Aggregated Quality Assurance for Systems

Bridging the gaps between safety and security processes: the AQUAS approach

14 September, 2018
IWES Workshop, Siena

Silvia Mazzini
(Intecs Solutions)

Credits to John Favaro, Peter Popov and Lorenzo Strigini

AQUAS SAFETY SECURITY PERFORMANCE

Outline

- **Project Overview**
- **Project Goals**
- **Interaction Points**

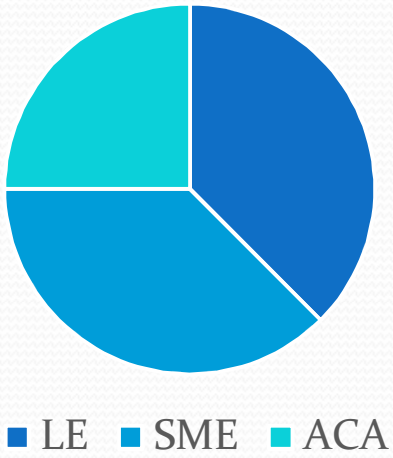
Project Overview

AQUAS SAFETY SECURITY PERFORMANCE

AQUAS Partners

23 partners in 7 countries

Partner Backgrounds



- 16 Saf-Sec
- 15 Saf-Perf
- 11 Sec-Perf
- 8 Product Lifecycle

AQUAS SAFETY SECURITY PERFORMANCE

CITY UNIVERSITY LONDON

AbsInt

Hochschule RheinMain
University of Applied Sciences
Wiesbaden Rüsselsheim

SYSGO EMBEDDING INNOVATIONS

ALL4TEC

magillem

SIEMENS

CLEARSY SYSTEM ENGINEERING

cea

TELECOM ParisTech

Une école de l'IMT

THALES

TrustPort Keep IT Secure

BRNO UNIVERSITY OF TECHNOLOGY

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

SIEMENS

ThalesAlenia Space
A Thales / Finmeccanica Company

tecnalia Inspiring Business

INTEGRASYS

RGB medical devices

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

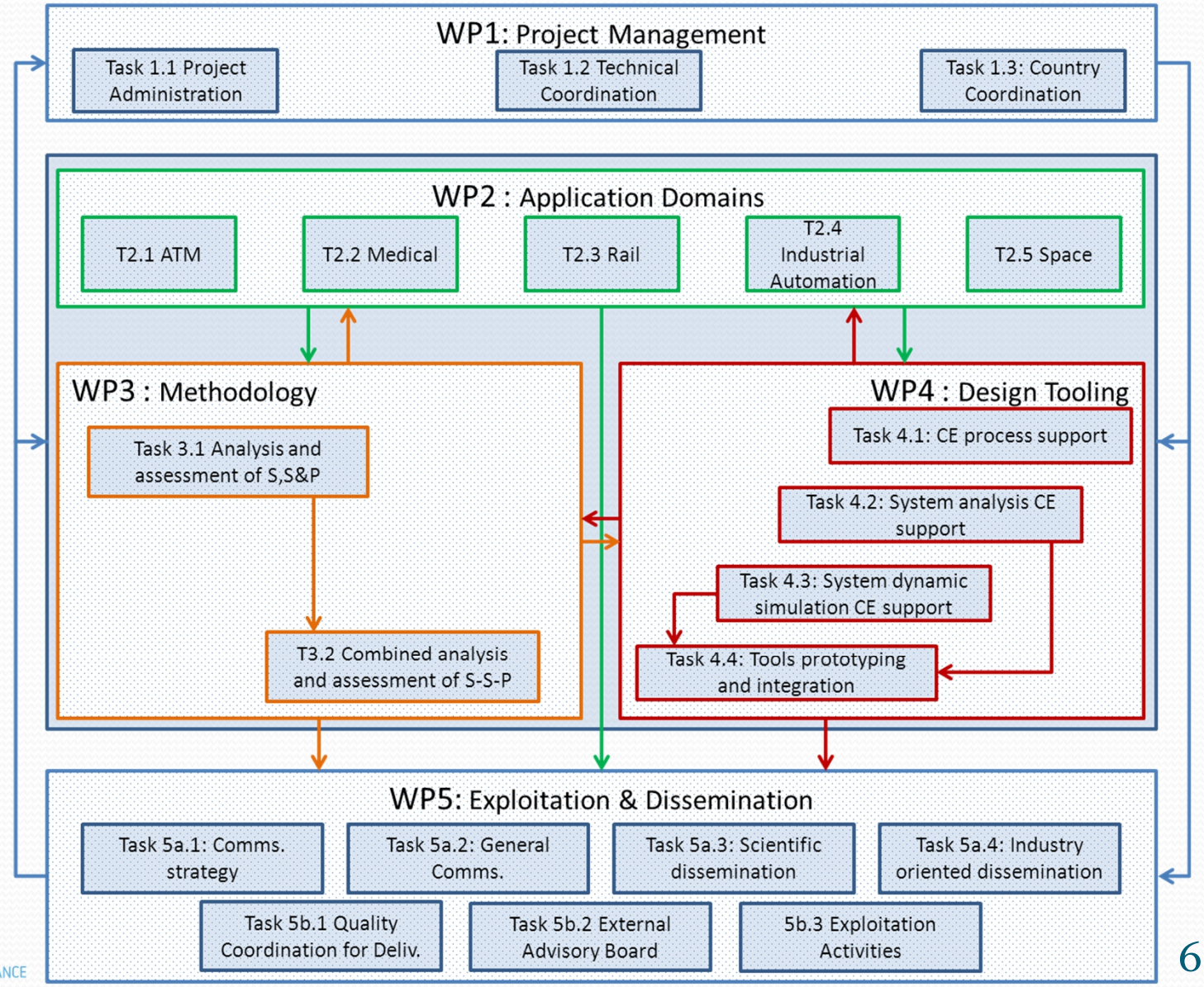
intecs Solutions
the Brainware company

Co-Engineering into mainstream practices

We are investigating Co-Engineering techniques for safety, security and performance of critical and complex embedded systems

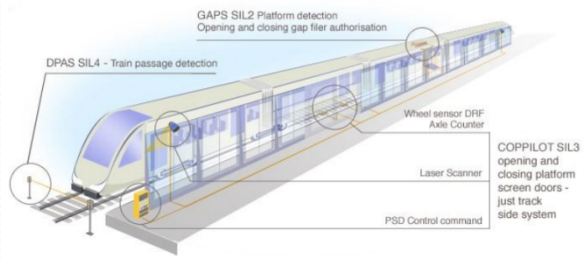
AQUAS SAFETY SECURITY PERFORMANCE

Project Structure



AQUAS SAFETY SECURITY PERFORMANCE

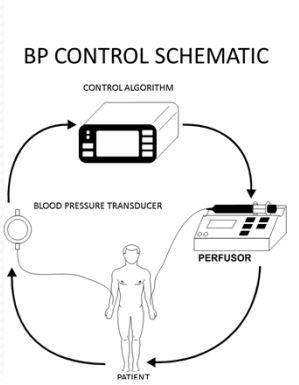
Application Domains



Rail Carriage Mechanisms

Air Traffic Management

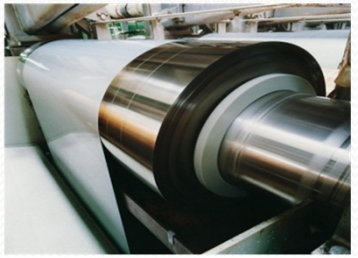
Medical Devices



Space Multicore Architectures

Safety, Security, Performance, System modelling

Industrial Drive



External Domains

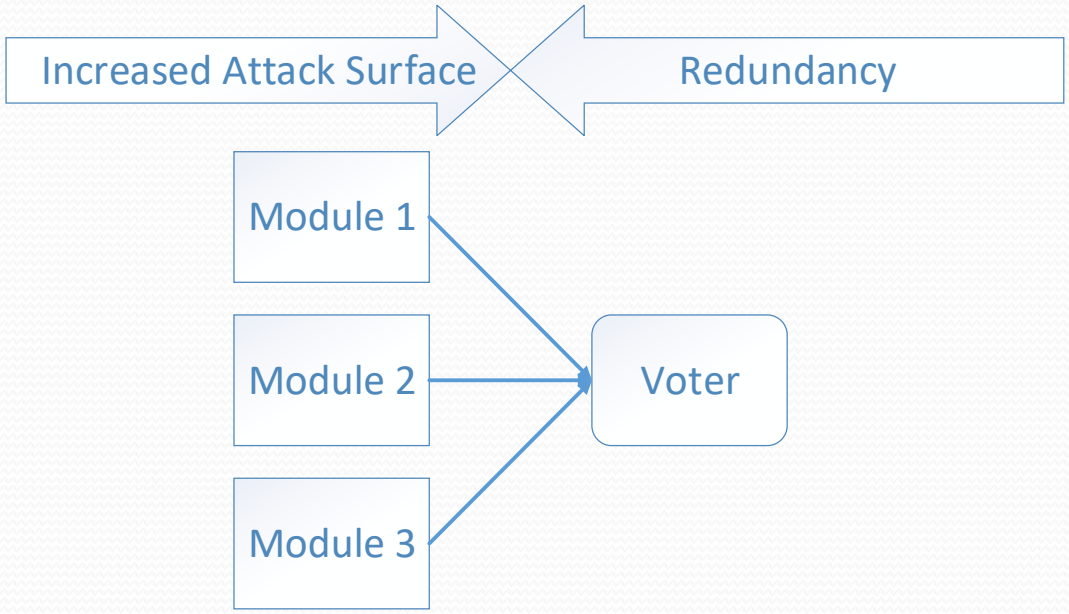
AQUAS SAFETY SECURITY PERFORMANCE

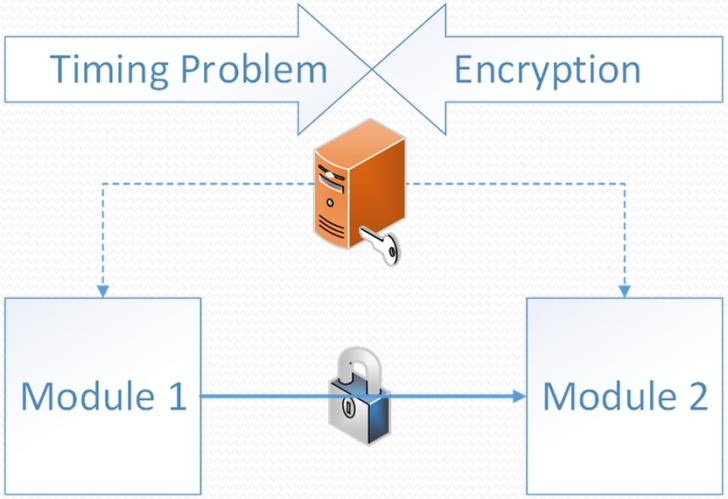
Project Goals

AQUAS SAFETY SECURITY PERFORMANCE

Co-Engineering Problem Statement

- Different quality attributes require different measures
- Safety systems were once constructed based on the assumption that they are isolated

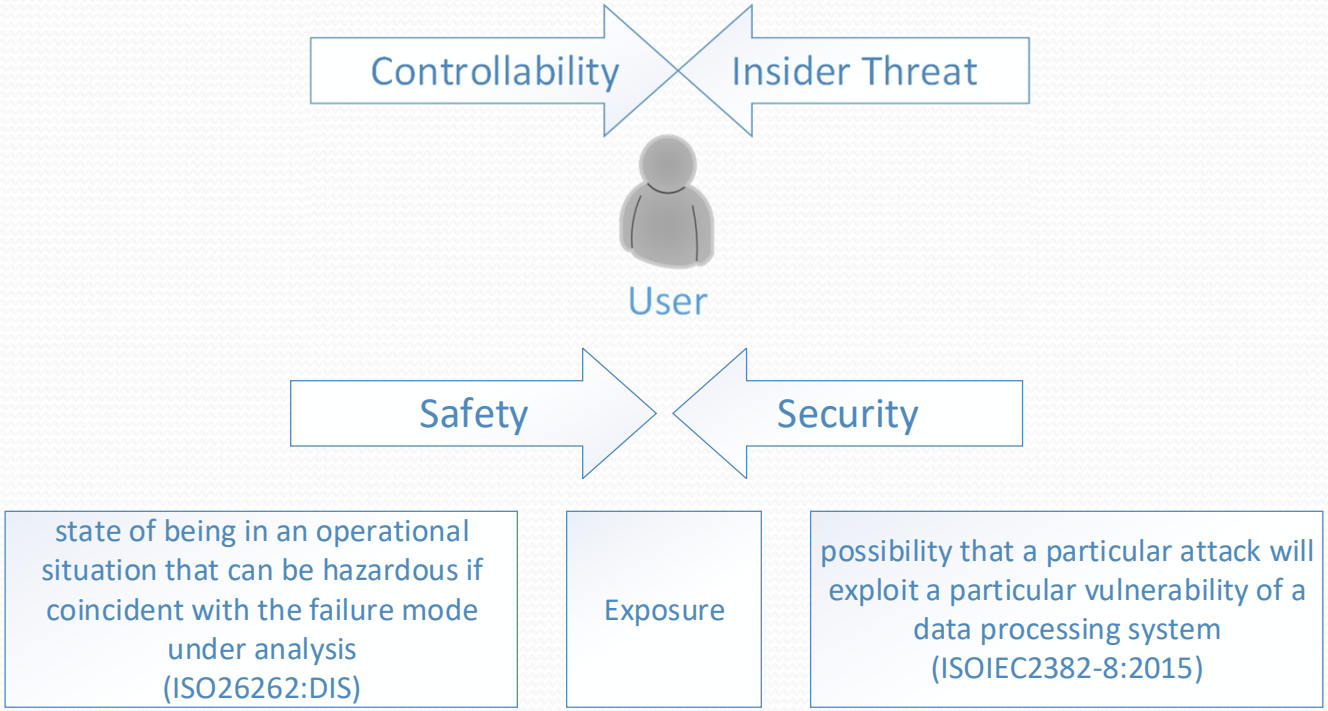




AQUAS SAFETY SECURITY PERFORMANCE

Co-Engineering Problem Statement

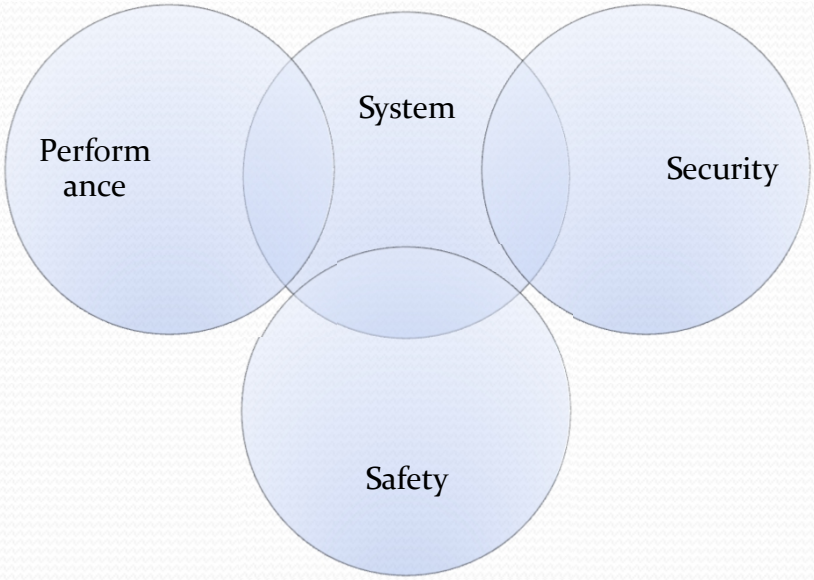
- Safety and security cultures are very diverse
- Safety & security people speak different languages



AQUAS SAFETY SECURITY PERFORMANCE

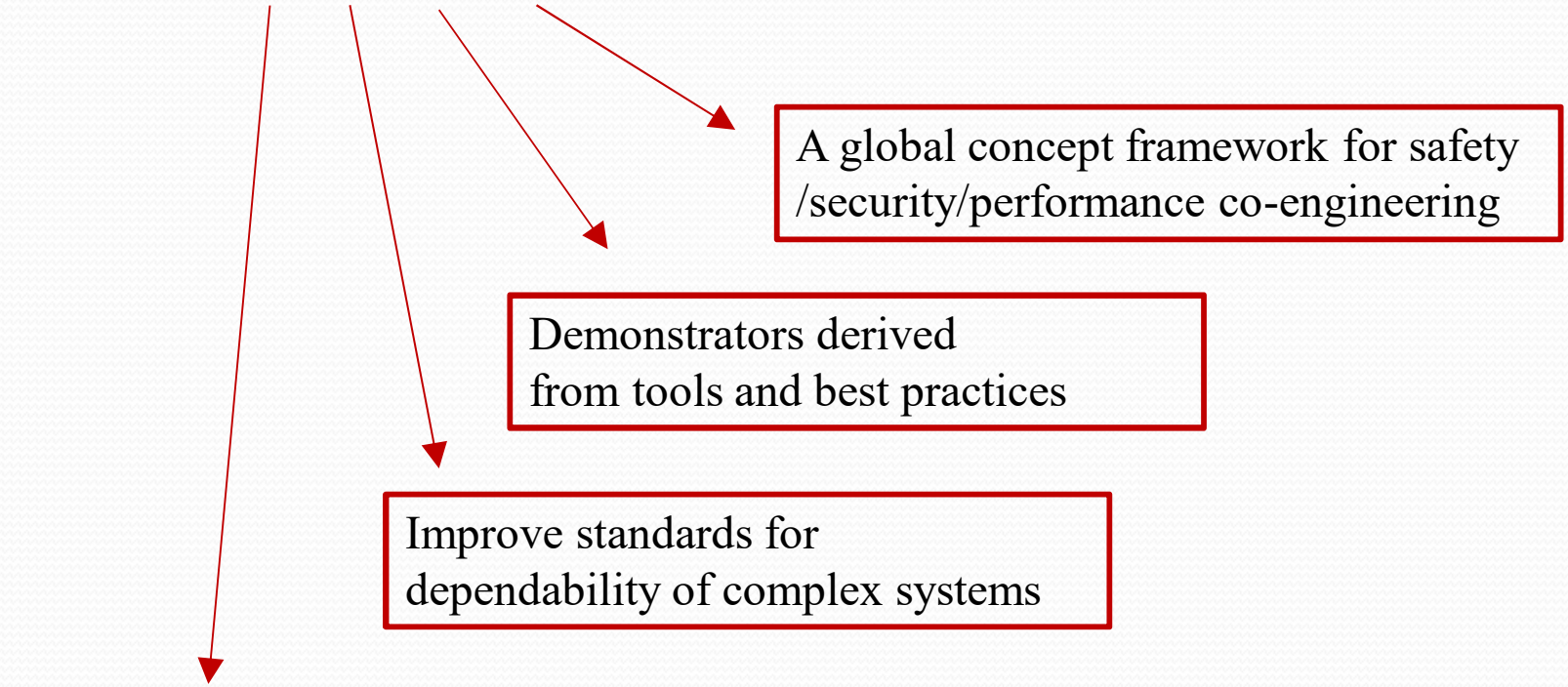
Co-Engineering Problem Statement

- Poorly understood influences between quality attributes consume money and time in lifecycle
- Safety & security people work independently, results partly incompatible



AQUAS SAFETY SECURITY PERFORMANCE

AQUAS Objectives



AQUAS SAFETY SECURITY PERFORMANCE

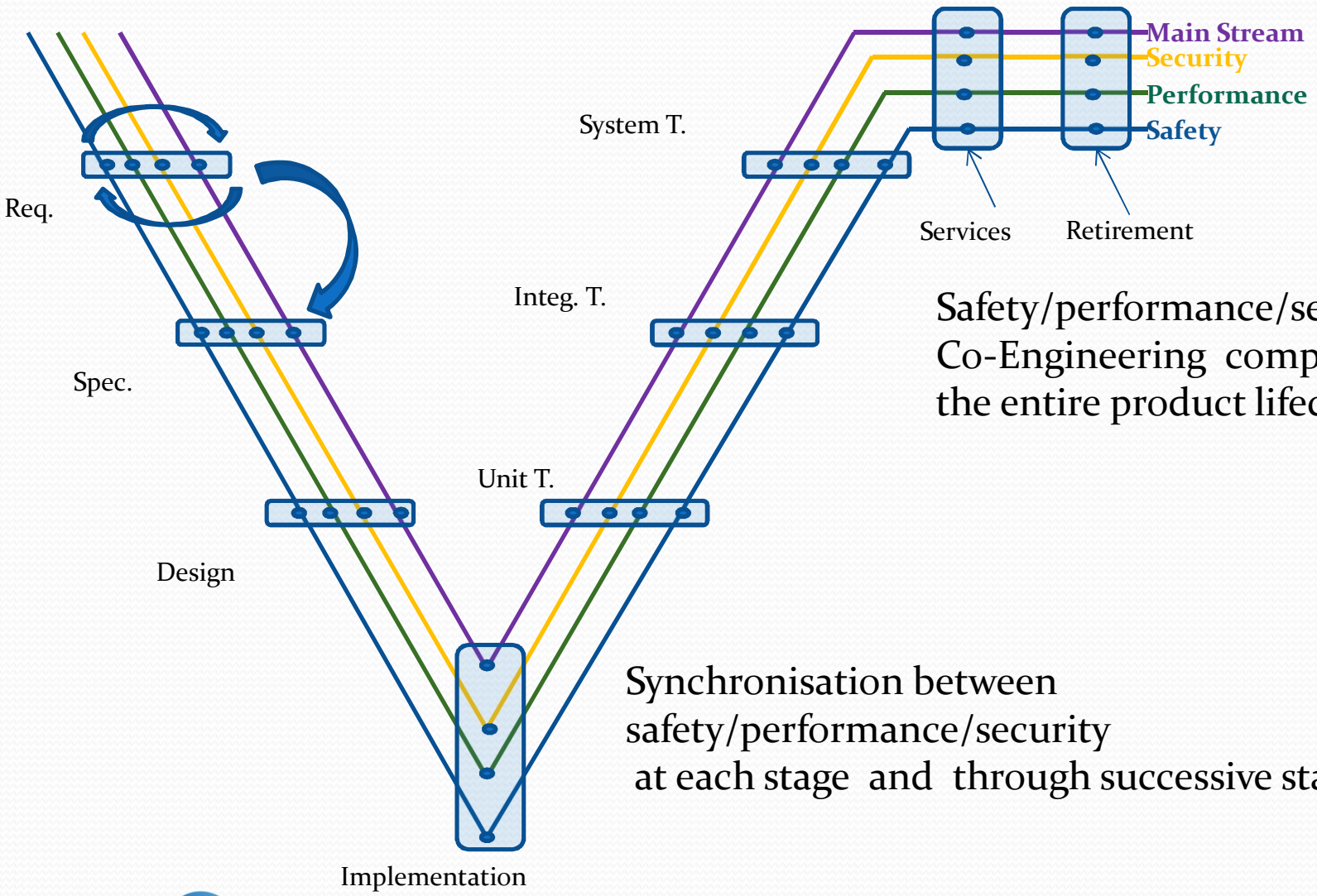
Co-engineering Objectives

A global concept framework for safety/security/performance co-engineering:

- Based on needs of industrial application domains.
- Support for balancing safety & security requirements with application specific performance requirements
- Established tools and platforms in combination with improved processes and methods for the co-engineering approaches and
- Complete product lifecycle and influencing of standards.
  - capability for system integration when sourced from subcontractors
  - capability for systems to evolve
  - Ease to qualify systems

AQUAS SAFETY SECURITY PERFORMANCE

AQUAS Work (Co-engineering)



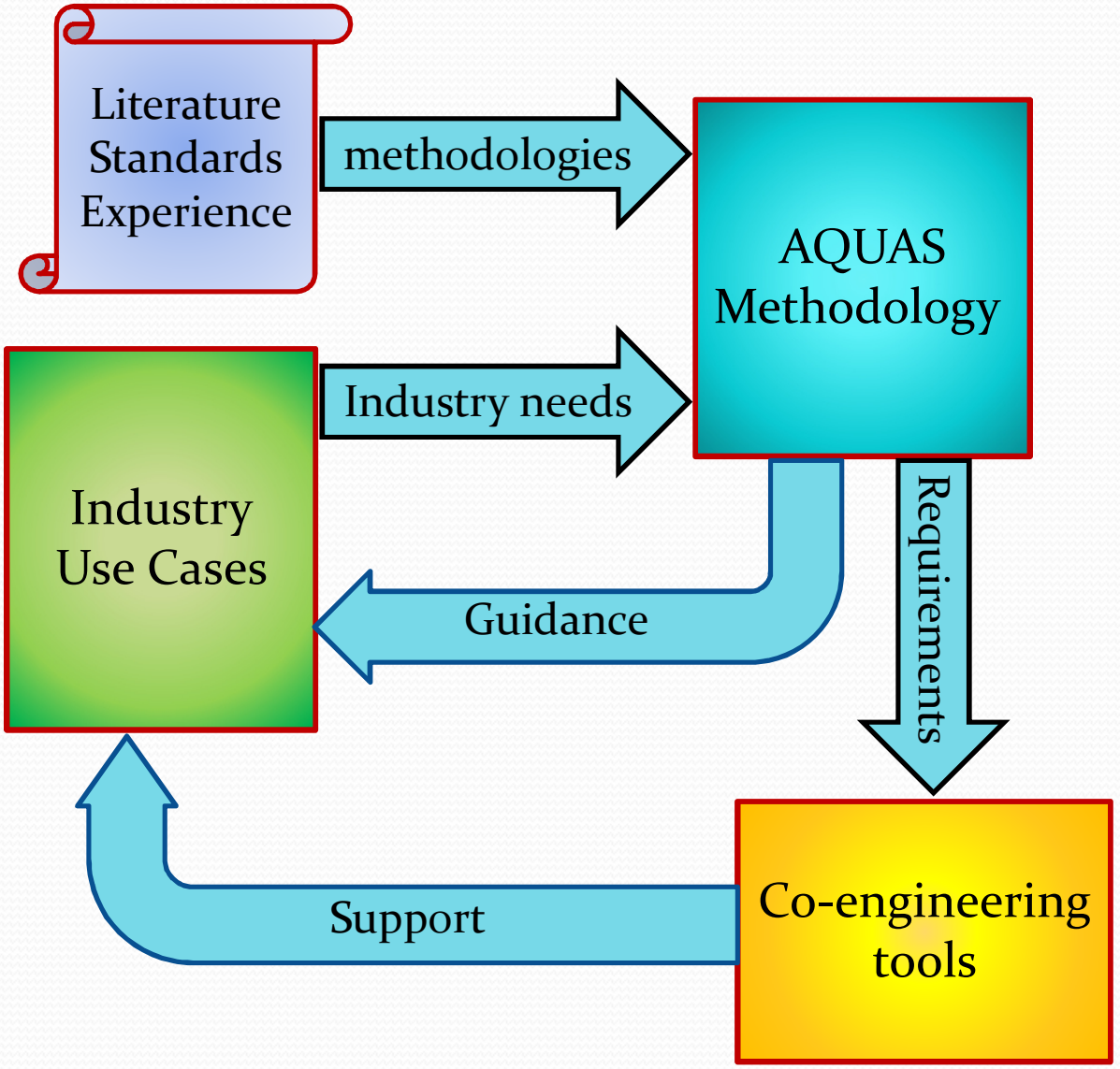
Safety/performance/security Co-Engineering comprises the entire product lifecycle.

Synchronisation between safety/performance/security at each stage and through successive stages.

AQUAS SAFETY SECURITY PERFORMANCE

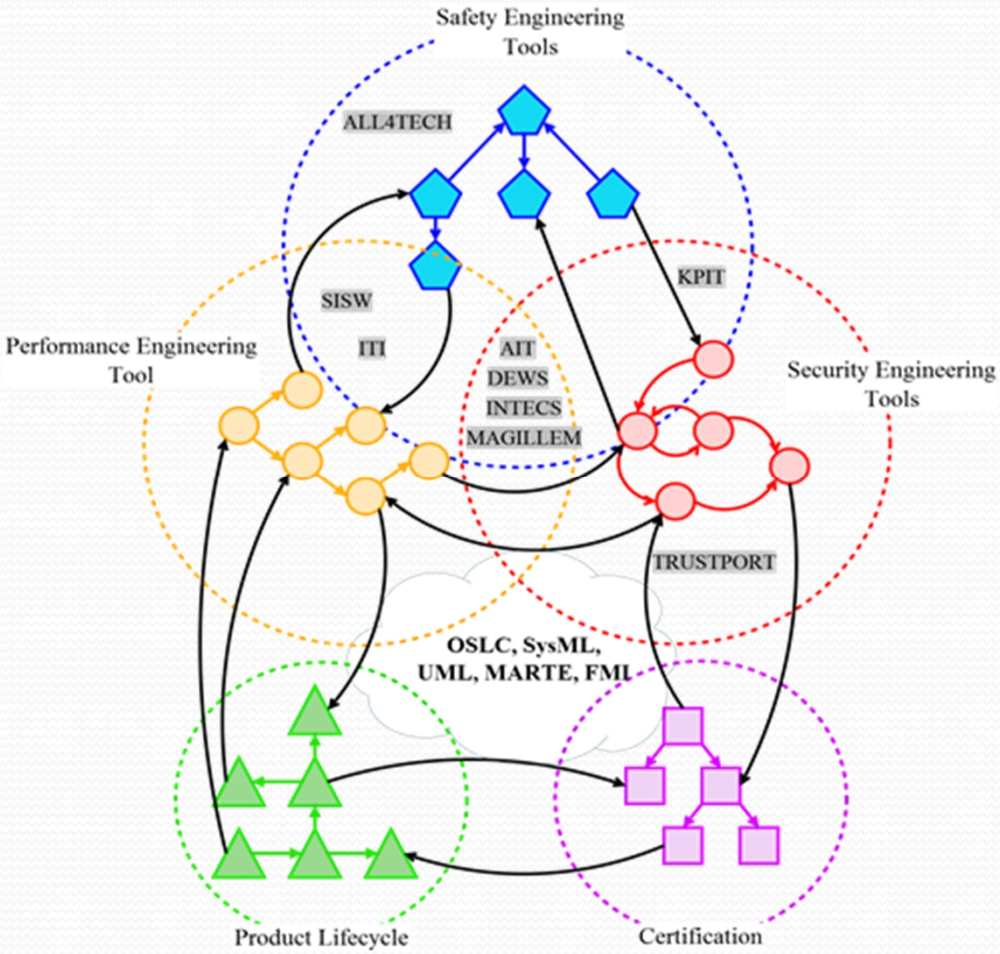
Developing the AQUAS Approach

- Iterative
- Out of use cases



AQUAS SAFETY SECURITY PERFORMANCE

AQUAS Tools

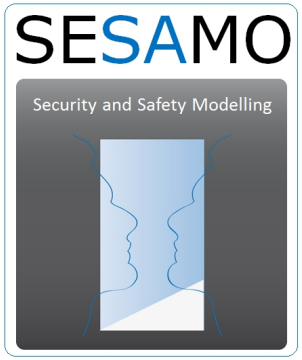


AQUAS SAFETY SECURITY PERFORMANCE

Interaction Points

SESAMO Background

- SESAMO (along with MerGe) is one of the major input projects to AQUAS
  - Started in 2012 – ended in 2015
- SESAMO was conceived on the principle of an integrated safety and security process
- Early in the project (2013) the consortium became aware of activities in standardization working groups concerning the relationship between the safety and security lifecycles
- The consortium decided to align its lifecycle framework with those activities, while retaining its core vision of integrating safety and security



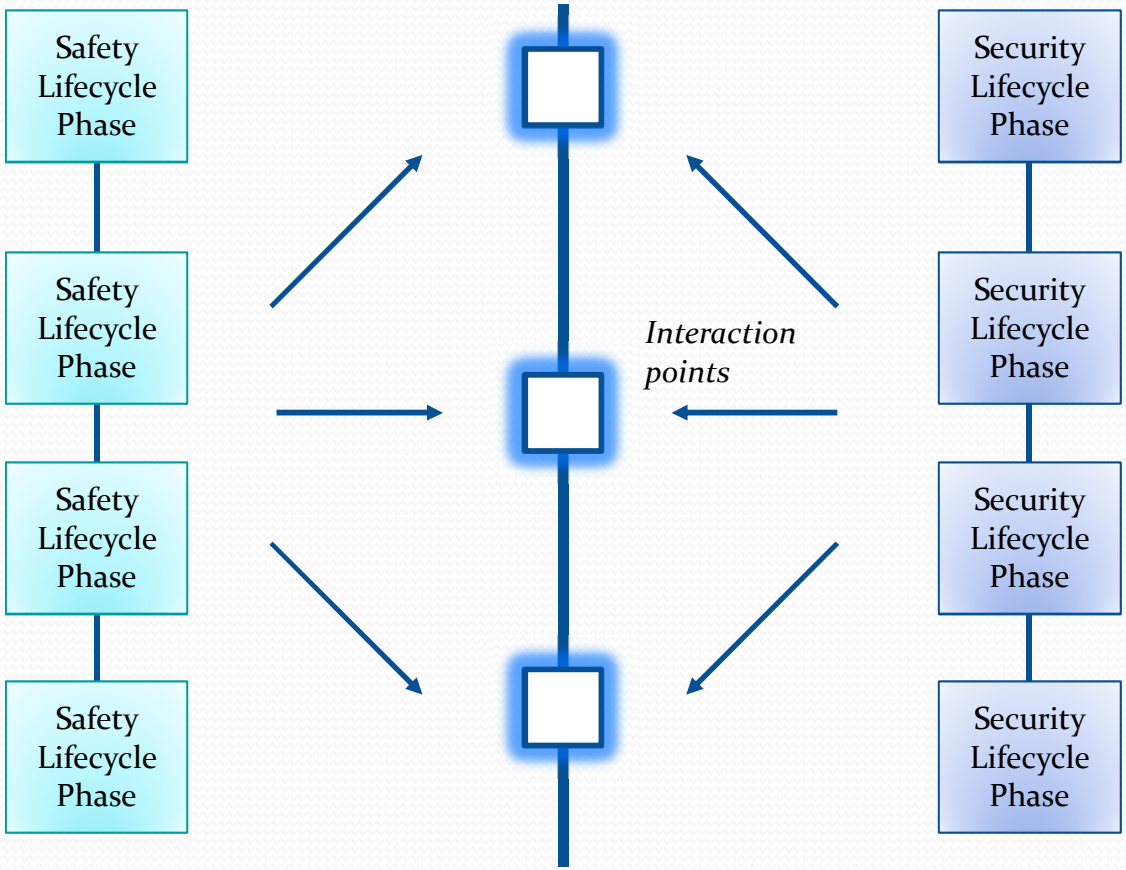
Position of Working Groups

- Concerning the relationship between the safety and security lifecycles
  - Cybersecurity is different (skills, process) from safety and more difficult than safety
  - Given the differences: separate processes
  - Do not add security requirements to ISO 26262 – safety experts should only focus on safety, security experts only on security
  - Rather, add requirement to establish communication channels between them, at specific identified interaction points

AQUAS SAFETY SECURITY PERFORMANCE

SAE Lifecycle

SURFACE VEHICLE RECOMMENDED PRACTICE	J3061™	JAN2016
	Issued 2016-01	
Cybersecurity Guidebook for Cyber-Physical Vehicle Systems		

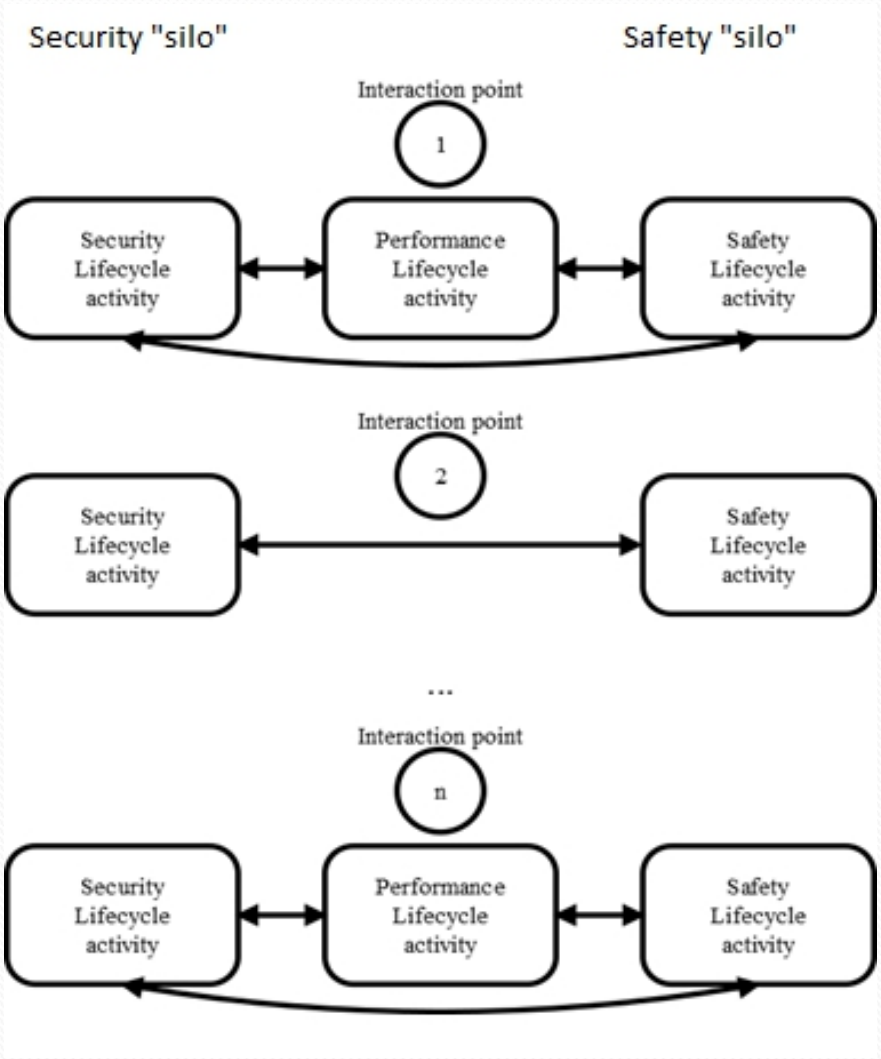


Interaction points: The Concept

At certain points in the product life-cycle (PLC), system developers/operators take decisions about how to progress with the development/apply patches/etc. These decisions require a *holistic view* on the system, and *trade-offs* to account simultaneously for all attributes of interest, safety, security and performance.

As development progresses, the initial decisions and allocation of goals and properties are subjected to ***refinements***. Each refinement step may or may not trigger an *interaction point*.

If as a result of a refinement *significant deviations* from the previous allocation of goals/properties are detected, a new trade-off has to be established between the assigned goals and component properties.



AQUAS SAFETY SECURITY PERFORMANCE

Interaction points: A Definition

- We call an "interaction point" both an **activity** and the **point** at which the activity occurs in a product life cycle (PLC).
- The activity is "interaction" in that:
  - experts in the various aspects of the system and its properties interact., e.g. security and safety experts
  - their analyses are combined in some way
    - anywhere in the range from informal discussion and mutual critique
    - to using mathematical models to assess various measures of interest for alternative design options, or even a single, summary measure to be optimised (e.g., probability of an undesired event)
  - the need for changes, or decisions affecting future development, may be recognised that require an integrated view, e.g. because of inevitable trade-offs between desirable properties, and these trade-offs are discussed between the various experts to produce recommendations/decisions.

AQUAS SAFETY SECURITY PERFORMANCE

Interaction points: Scheduling

- Interaction points could be *statically* or *dynamically* scheduled
  - Similar to preventive (i.e. statically scheduled) maintenance vs. reactive (i.e. on-demand) maintenance
  - These two alternatives are not mutually exclusive

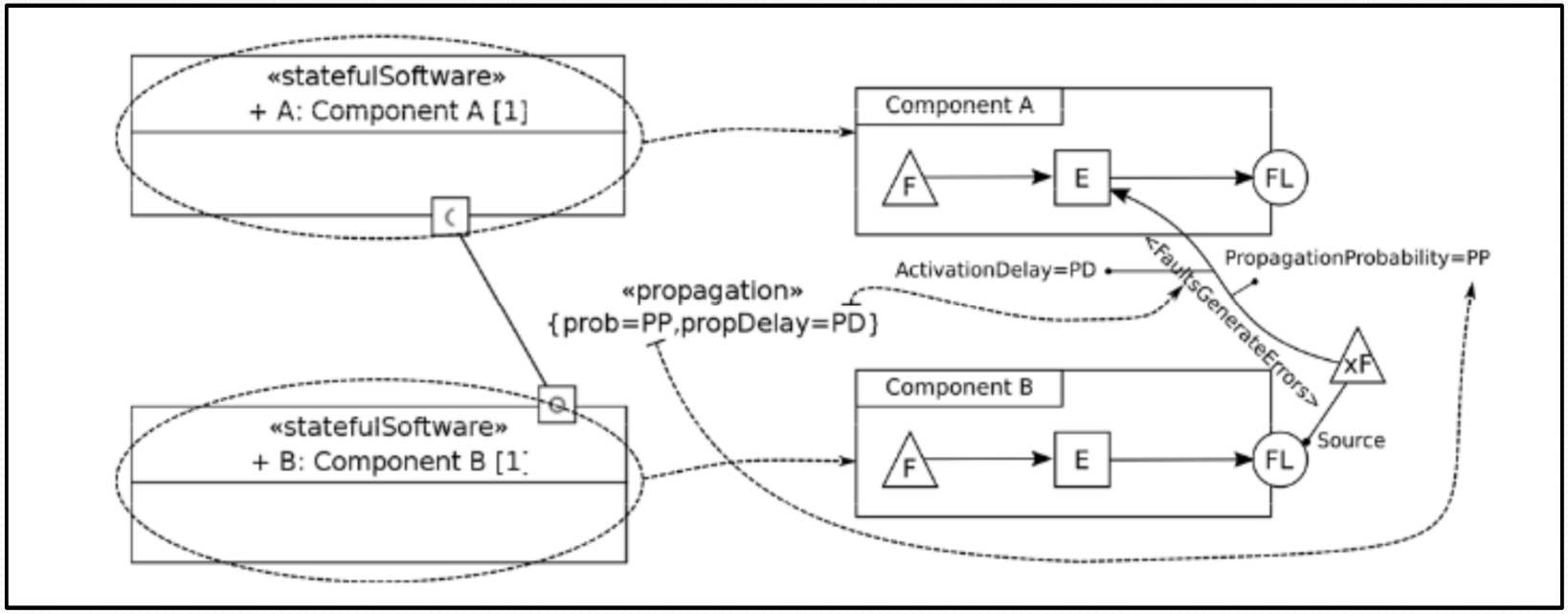
- UCs are initially planning "static" IPs, but an aspiration is to provide insight as to schedule interaction points cost-effectively, both statically or dynamically, evolve a “risk-based” approach to combined analysis.

IPs and "combined" (S/S/P) analysis

- At IPs, some form of combined analysis is undertaken
  - This analysis is based on models (ideally with adequate tool support), derived from a model of the system (e.g. a SysML model) under development (architecture, including h/w and s/w, etc.)
  - Combined analysis checks whether non-functional requirements are satisfied ***simultaneously***
    - If they are, the system model (design) is accepted and passed for further refinement by the development teams
    - If the analysis establishes that requirements ***cannot be met*** (or there are serious doubts whether they can be met), the system architecture must be corrected
      - The space of options must be explored until a solution is found with which all requirements are satisfied:
        - Either by ***changing the system architecture*** (e.g. by adding additional safety mechanisms/security controls), or
        - By ***changing the set of requirements*** of the system
        - or of subsystems (e.g. reallocating time or acceptable risk between them) so that they become achievable
  - Trade-off analysis of non-functional properties is essential

Tool support: System Development vs. Analysis

- A range of tools in AQUAS offer models for system development (SysML/UML) AND models for S/S/P analysis, which will be extended
  - FTA/attack trees, FME(C)A – FMEVA, etc.
  - Difference analyses require different models
- Many tools rely in AQUAS use analyses by 3rd party tools and offer model-transformation capabilities. Extending these to model dependence between S/S/P is under way:
  - Example: CHESS tool's dependability plug-in (and its language) will be to extended to generate a stochastic model (e.g. SAN) in which dependencies are adequately captured.



AQUAS SAFETY SECURITY PERFORMANCE

Ongoing Work

- Explain how the ***models*** used at IPs at different stages of the development are ***related***
  - Trade-off analyses at earlier stages of the PLC may be based on ***assumptions*** made before system design details become available.
  - These need to be checked at later stages.

- Experiment on ***example problems*** (typically simplified fragments of the AQUAS use cases developed in WP2), with IPs starting from the early stages of PLC.

- Learn how ***complexity*** of the modelled system ***impacts IPs*** and tool support.
  - We will start with small systems … and ***by the end of the project*** will apply the methodology to some of the ***full demonstrators***.
    - "AQUAS methodology" to emerge at the end of the project
- ***Trade-off analysis*** requires truly ***combined analysis***, *with* an explicit and credible ***model of dependence*** between the properties of interest

AQUAS SAFETY SECURITY PERFORMANCE

THANK YOU

ECSEL JU

AQUAS Partner Acronyms

TASE	**Thales Alenia Space Espana, SA - project coordinator**
TRT	Thales SA
Integrasys	Integrasys SA
RGB	R G B Medical Devices SA
CITY	City University Of London
AIT	Austrian Institute Of Technology Gmbh
UNIVAQ	Universita Degli Studi Dell'aquila
SISW	Siemens Industry Software SAS
MDS	Magillem Design Services SAS
ClearSy	Clearsy SAS
CEA	Commissariat A L'Energie Atomique Et Aux Energies Alternatives
TrustPort	Trustport, A.S.
MTTP	Institut Mines-Telecom
Tecnalia	Fundacion Tecnalia Research & Innovation
BUT	Brno University of Technology
All4Tec	Alliance Pour Les Technologies De L'informatique
ITI	Instituto Tecnologico De Informatica
Intecs	Intecs Solutions SPA
SAG	Siemens Aktiengesellschaft Oesterreich
HSRM	Hochschule Rheinmain
AMT	Ansys Medini Technologies AG
SYSGO	Sysgo AG
AbsInt	Absint Angewandte Informatik Gmbh