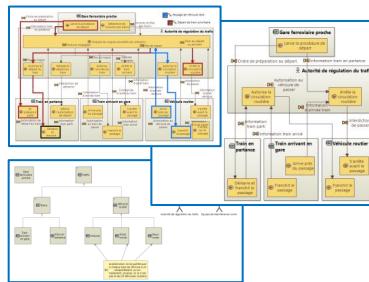


MBSE Confidentiality Management and Security Analysis of Capella Designs

Michel Bourdellès
Univ. Bretagne Sud
Vannes, France
michel.bourdelles@univ-ubs.fr

Capella Confidentiality Management

Control Access up to confidentiality level **n**



Control Access up to confidentiality level **m**

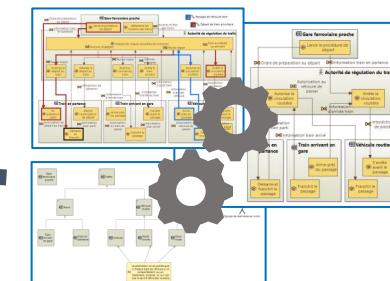
Security Analysis of Capella Designs

Risk Analysis



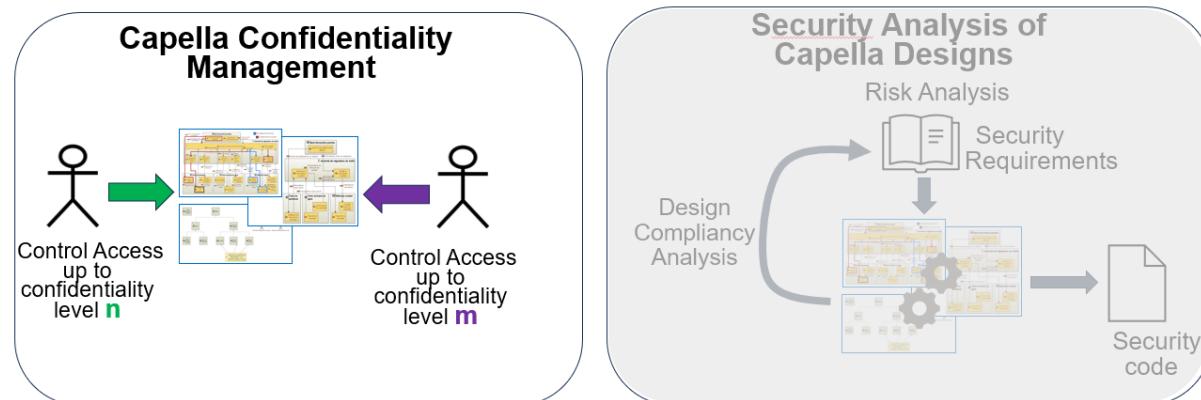
Security Requirements

Design Compliancy Analysis

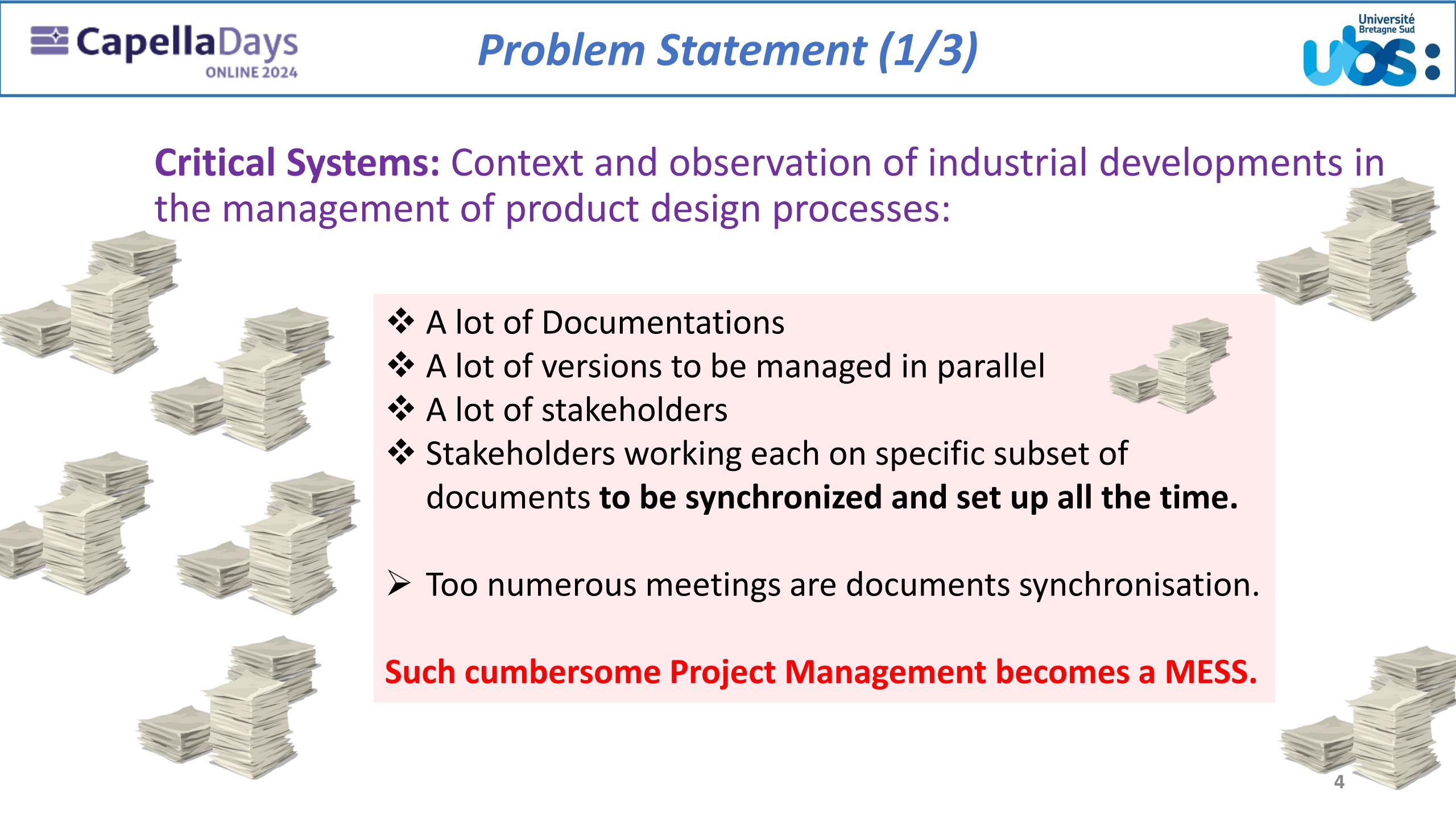


Security code

MBSE Confidentiality Management and Security Analysis of Capella Designs



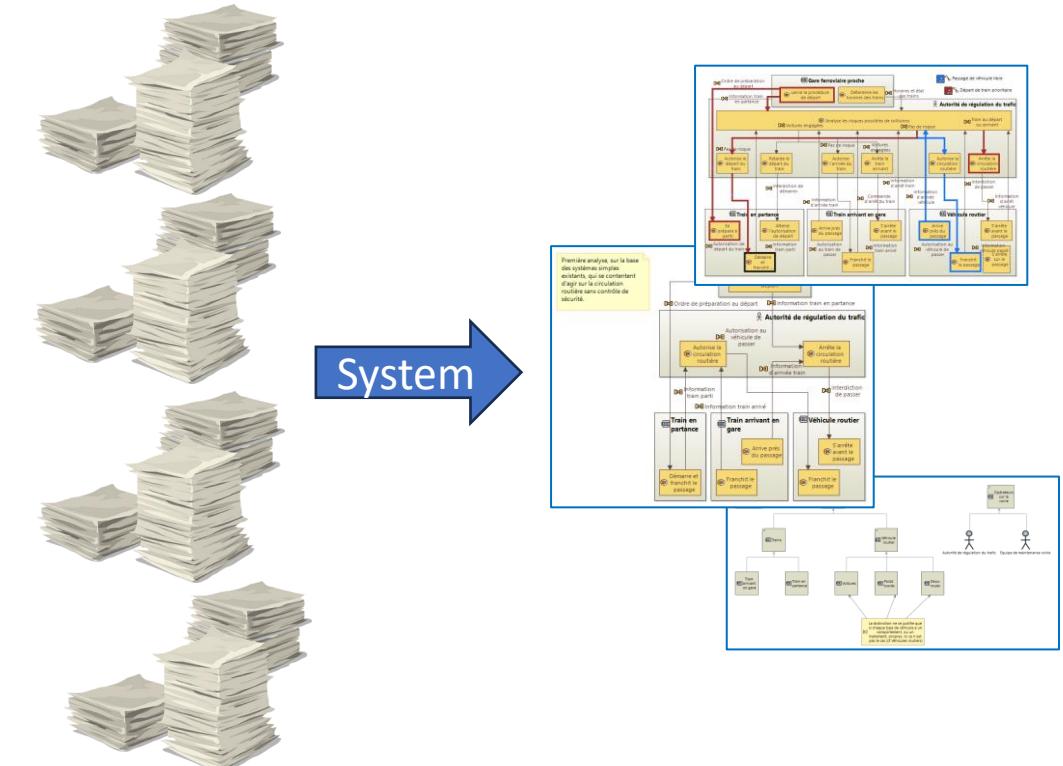
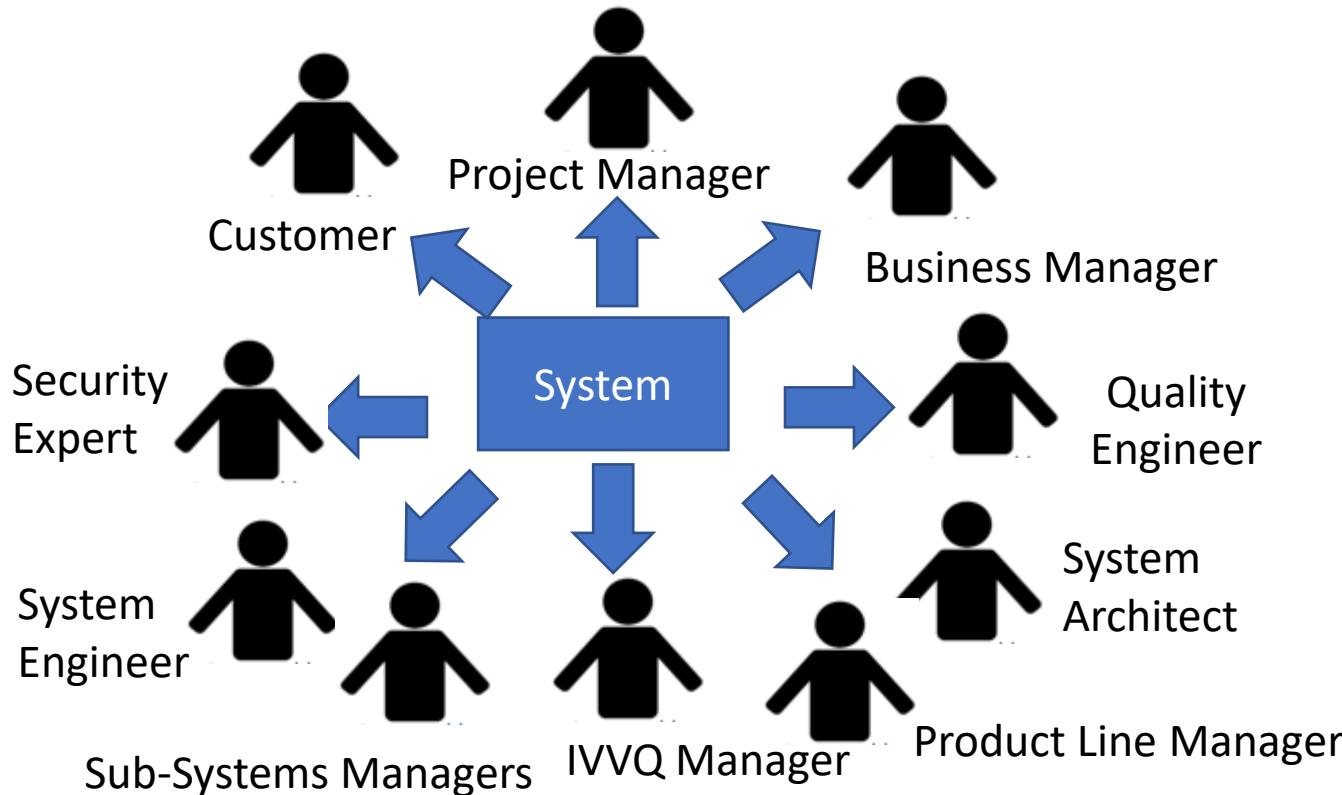
Critical Systems: Context and observation of industrial developments in the management of product design processes:

- 
- ❖ A lot of Documentations
 - ❖ A lot of versions to be managed in parallel
 - ❖ A lot of stakeholders
 - ❖ Stakeholders working each on specific subset of documents **to be synchronized and set up all the time.**
- Too numerous meetings are documents synchronisation.

Such cumbersome Project Management becomes a MESS.

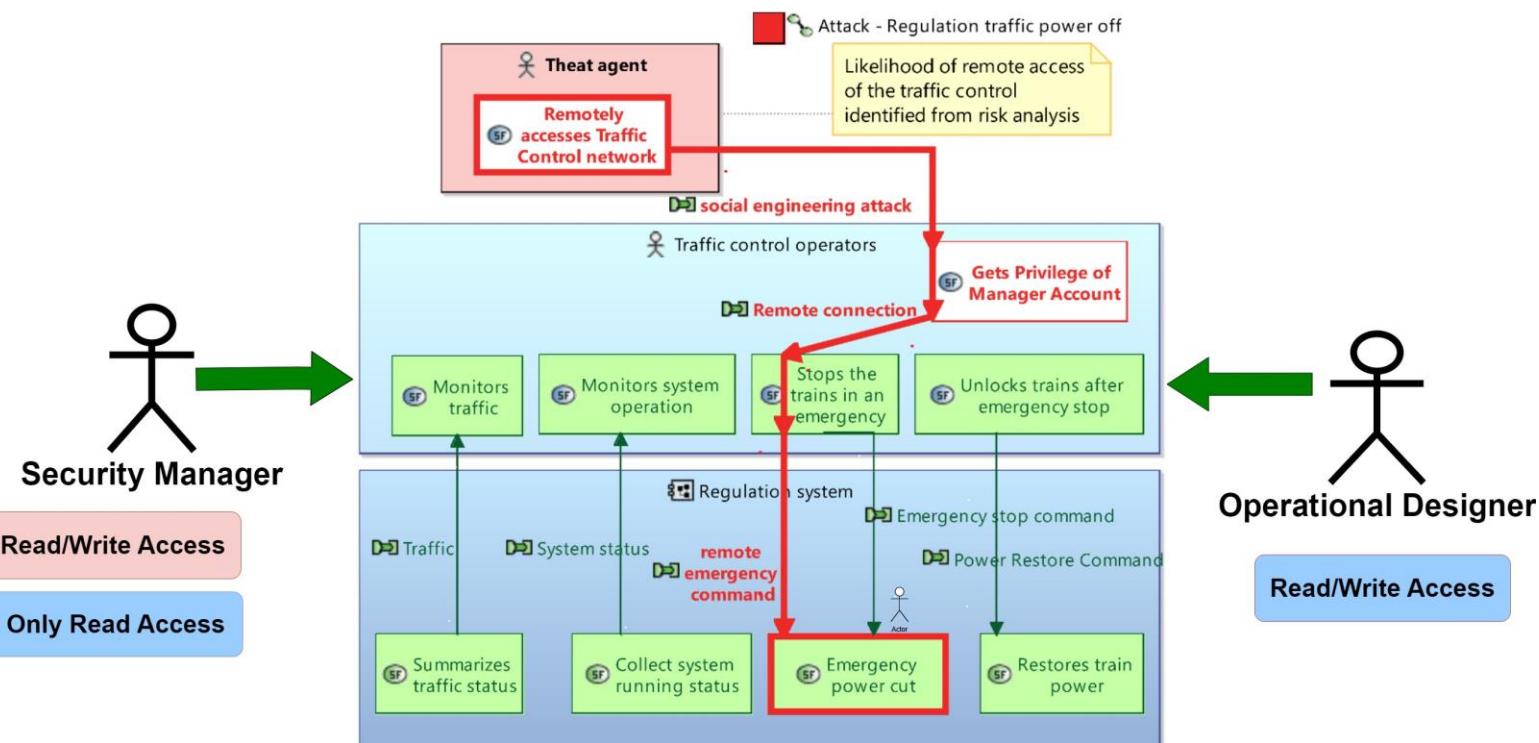
Industrial Proposal: Moving from Document Driven Process to Modelling Driven Process [INCOSE – Prospective 2030 recommendation]

- Modelling of the Operational Design needs: *Capella, SysML, Cameo, etc.*
- One Model shared by all the stakeholders.



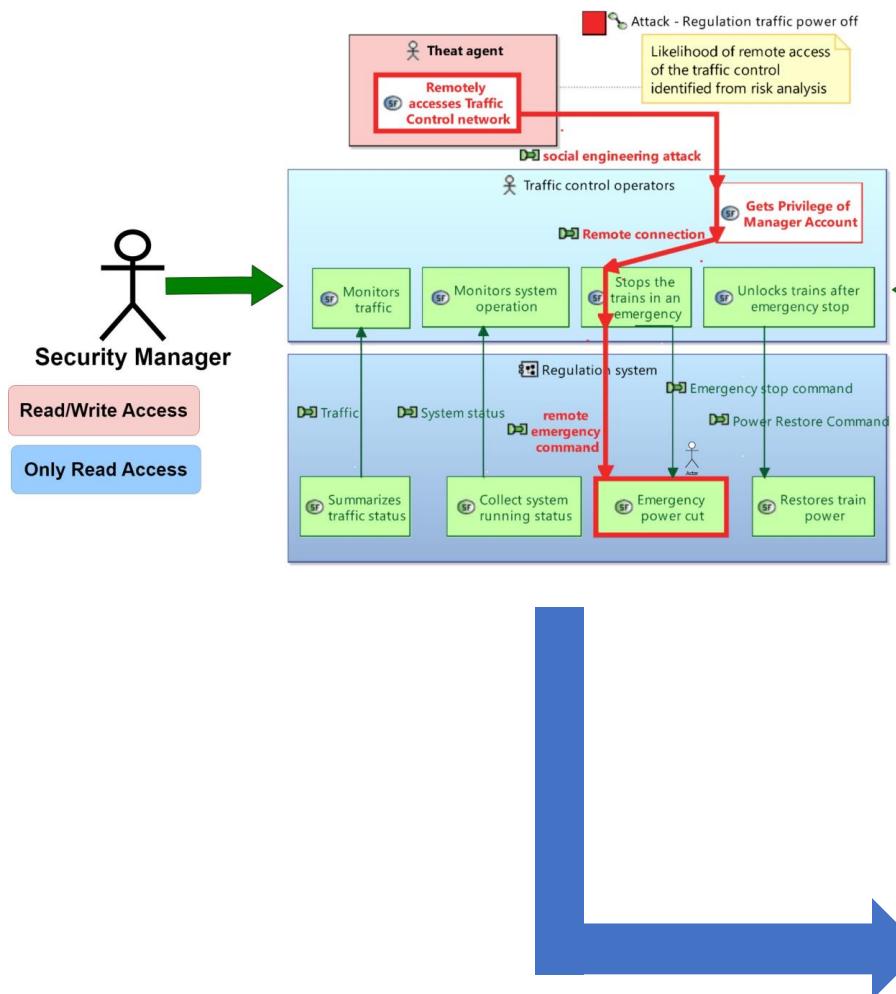
Moving from Documentation to Model Based System Engineering

- A lot of advantages: Consistency, On-The-Fly Change Information Notification, Homogeneous notations and Practices
- Some drawbacks: Reluctance to Change, Straitjacket imposed by Modelling
- One is related to Confidentiality Management of modelling elements



*Level-Crossing Traffic Control
from
mbse-capella.org*

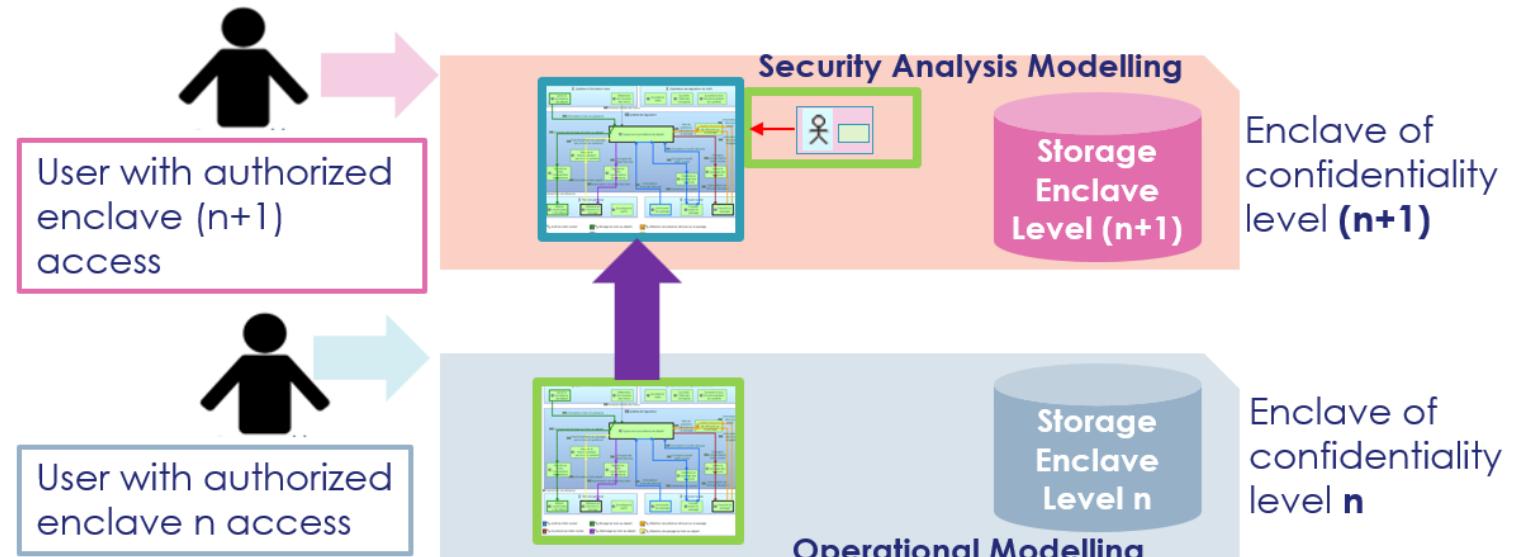
- ✓ Confidentiality, Integrity, Consistency
- ✓ No leak
- ✓ Storage confidentiality
- ✓ No manual labelling
- ✓ Iterative Design Flow Compliance
- ✓ Genericity of the Solution



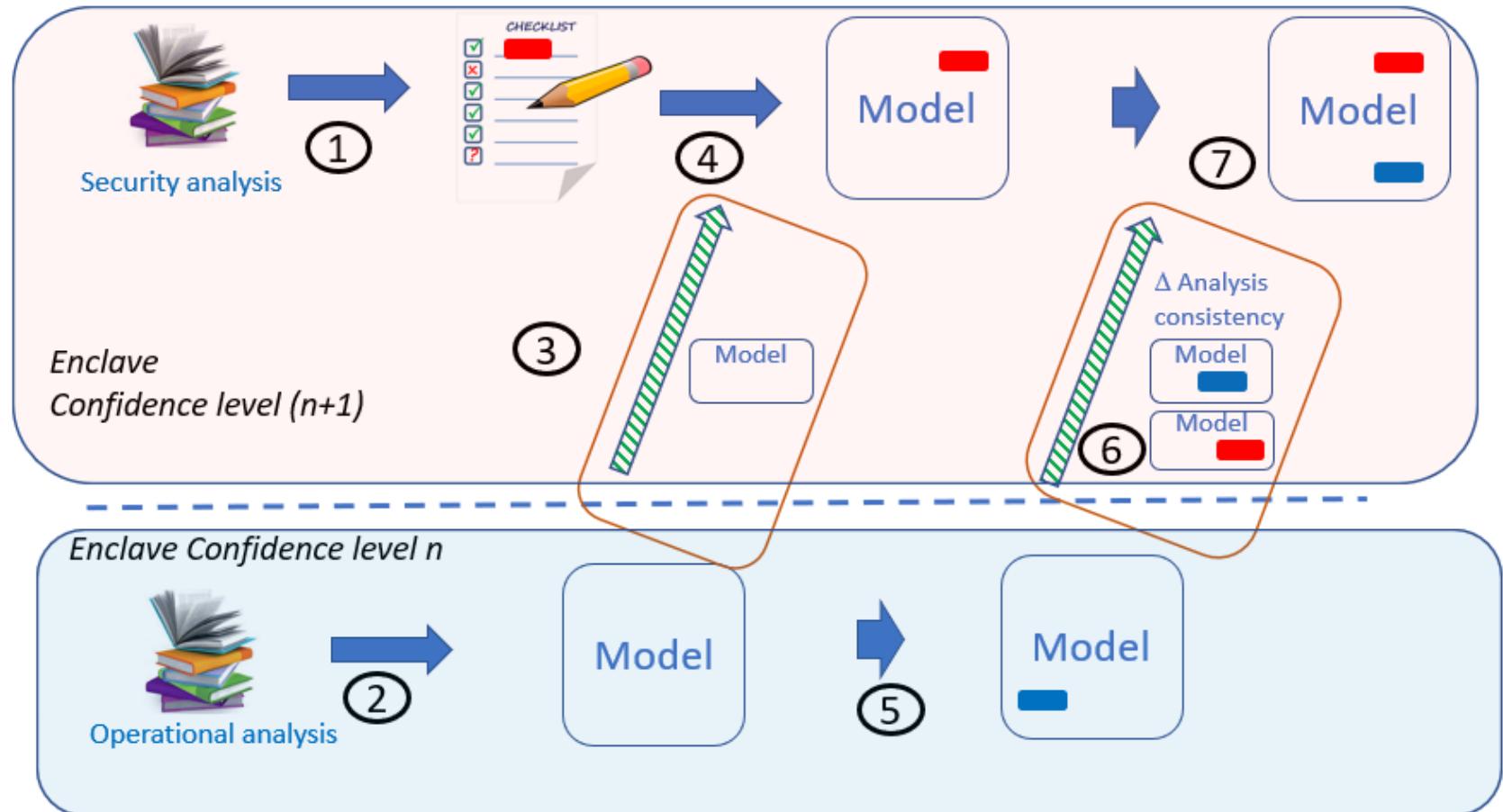
Main Ideas :

- Enclave Separation with Access Control
- Apply the Bell-Lapadula Principles

- *Simple security: no read up*
- *Star-security : no write down*



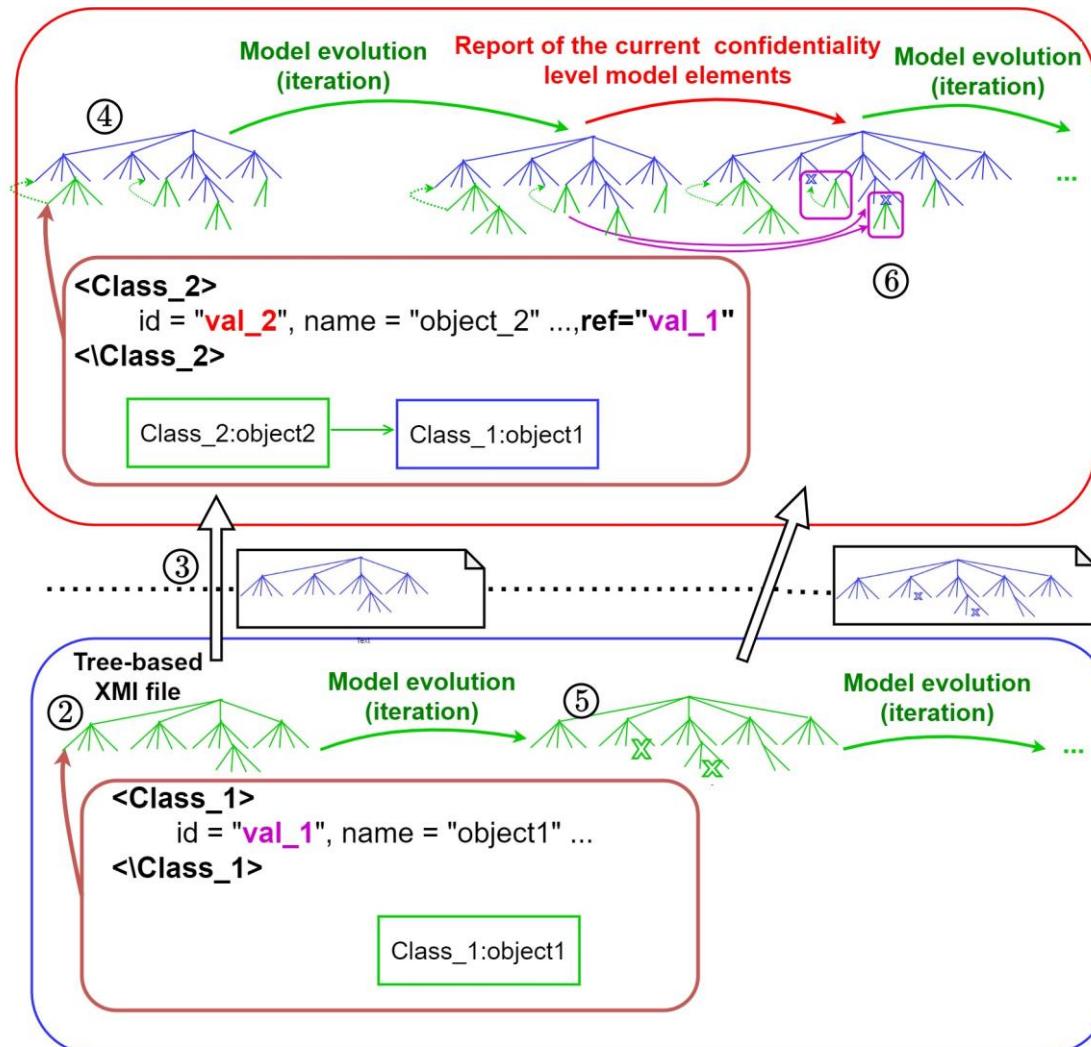
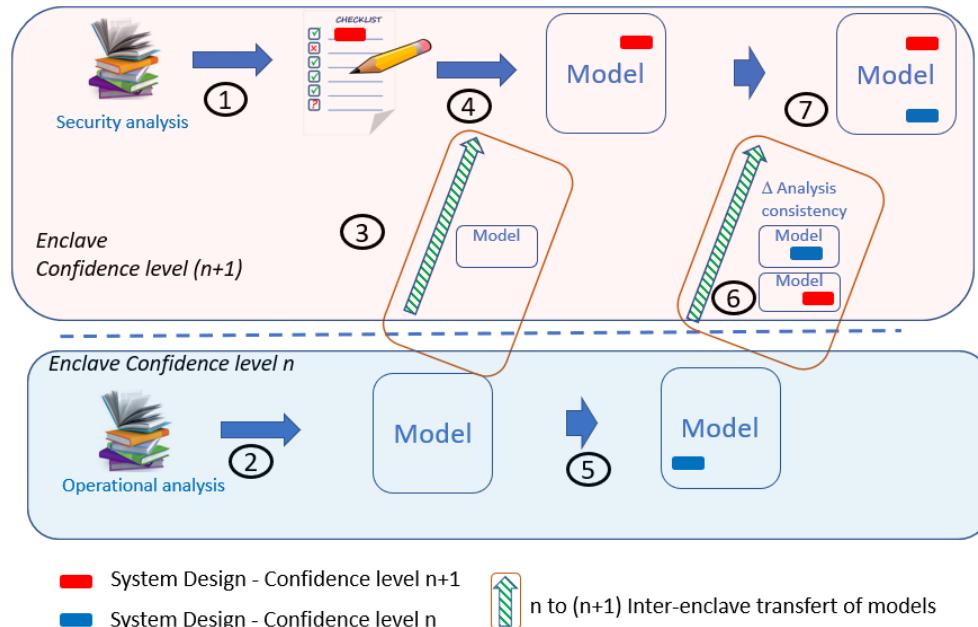
■ Read only access ■ Read/write access



- System Design - Confidence level $n+1$
- System Design - Confidence level n

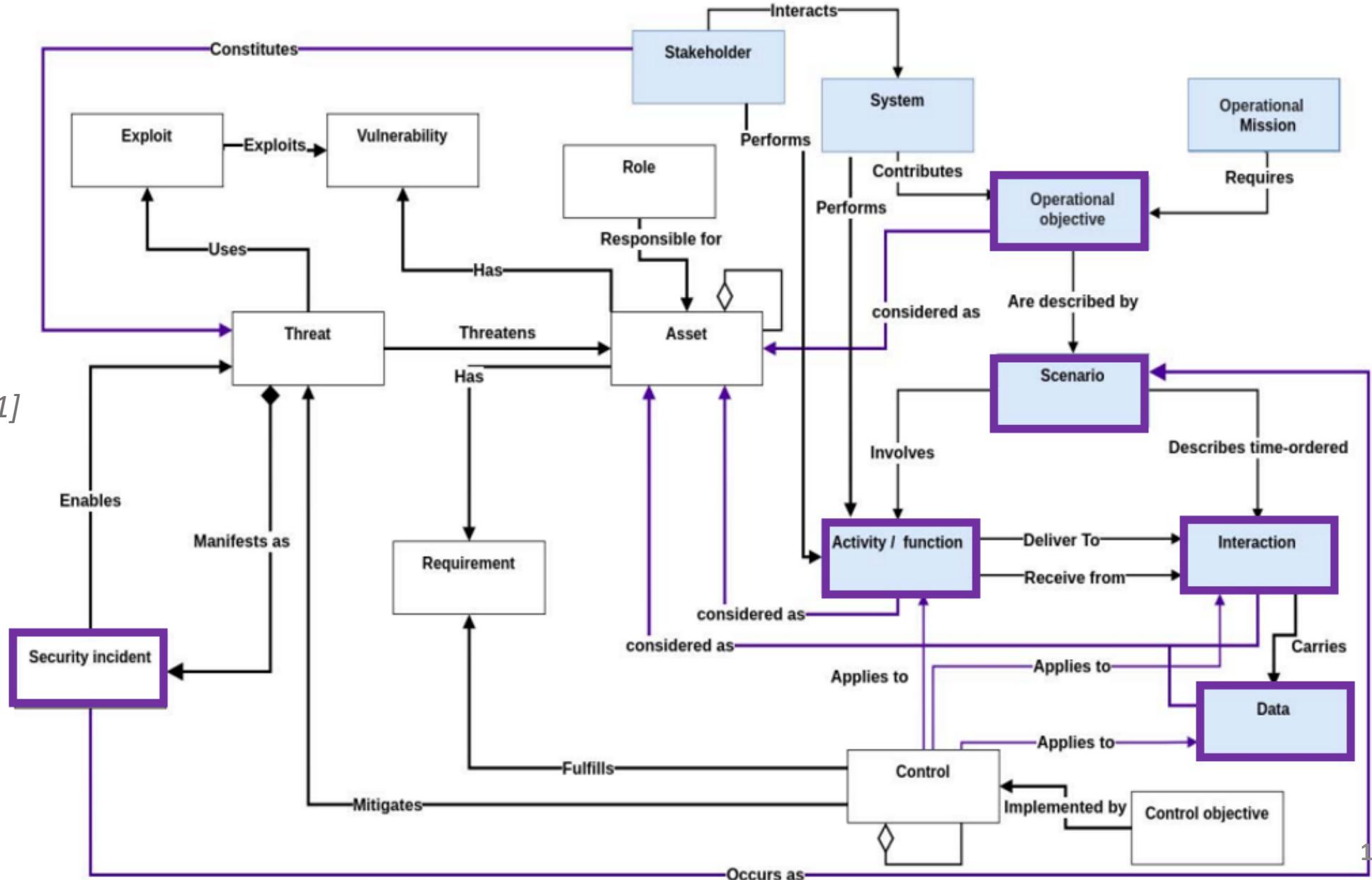


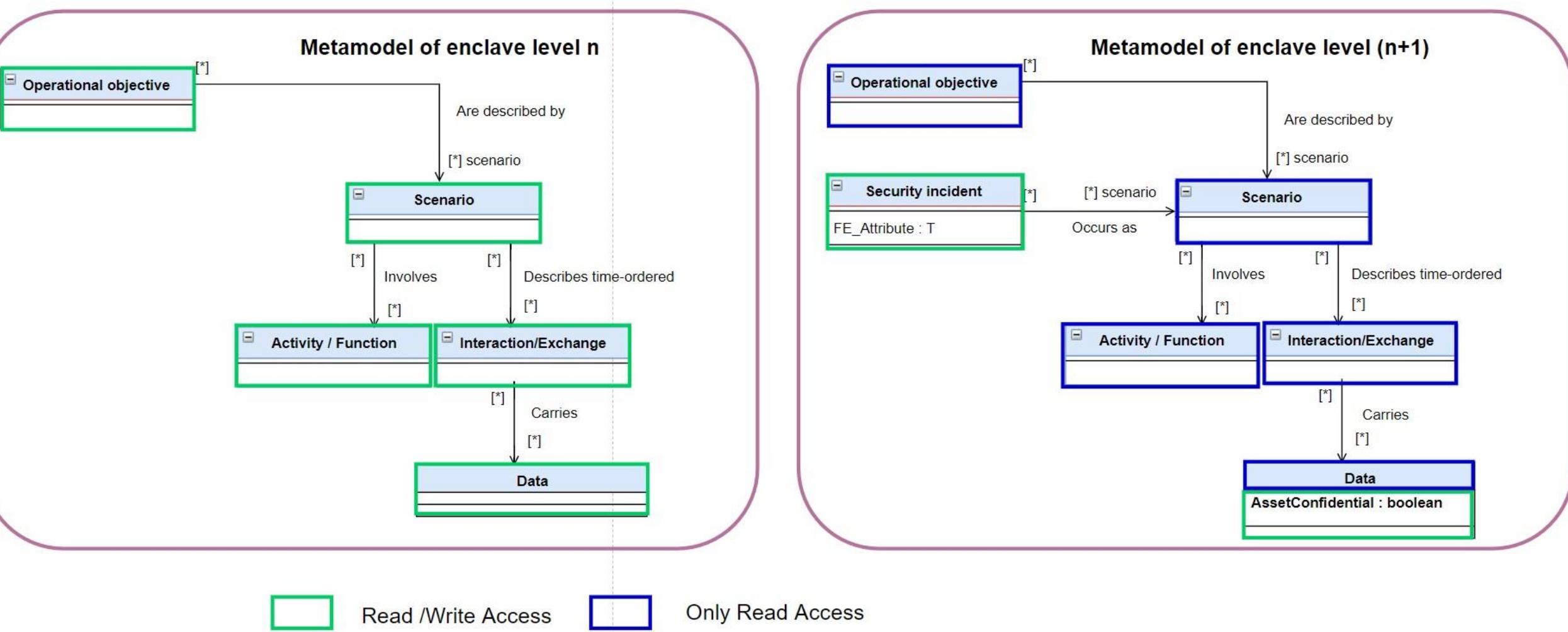
n to $(n+1)$ Inter-enclave transfert of models



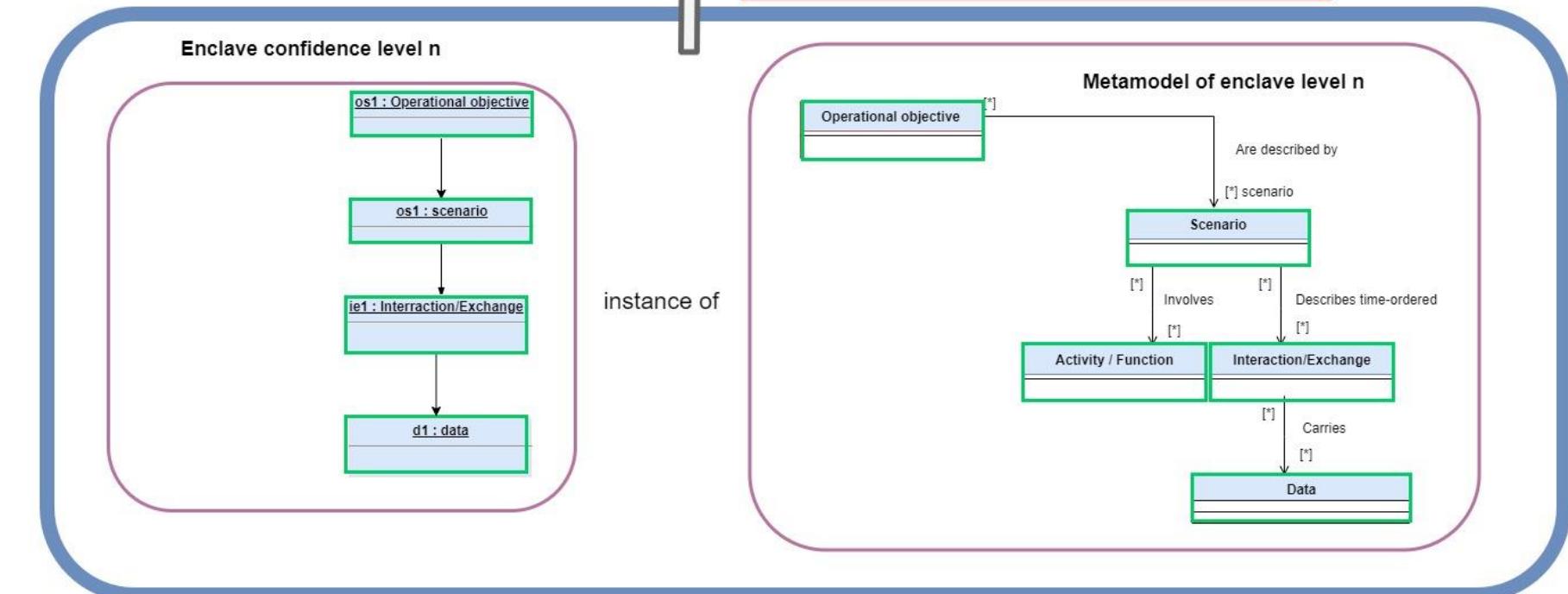
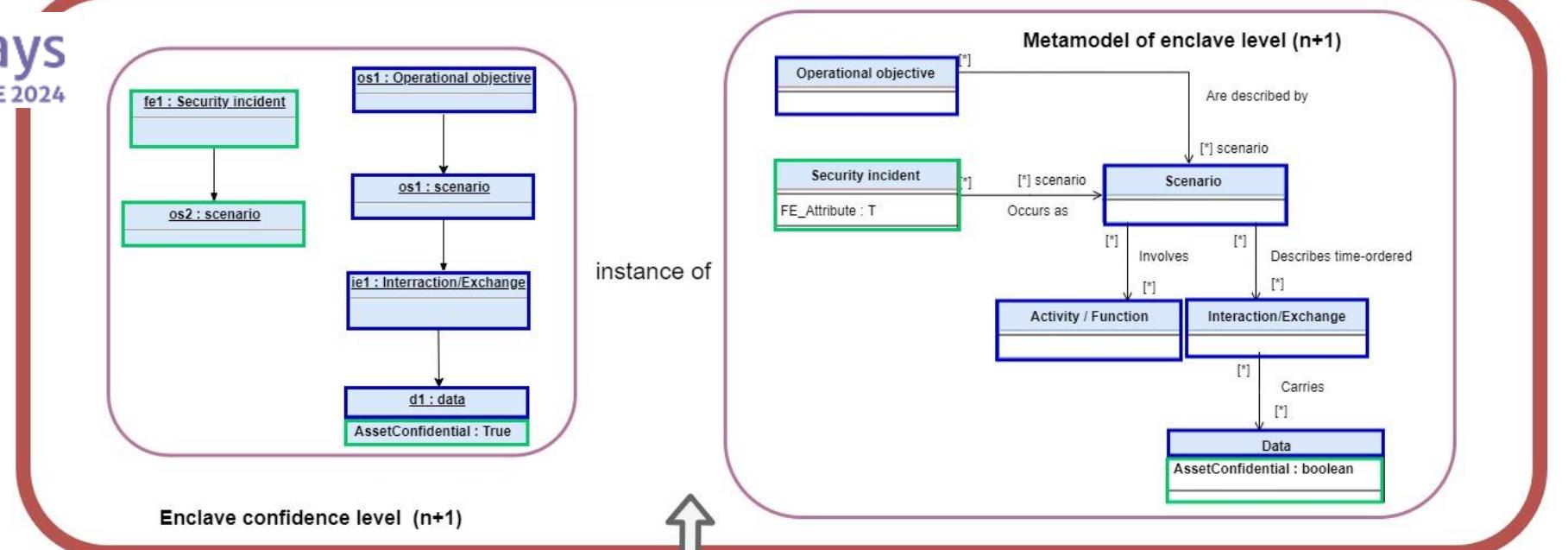
- Green triangle: Read-write part of tree-based xmi file
- Blue triangle: Read-only part of tree-based xmi file
- Red 'X': XMI file element suppression
- Yellow square: Inconsistency Identified by structural analysis due to XMI file element suppression

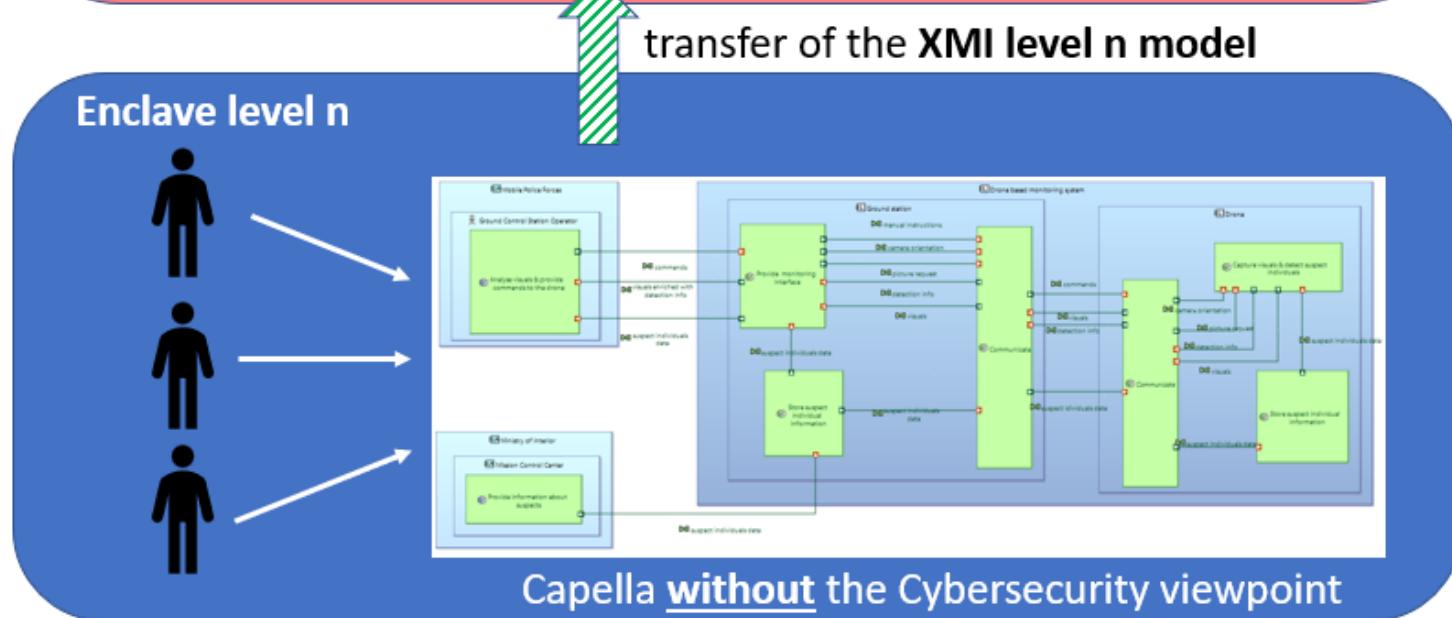
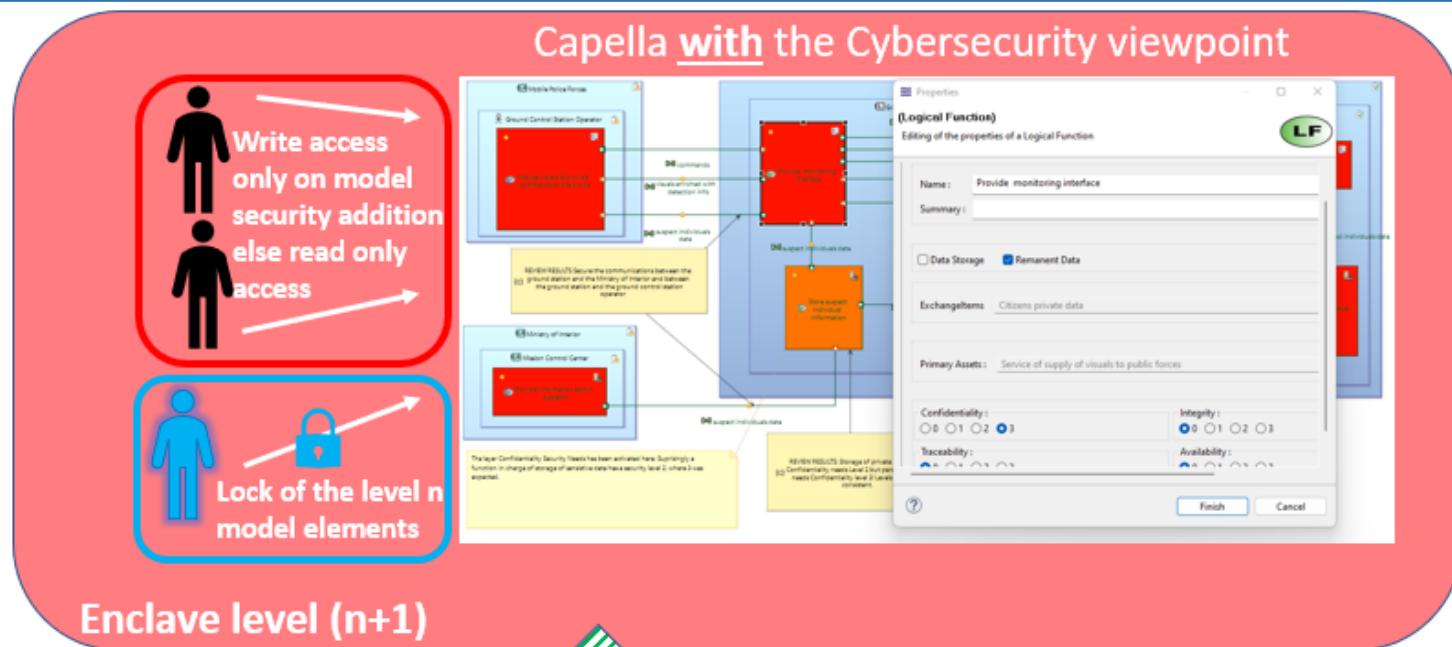
Application Example (1/3)





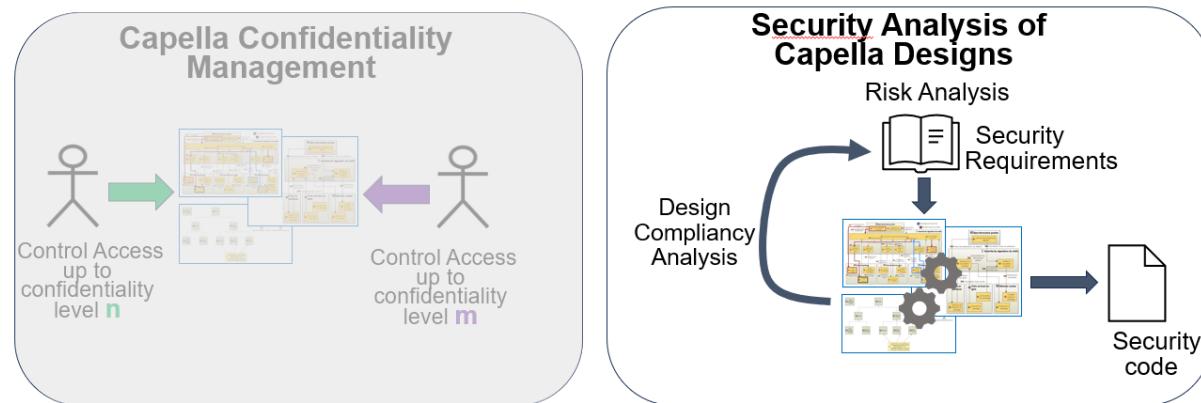
Application Example (3/3)



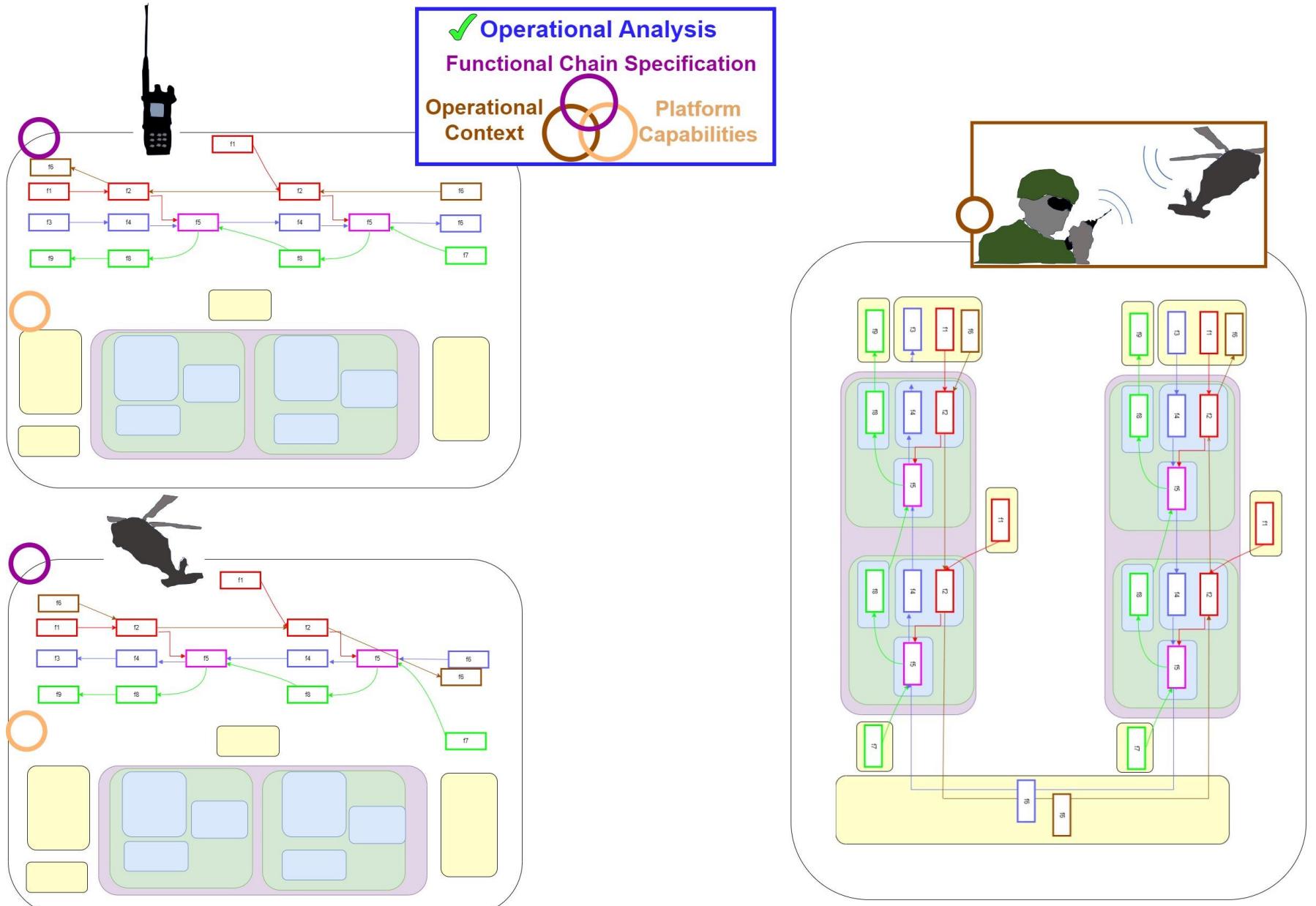


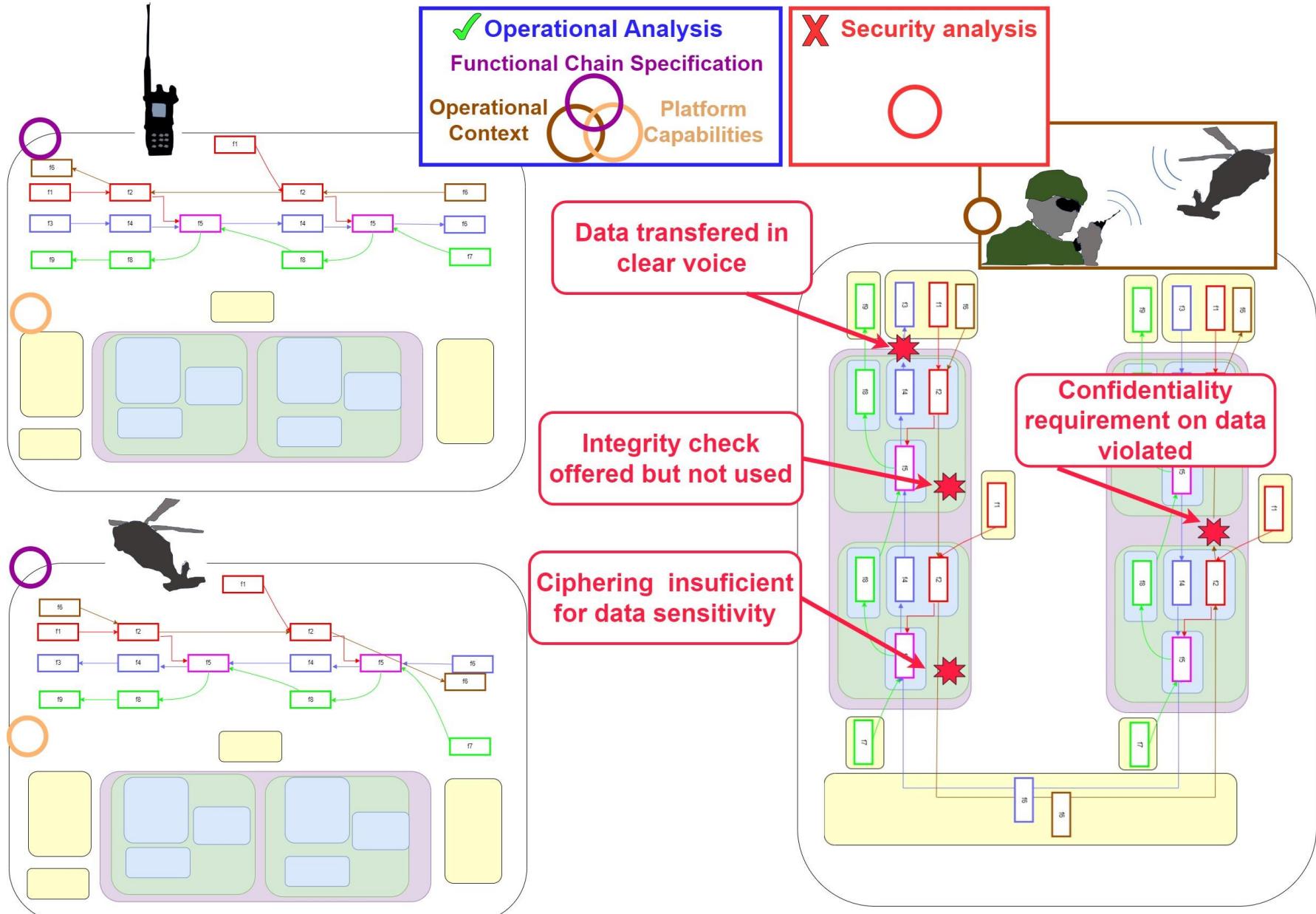
- ***Solution for the Complex Systems Design Confidentiality Management***
- ***Assessment Criteria:***
 - ✓ Confidentiality, Integrity, Consistency 
 - ✓ No leak 
 - ✓ Storage confidentiality 
 - ✓ No manual labelling 
 - ✓ Iterative Design Flow Compliance 
 - ✓ Genericity of the Solution 
 - ✓ Current modelling tools integration 
- ***First stone of the enrichment of the product process flow, to guarantee the confidentiality of security specification, design and processing***

MBSE Confidentiality Management and Security Analysis of Capella Designs



Problem Statement (1/3)





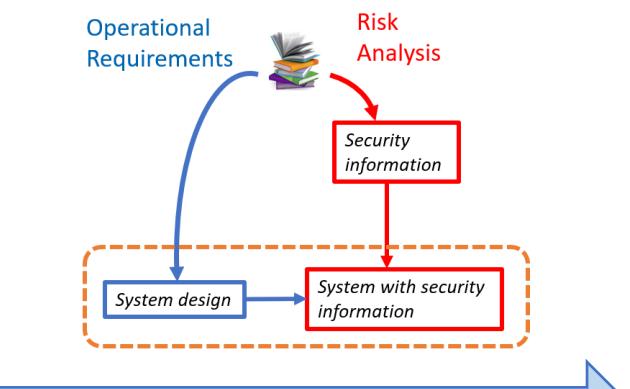
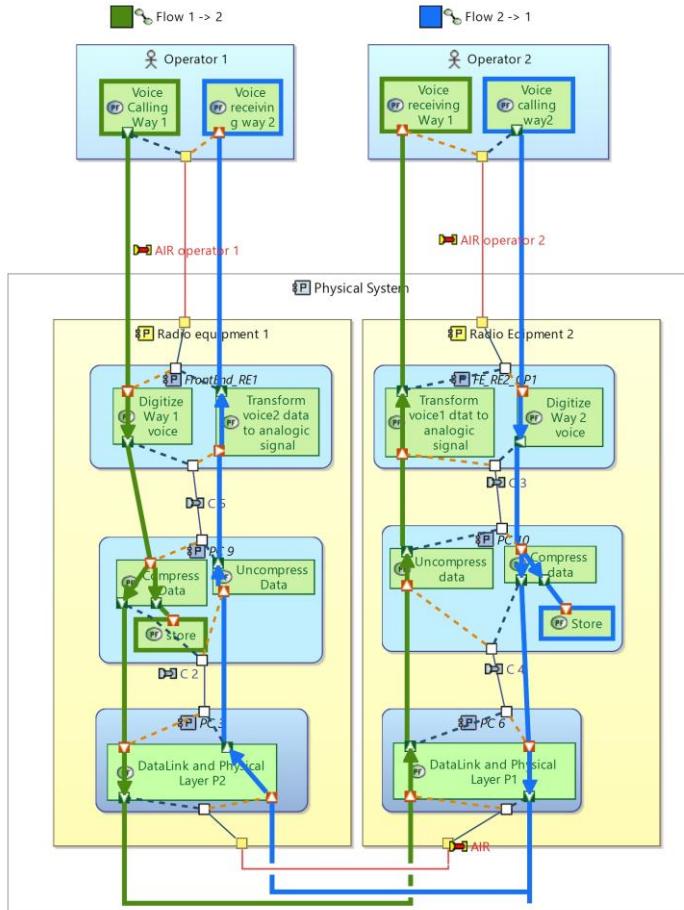
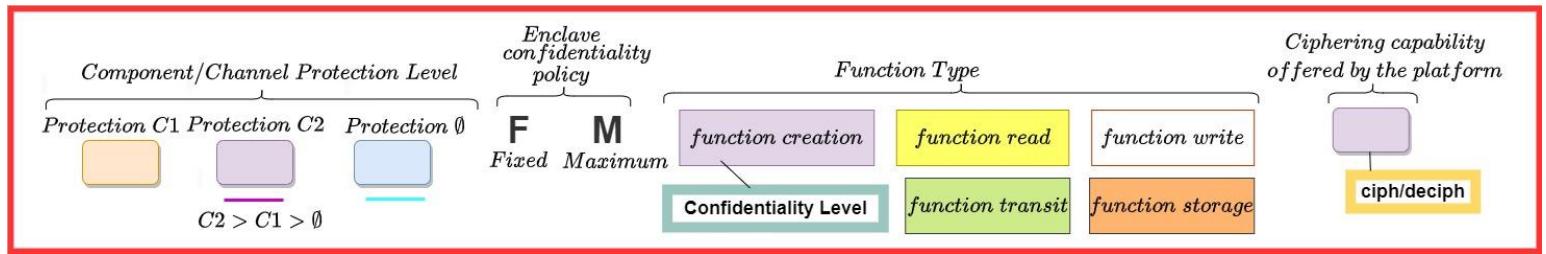
Complex Critical Systems: Sensitive data flows to protect.

- Weak tooled process to face automatic security requirements assessment in systems process designs.

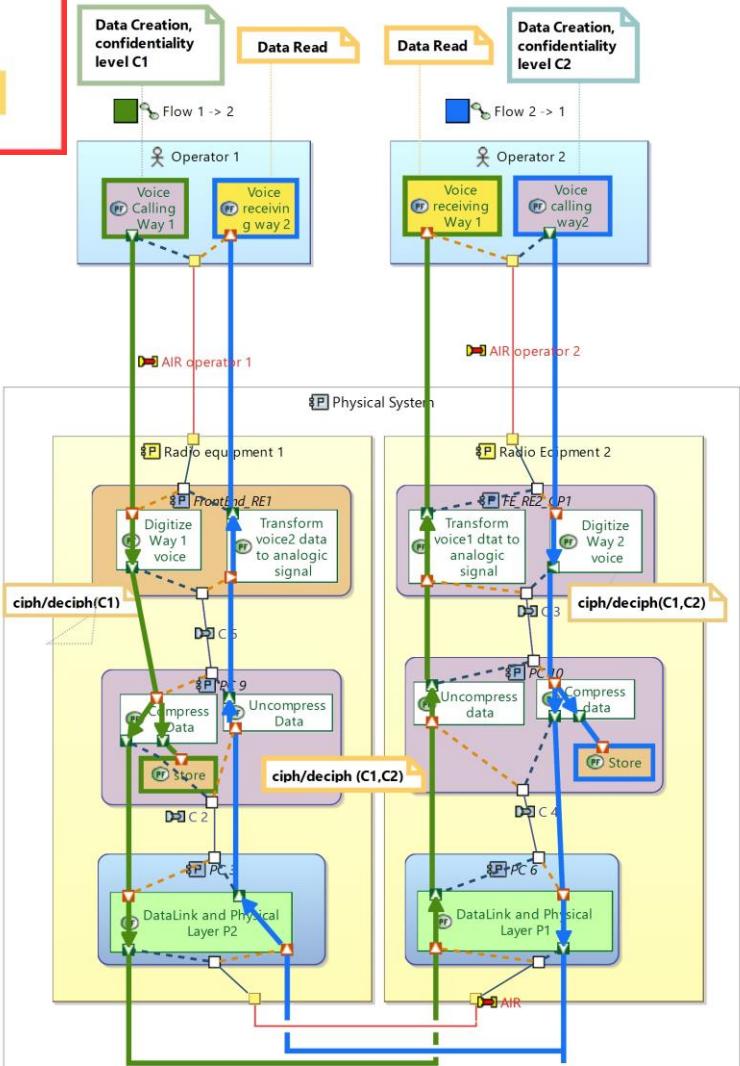
Solution presented

- ❖ Annotation of the System models with security information deduced from a risk analysis.
- ❖ Exploitation of the information to analyse the compliance of the system design choices with initial security requirements.
- ❖ Automatically generate security code to assess the confidentiality and integrity of the sensitive data in the system.

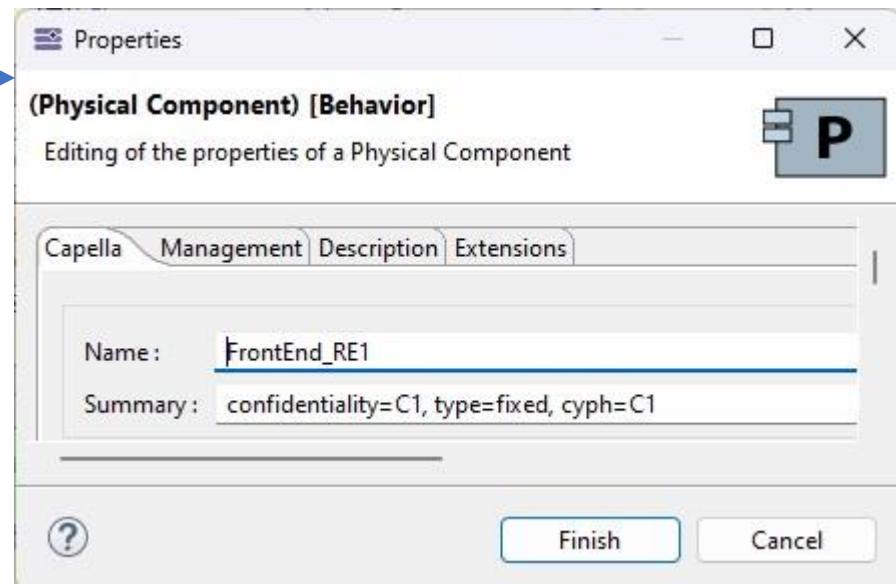
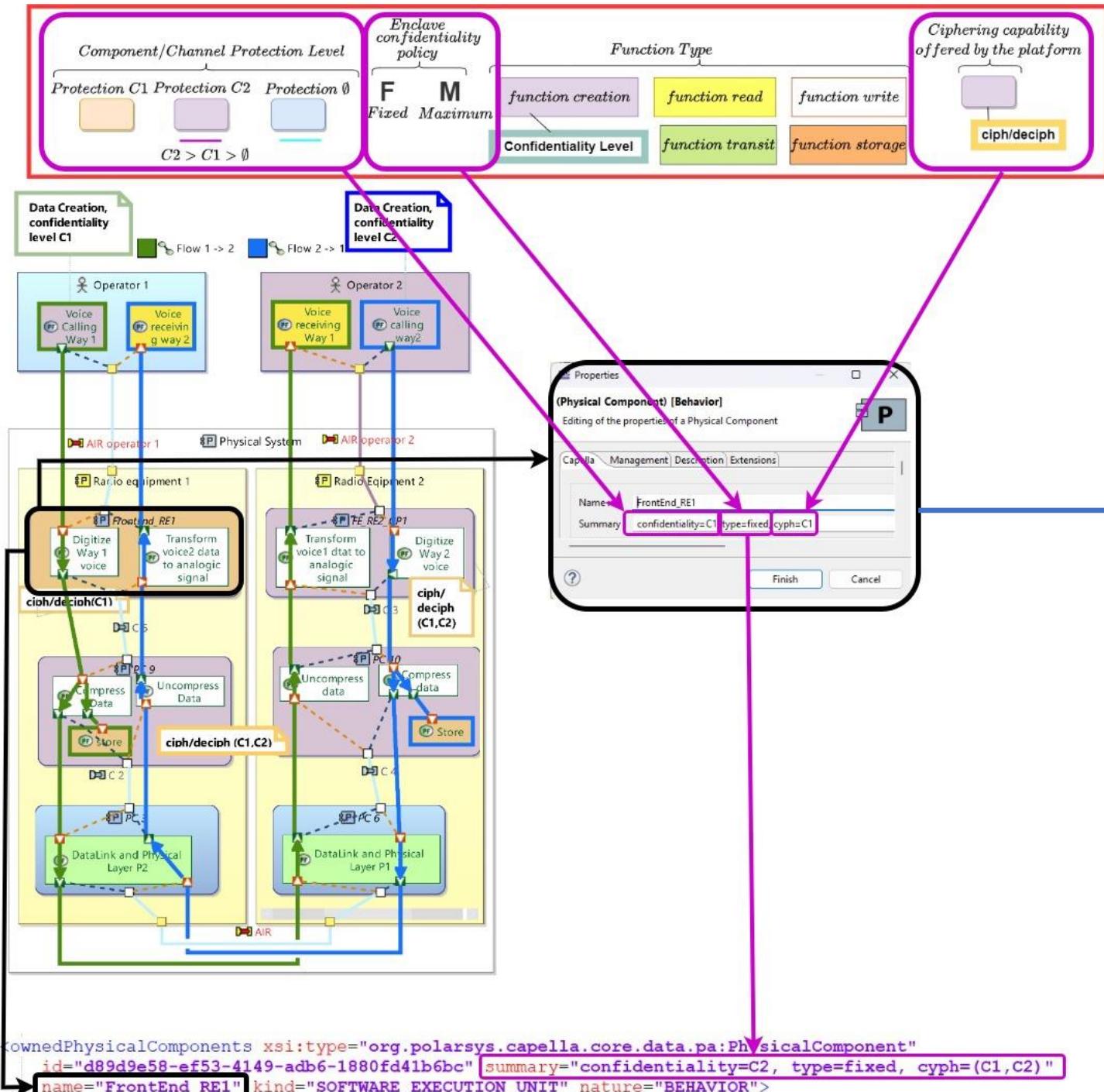
Security Requirements Elicitation

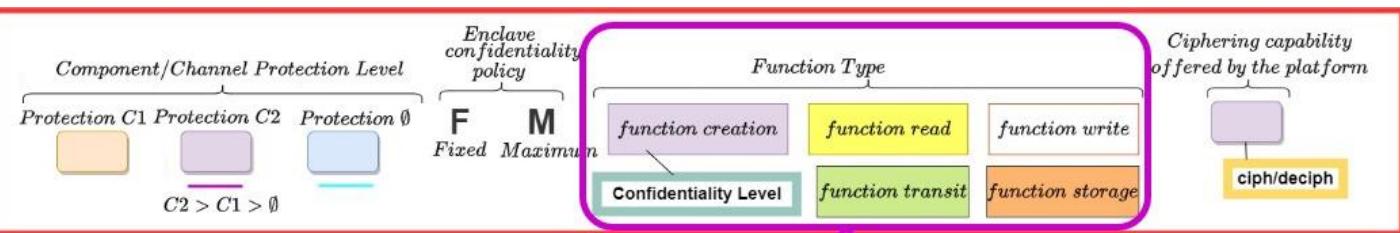


SAC'2024
ICECCS 2024

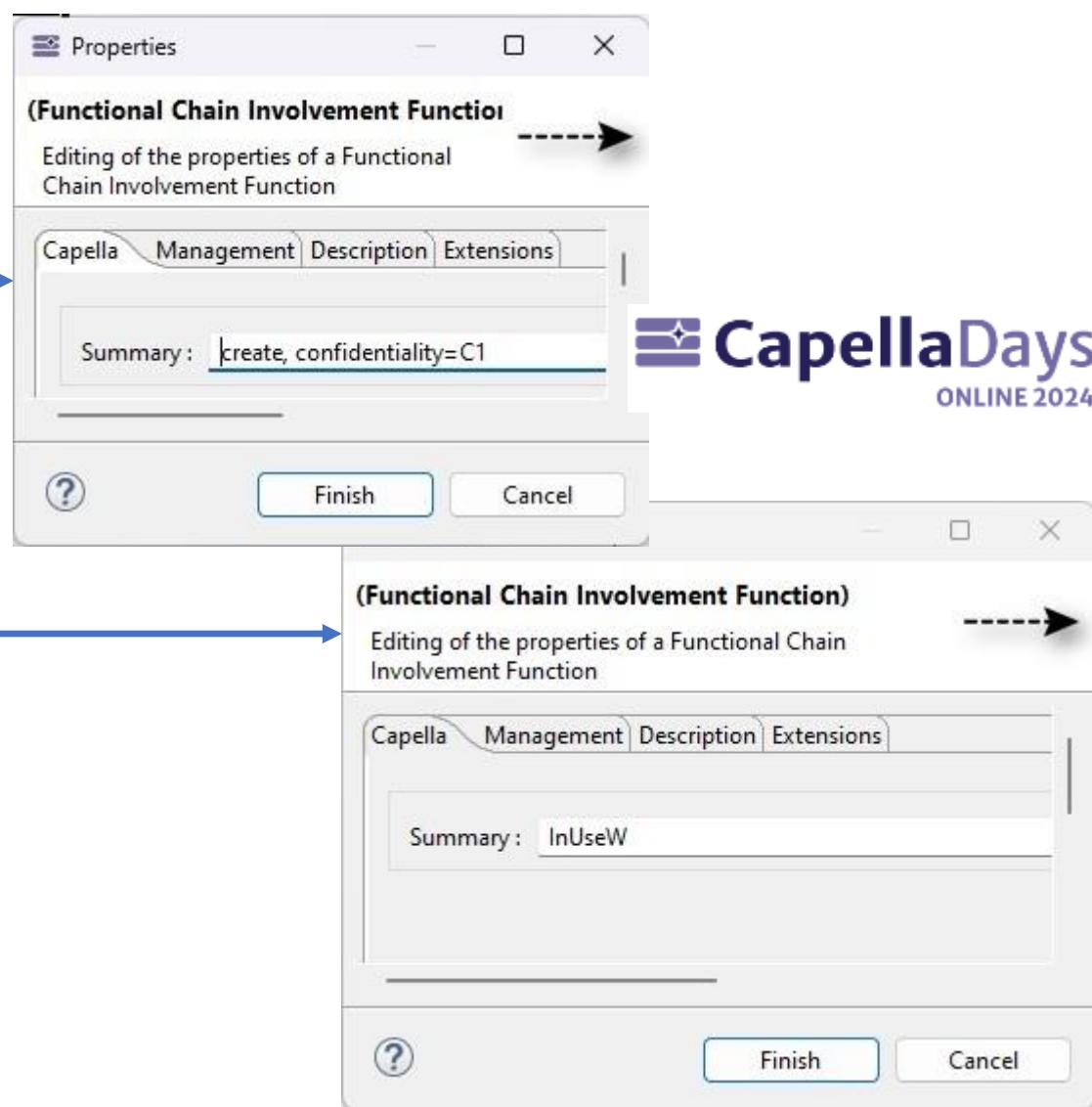
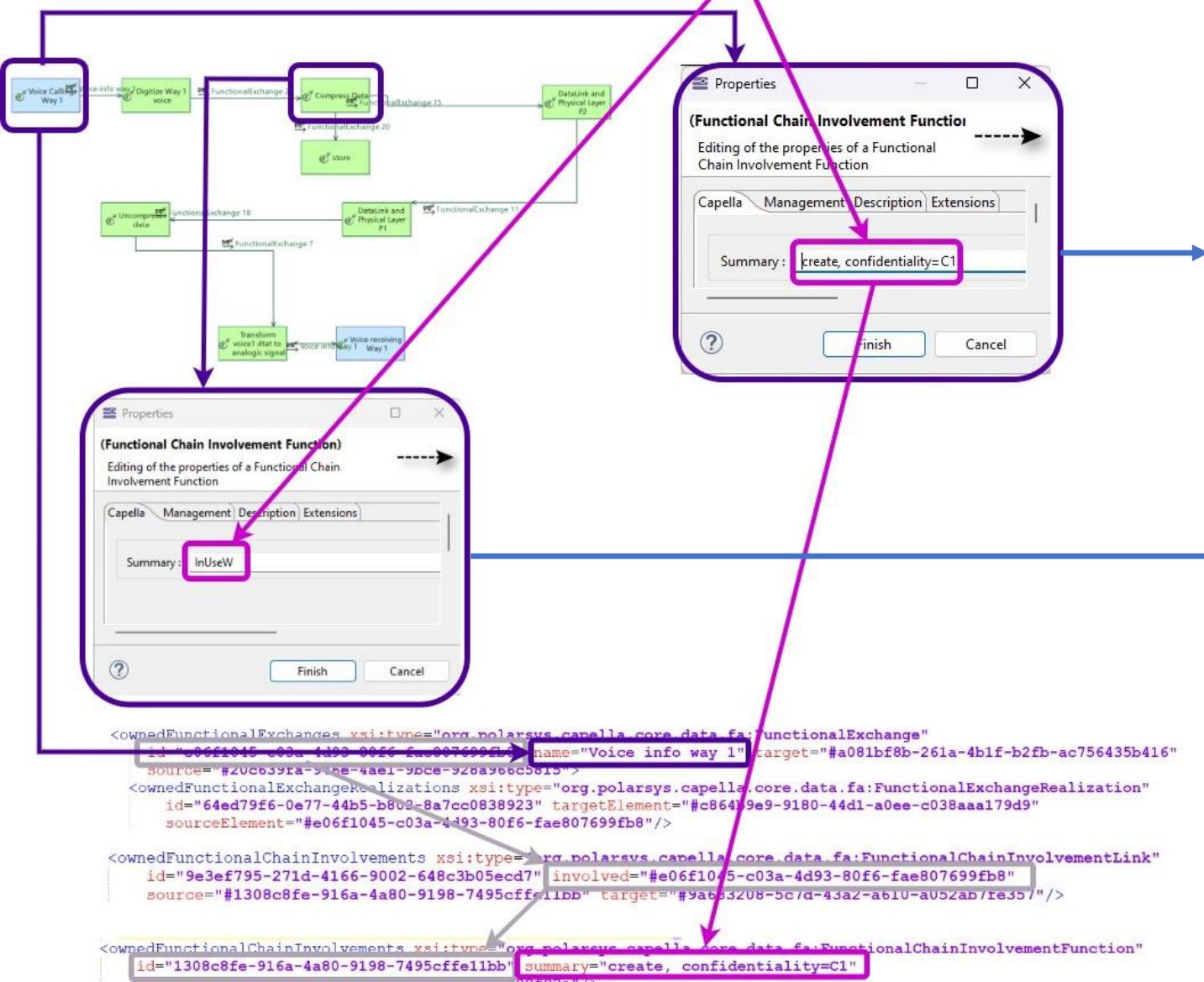


Tool implementation: Analysis From Capella





Tool implementation – Analysis From CapellaDesigns



● ● ● *Data sensibility set at creation*

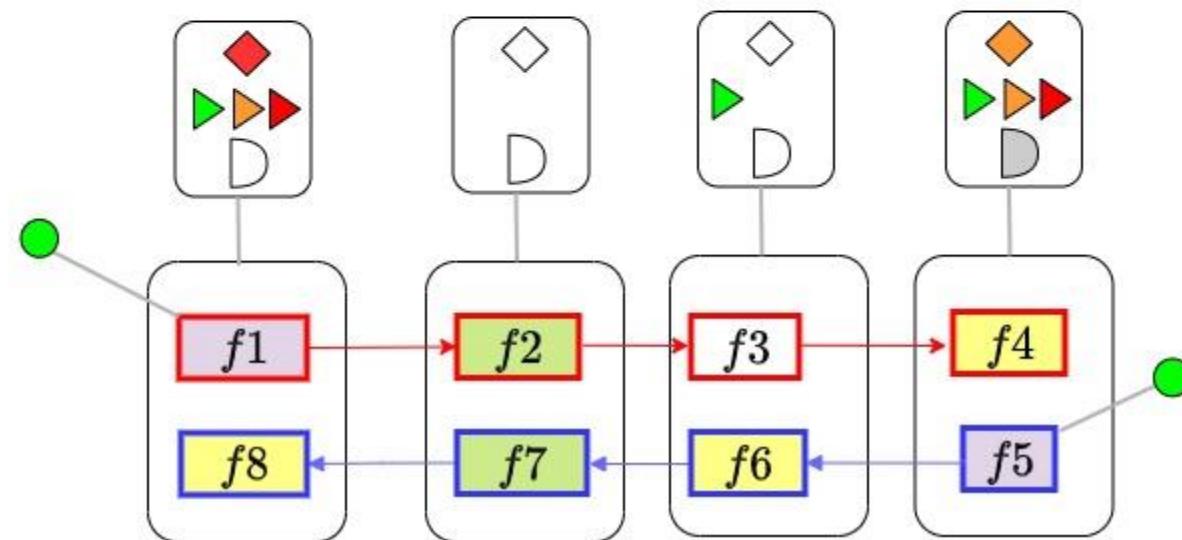
◆ ◆ ◆ *Enclave protection offered*

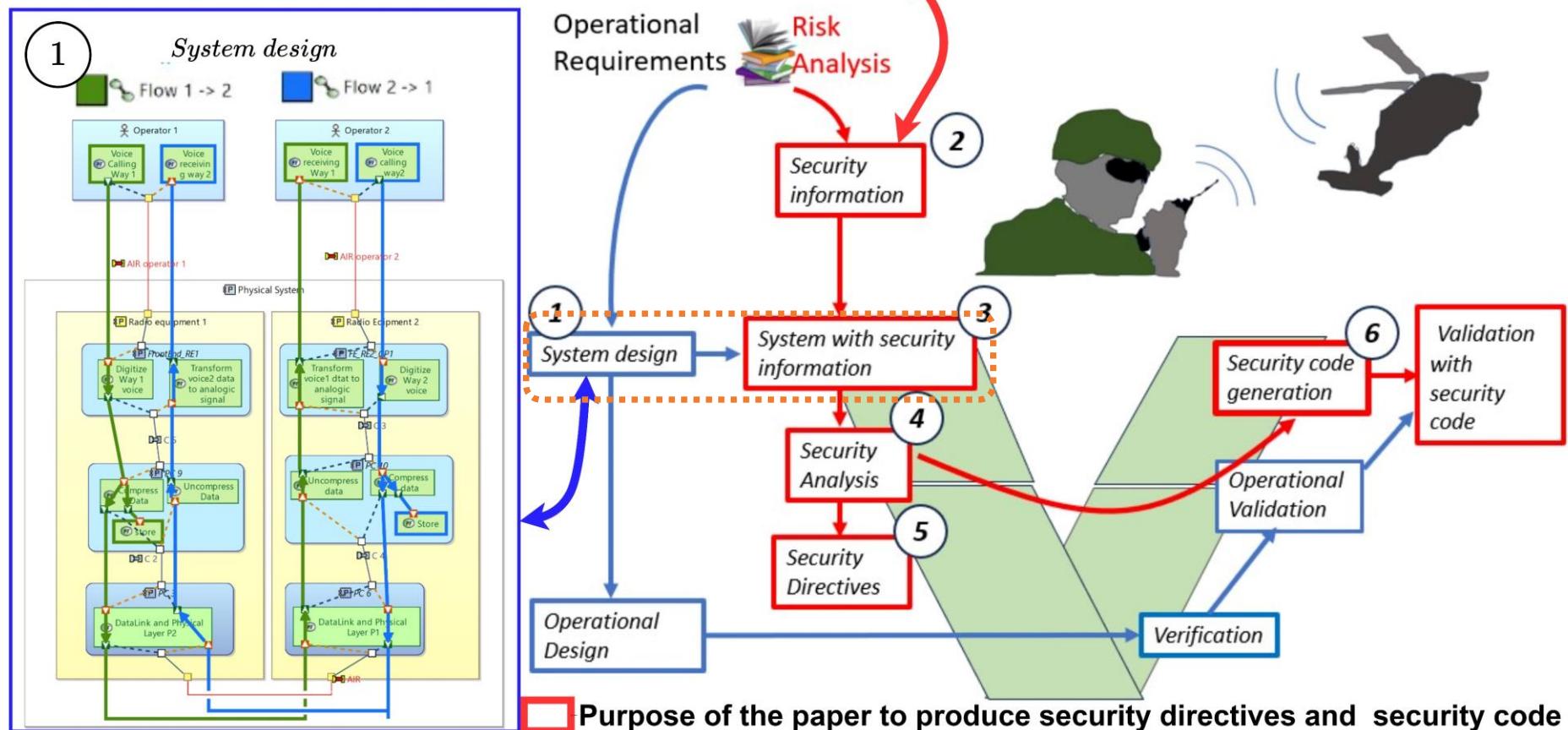
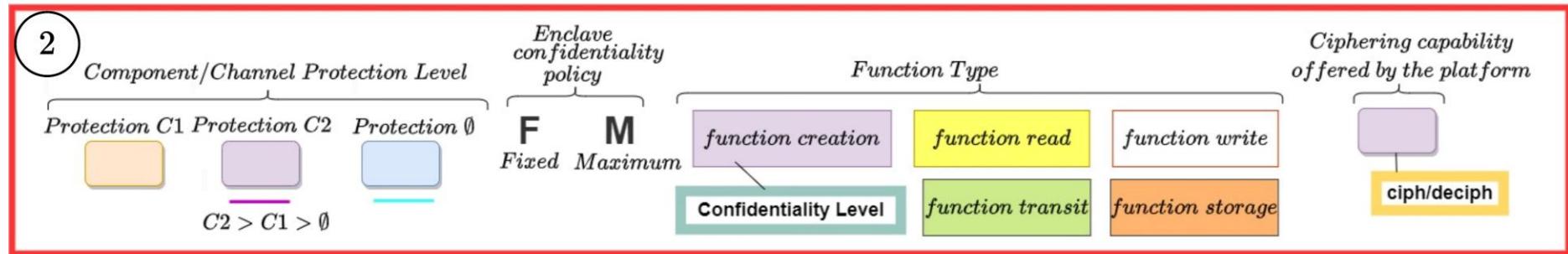
▶ ▶ ▶ *Enclave ciphering capabilities offered*

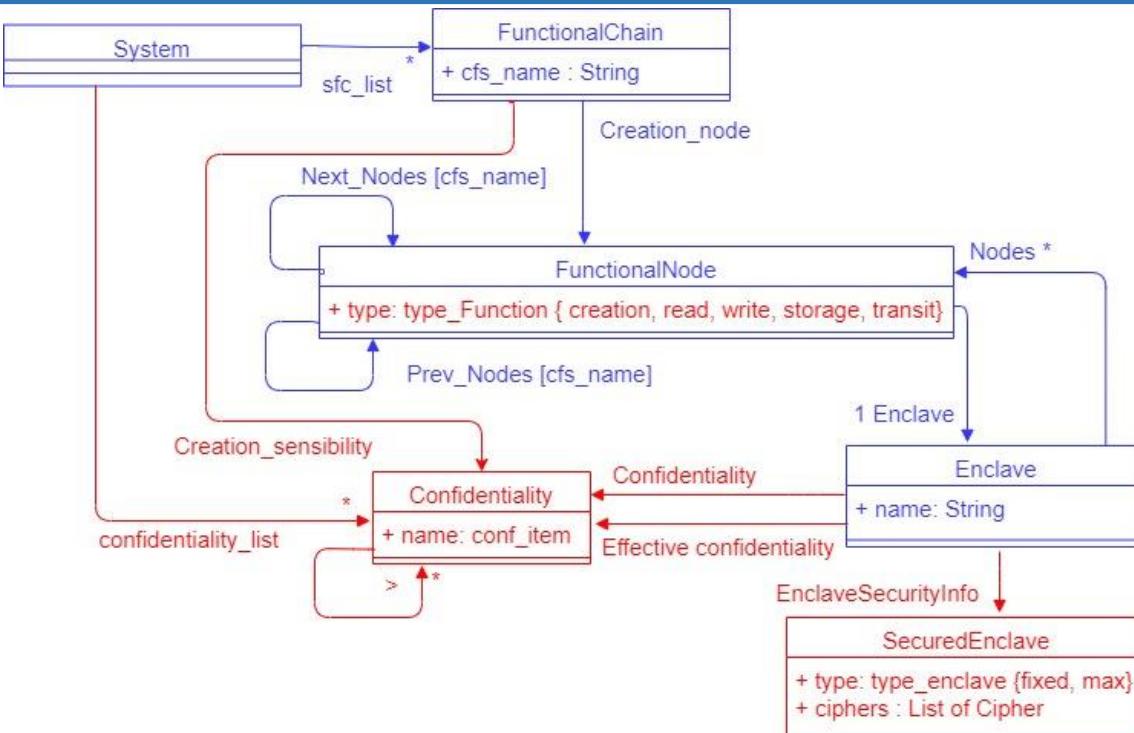
□ □ *Enclave Protection Type (fixed, maximum)*

[f] [f] [f] [f] *Functions status in creation, write, read and Transit*

[f] → [f] → [f] *Functional chain*



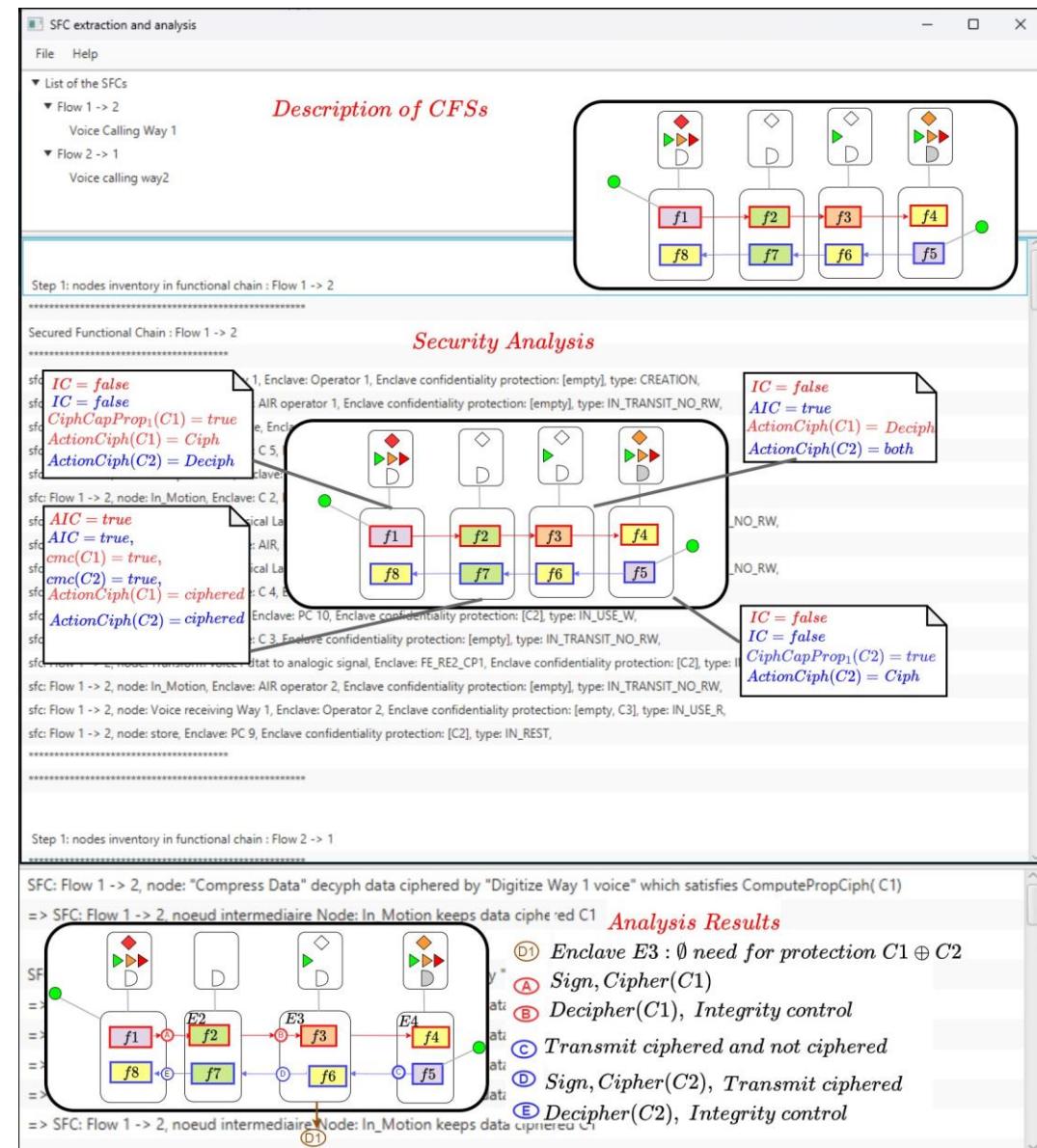




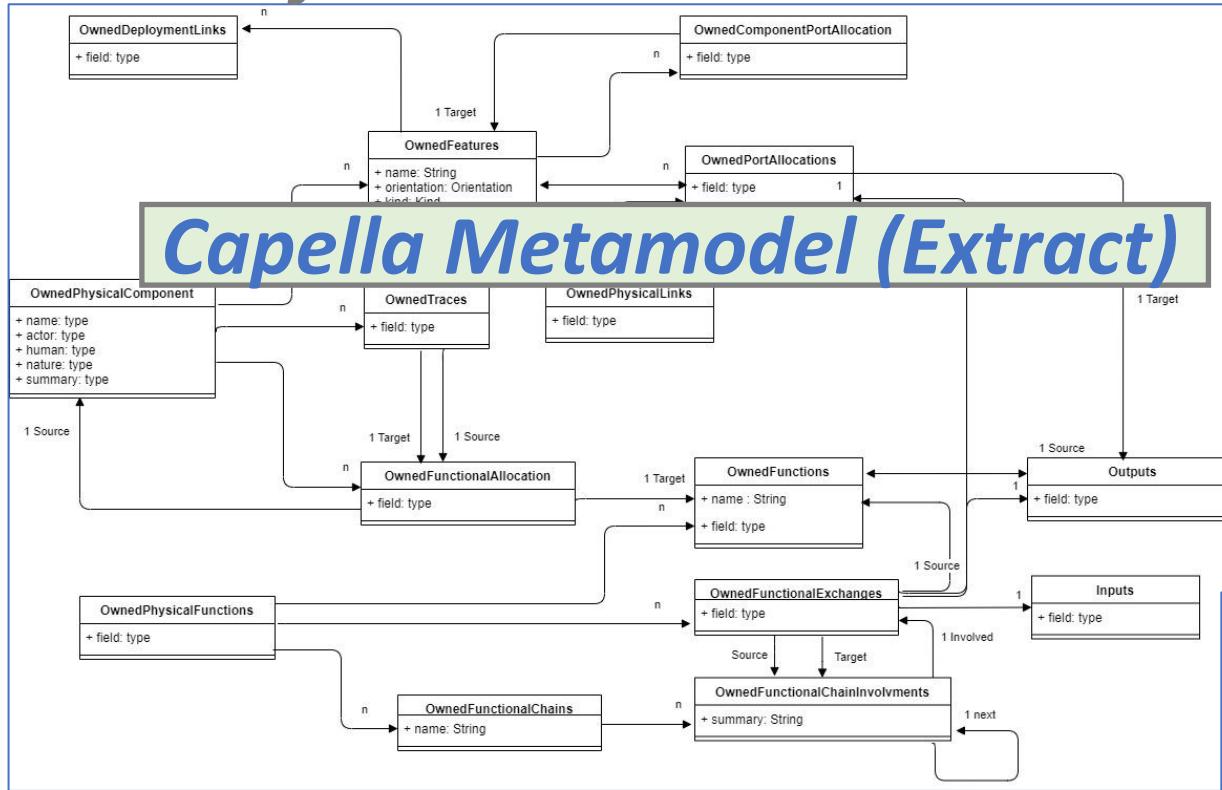
Metamodel of the System as a set of SFCs.

Implemented in the Analysis Tool to generate Security Directives and Security Code.

➤ *Inputs: Stand alone SFC or Labelled Capella Designs.*



Instance of ...

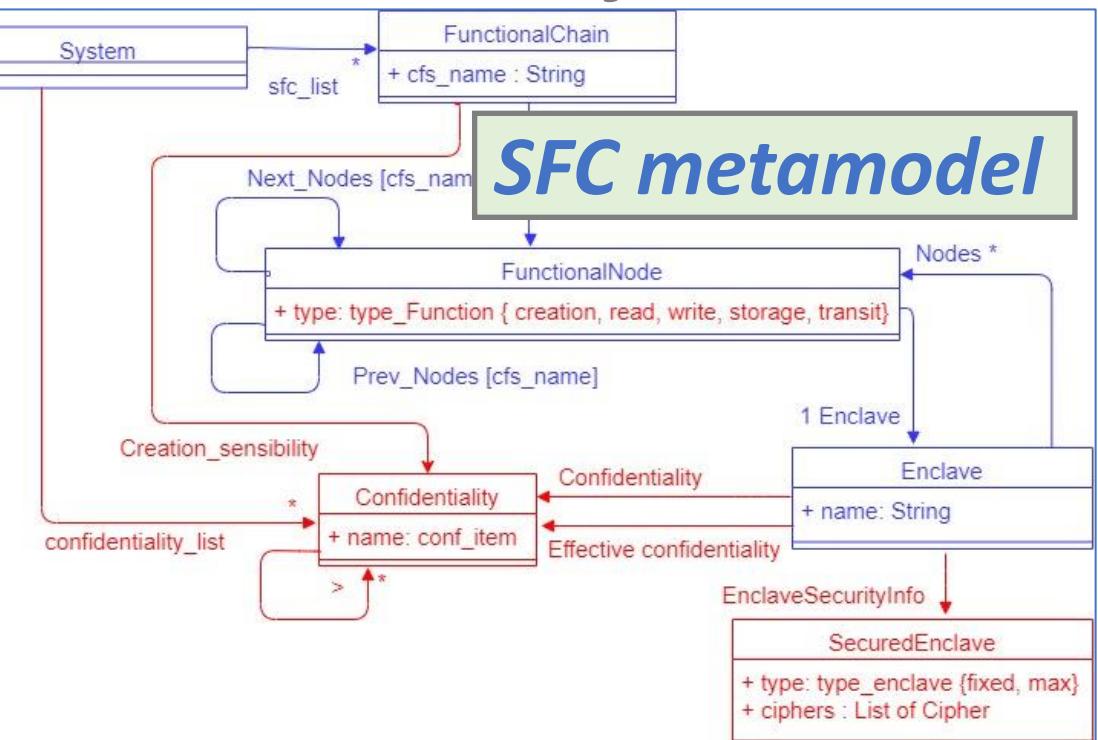


**Model Transformation
(Summary fields exploitation)**

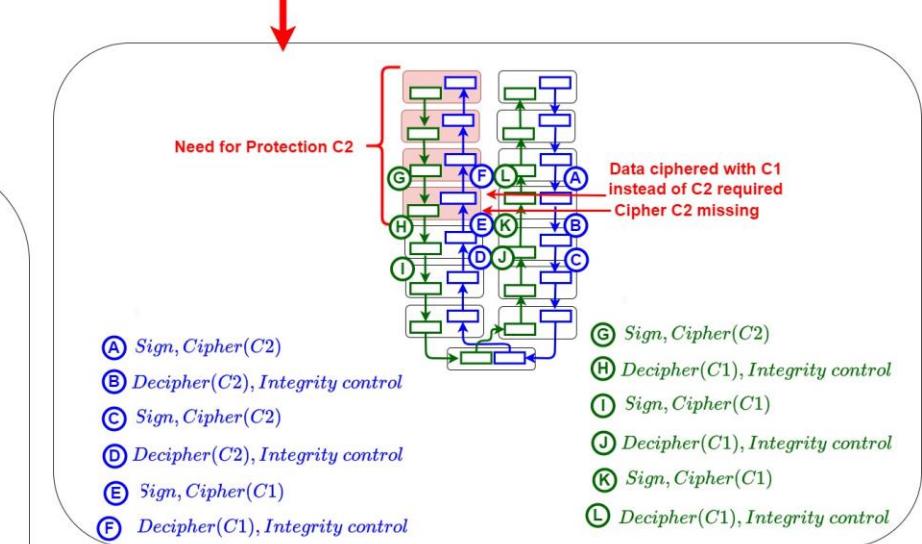
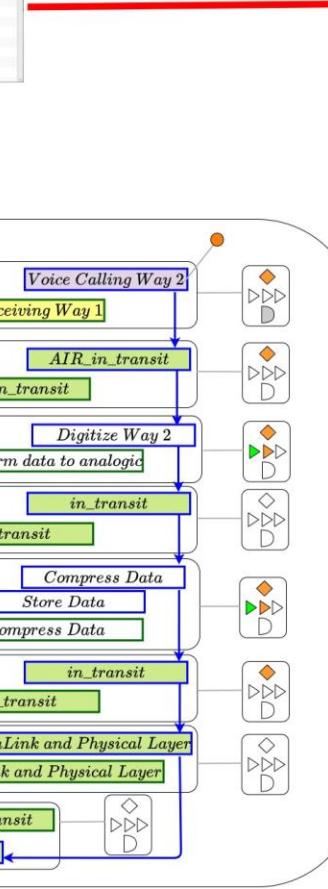
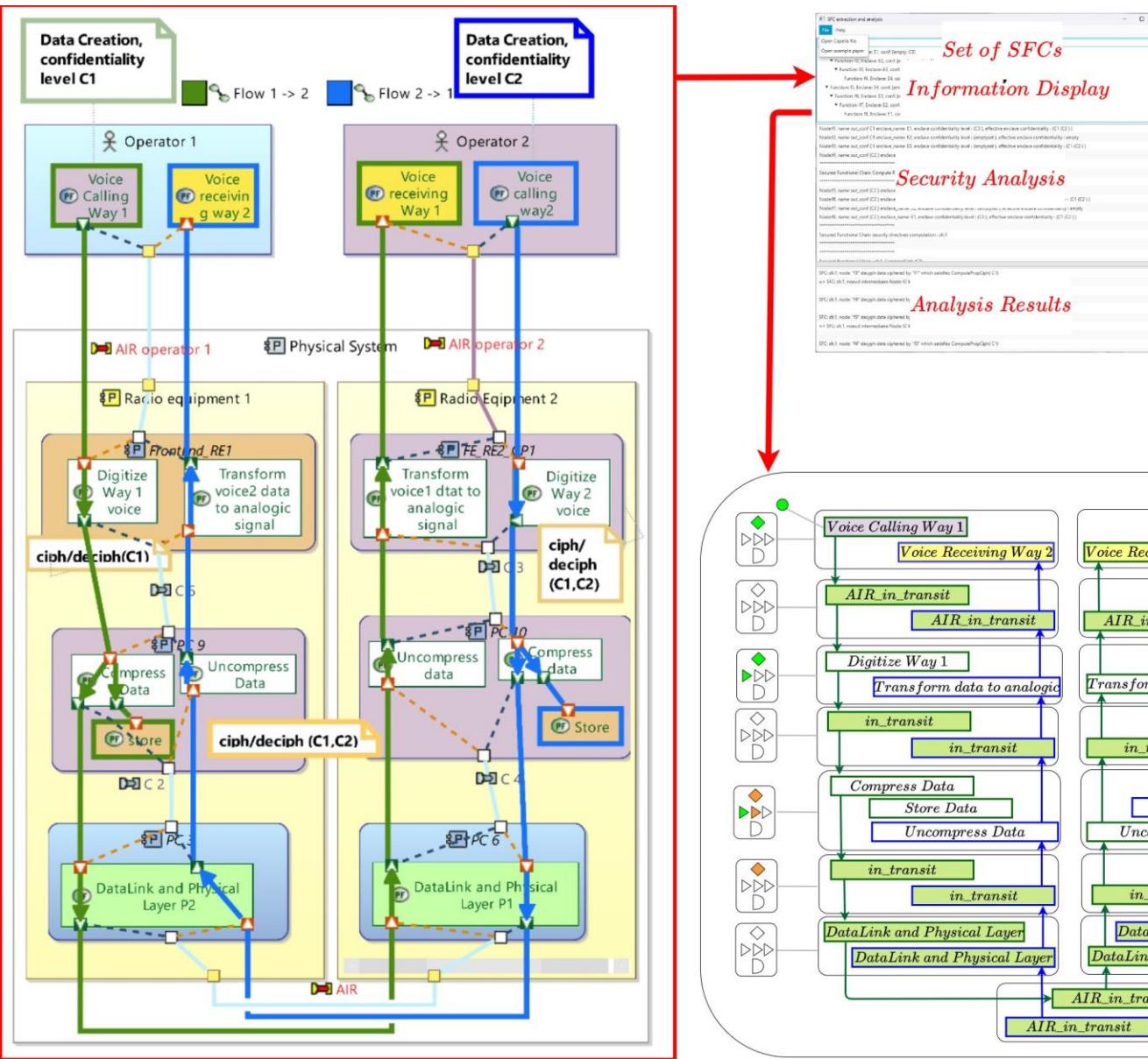
Tool implementation -**ubs**: Analysis From Capella Designs.



... to Instance of



Tool implementation – Analysis From Capella Designs



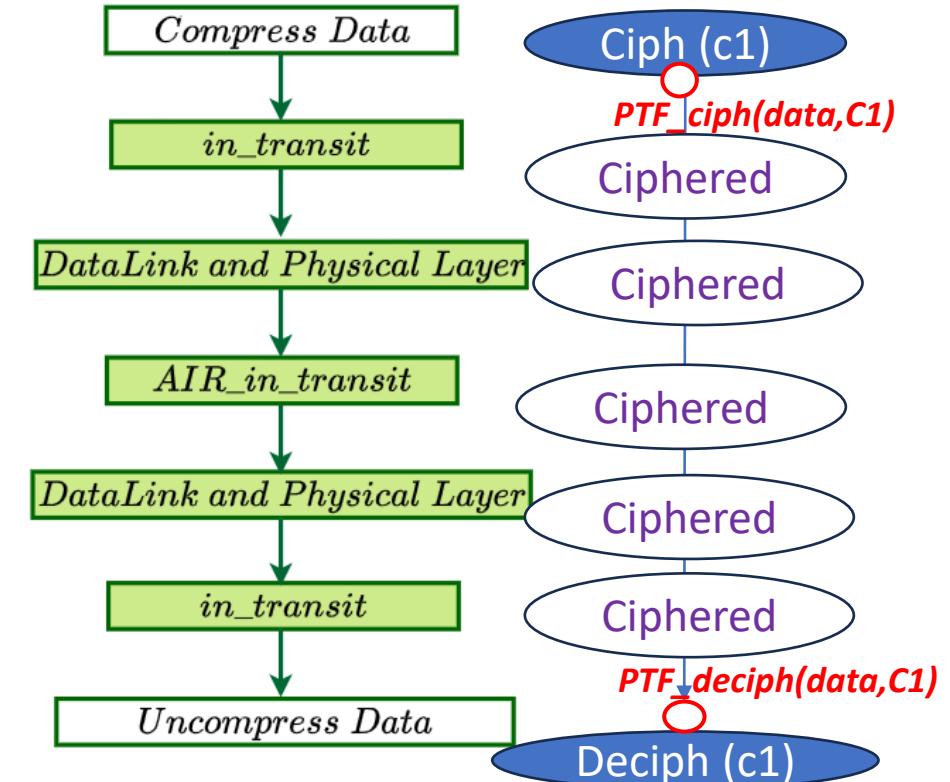
A Short Demo

A Short Demo (analysis)

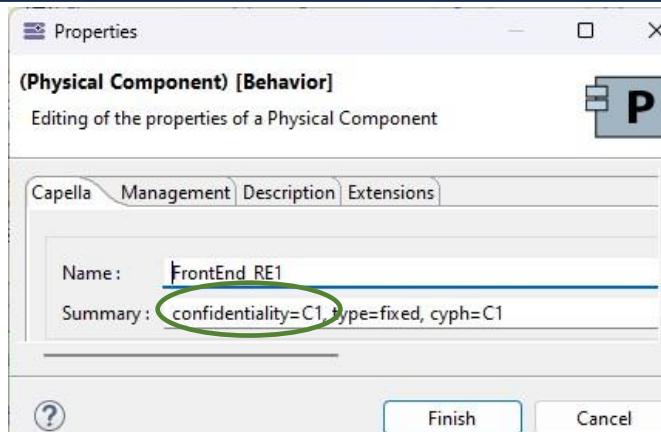
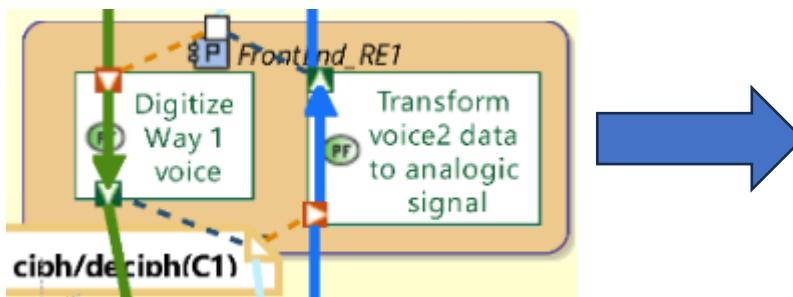
```

node: Compress Data decyph data ciphered by Digitize Way 1 voice which satisfies ComputePropCiph( C1)
noeud intermediaire: Digitize Way 1 voice statut: CIPH
noeud intermediaire: In_Motion statut: CIPHERED
node: Uncompress data decyph data ciphered by Compress Data which satisfies ComputePropCiph( C1)
noeud intermediaire: Compress Data statut: CIPH
noeud intermediaire: In_Motion statut: CIPHERED
noeud intermediaire: DataLink and Physical Layer P2 statut: CIPHERED
noeud intermediaire: In_Motion statut: CIPHERED
noeud intermediaire: DataLink and Physical Layer P1 statut: CIPHERED
noeud intermediaire: In_Motion statut: CIPHERED
node: Transform voice1 ddat to analogic signal decyph data ciphered by Uncompress data which satisfies ComputePropCiph( C1)
noeud intermediaire: Uncompress data statut: CIPH
noeud intermediaire: In_Motion statut: CIPHERED
node: store decyph data ciphered by Compress Data which satisfies ComputePropCiph( C1)
noeud intermediaire: Compress Data statut: CIPH

```

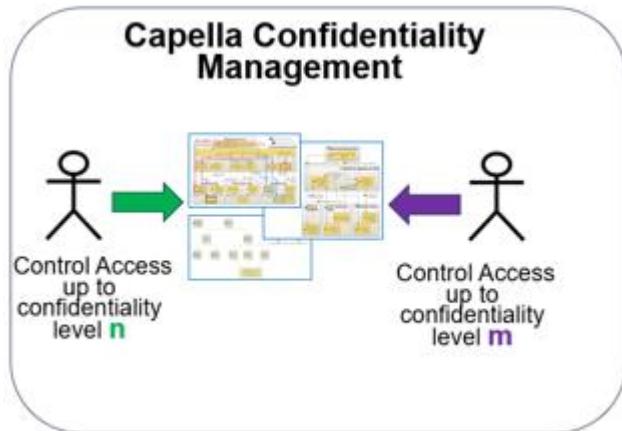


EnclaveFrontEnd_RE1, enclave confidentiality: (C1) enclave effective confidentiality: (C1 (C2))

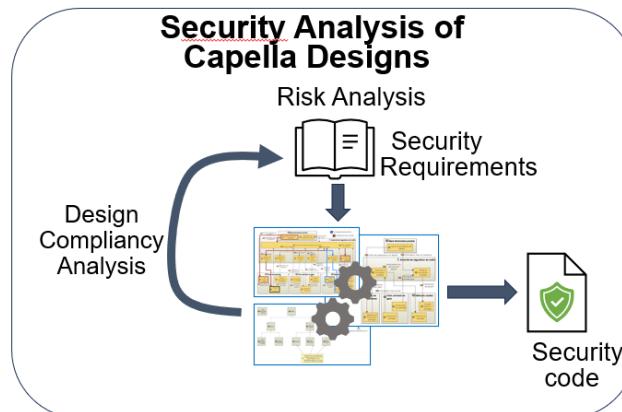


Alert
(needs for **C2** Protection for
EnclaveFrontEnd_RE1)

Perspectives



- Tooling the inter-enclave models inconsistency analysis.
- Variability PLM as a generalization of Confidentiality PLM.



- Demonstrator provision as a paper software artefact.
- Refinement to integrity requirements analysis.
- Securized Architecture Patterns Catalogue.
- Composition and hiding.
- Key Exchange Platform Service.
- Security Code Generation as a Platform Service.

At first glance, **security** management of complex system **prevents the use of MBSE** (confidentiality constraints , complexity to elicit, label and exploit information of security requirements, composability and hiddening of sensitive internal behaviors).

These drawbacks are **raised** and **solved** in this presentation, with an application in a POC applied to Capella designs.

Security Management of critical complex systems may finally become an « ideal » use case for MBSE adoption.

Thank you for your attention

Contact: Michel.Bourdelles@univ.ubs.fr