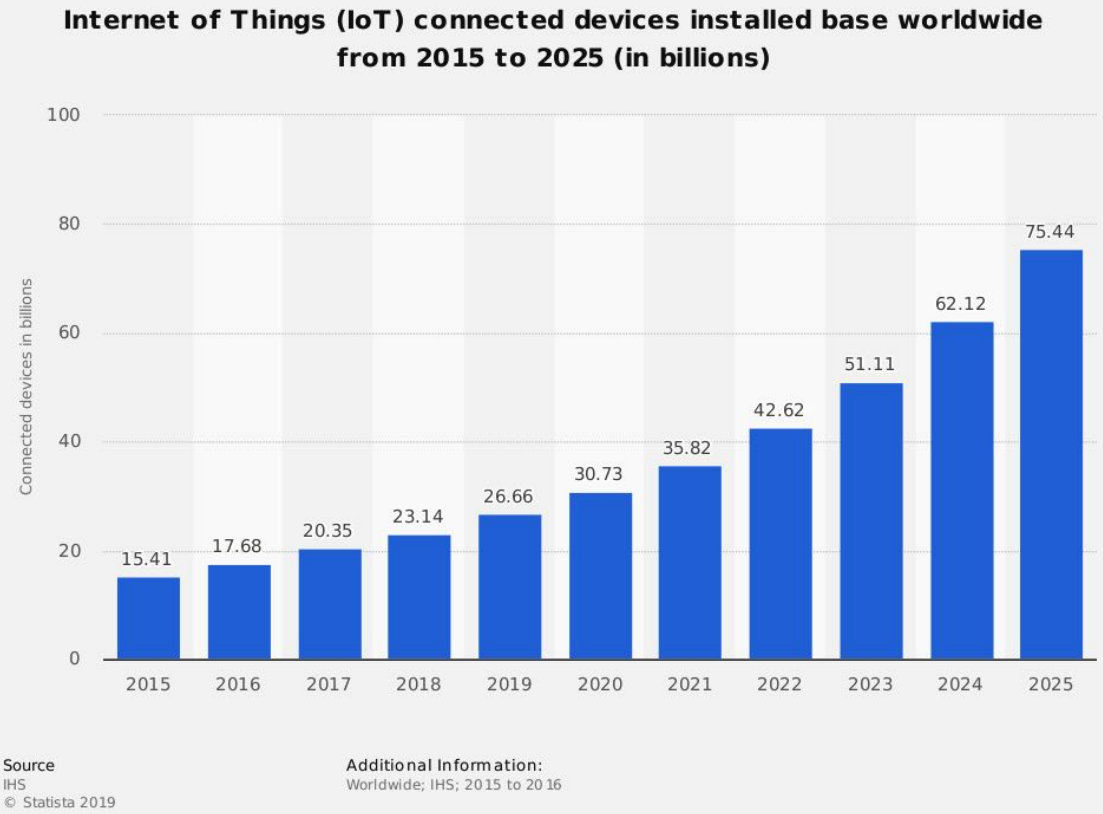
THALES

Towards a model-based approach to Systems and Cybersecurity Co-Engineering

THALES Group

Juan Navas
Jean-Luc Voirin
Stephane Paul
Stephane Bonnet

A WORLD IN MOTION
Systems Engineering Vision • 2025



75 billion

of smart objects with high connectivity capability in 2025

3 times

more than in 2019

The ever increasing number of connected devices creates an exponential number of opportunities to orchestrate them on innovative ways and to provide new services

… and also an exponential number of cybersecurity vulnerabilities!

BUSINESS REFERENCES

2 out of 3 Aircraft in the world take off and land using Thales equipment

Thales protects **80%** of the world's banking transactions and secures information systems of **19 of the world's 20 largest banks**

Thales contributes to the transportation of **3 billion** passengers across **86 metro lines** in 40 of the world's largest cities.

1 million Passengers use Thales inflight entertainment systems every day

More than **2 billion** people and **200 state** programmes benefit from Gemalto's solutions

Thales systems and equipments represent close to **25%** of the total value of the **Rafale Combat Aircraft.**

Thales equips over **70 Types of Aircraft** (fighters, military, transports, helicopters, drones etc.),

50 Navies (from submarines to aircraft carriers)

50 Land Forces (from infantry to vehicles)

Thales Alenia Space

has supplied **50%** of the pressurised volume of the International Space Station

is the prime contractor for **EXOMARS**

Thales helps secure **83.6 million** passengers transiting through Dubai Airport each year

Thales sold over **800,000 military tactical radios** across more than 50 countries over the past 30 years

GROUP KEY FIGURES

80,000 employees across **68** countries

1 new job at Thales = **3 jobs** in a SME

19 billion Euros of sales in 2018

1 billion Euros in self-funded R&D

20,500 patents with 400 new requests in 2018

THALES
Decisive technology for decisive moments

Search: Thalesgroup

In order to address cybersecurity threats to the solutions we deliver to our customers, we must integrate the cybersecurity concerns into our systems engineering processes

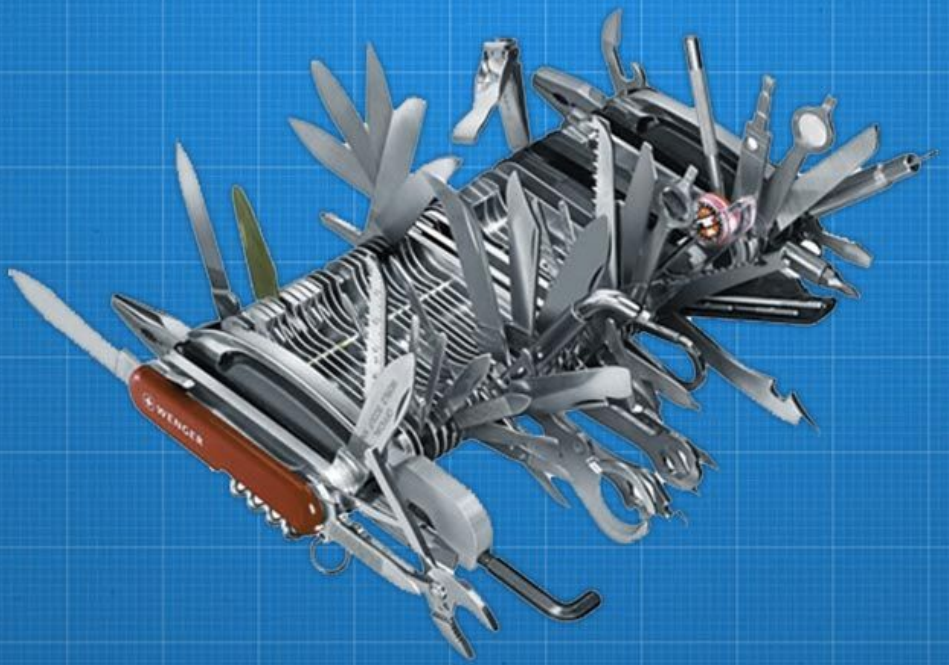
The context

Integrating Cybersecurity and MBSE

3 days before submission of security file to certification / accreditation authority…

- → **Poor confidence**
- → **Late requirements**
- → **Strong design changes**
- → **Delays & cost overhead**

OVERDESIGN? OVERSTAFFING?



Rather a **cybersecurity-by-design** approach

Architecture is what defines connections between building blocks, coordinating them so as to reach a common and shared purpose, which is the reason to exist of the system they make part of

Cybersecurity concerns shall be integrated in the systems' architectural design

The context

Integrating Cybersecurity and MBSE

The proposed integration approach is based on 3 enablers

Apprehend the system

Reach a consistent design of the solution fulfilling stakeholders expectations

Enable effective communication

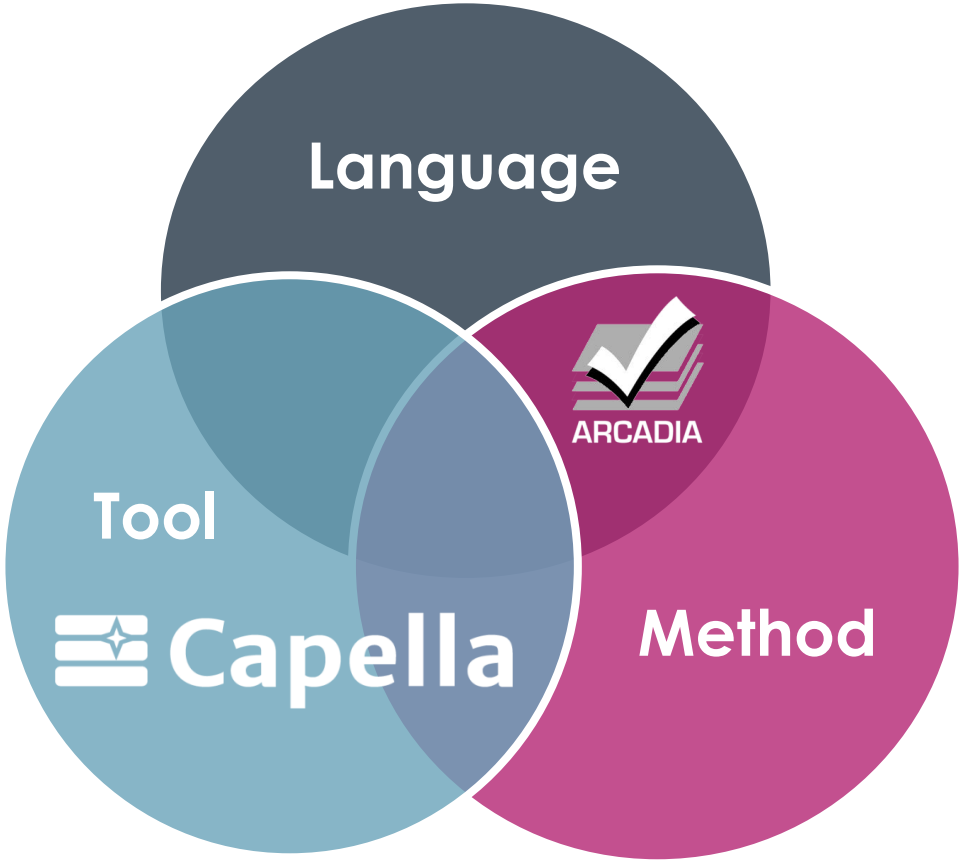
Between Security and Systems Engineering teams, about their concerns

Dedicated practices

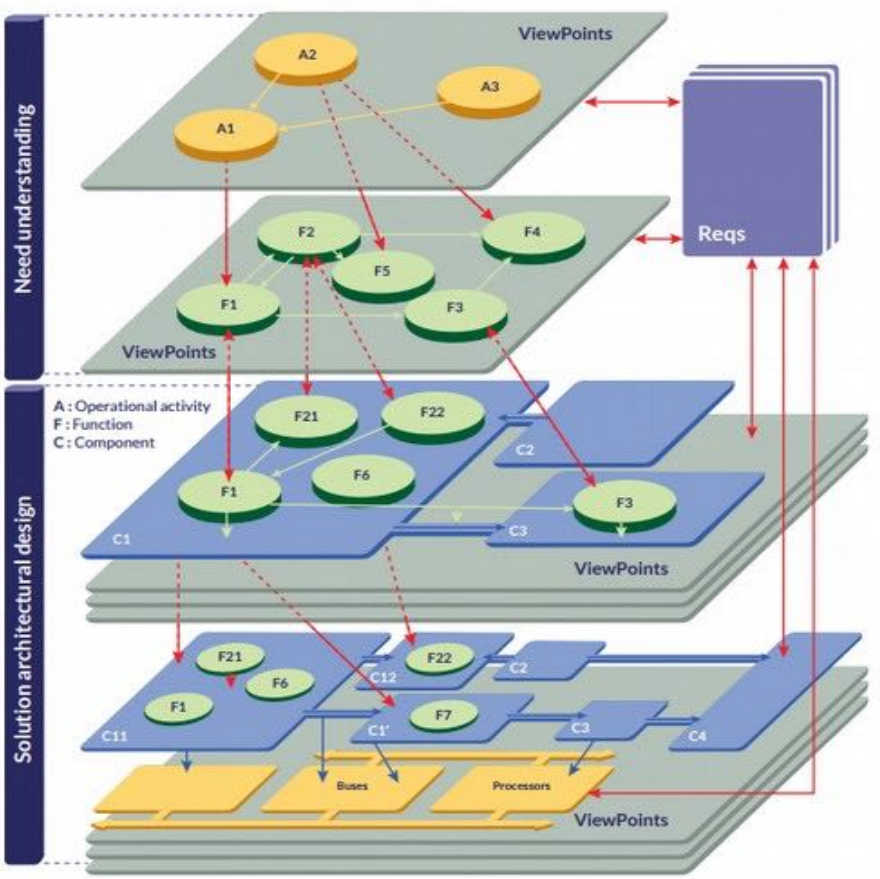
Enabling the proper handling of cybersecurity concerns into the systems engineering workflow

Our Model-Based Systems Engineering (MBSE) approach

Apprehend the system



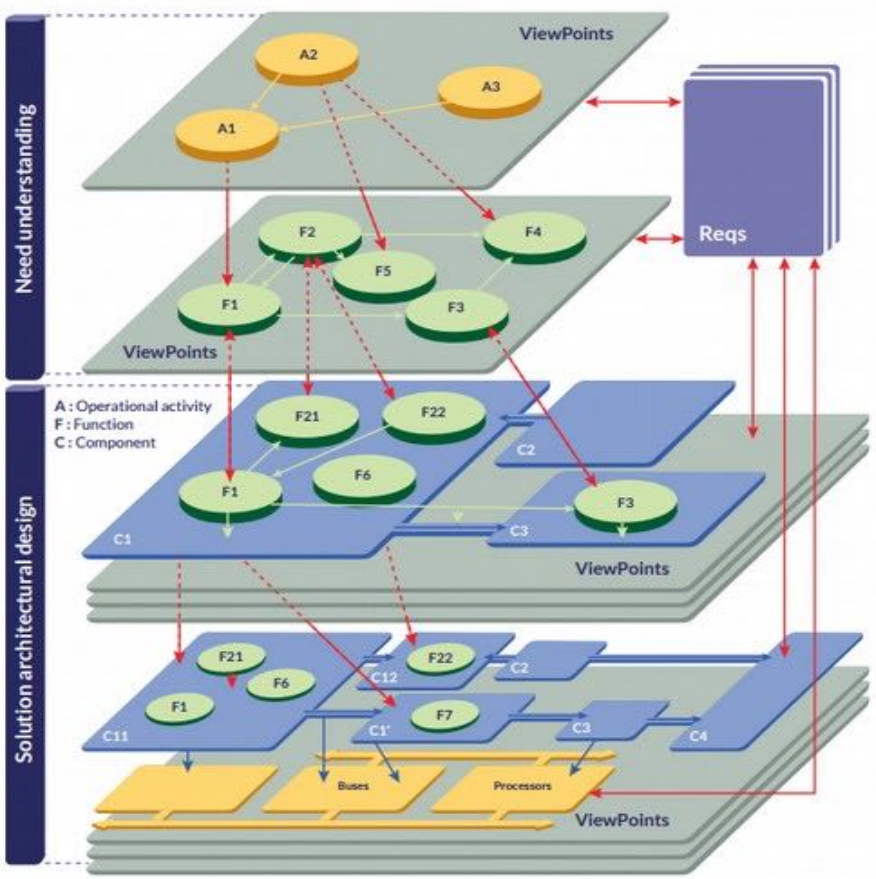
The ARCADIA method defines common engineering practices and concepts



The **environment** and the **purpose** of the system – what the system has to accomplish to fullfil the stakeholders' expectations

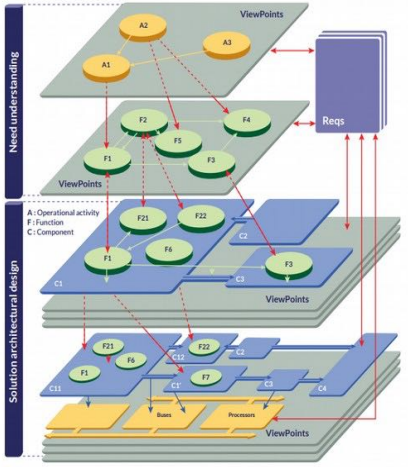
The **form** of the system: the elements composing the system, what they shall do and how they will be implemented in order to fulfill the expectations

The ARCADIA method defines common engineering practices and concepts



Symbol	Concept	Definition (extract)
	Actor	Real-world entity involved in operational activities to which the system of interest or its stakeholders should contribute
	Function	Action, operation or service performed by the system, or by an actor interacting with the system
	Exchange Item	Set of elements gathered during an exchange between functions or components
	Functional Chain	Arrangement of functions and exchanges, describing an expected behavior of the system in a given context
	Component	A constituent part of the system, responsible for implementing some of the functions

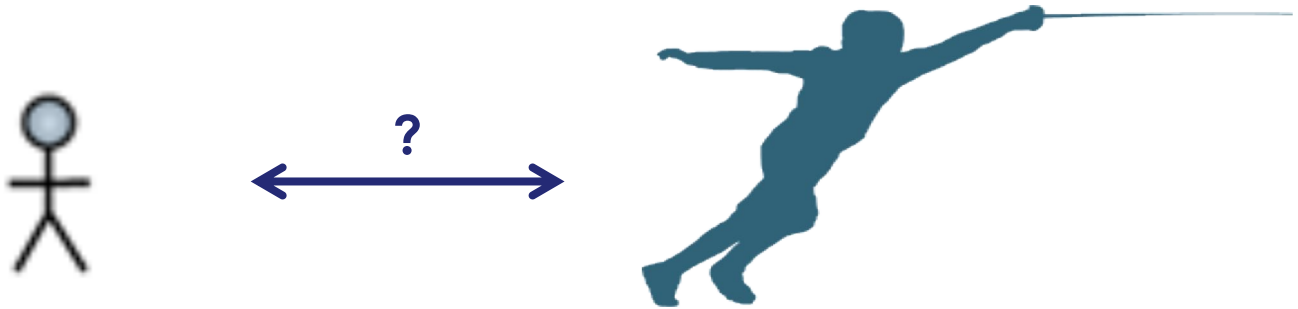
The CAPELLA tool tightly integrates the method, efficiently supporting daily work



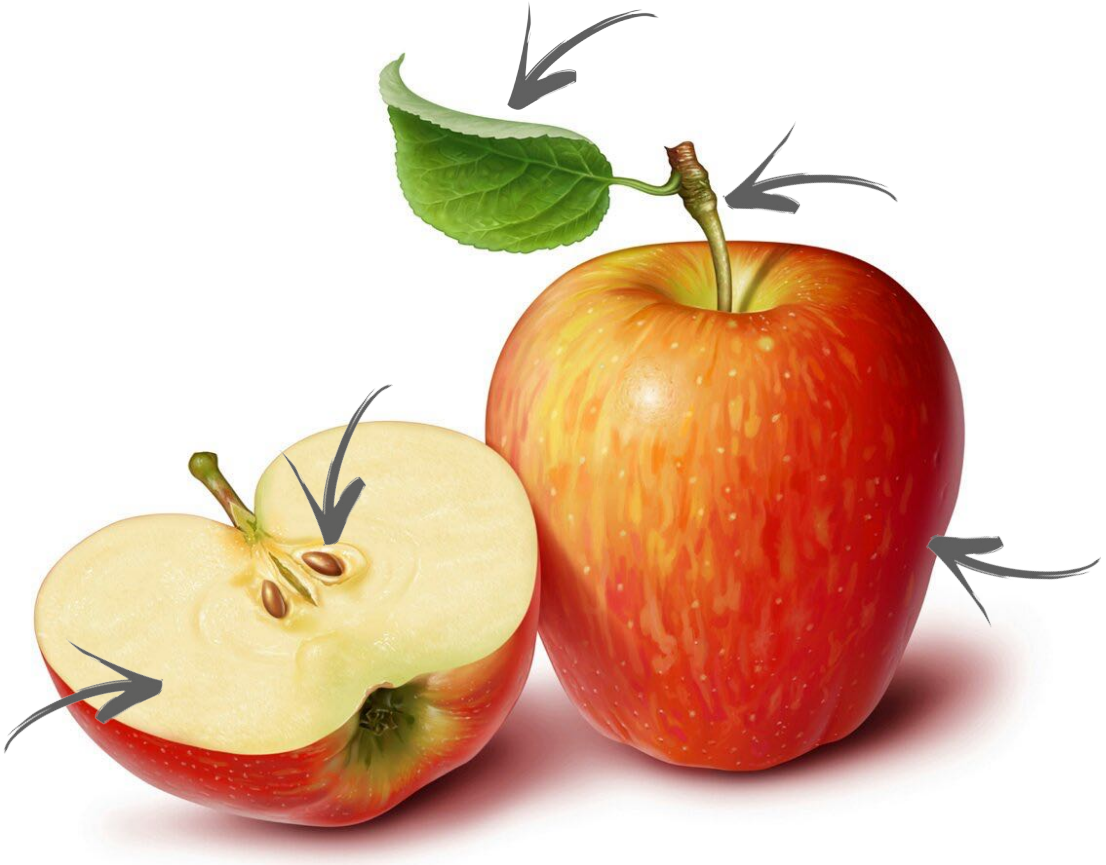
ARCADIA

Capella

Enable effective comm.



What is the **Primary Asset** of this “system”?



Enable effective comm.

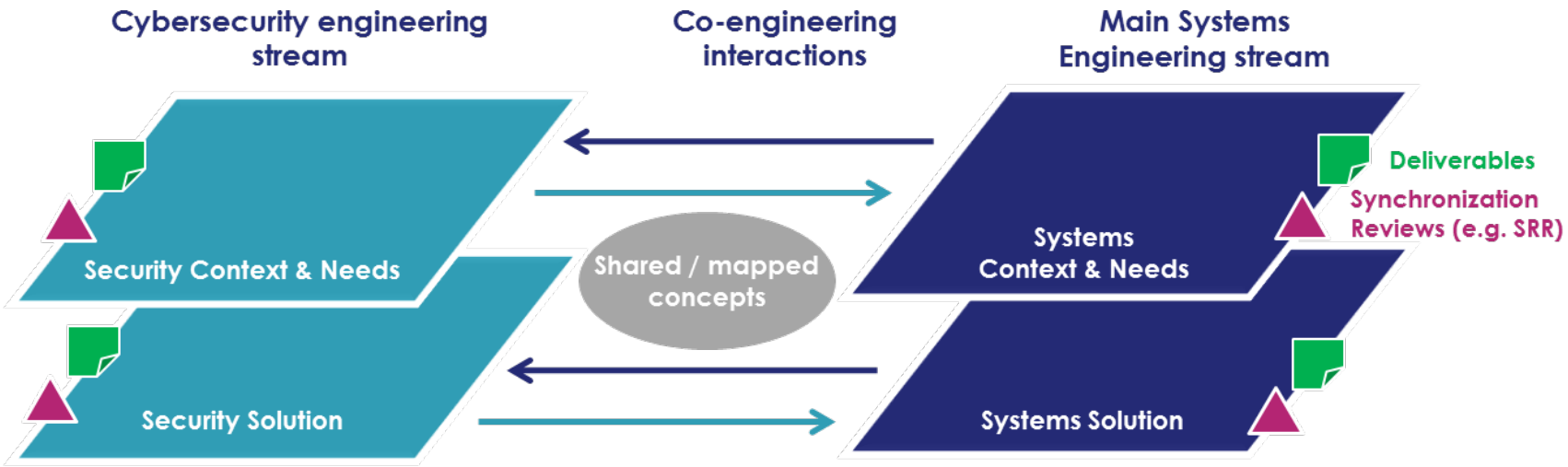
A **mapping** between Cybersecurity and Systems Engineering concepts is the basis for **reaching a common and shared vocabulary between disciplines**

A model element may be considered as a cybersecurity concept, and hence may have cybersecurity properties

Cybersecurity		Systems Engineering (Arcadia)
Threat Source		Operational Entity/Actor
Feared Event		*New concept*
Asset	Primary Asset (service-kind)	Functional Chain, Function
	Primary Asset (information-kind)	Exchange Item
	Supporting Asset	Physical Component, Physical Link
Security Control		Function

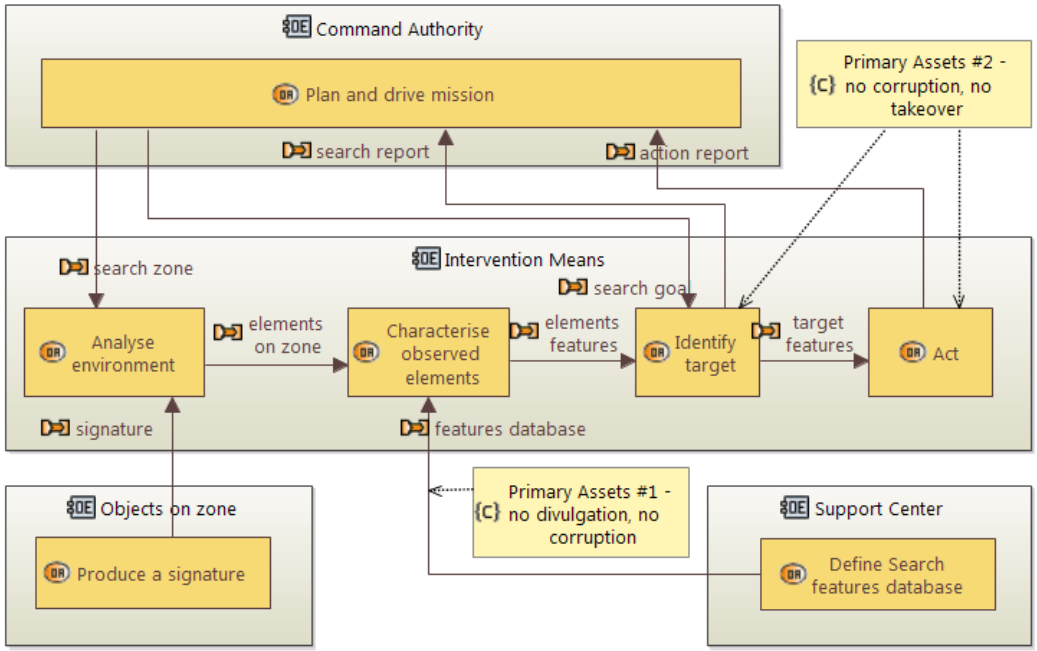
(extract of the mapping)

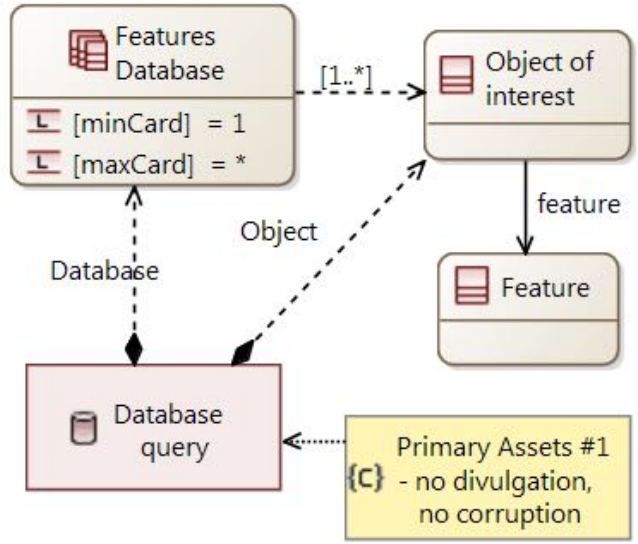
A set of **key moments** where Cybersecurity concerns shall be **reconciled** with the systems engineering work products



Analysis of the system's cybersecurity context and needs

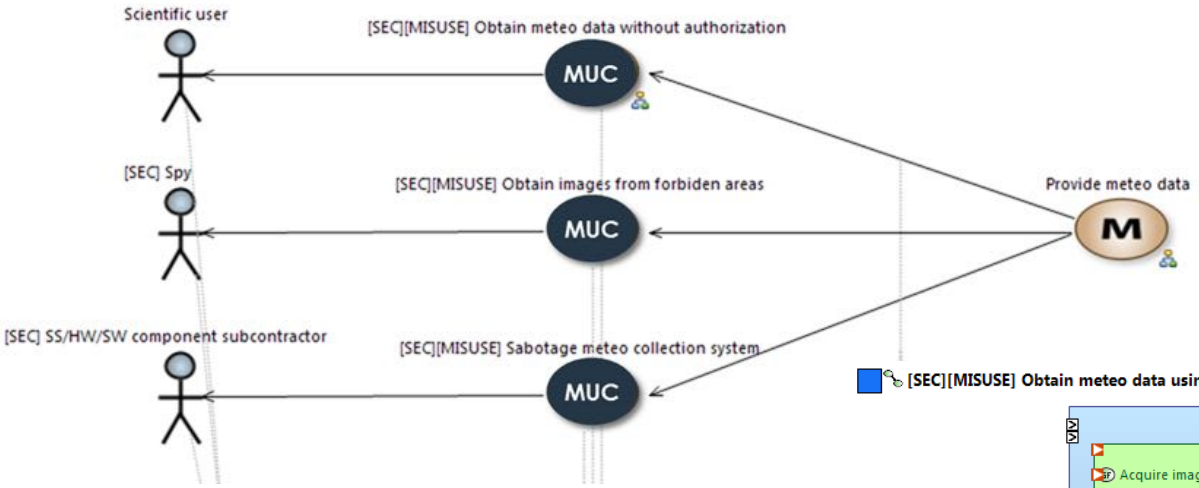
Dedicated practices





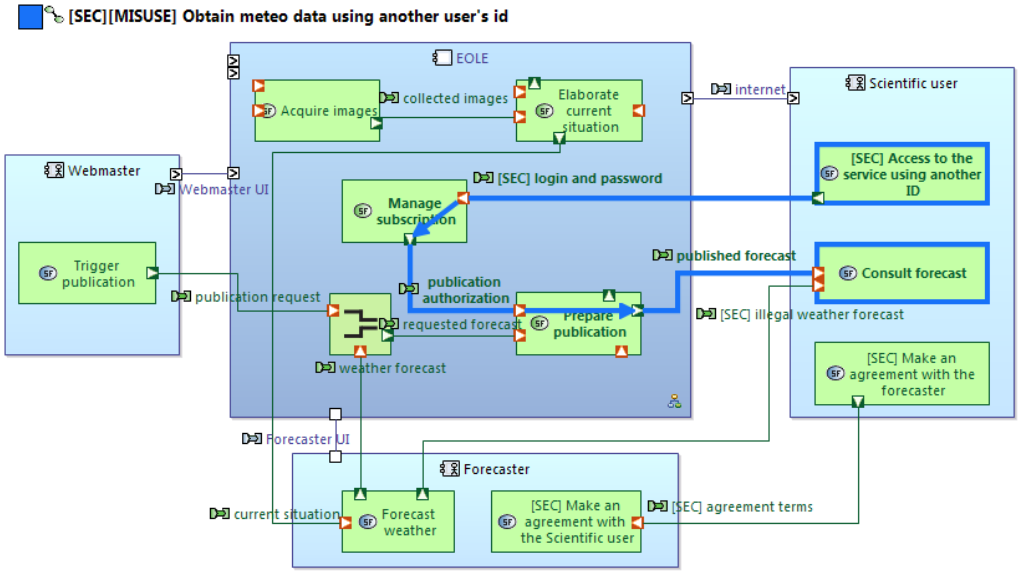
The analysis of the expectations of stakeholders leads to identification of **threat sources**, their goals and intents, how they may attack the system. It also leads to the identification and characterization of **primary assets**

Analysis of the system's cybersecurity context and needs

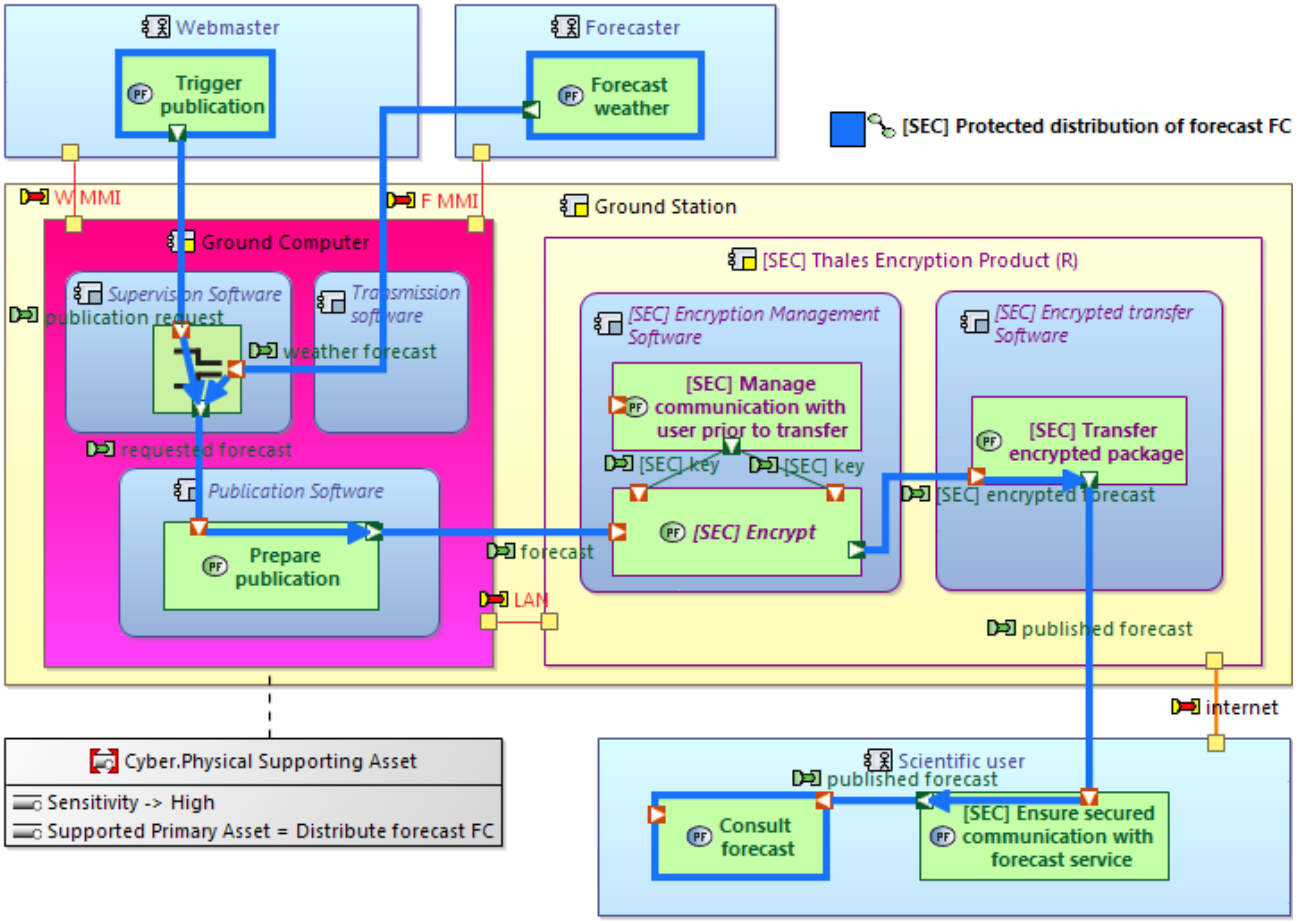


The analysis of the solution needs integrates the characterization of **threats**: the stakeholders involved on its realization, …

… the way it can be realized, the system functions that may be affected, the system **interfaces** playing a role on the realization of threats, and the security levels required for them



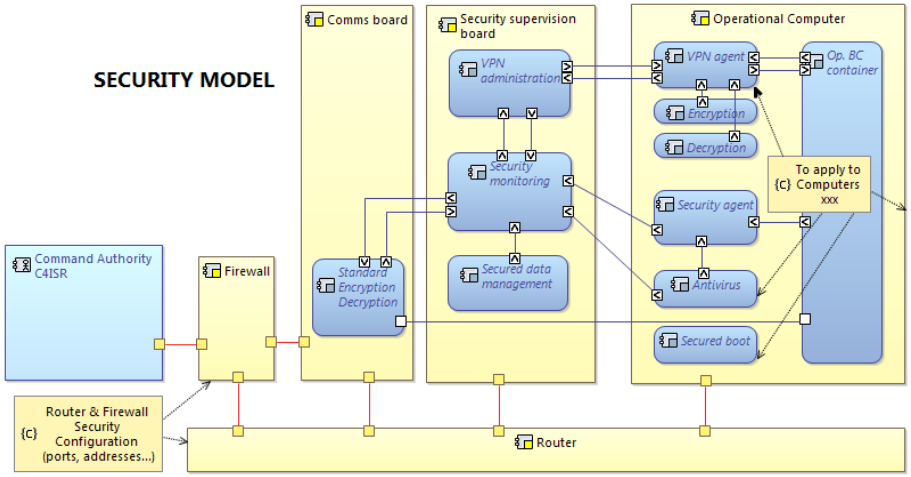
Design of cybersecurity-aware systems architectures



The definition of the architecture includes the identification of the **supporting assets** to be protected, and the functions and components that will implement the **security controls.**

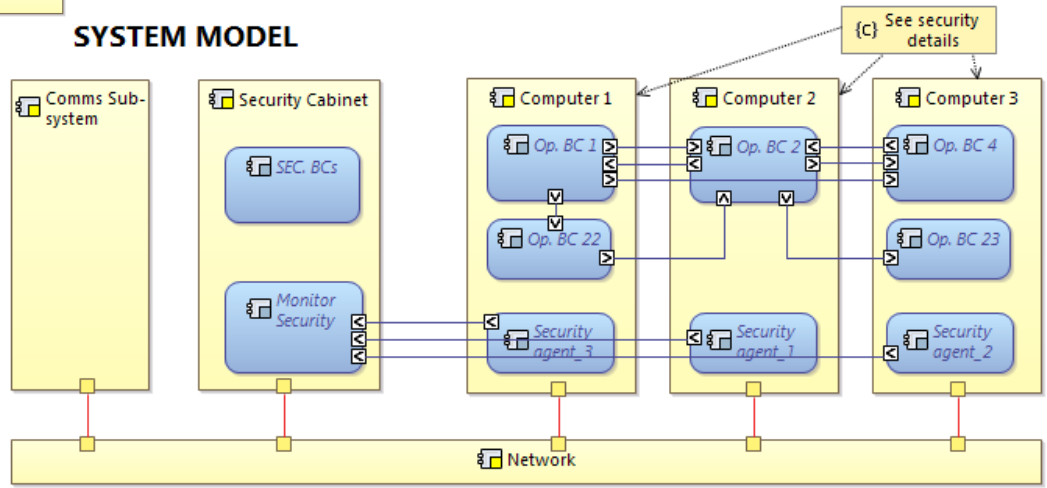
At this stage, trade-offs analysis shall be conducted to elicitate the architecture representing the best compromise.

Handling the complexity of the co-engineering effort

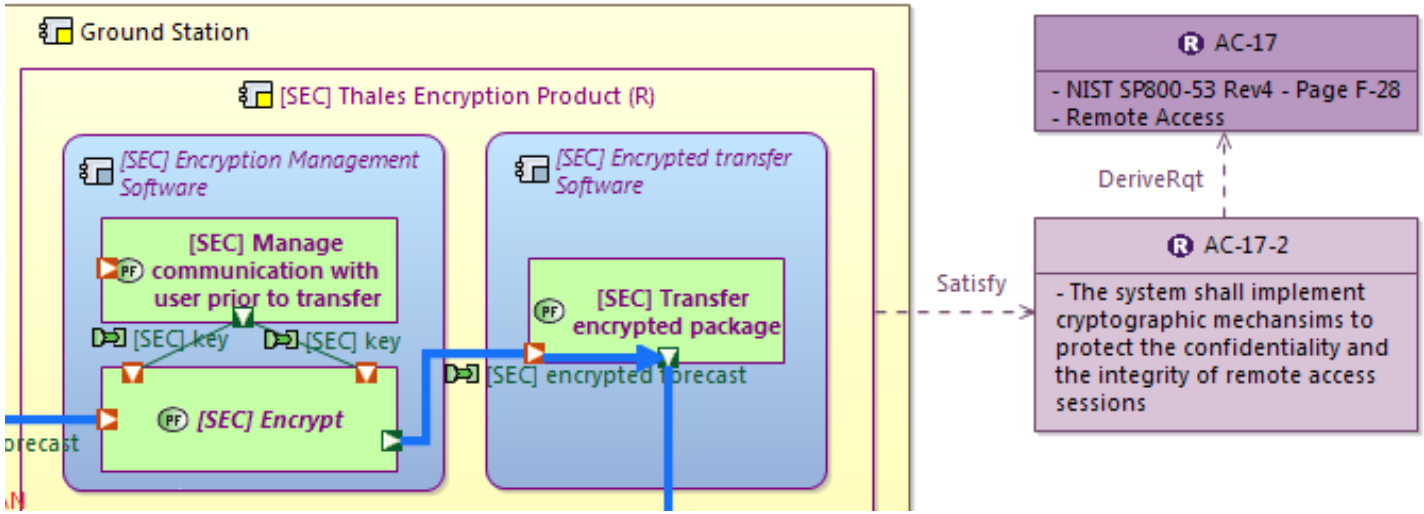


Cybersecurity-dedicated view - the Operational Computer physical component is a "representative" of several physical components in the system model. A set of behavioral components represent the cybersecurity-specific features that the latter shall implement.

System-dedicated view – only those cybersecurity aspects impacting the system-level evaluations (sizing, interfaces,...) are represented, irrelevant details are omitted (e.g. Security Cabinet)



Early verification and validation of cybersecurity-aware systems architectures



The assessment of how and how well the architecture elements contribute to the satisfaction of cybersecurity requirements, allow co-engineering teams to gain confidence on the solution architecture

Effective integration of cybersecurity concerns into systems engineering is reached through:

Apprehend the system

Leverage on MBSE to share a common understanding on the solution at its stakes

Enable effective communication

Define a common vocabulary and the key reconciliation milestones in the engineering process

Dedicated practices

Targeted model-based practices to analyze, design and justify the solution

Q&A