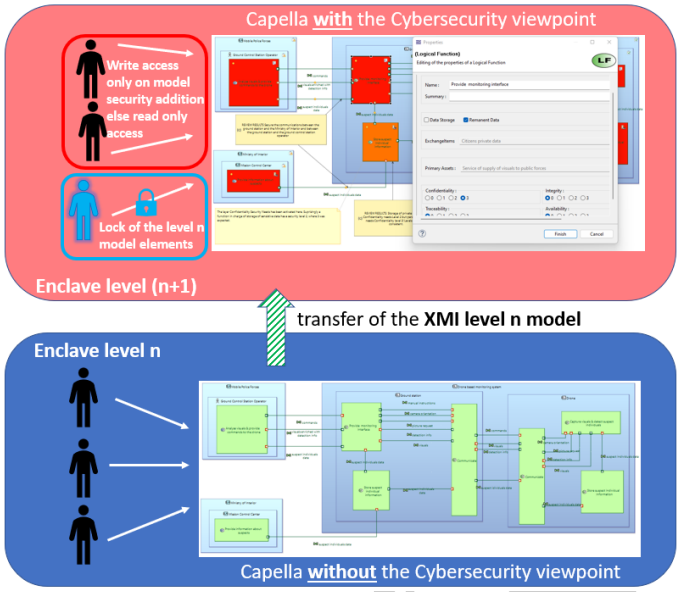

Fig. 8. Integration proposal in Capella

B. Security Analysis Based on the Proposed Confidentiality Management

In this paper, we presented a tooled process allowing the design of systems with information confidentiality protection. This work constitutes a first step in the more global tooling of the product development process to ensure the security of systems.

We describe in Figure 9 this process as part of a more global integration of information elements, processing, production of artifacts in order to improve the product development process to produce equipment from more secure complex systems.

With this in mind, we are now working on a characterization of the information to be injected into a system design. We choose this information so that it is available during the specification phase, therefore by exploiting information from a risk analysis.

At the end of the design phase, in the enclave of confidentiality level allowing us to benefit from all the information, we work on a security analysis in order to allow on the one hand the production of security directives and on the other hand the production of security code for its use in the validation phase of operational and security requirements.

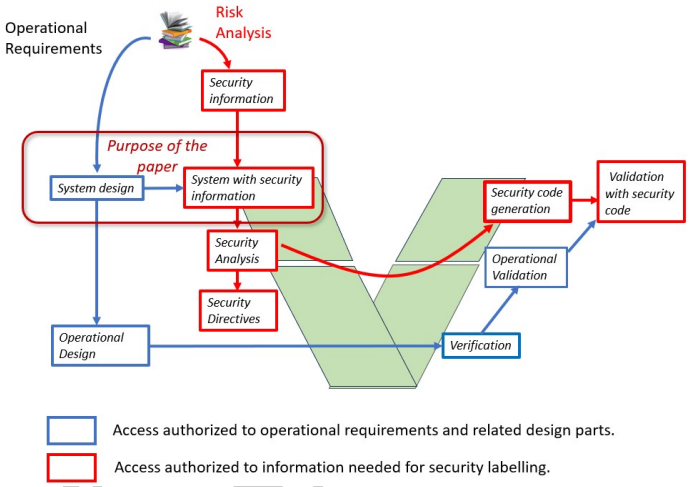

Fig. 9. Security Information exploitation

IX. Conclusion

In this paper, we propose a solution to ensure requirements confidentiality in system modelling designs including information with different levels of confidentiality. The proposed solution includes a set of criteria to assess a system multi-level confidentiality, a design process to ensure requirements confidentiality and mitigate inter-enclave design inconsistency.

At first glance, the multi-enclave management of models combining elements of different levels of confidentiality with respect to integrity could be very complex to implement. Our solution shows that not only this is not the case, but that the MBSE tools by their collaborative requirement engineering capabilities often already implement all the functionalities allowing the setting implementation of this solution.

It's true that the solution we propose allows the designer to define the different levels of confidentiality, but it doesn't help her/him to define them consistently with the risk analysis. As future work, we plan to formalise the dependencies between the assets defined during the risk analysis and the design elements. This will give us the opportunity to carry out a consistency analysis between the recommendations of the risk analysis and the definition of the enclaves.

References

[1] "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, US, Standard, Sep. 2020.

[2]https://www.eclipse.org/capella/download.html (access september 2023)

[2] J.-L. Voirin, O. Constant, E. Lépicier, and F. Maraux, "Dream the future: Systems engineering in 2030," *INCOSE International Symposium*, vol. 30, no. 1, pp. 771–782, 2020. [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2020.00754.x

[3] UAF, *Unified Architecture Framework (UAF) Domain Metamodel*. OMG, 2022. [Online]. Available: https://www.omg.org/spec/UAF/1.2

[4] Y. Roudier and L. Apvrille, "Sysml-sec: A model driven approach for designing safe and secure systems," in *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, 2015, pp. 655–664.

[5] D. Mažeika and R. Butleris, "Mbsesec: Model-based systems engineering method for creating secure systems," *Applied Sciences*, vol. 10, p. 2574, 04 2020.

[6] J. Navas, J.-L. Voirin, S. Paul, and S. Bonnet, "Towards the integration of cybersecurity risk assessment into model-based requirements engineering," in *INCOSE International Symposium, Volume 29, Issue 1, Orlando, USA, September 2019*. Wiley, 2019, pp. 850–865. [Online]. Available: https://doi.org/10.1002/j.2334-5837.2019.00639.x

[7] D. Naouar, J. E. Hachem, J. Voirin, J. Foisil, and Y. Kermarrec, "Towards the integration of cybersecurity risk assessment into model-based requirements engineering," in *29th IEEE International Requirements Engineering Conference, RE 2021, Notre Dame, IN, USA, September 20-24, 2021*. IEEE, 2021, pp. 334–344. [Online]. Available: https://doi.org/10.1109/RE51729.2021.00037

[8] M. Derdour, A. Alti, M. Gasmi, and P. Roose, "Security architecture metamodel for model driven security," *Journal of Innovation in Digital Ecosystems*, vol. 2, no. 1, pp. 55–70, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352664515000206

[9] J. El Hachem, Z. Y. Pang, V. Chiprianov, A. Babar, and P. Aniorte, "Model driven software security architecture of systems-of-systems," in *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*, 2016, pp. 89–96.

[10] E. Fernández-Medina, J. Jurjens, J. Trujillo, and S. Jajodia, "Model-driven development for secure information systems," *Information and Software Technology*, vol. 51, no. 5, pp. 809–814, 2009, sPECIAL ISSUE: Model-Driven Development for Secure Information Systems. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584908000761

[11] X. Hu, Y. Zhuang, Z. Cao, T. Ye, and M. Li, "Modeling and validation for embedded software confidentiality and integrity," *12th International Conference on Intelligent Systems and Knowledge Engineering*, pp. 1–6, 2017.

[12] H. Xu and M. R. Lyu, "Assessing the security properties of software obfuscation," *IEEE Security Privacy*, vol. 14, no. 5, pp. 80–83, 2016.

[13] M. Johnson and P. Stevens, "Confidentiality in the process of (model-driven) software development," in *Proceedings of 2nd International Conference on the Art, Science, and Engineering of Programming(Companion)*. ACM, Apr. 2018, pp. 1–8. [Online]. Available: https://2018.programming-conference.org

[14] D. E. Denning, T. F. Lunt, R. R. Schell, M. R. Heckman, and W. R. Shockley, "A multilevel relational data model," *1987 IEEE Symposium on Security and Privacy*, pp. 220–220, 1987.

[15] A. I. Sallam, S. M. Elrabie, and O. S. Faragallah, "Comparative study of polyinstantiation models in mls database," in *2010 International Computer Engineering Conference (ICENCO)*, 2010, pp. 158–165.

[16] A. Brodsky, C. Farkas, and S. Jajodia, "Secure databases: constraints, inference channels, and monitoring disclosures," *IEEE Transactions on Knowledge and Data Engineering*, vol. 12, no. 6, pp. 900–919, 2000.

[17] C. Morlet, A. González Fernández, R. Dellago, S. Bouchired, G. Lopez-Risueno, M. Manteiga Bautista, C. Ruta, R. Dall'Ora, T. Bey, and M. Chattou, "Embarking to end-to-end system modelling for galileo second generation," 11 2022.

[18] NATO, *SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO), C-M(2002)49-REV1*, 2020. [Online]. Available: https://www.nbf.hu/docs/C-M(2002)49-REV1.pdf

[19] "Risk management - guidelines," International Organization for Standardization, Geneva, CH, Standard, Jun. 2018.

[20] J.-L. Voirin, *Model-based system and architecture engineering with the arcadia method*, 11 2017.

[21] D. Bell and L. LaPadula, *A mathematical model, Technical report esd-tr-278, vol. 2, Bedford*. The Mitre Corporation, 1973.

[22] K. L. Beck, M. A. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Grenning, J. Highsmith, A. Hunt, R. Jeffries, J. Kern, B. Marick, R. C. Martin, S. J. Mellor, K. Schwaber, J. Sutherland, and D. A. Thomas, "Manifesto for agile software development," 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:109006295

[23] IGI-1300, *INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE*. Secrétariat général de la défense et de la sécurité nationale, 2020. [Online]. Available: http://www.sgdsn.gouv.fr/uploads/2016/10/igi-1300-20210809.pdf

[24] M. Koegel and J. Helming, "Emfstore: A model repository for emf models," in *Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering - Volume 2*, ser. ICSE '10, 2010, p. 307–308. [Online]. Available: https://doi.org/10.1145/1810295.1810364

[25] G. Kramler, G. Kappel, T. Reiter, E. Kapsammer, W. Retschitzegger, and W. Schwinger, "Towards a semantic infrastructure supporting model-based tool integration," in *Proceedings of the 2006 International Workshop on Global Integrated Model Management*, ser. GaMMa '06, 2006, p. 43–46. [Online]. Available: https://doi.org/10.1145/1138304.1138314

[26] A. Garcia-Dominguez, K. Barmpis, D. S. Kolovos, M. A. A. da Silva, A. Abherve, and A. Bagnato, "Integration of a graph-based model indexer in commercial modelling tools," in *Proceedings of the ACM/IEEE 19th International Conference on Model Driven Engineering Languages and Systems*, ser. MODELS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 340–350. [Online]. Available: https://doi.org/10.1145/2976767.2976809

[27] C. Boudjennah, B. Combemale, D. Exertier, S. Lacrampe, and M. Peraldi-Frati, "CLARITY: open-sourcing the model-based systems engineering solution capella," in *Proceedings of the International Workshop on Open Source Software for Model Driven Engineering Ottawa, Canada*, 2015.