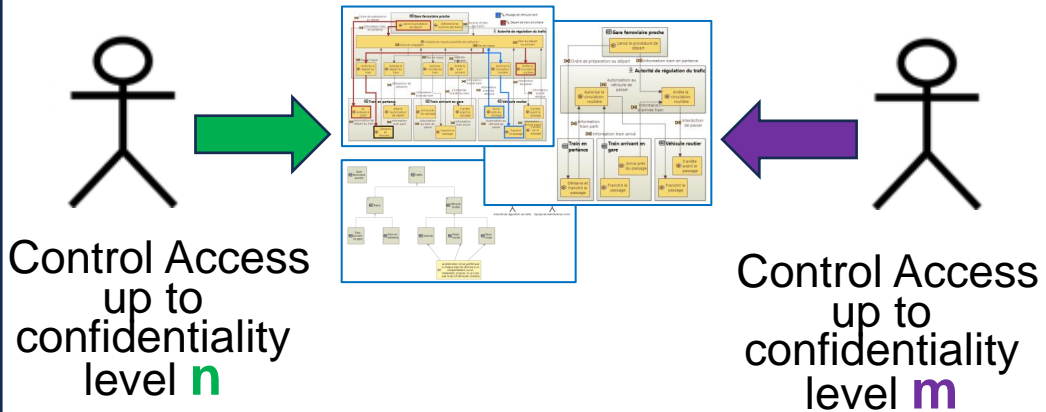


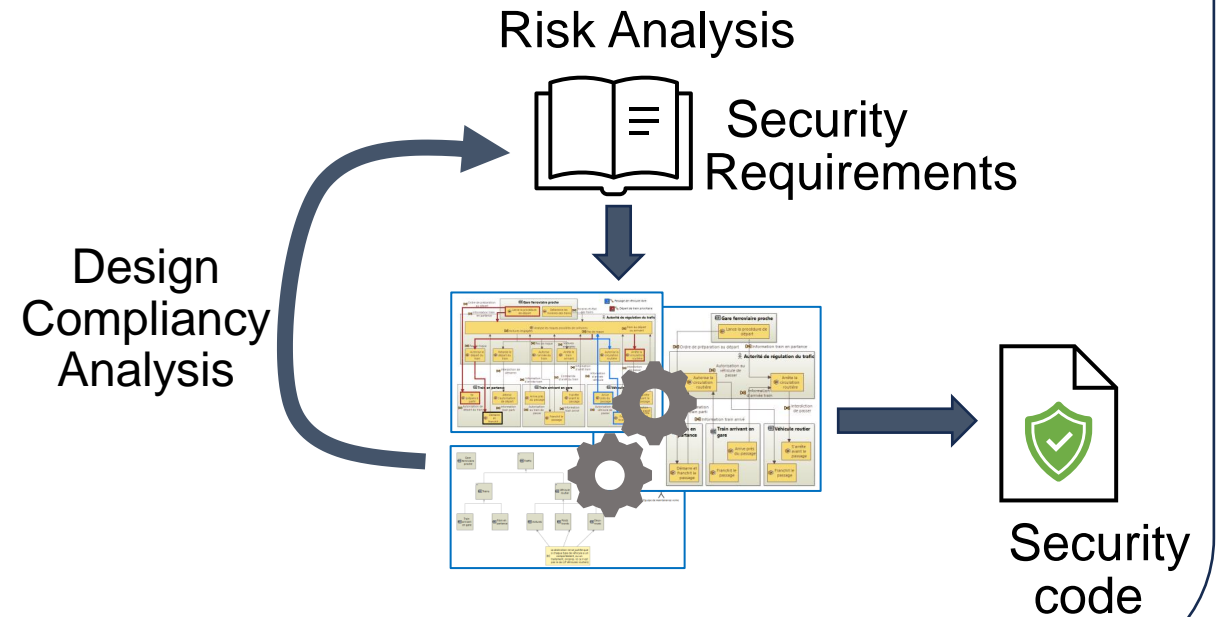
# MBSE Confidentiality Management and Security Analysis of Capella Designs

Michel Bourdellès  
Univ. Bretagne Sud  
Vannes, France  
[michel.bourdelles@univ-ubs.fr](mailto:michel.bourdelles@univ-ubs.fr)

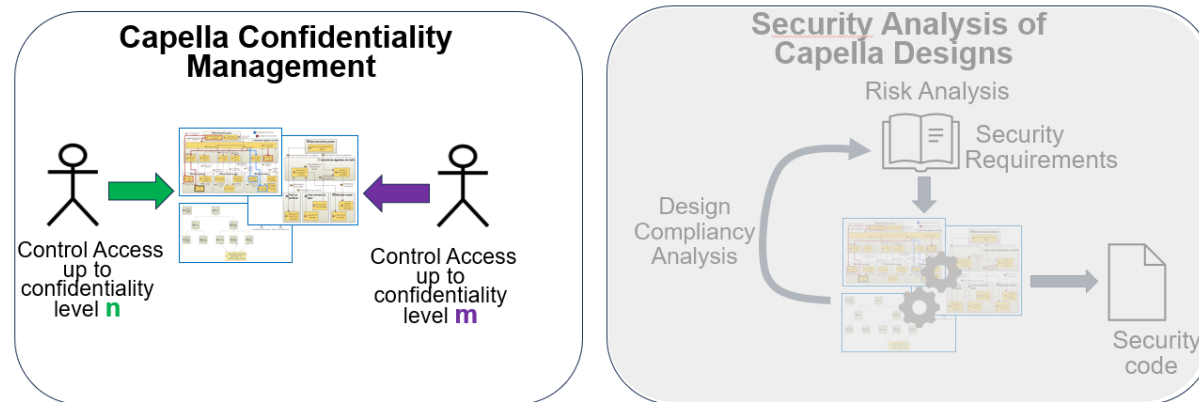
## Capella Confidentiality Management



## Security Analysis of Capella Designs



# 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.

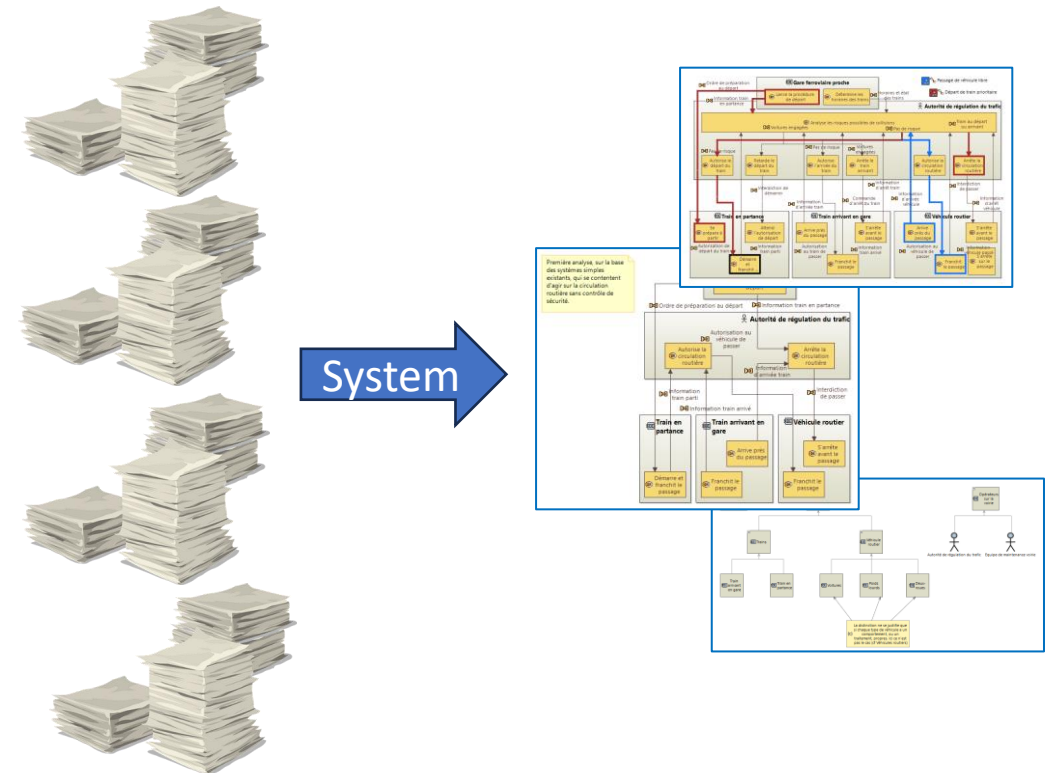
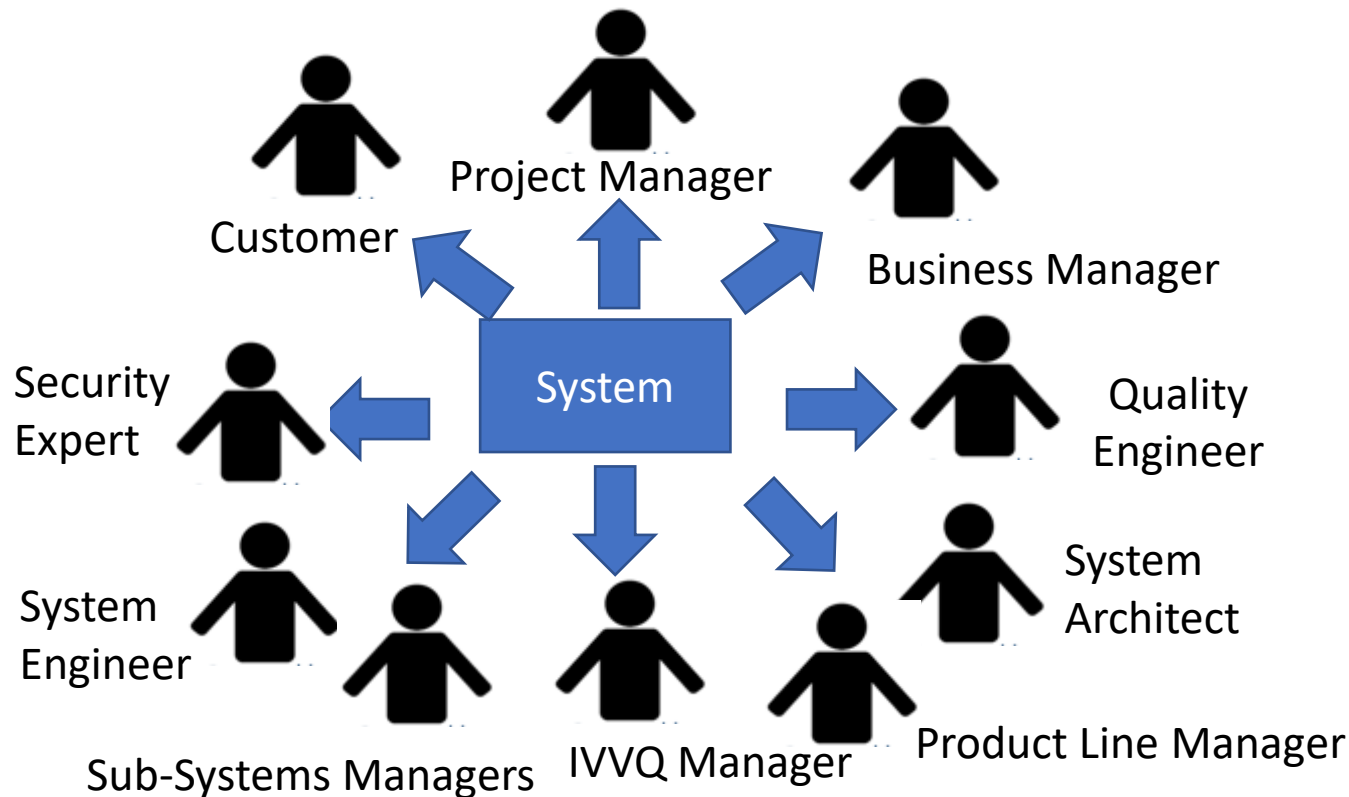


**Such cumbersome Project Management becomes a MESS.**



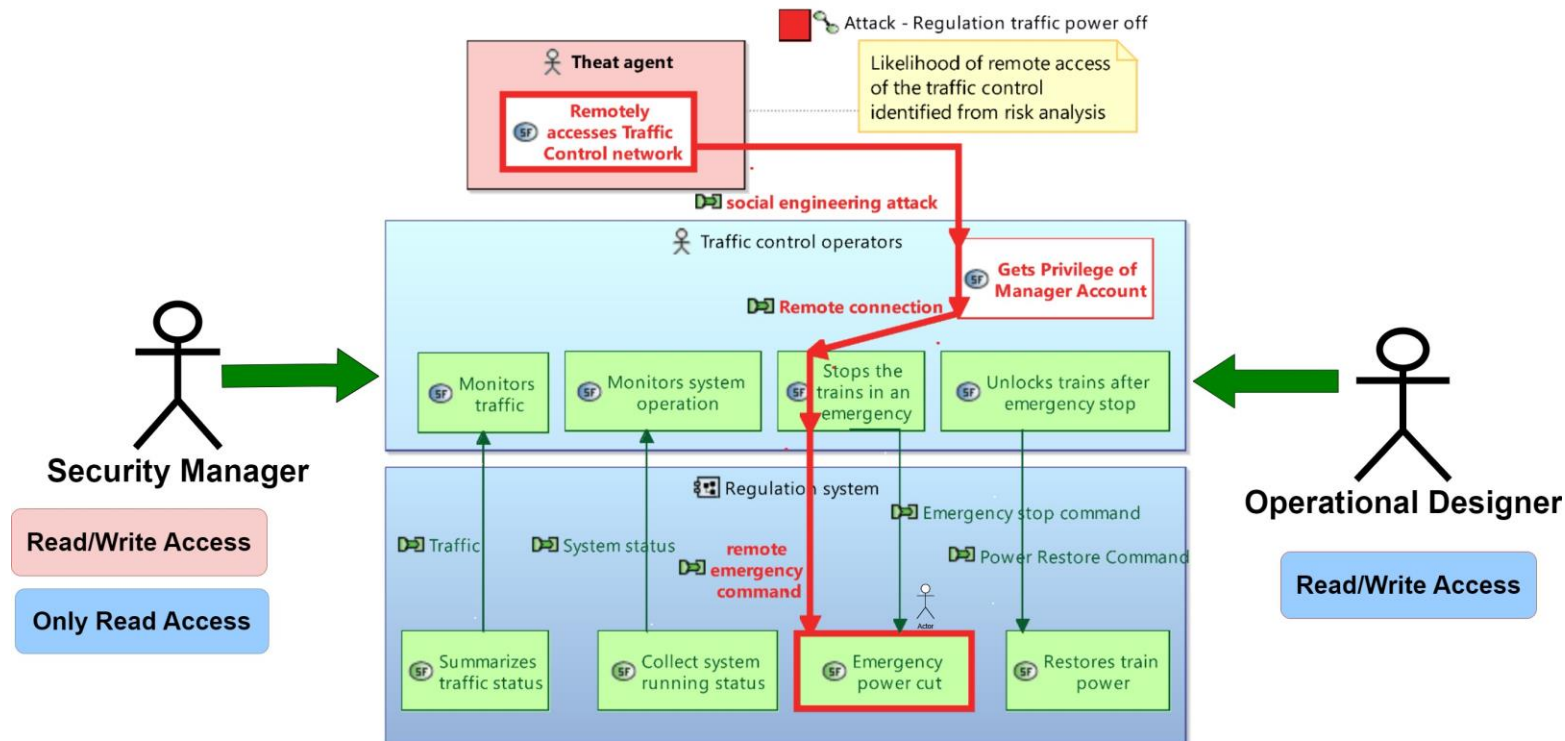
## Industrial Proposal: Moving from Document Driven Process to Modelling Driven Process [INCOSE – Prospective 2030 recommendation]

- 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](http://mbse-capella.org)*

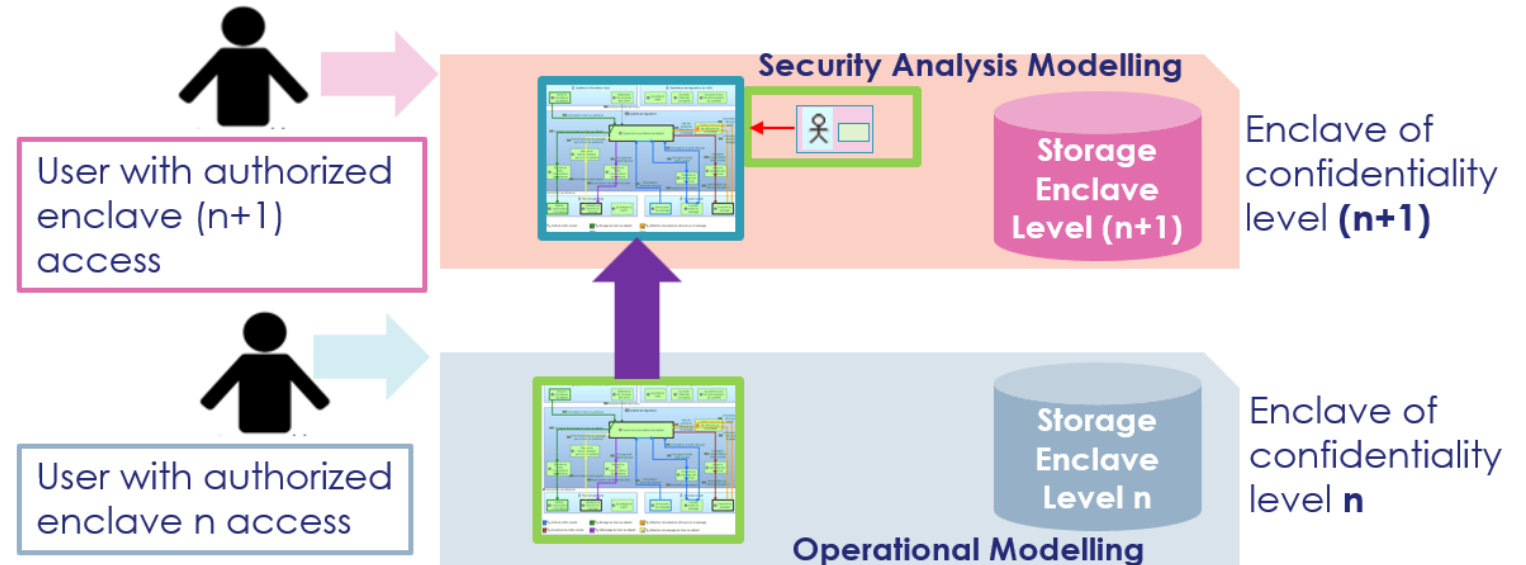
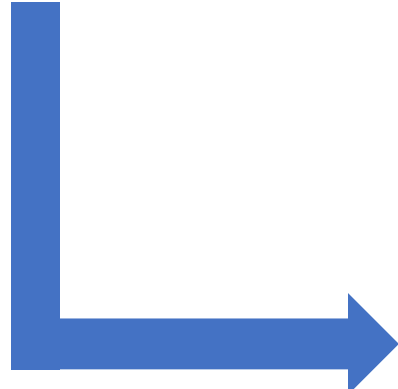
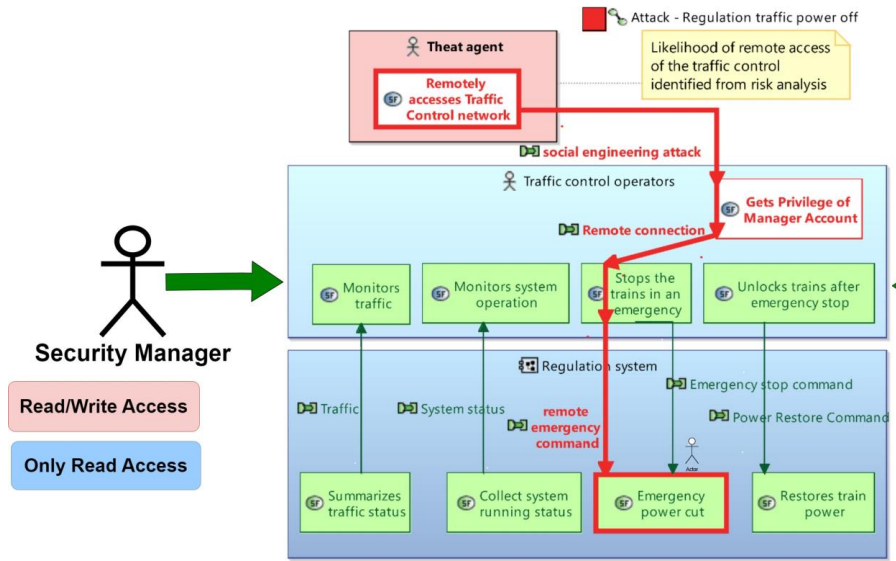
- ✓ Confidentiality, Integrity, Consistency
- ✓ No leak
- ✓ Storage confidentiality
- ✓ No manual labelling
- ✓ Iterative Design Flow Compliance
- ✓ Genericity of the Solution



## Main Ideas :

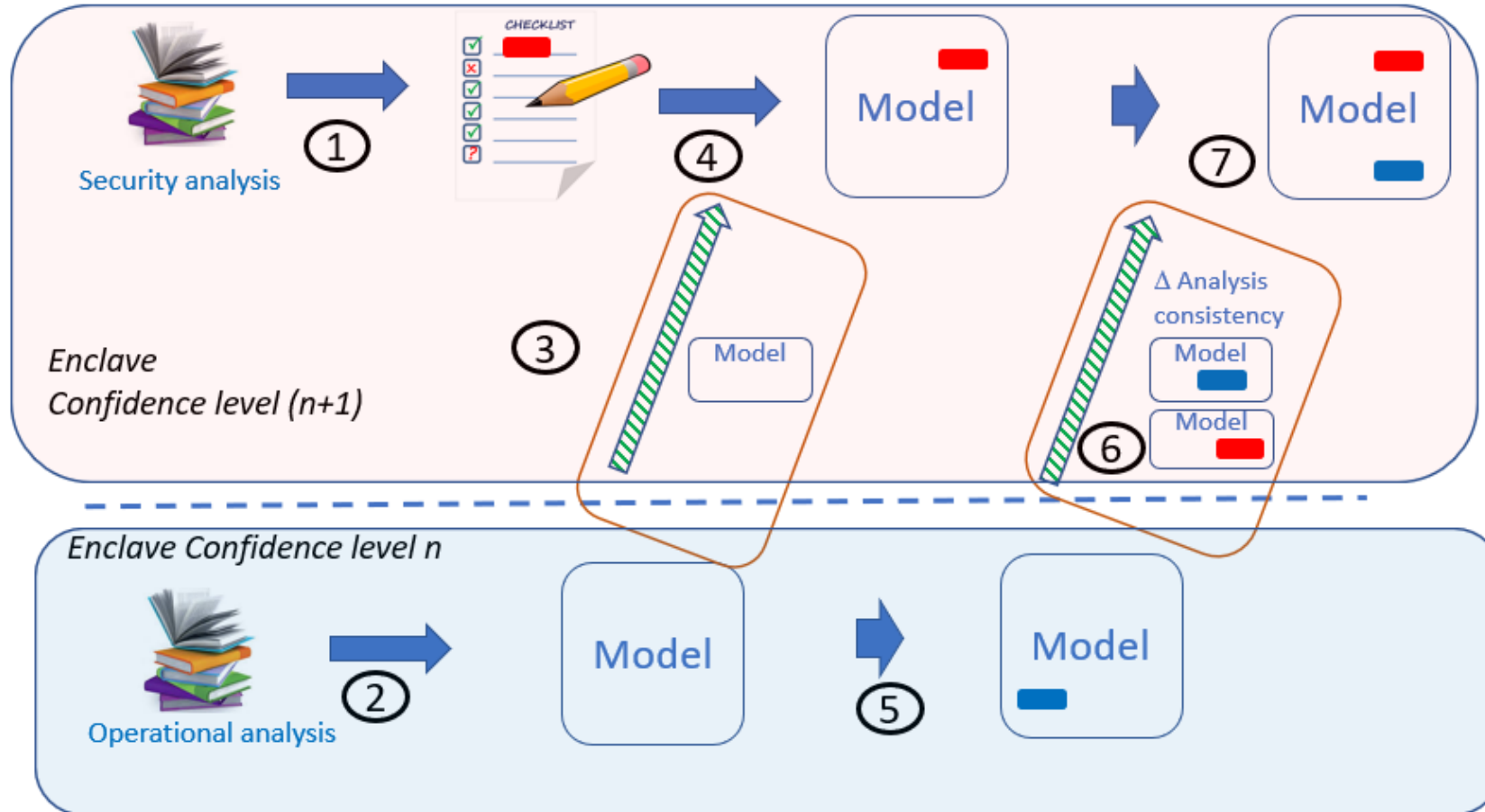
- Enclave Separation with Access Control
- Apply the Bell-Lapadula Principles


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




Read only access     Read/write access



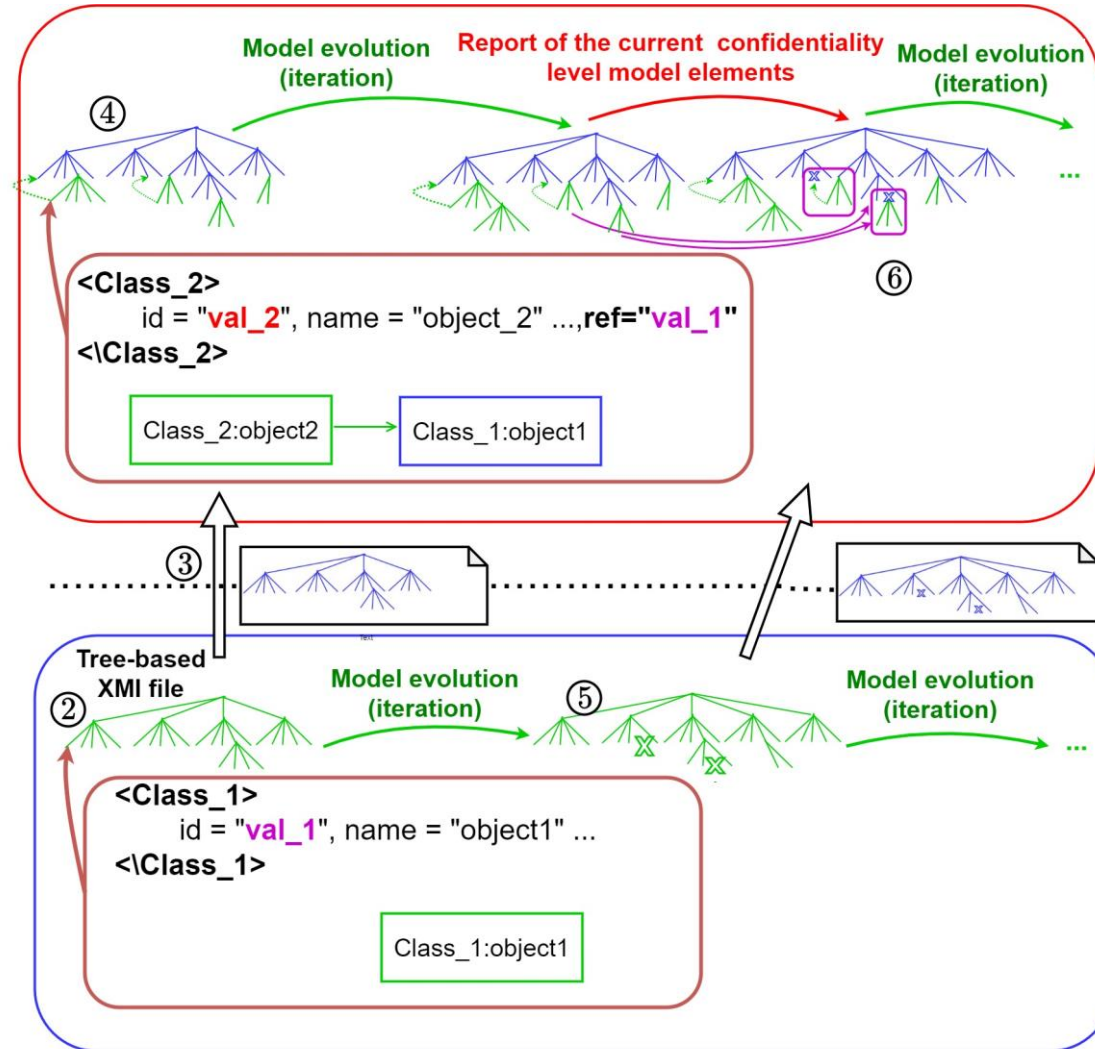
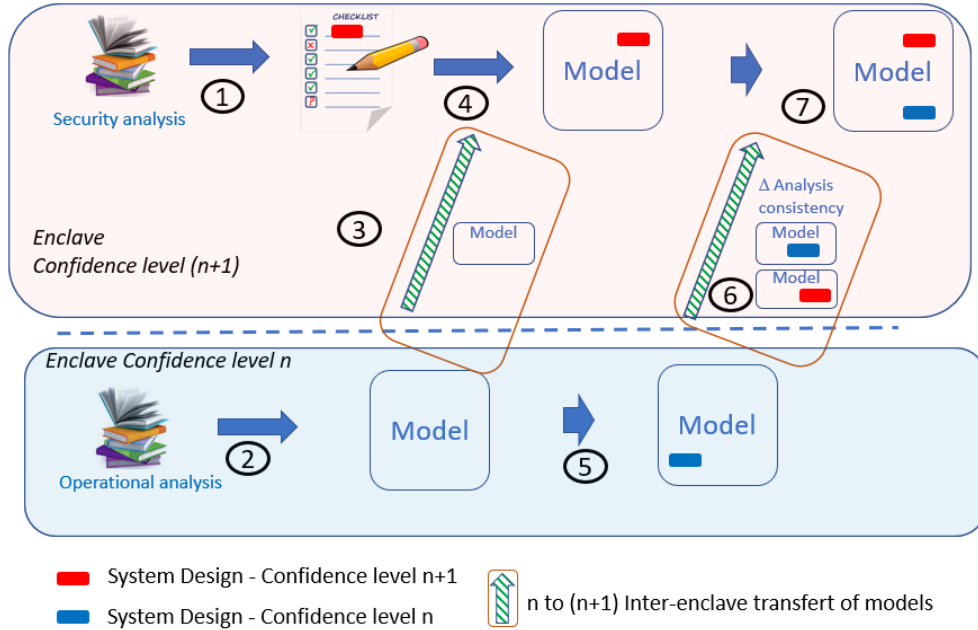


 System Design - Confidence level n+1

 System Design - Confidence level n



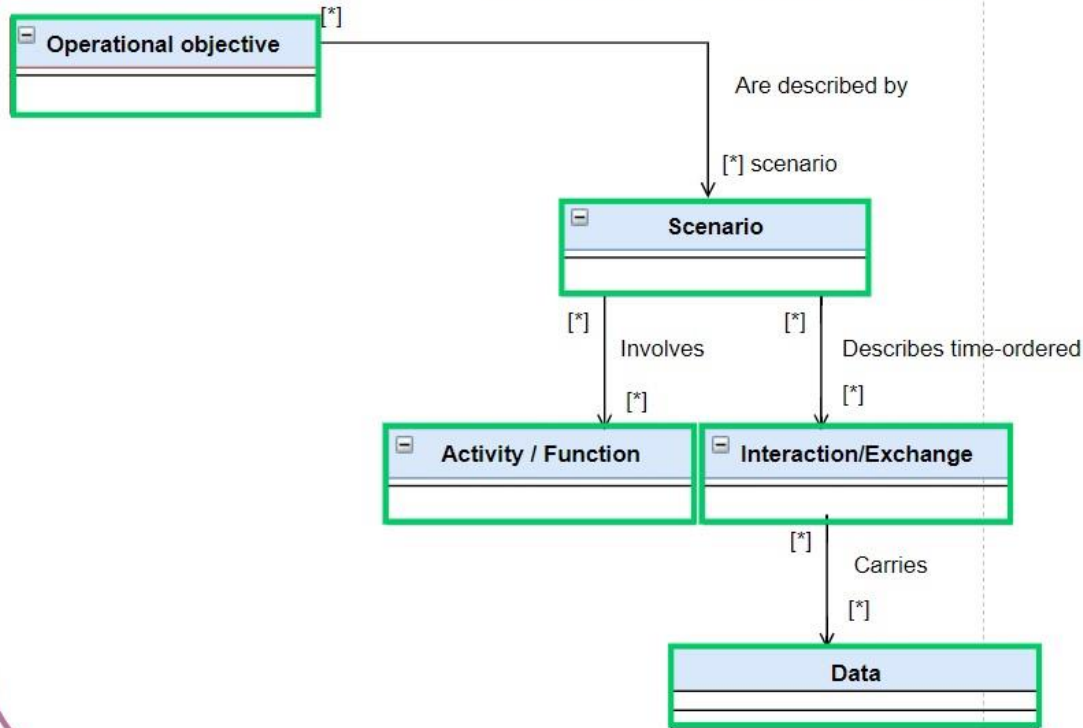
n to (n+1) Inter-enclave transfert of models



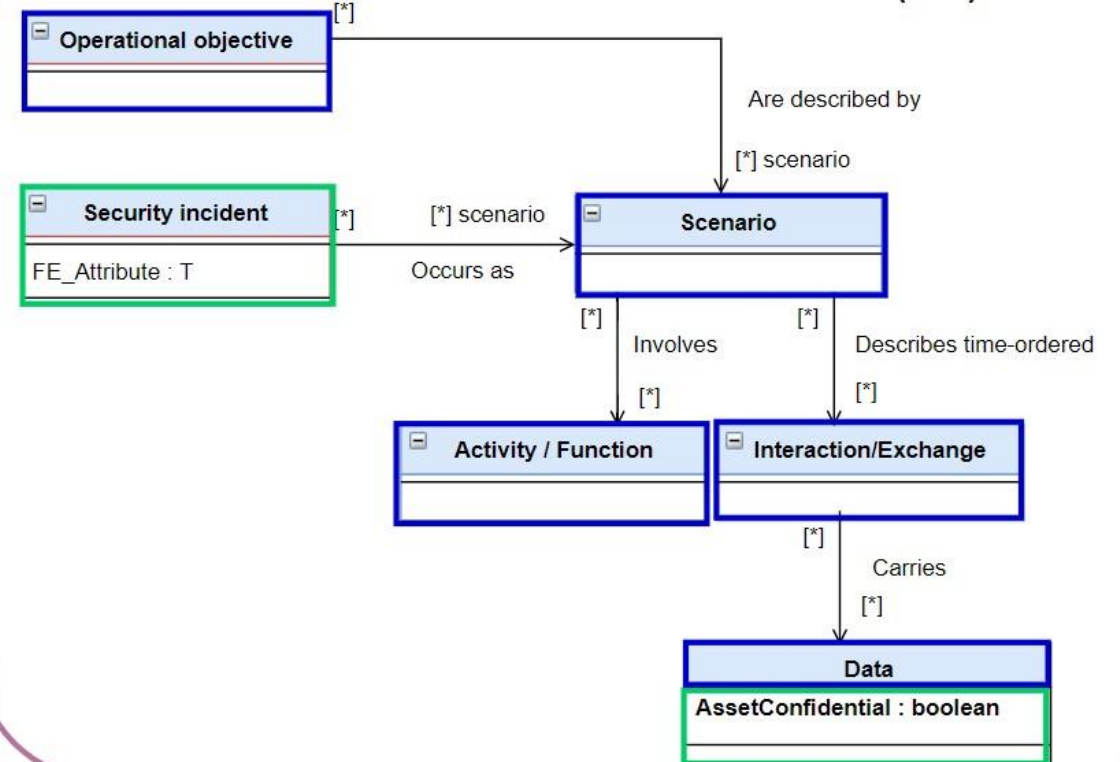
- Read-write part of tree-based xmi file
- Read-only part of tree-based xmi file
- XMI file element suppression
- Inconsistency Identified by structural analysis due to XMI file element suppression



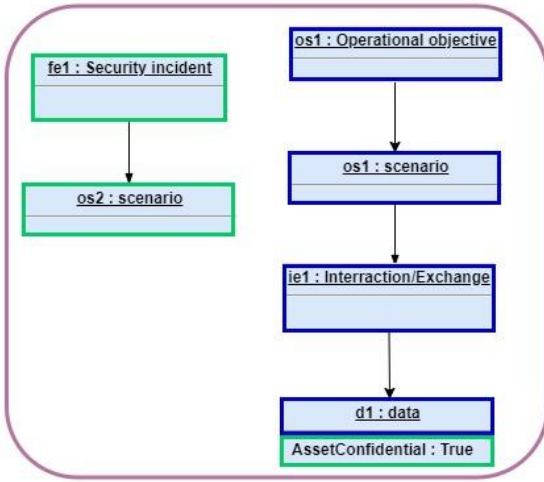
Metamodel of enclave level n



Metamodel of enclave level (n+1)

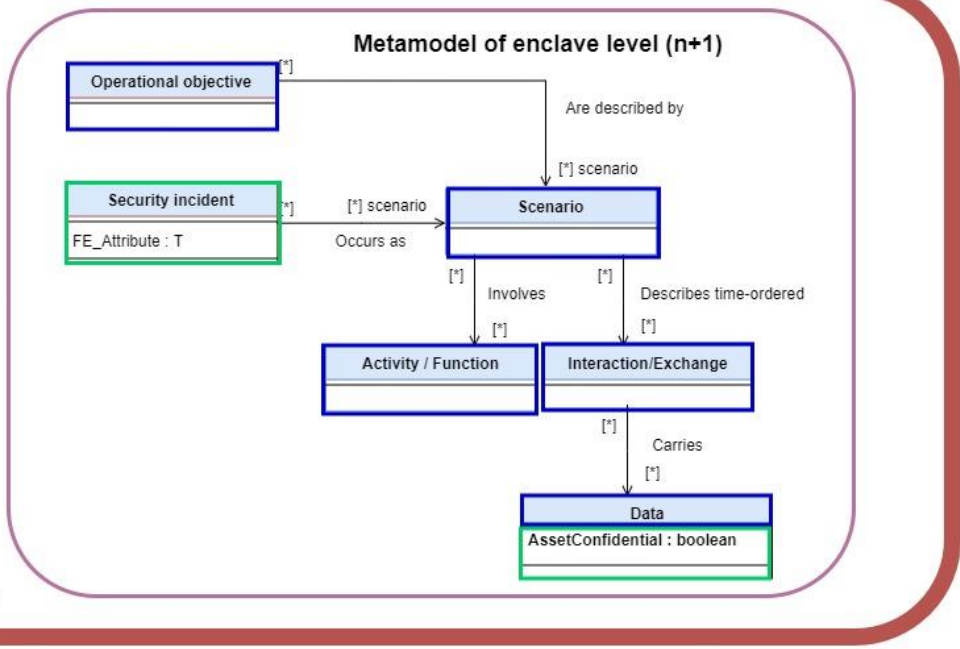


Read /Write Access     Only Read Access



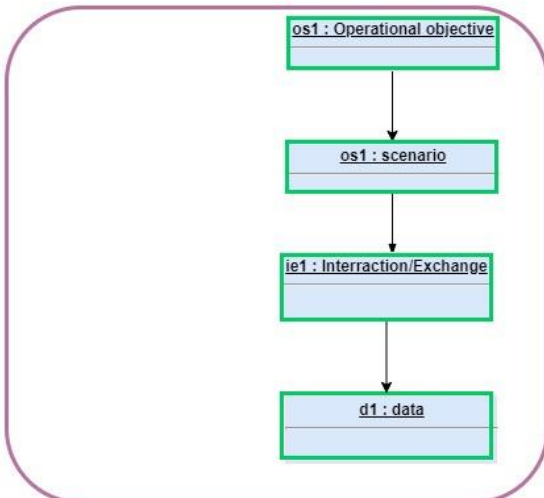
Enclave confidence level (n+1)

instance of

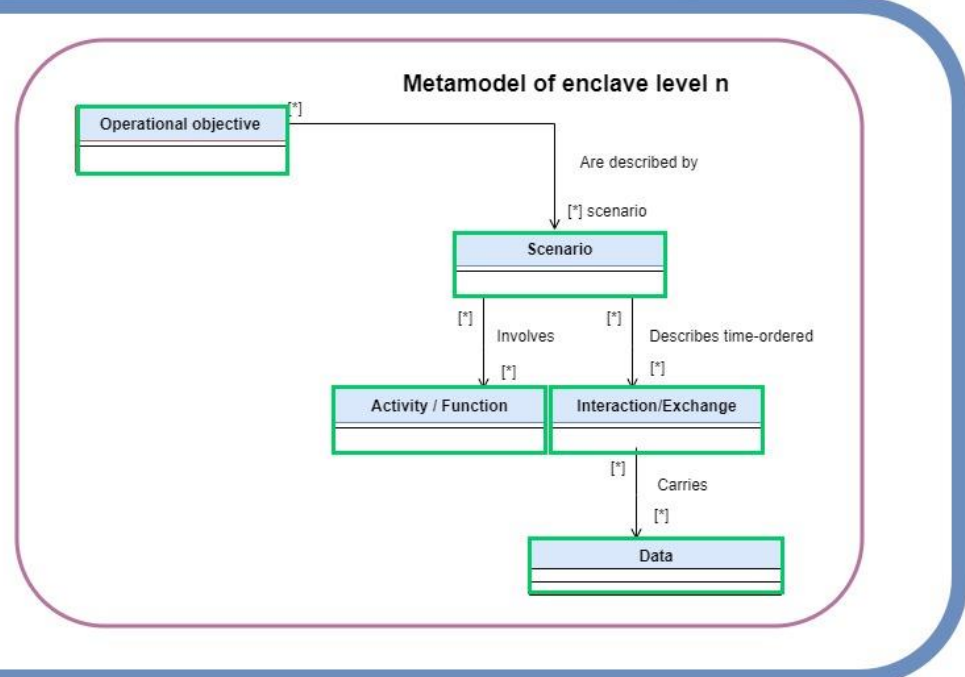


n to (n+1) Inter-enclave transfert of models

Enclave confidence level n

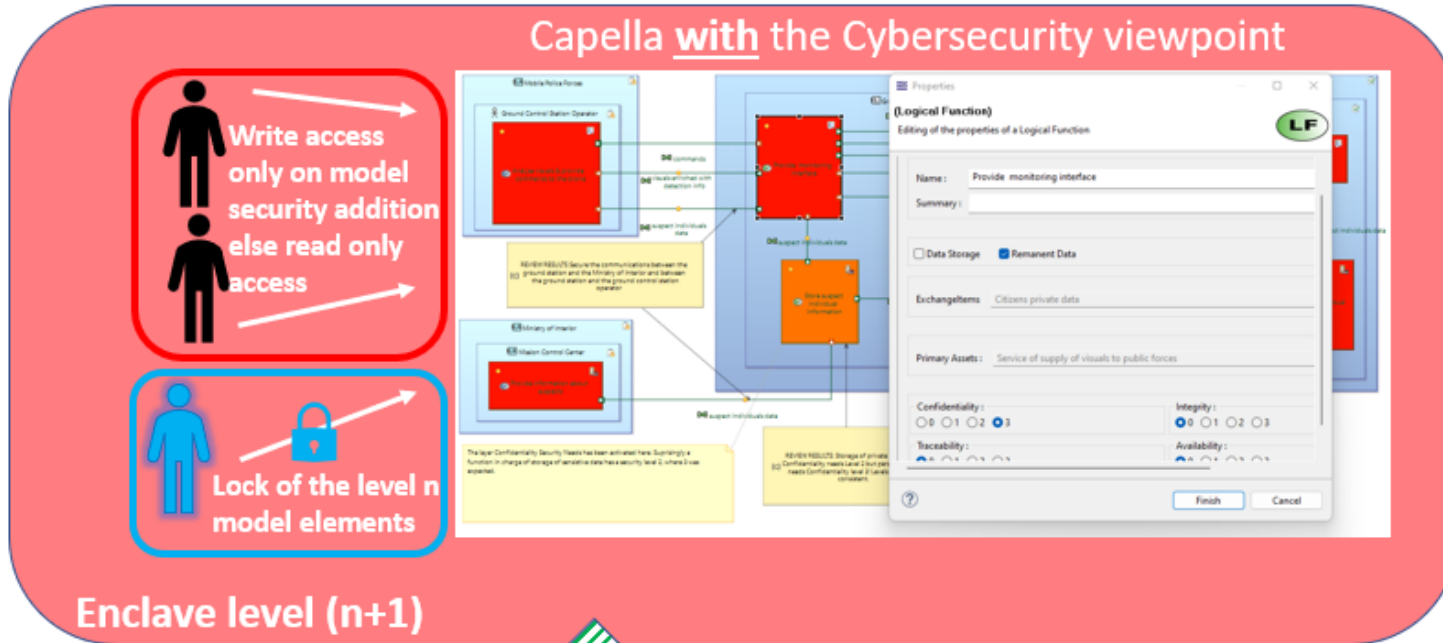


instance of

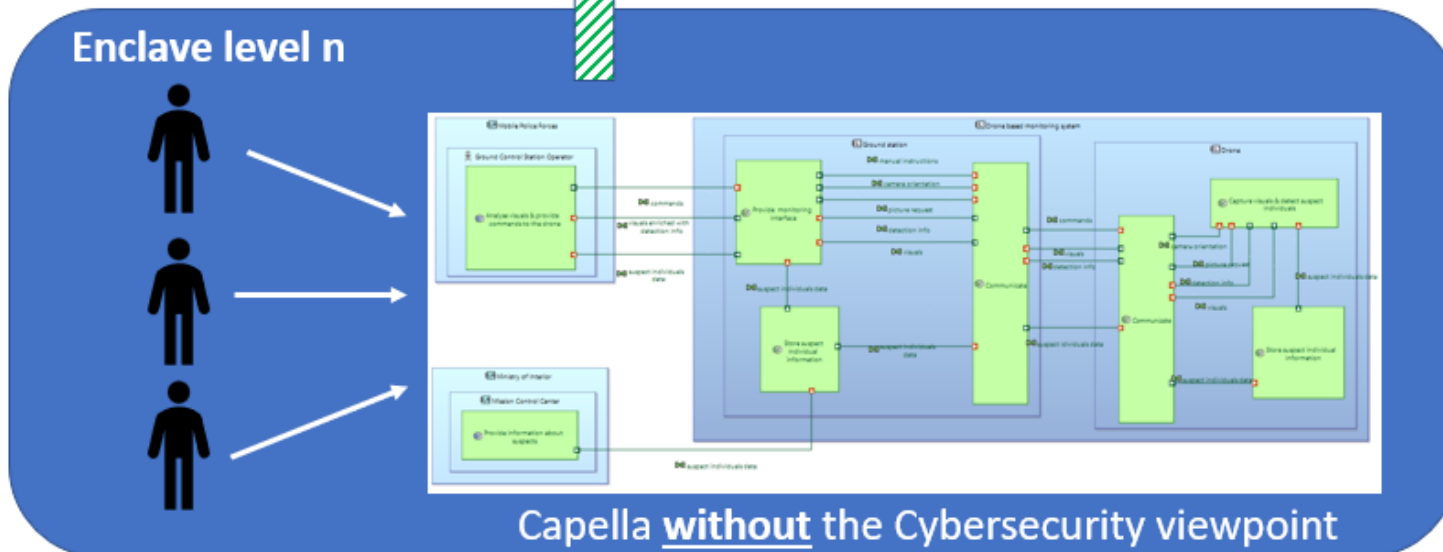


Application  
Example  
(3/3)












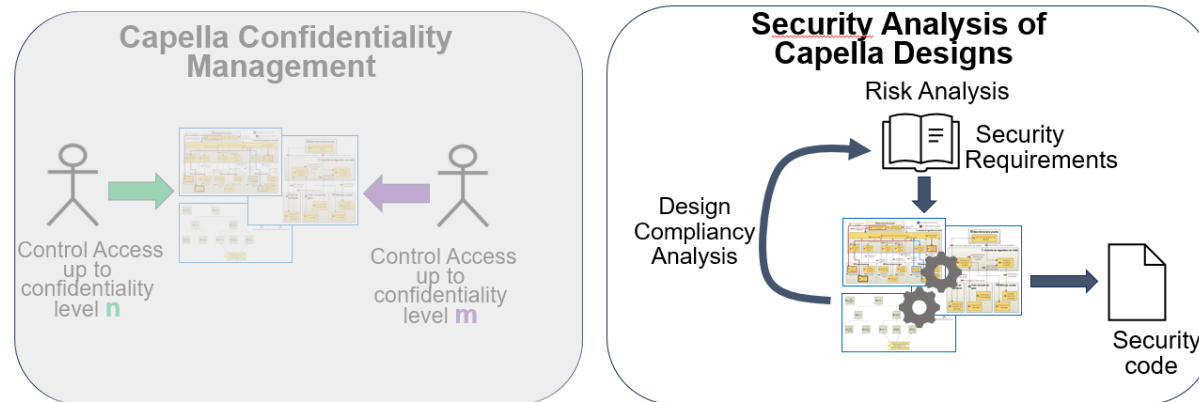
transfer of the XMI level n model





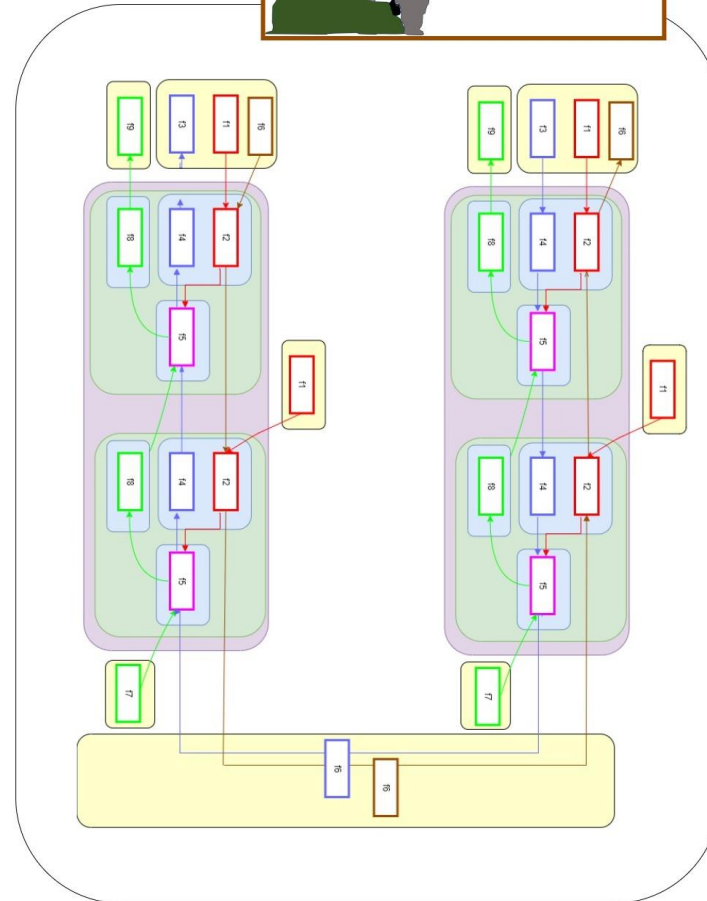
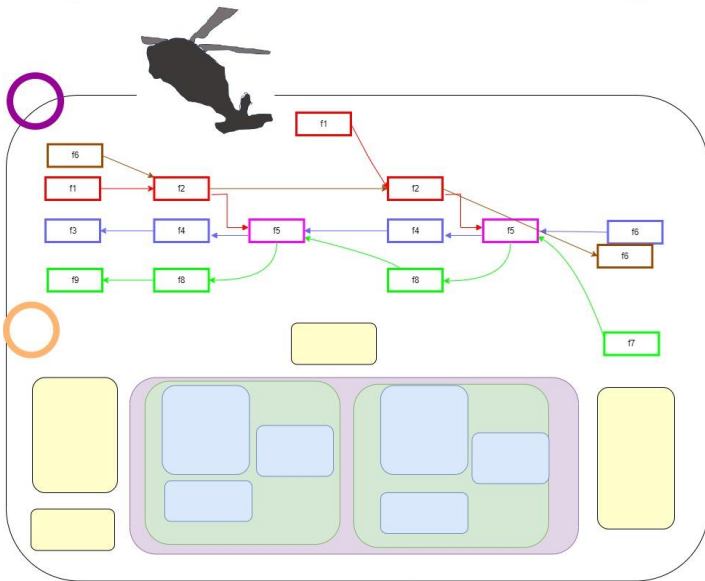
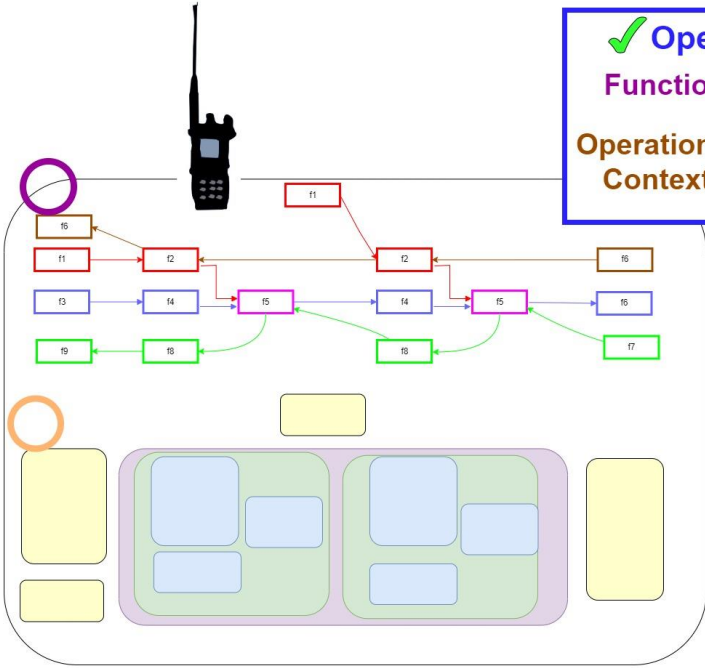
- ***Solution for the Complex Systems Design Confidentiality Management***
- ***Assessment Criteria:***
  - ✓ Confidentiality, Integrity, Consistency 
  - ✓ No leak 
  - ✓ Storage confidentiality 
  - ✓ No manual labelling 
  - ✓ Iterative Design Flow Compliance 
  - ✓ Genericity of the Solution 
  -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

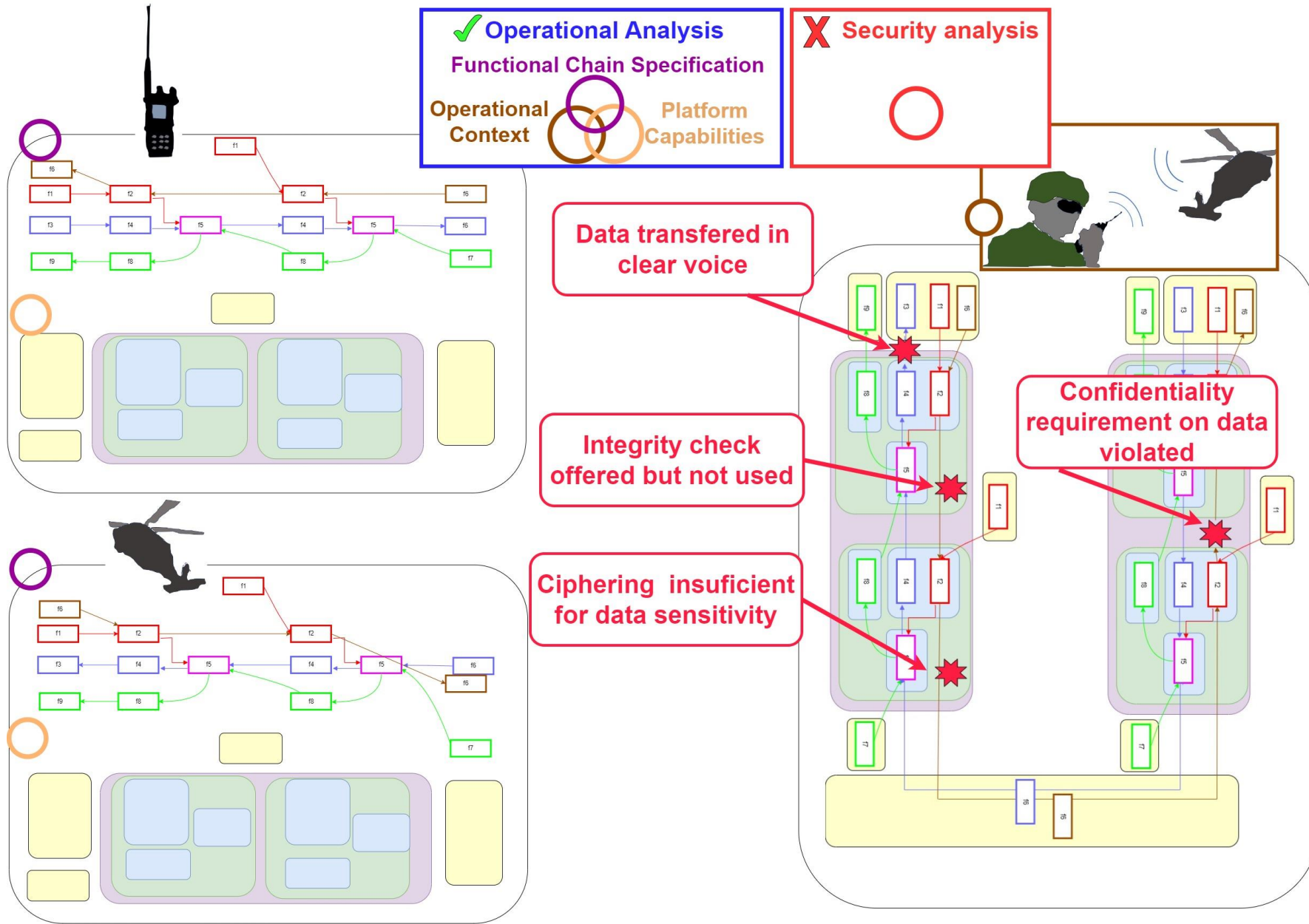
# MBSE Confidentiality Management and Security Analysis of Capella Designs



✓ Operational Analysis  
Functional Chain Specification

Operational Context      Platform Capabilities





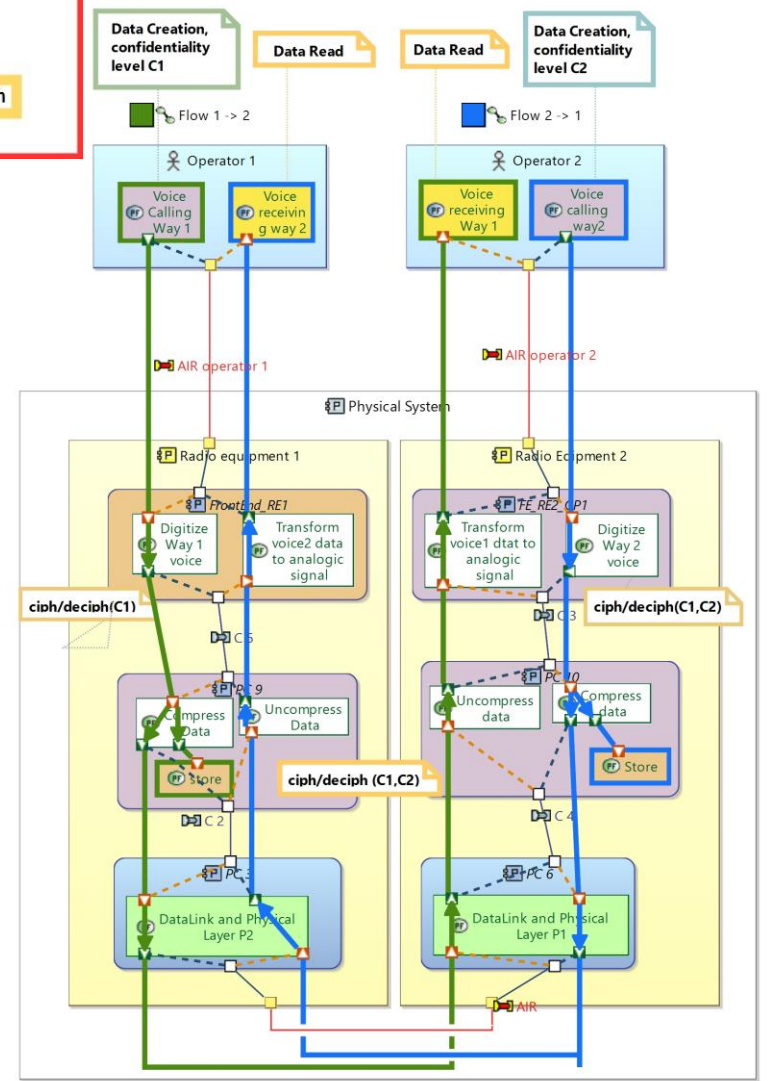
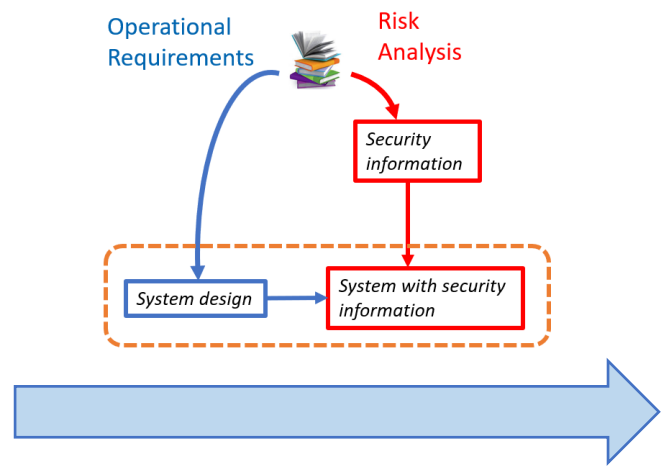
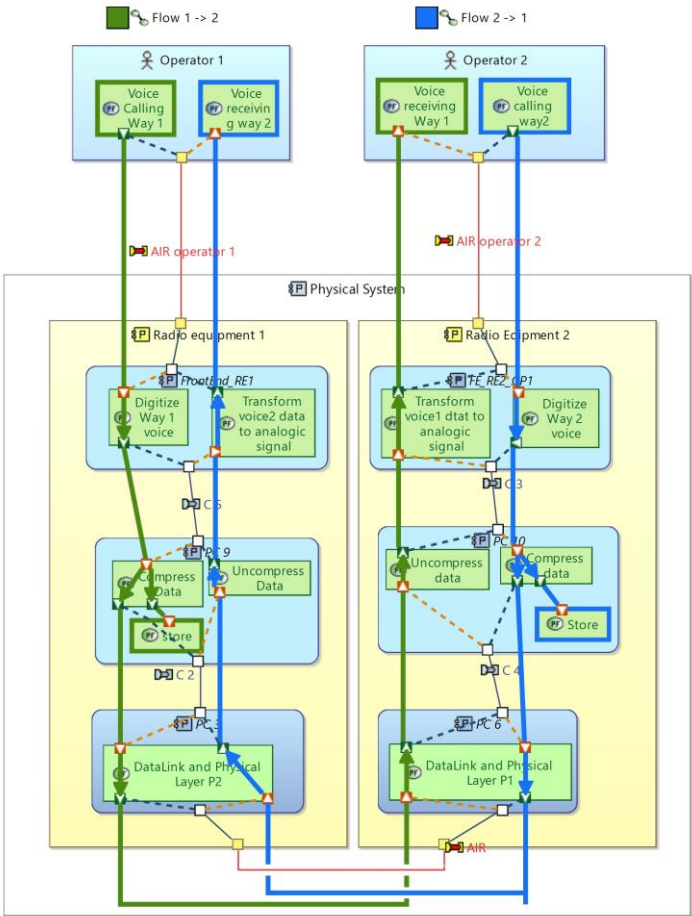
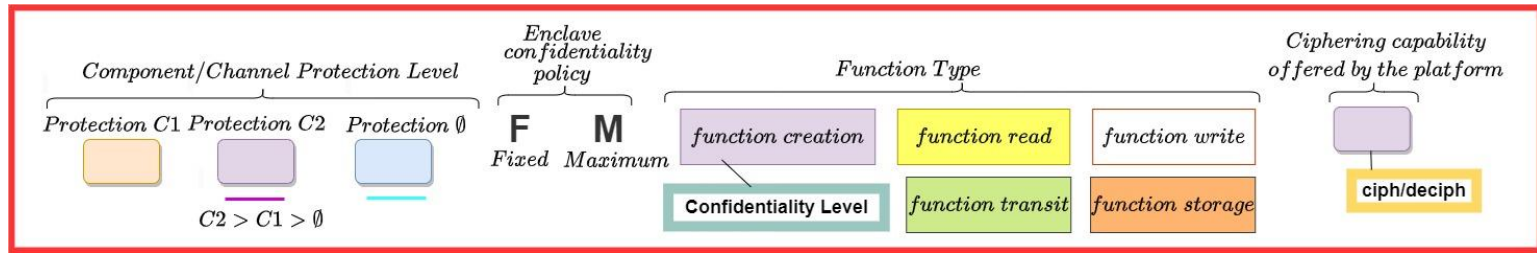
**Complex Critical Systems:** Sensitive data flows to protect.

- **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.

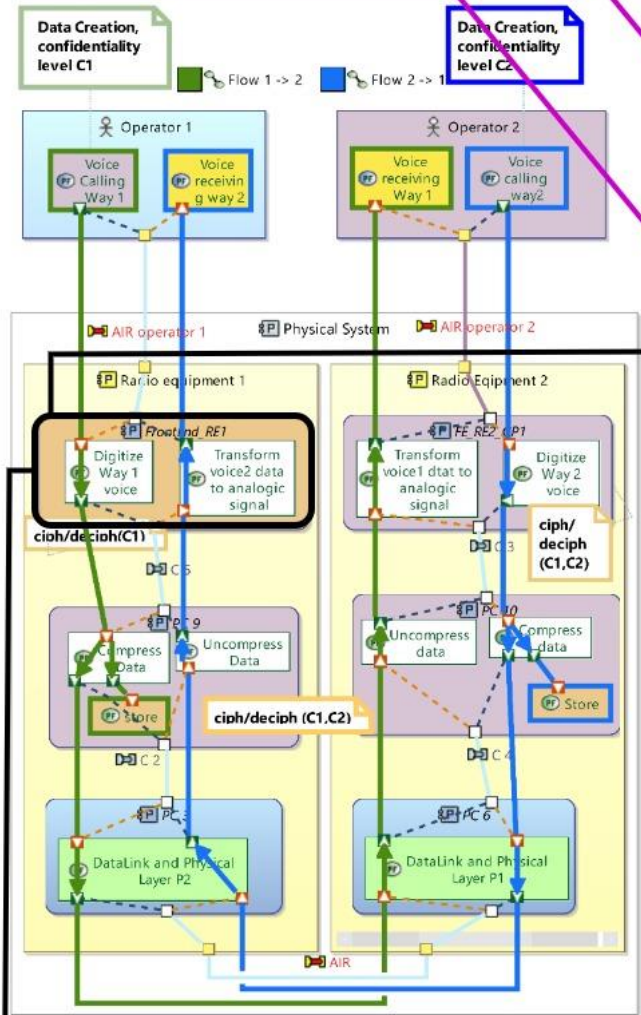
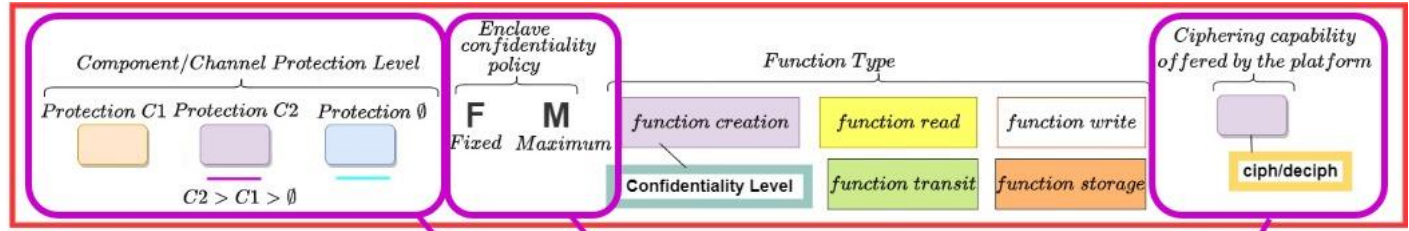




SAC'2024  
ICECCS 2024



# Tool implementation Analysis From Capella



Properties (Physical Component) [Behavior]  
 Editing of the properties of a Physical Component

Capella Management Description Extensions

Name: FrontEnd\_RE1  
 Summary: confidentiality=C1, type=fixed, cyph=C1

Buttons: Finish, Cancel

Properties (Physical Component) [Behavior]  
 Editing of the properties of a Physical Component

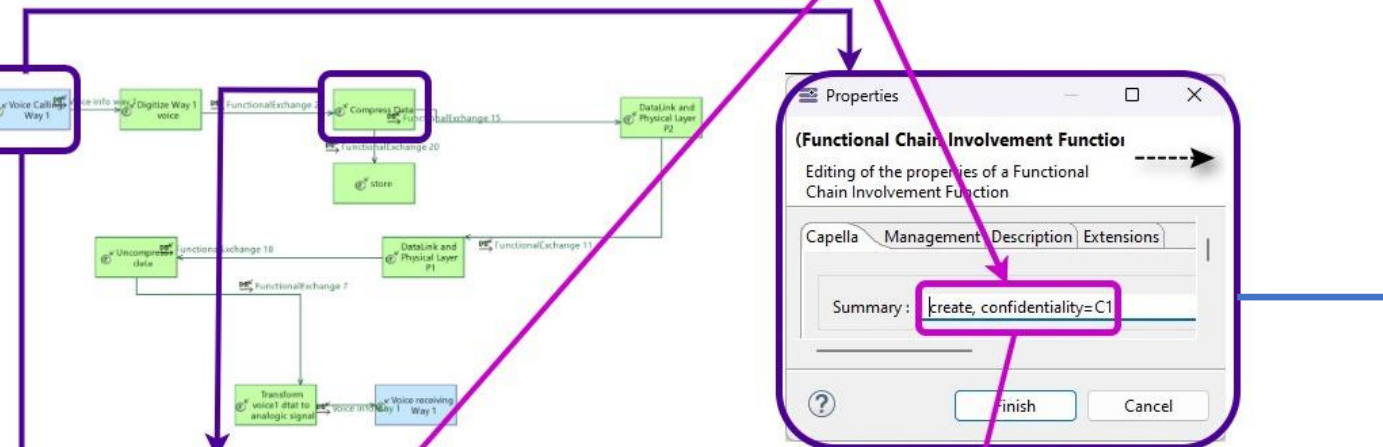
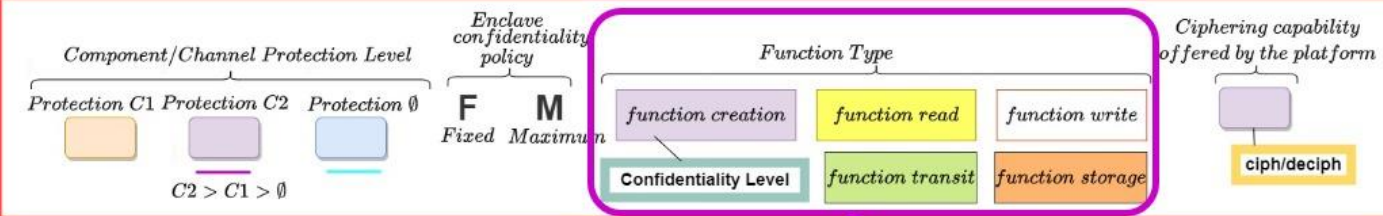
Capella Management Description Extensions

Name: FrontEnd\_RE1  
 Summary: confidentiality=C1, type=fixed, cyph=C1

Buttons: Finish, Cancel

```
ownedPhysicalComponents xsi:type="org.polarsys.capella.core.data.pa:PhysicalComponent"
  id="d89d9e58-ef53-4149-adb6-1880fd41b6bc" summary="confidentiality=C2, type=fixed, cyph=(C1,C2)"
  name="FrontEnd_RE1" kind="SOFTWARE_EXECUTION_UNIT" nature="BEHAVIOR">
```

# Tool implementation – Analysis From CapellaDesigns



Properties

(Functional Chain Involvement Function)

Editing of the properties of a Functional Chain Involvement Function

Capella Management Description Extensions

Summary: **create, confidentiality=C1**

Finish Cancel

Properties

(Functional Chain Involvement Function)

Editing of the properties of a Functional Chain Involvement Function

Capella Management Description Extensions

Summary: **create, confidentiality=C1**

Finish Cancel



Properties

(Functional Chain Involvement Function)

Editing of the properties of a Functional Chain Involvement Function

Capella Management Description Extensions

Summary: **InUseW**

Finish Cancel

(Functional Chain Involvement Function)

Editing of the properties of a Functional Chain Involvement Function



Capella Management Description Extensions




Summary: **InUseW**

Finish Cancel


```





<ownedFunctionalExchanges xsi:type="org.polarsys.capella.core.data.fa:FunctionalExchange"
  id="c06f1045-c03a-4493-80f6-fae807699fb8" name="Voice info way 1" target="#a081bf8b-261a-4b1f-b2fb-ac756435b416"
  source="#20c639ra-91be-4ae1-9bce-926a966c5015"/>
<ownedFunctionalExchangeRealizations xsi:type="org.polarsys.capella.core.data.fa:FunctionalExchangeRealization"
  id="64ed79f6-0e77-44b5-b802-8a7cc0838923" targetElement="#c86419e9-9180-44d1-a0ee-c038aaa179d9"
  sourceElement="#e06f1045-c03a-4493-80f6-fae807699fb8"/>
<ownedFunctionalChainInvolvements xsi:type="org.polarsys.capella.core.data.fa:FunctionalChainInvolvementLink"
  id="9e3ef795-271d-4166-9002-648c3b05ecd7" involved="#e06f1045-c03a-4d93-80f6-fae807699fb8"
  source="#1308c8fe-916a-4a80-9198-7495cffe11bb" target="#9a683208-5c7d-43a2-a610-a052ab7fe357"/>
<ownedFunctionalChainInvolvements xsi:type="org.polarsys.capella.core.data.fa:FunctionalChainInvolvementFunction"
  id="1308c8fe-916a-4a80-9198-7495cffe11bb" summary="create, confidentiality=C1"
  source="#1308c8fe-916a-4a80-9198-7495cffe11bb" target="#9a683208-5c7d-43a2-a610-a052ab7fe357"/>
  
```

   Data sensibility set at creation

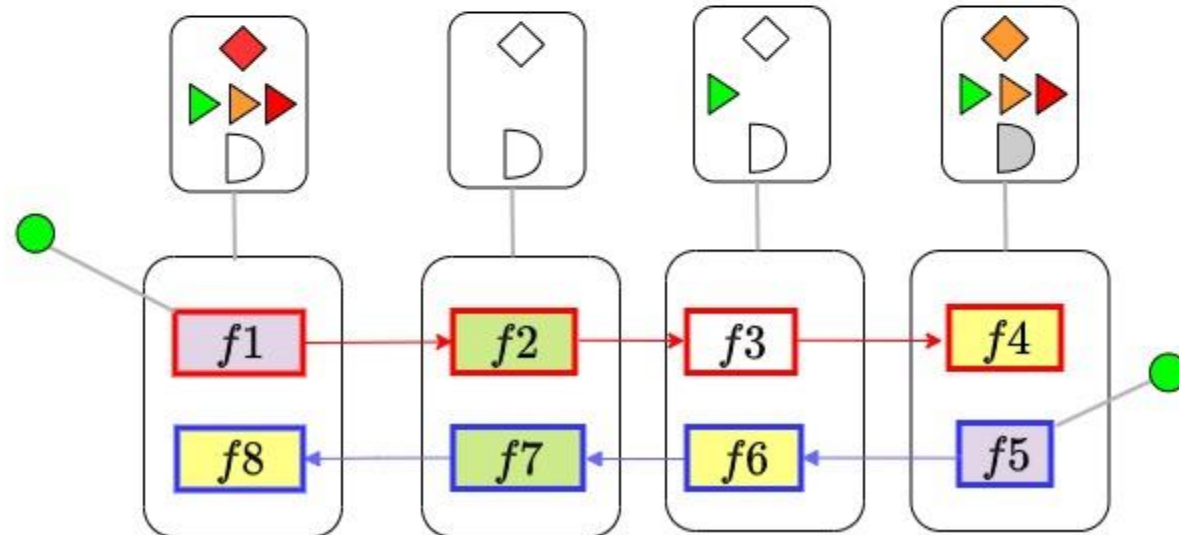
   Enclave protection offered

   Enclave ciphering capabilities offered

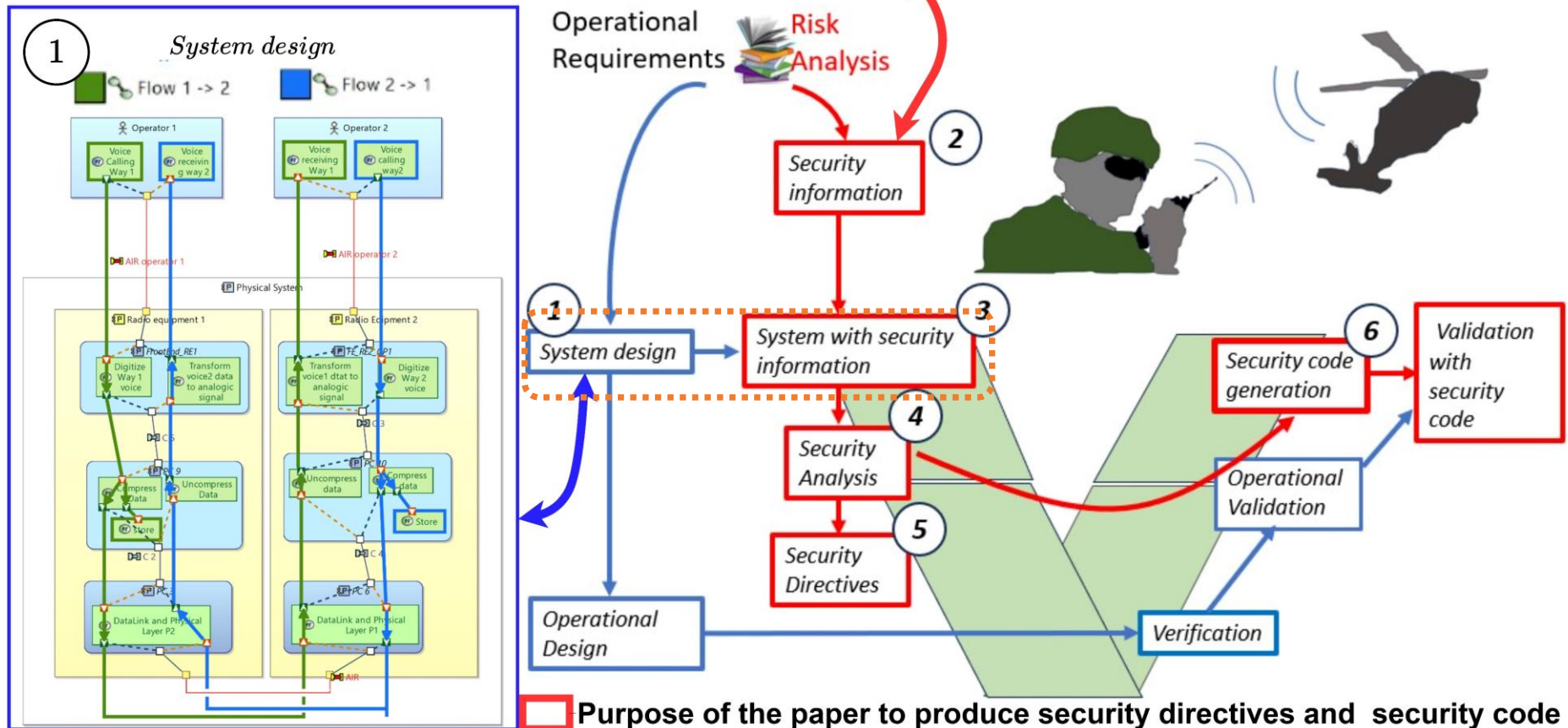
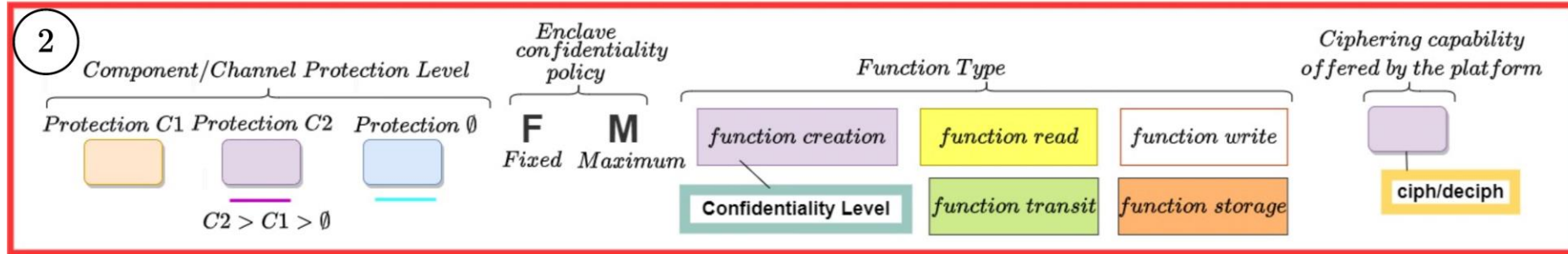
  Enclave Protection Type (fixed, maximum)

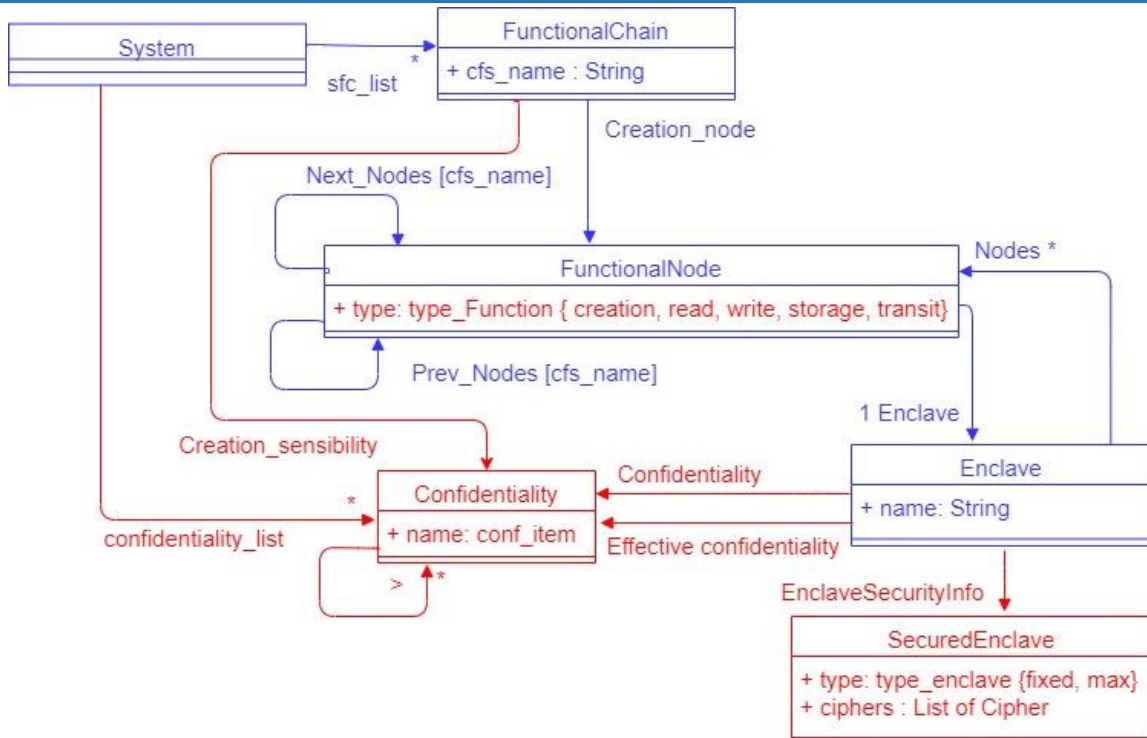
    Functions status in creation, write, read and Transit

   Functional chain





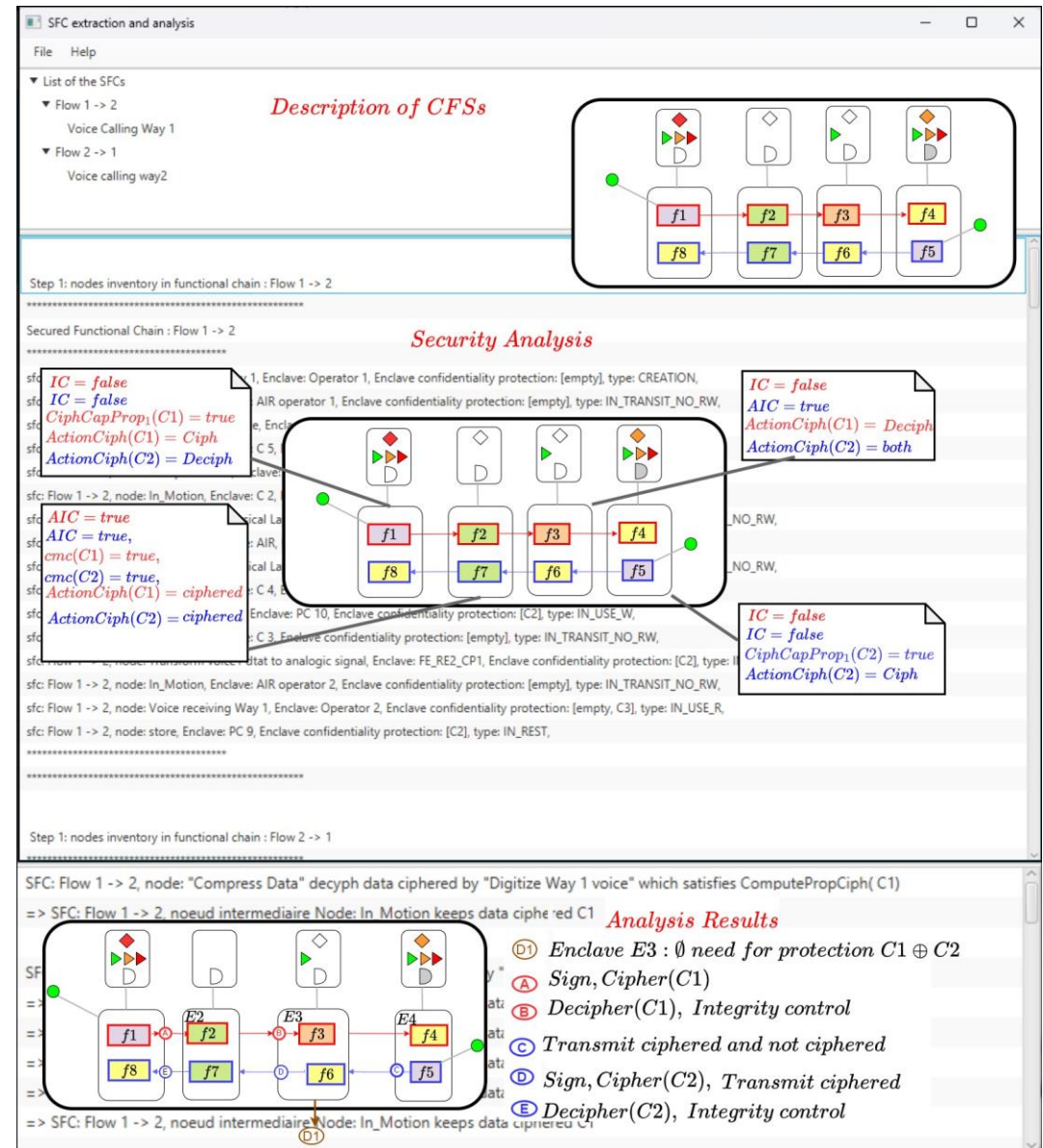




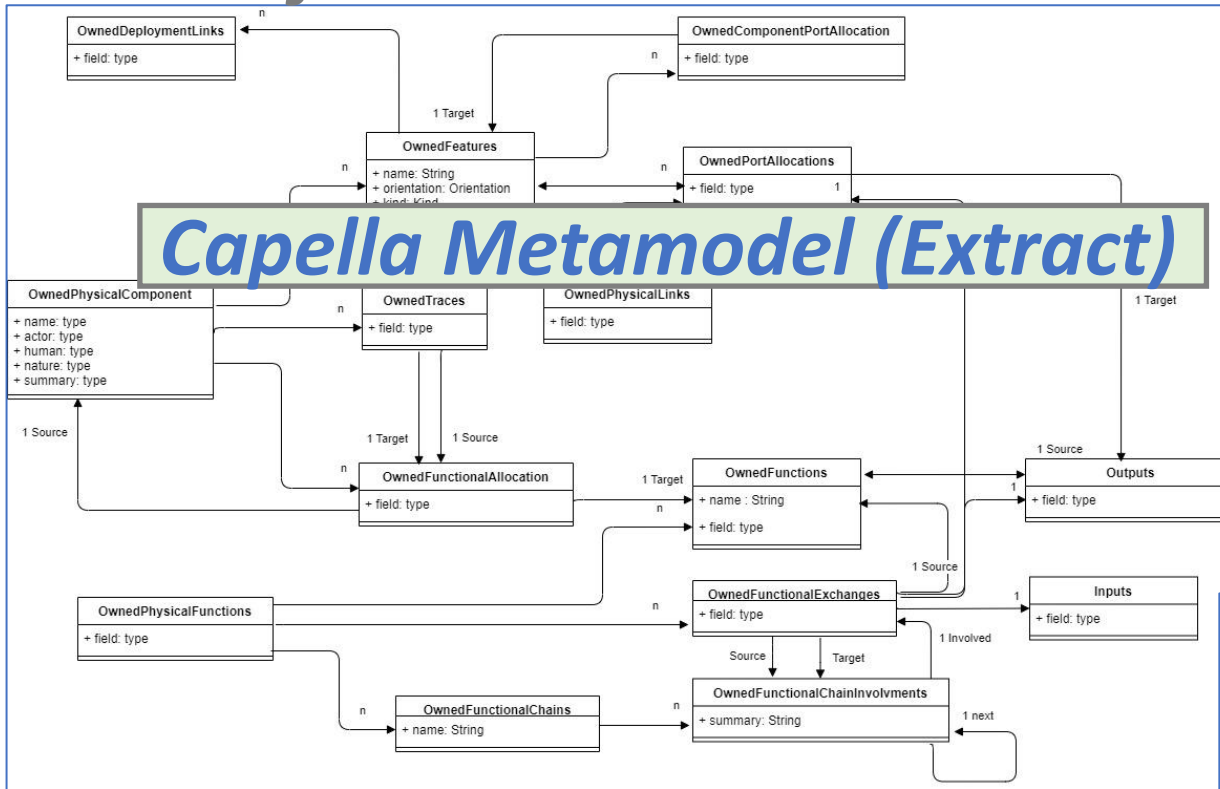
**Metamodel of the System as a set of SFCs.**

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

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



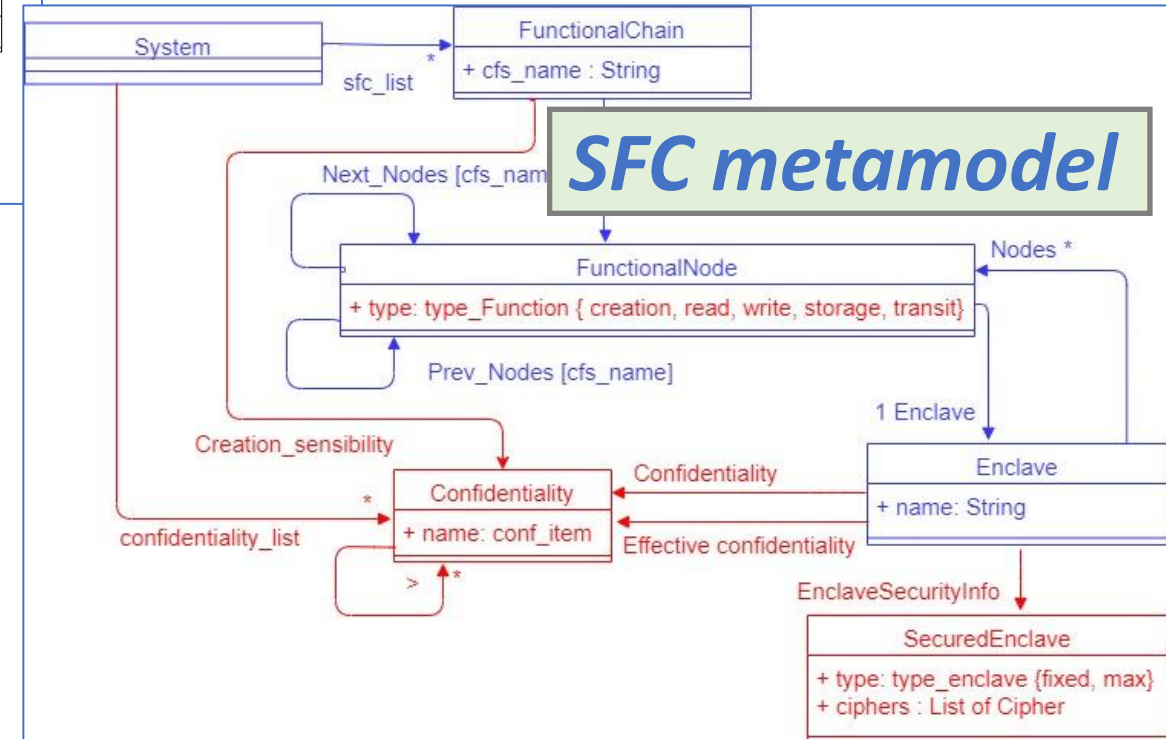
Instance of ...



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



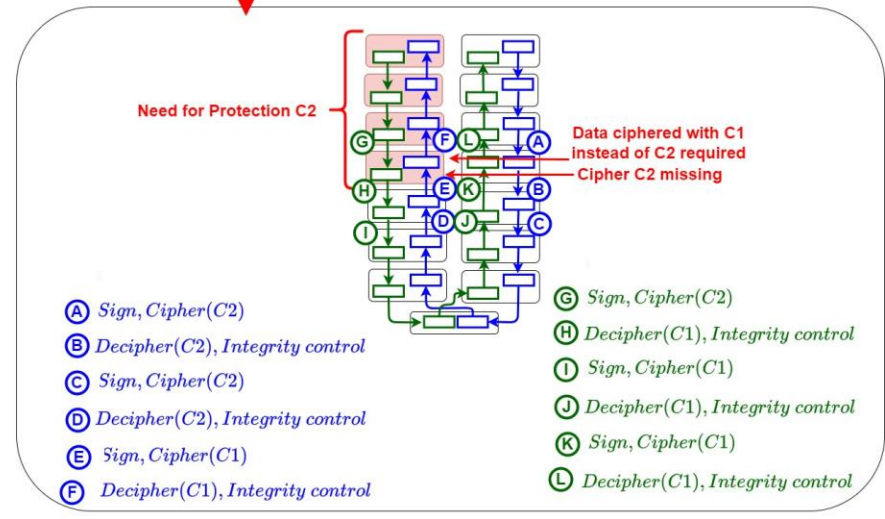
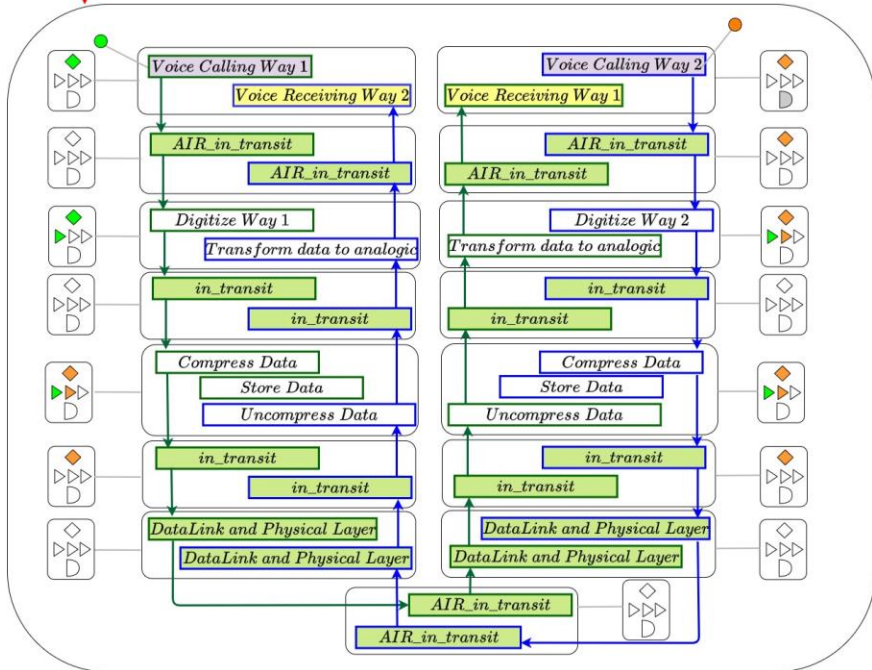
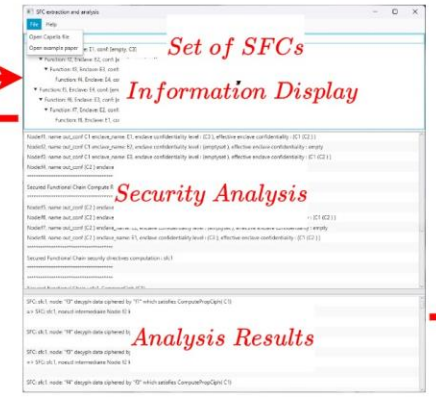
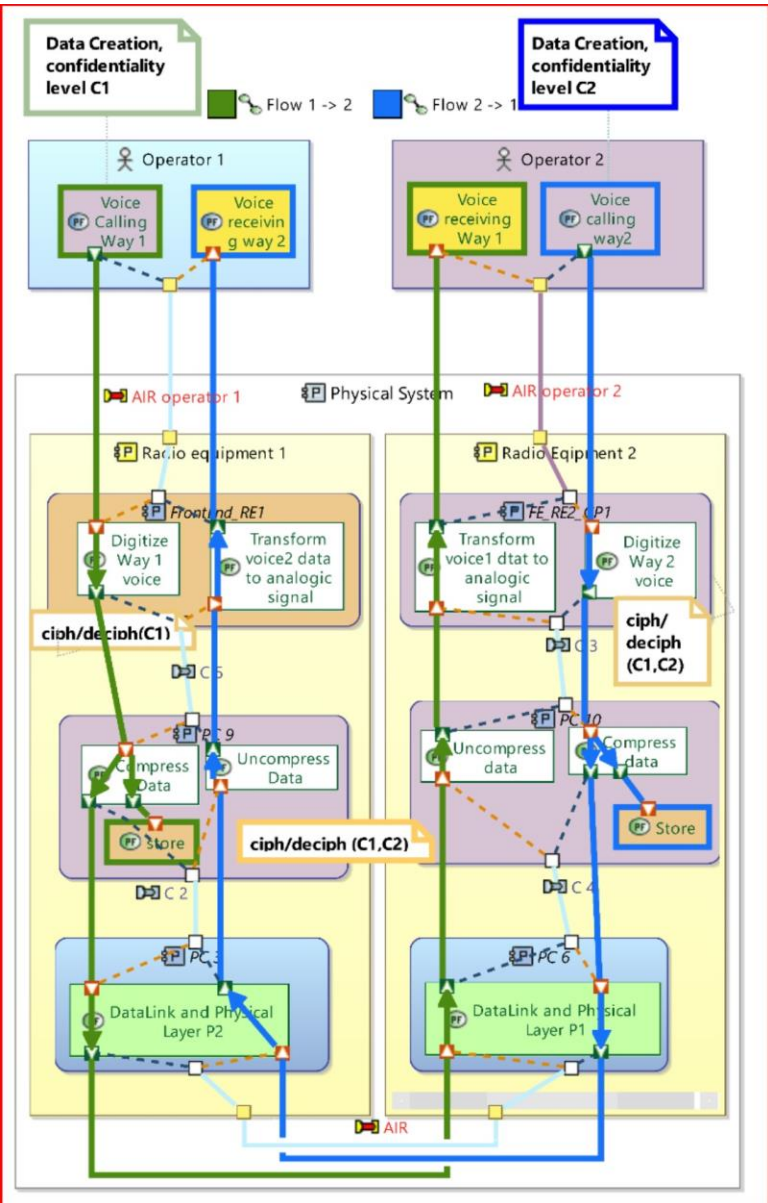
... to Instance of



**Model Transformation**  
(Summary fields exploitation)

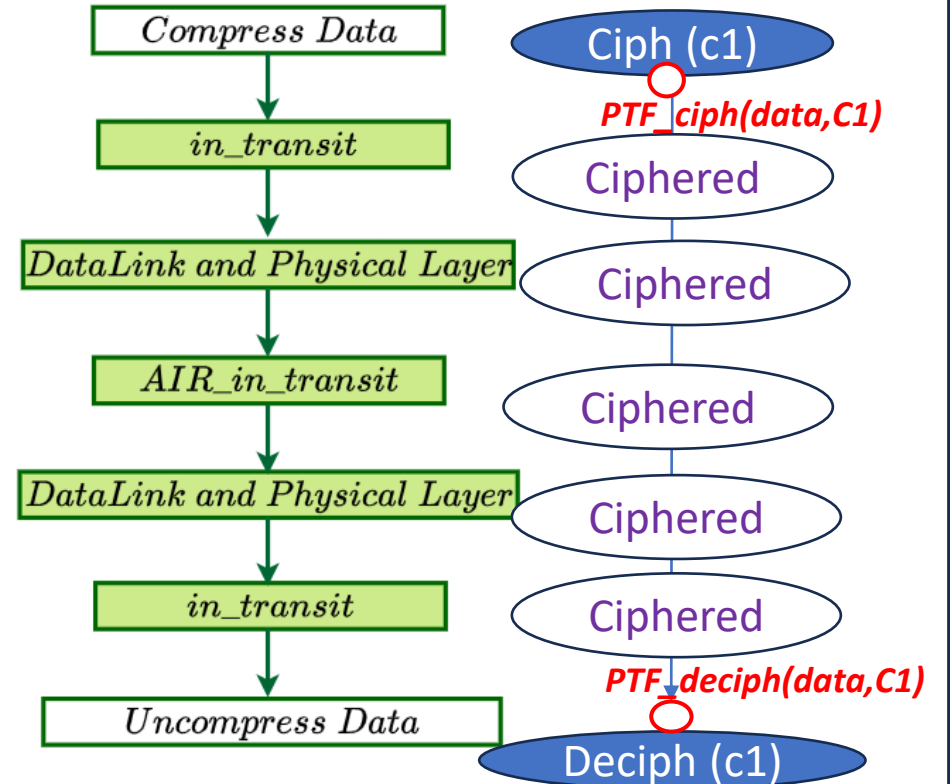


# Tool implementation – Analysis From Capella Designs

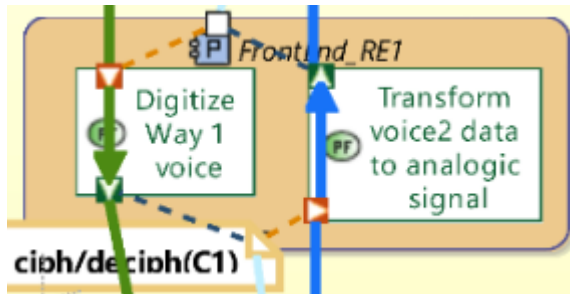


## *A Short Demo*

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 dtat 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))



Properties

(Physical Component) [Behavior]

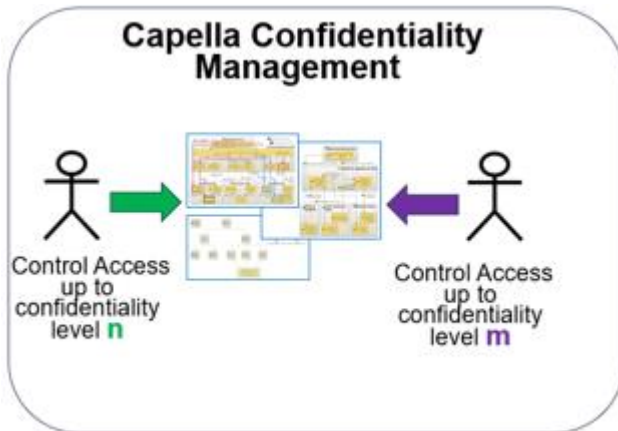
Editing of the properties of a Physical Component

Capella	Management	Description	Extensions
Name:	FrontEnd_RE1		
Summary:	confidentiality=C1, type=fixed, cyph=C1		

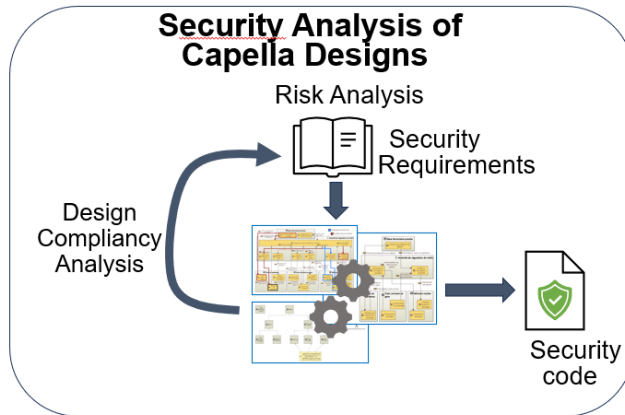
Buttons: Finish, Cancel

**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 hiding 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](mailto:Michel.Bourdelles@univ.ubs.fr)*