ECSEL
Joint Undertaking

European Commission

AMASS

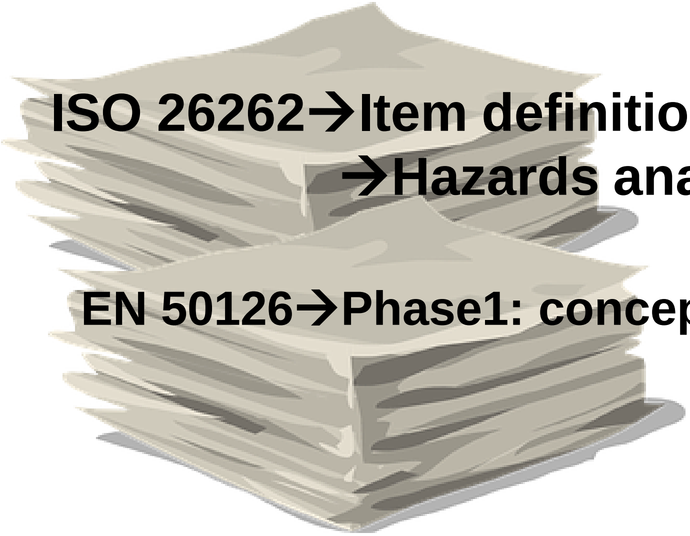
Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

AMASS: Technical Vision

First EAB Workshop
Trento, September 11, 2017

Barbara Gallina, Ph.D.
TM, WP6 Leader, T6.1-2 Leader
MÄLARDALEN UNIVERSITY
SWEDEN

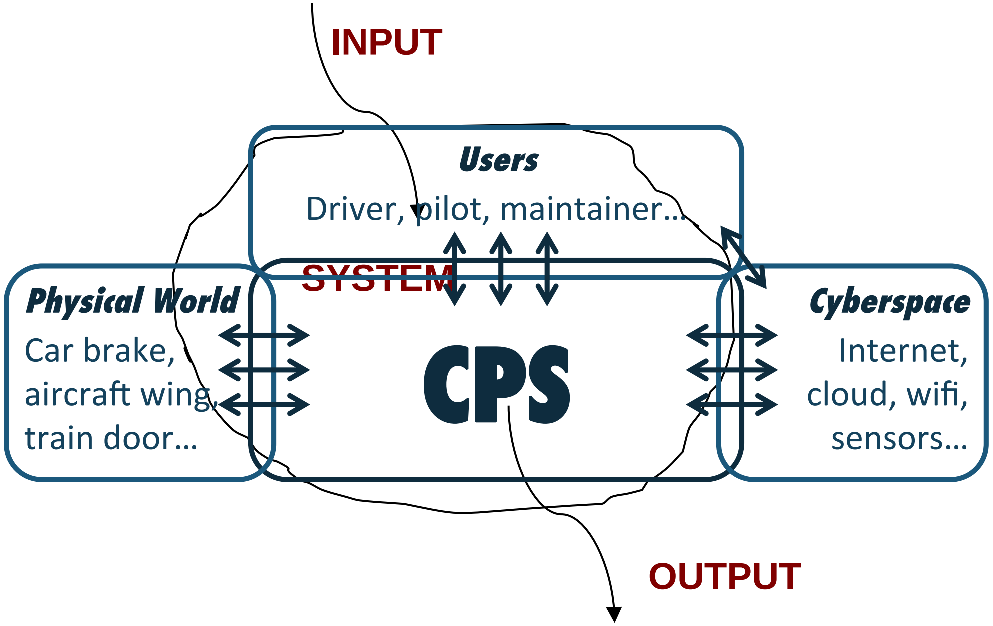
Context and motivation



ISO 26262→Item definition

→Hazards analysis and risk assessment

EN 50126→Phase1: concept



INPUT

SYSTEM

OUTPUT

Users

Driver, pilot, maintainer…

Physical World

Car brake, aircraft wing, train door…

CPS

Cyberspace

Internet, cloud, wifi, sensors…

BOUNDARY OF SYSTEM/INTERFACES
ENVIRONMENT OF THE SYSTEM

?

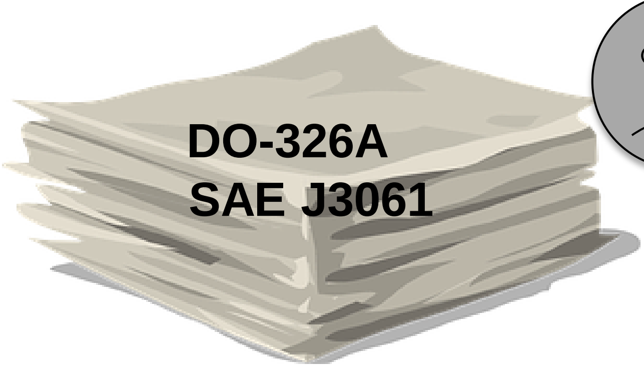
Context and motivation

- Process engineer addressing the safety process
- Architect addressing safety

ARP4761

ISO 26262

- Process engineer addressing the security process
- Architect addressing security



DO-326A

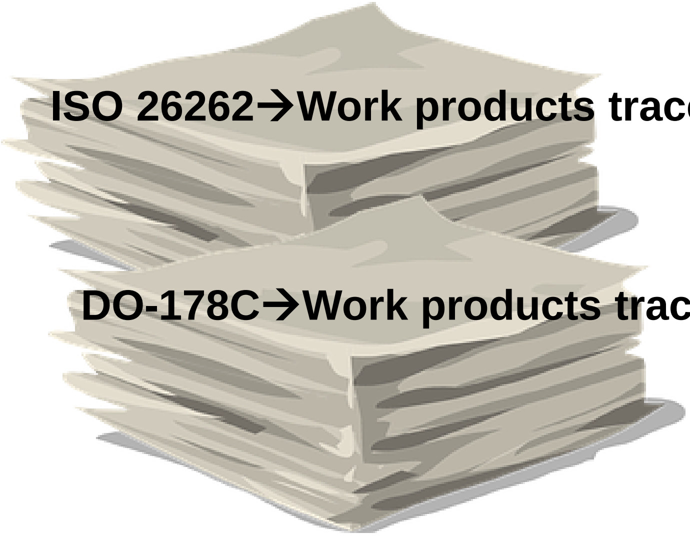
SAE J3061

→ **Redundant and conflicting documentation/solutions**

→ **Waste of time and money**

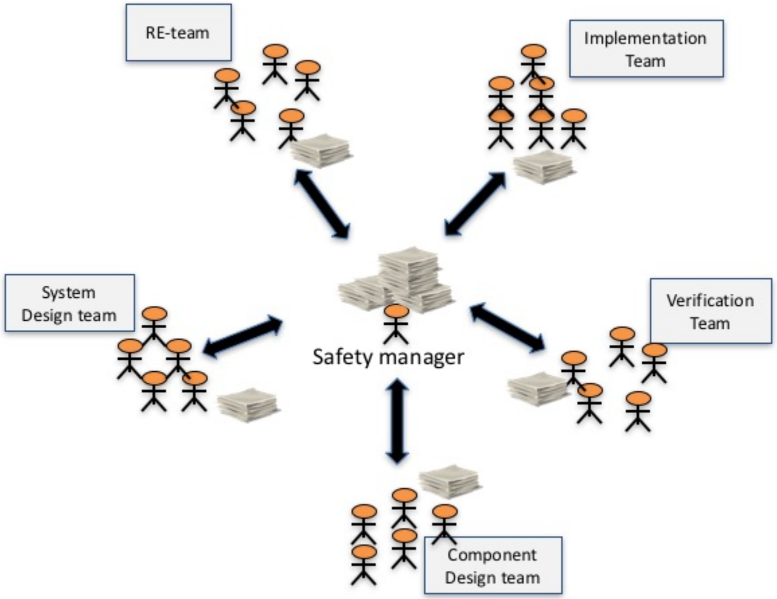
→ **Risk for lower quality**

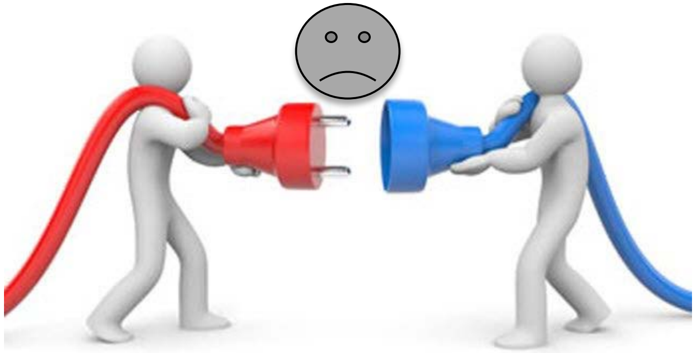
Context and motivation



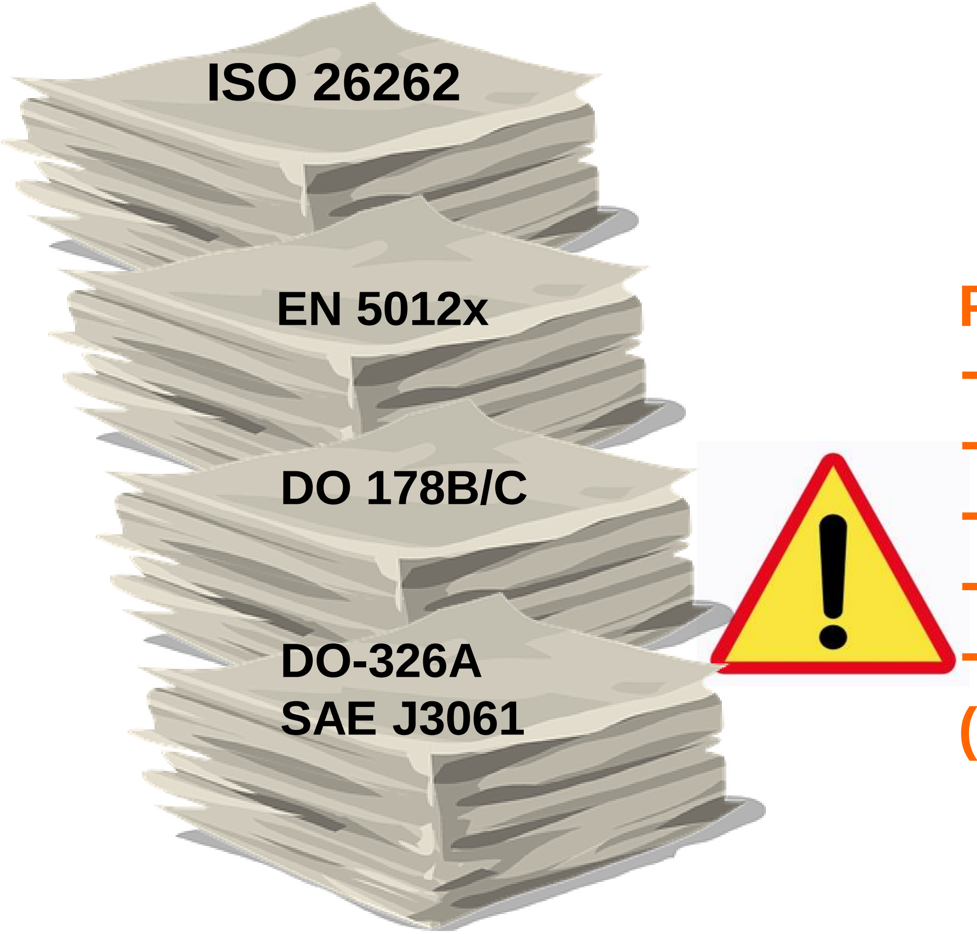
ISO 26262→Work products traceability

DO-178C→Work products traceability



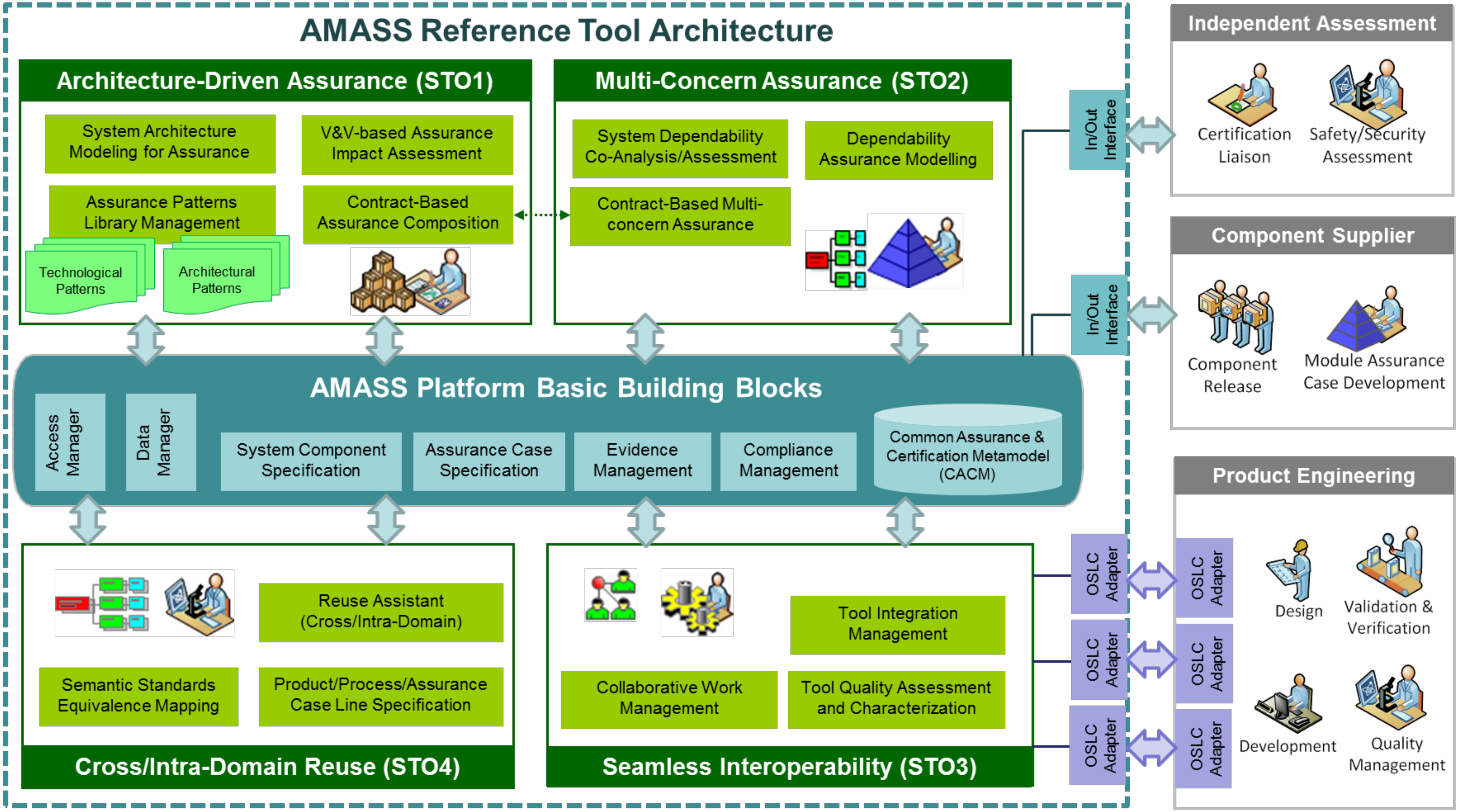


Context and motivation



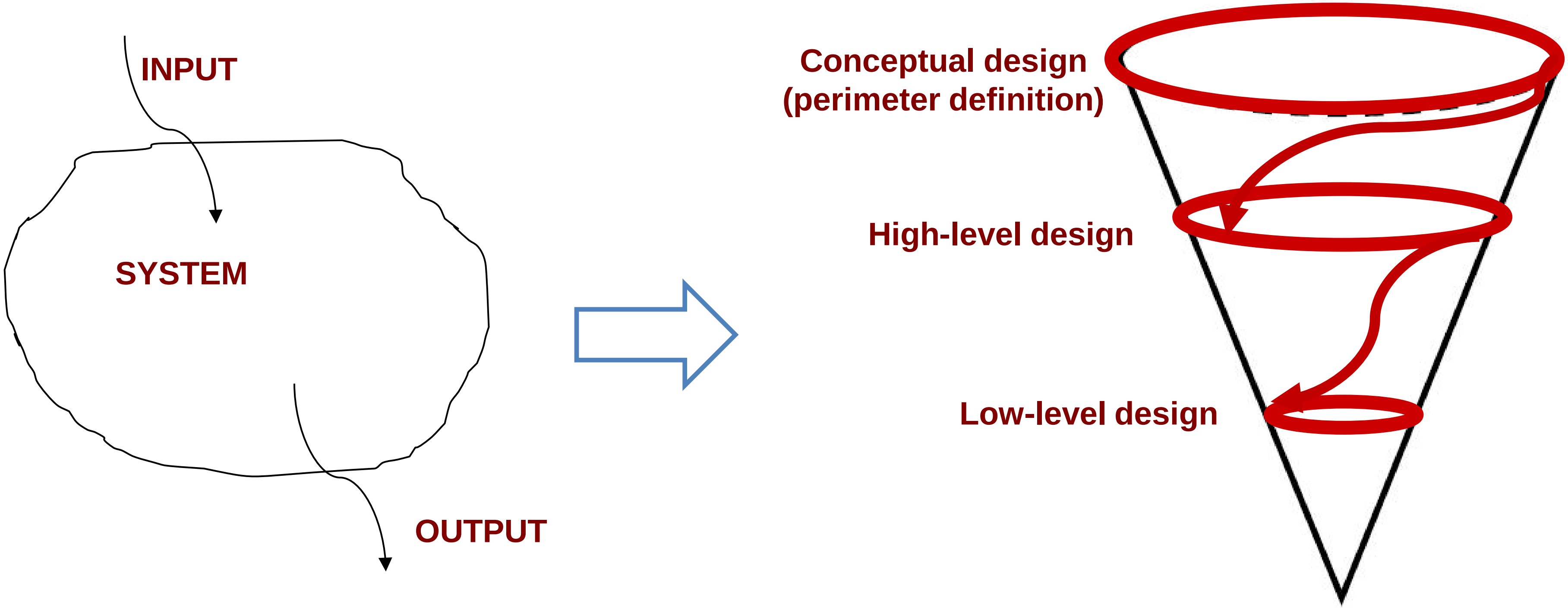
Proliferation of standards
→thousands of pages!
→terminological inconsistency
→increasing complexity
→intellectual unmanageability
→(re)certification is inefficient
(time consuming and expensive!)

AMASS



AMASS Reference Tool Architecture
Architecture-Driven Assurance (STO1)
System Architecture Modeling for Assurance
V&V-based Assurance Impact Assessment
Assurance Patterns Library Management
Contract-Based Assurance Composition
Technological Patterns
Architectural Patterns
Multi-Concern Assurance (STO2)
System Dependability Co-Analysis/Assessment
Dependability Assurance Modelling
Contract-Based Multi-concern Assurance
AMASS Platform Basic Building Blocks
Access Manager
Data Manager
System Component Specification
Assurance Case Specification
Evidence Management
Compliance Management
Common Assurance & Certification Metamodel (CACM)
Reuse Assistant (Cross/Intra-Domain)
Semantic Standards Equivalence Mapping
Product/Process/Assurance Case Line Specification
Cross/Intra-Domain Reuse (STO4)
Tool Integration Management
Collaborative Work Management
Tool Quality Assessment and Characterization
Seamless Interoperability (STO3)
In/Out Interface
In/Out Interface
Independent Assessment
Certification Liaison
Safety/Security Assessment
Component Supplier
Component Release
Module Assurance Case Development
Product Engineering
OSLC Adapter
OSLC Adapter
OSLC Adapter
OSLC Adapter
OSLC Adapter
OSLC Adapter
Design
Validation & Verification
Development
Quality Management

Architecture-driven



INPUT

SYSTEM

OUTPUT

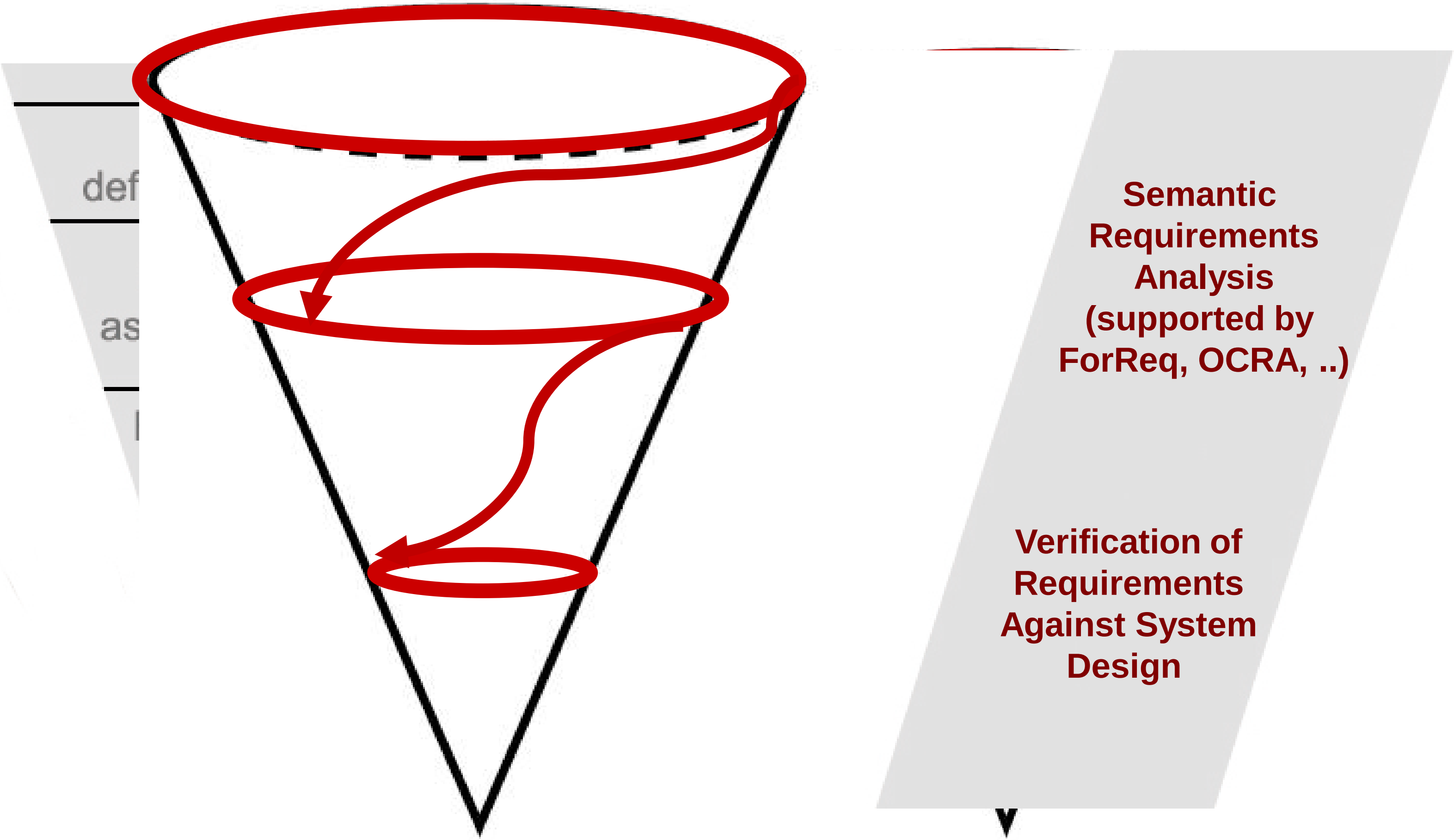
Conceptual design (perimeter definition)

High-level design

Low-level design

Architecture-driven

Contract-based, component based systems engineering

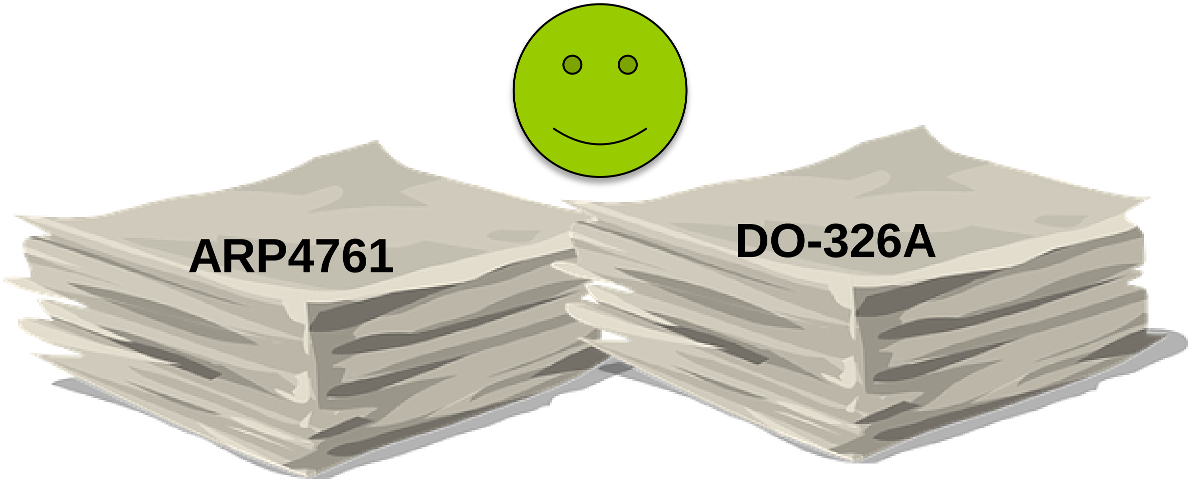


Semantic Requirements Analysis (supported by ForReq, OCRA, ..)

Verification of Requirements Against System Design

Multi-concern assurance

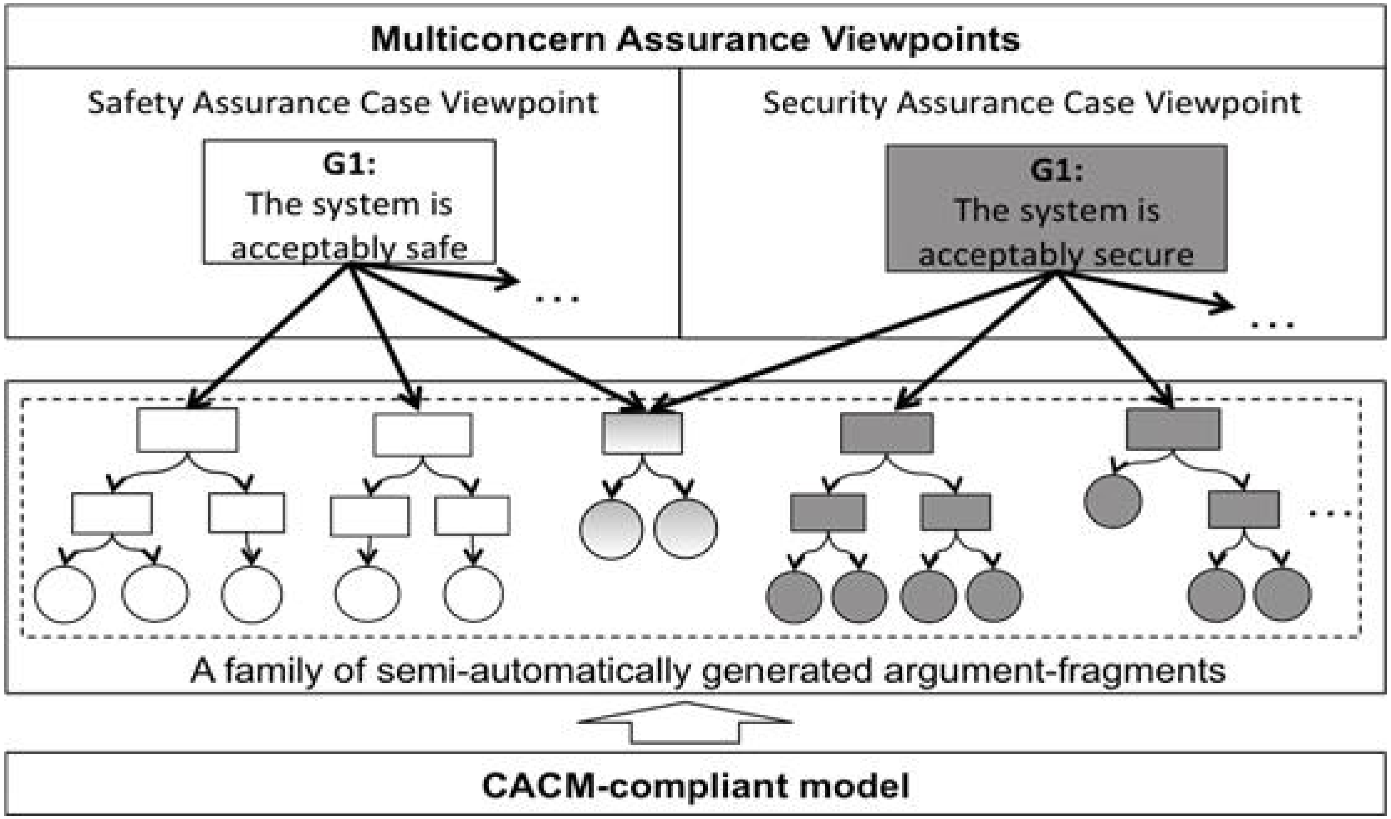
- Process engineer(s) addressing the security & safety process
- Architect jointly interacting with safety and security managers



→ **Synergically conceived documentation/solutions**
→ **Increased quality**

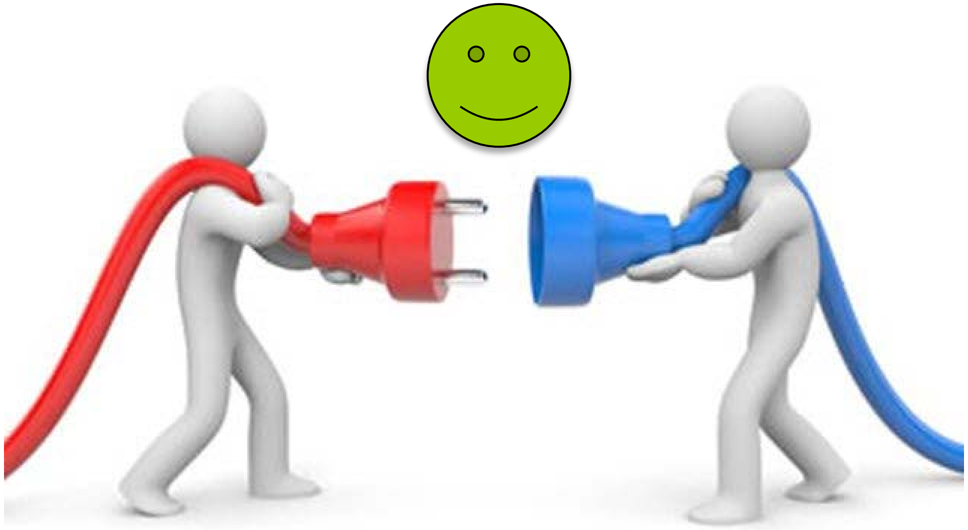
Multi-concern assurance

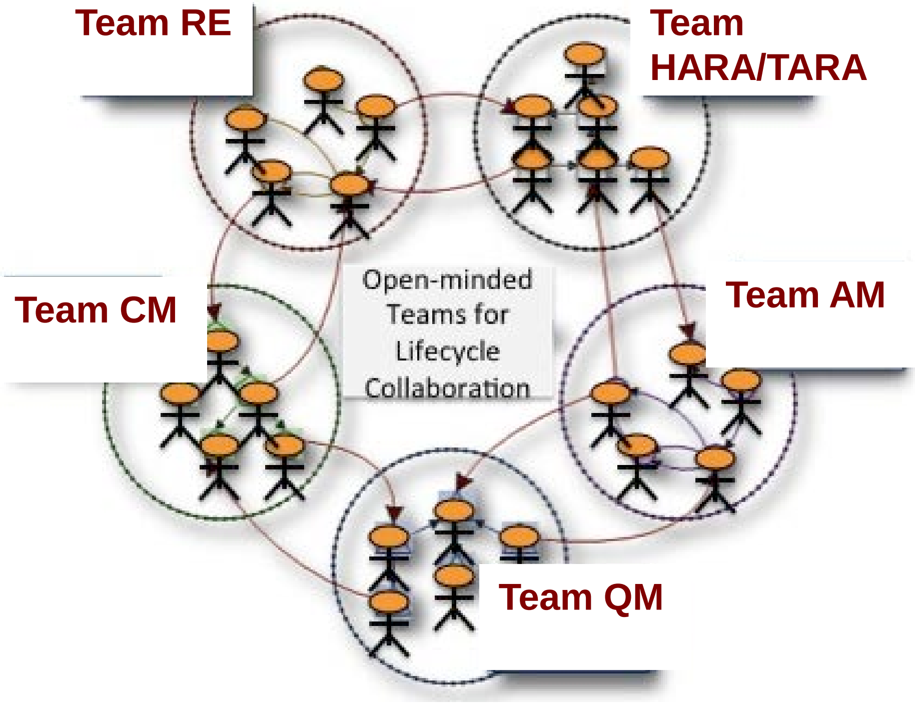
Trade-off analysis, Process-related co-assessment


Multiconcern Assurance Viewpoints
Safety Assurance Case Viewpoint
G1:
The system is acceptably safe
...
Security Assurance Case Viewpoint
G1:
The system is acceptably secure
...
...
A family of semi-automatically generated argument-fragments
CACM-compliant model

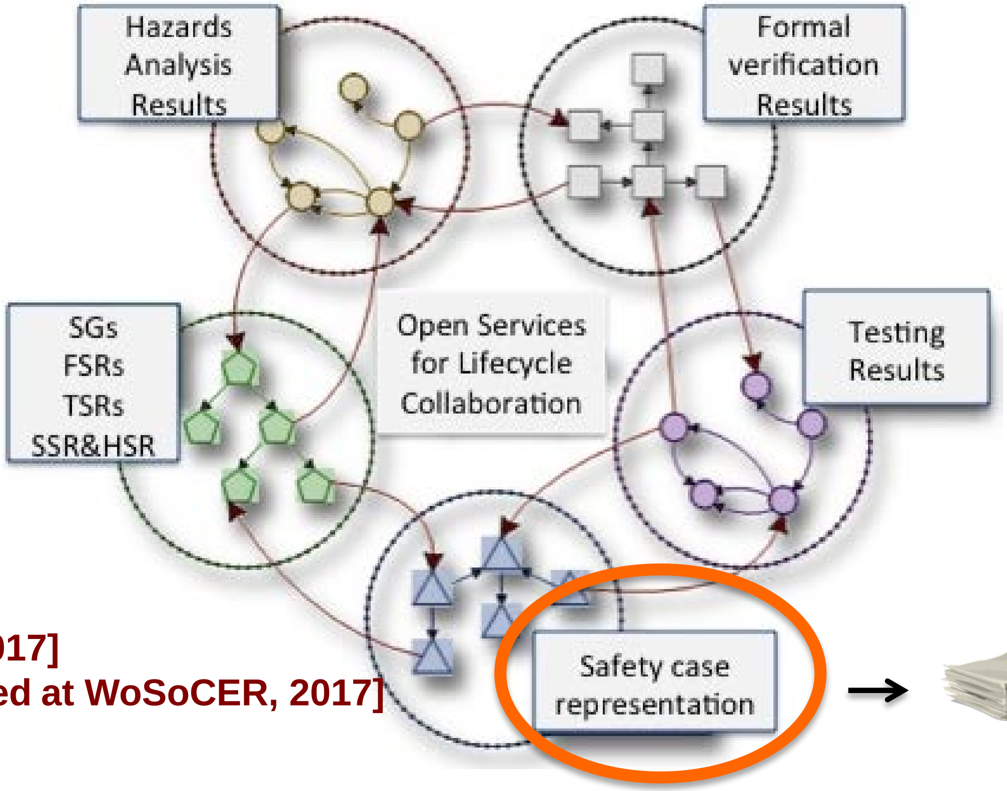
[Presented at ISSA, 2016]

Seamless interoperability





Seamless interoperability


Hazards Analysis Results
Formal verification Results
SGs
FSRs
TSRs
SSR&HSR
Open Services for Lifecycle Collaboration
Testing Results
Safety case representation

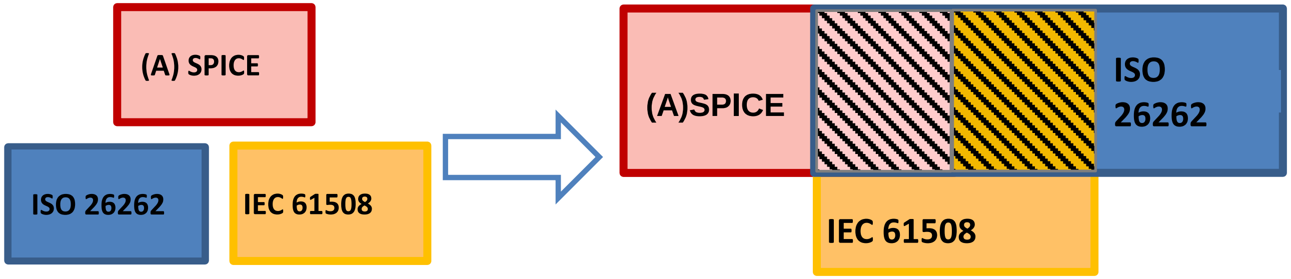
[Presented at RSSRail, 2017]
[Evolution, to be presented at WoSoCER, 2017]

→ Safety case

Safety Case-Argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development.
ISO 26262- Part 1, Definition 1.106

Cross and intra domain reuse

Intra domain: Automotive normative space


(A) SPICE

ISO 26262

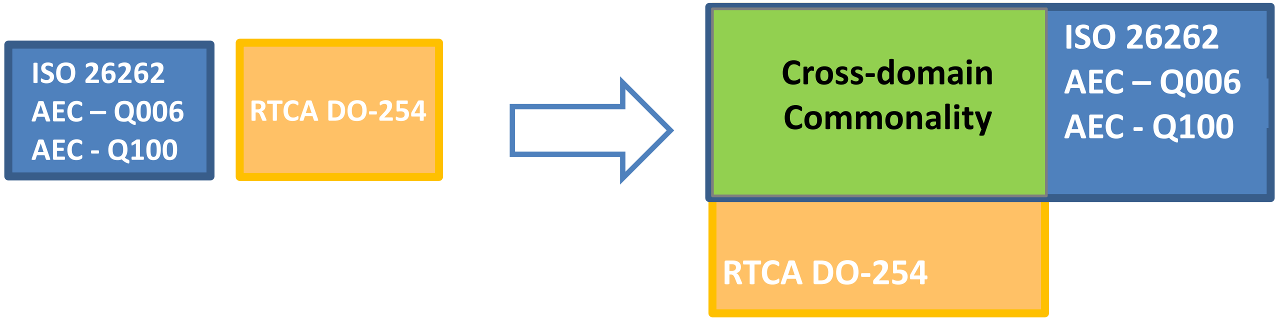
IEC 61508

(A)SPICE

ISO 26262

IEC 61508

Cross-domain: Automotive/Avionics


ISO 26262
AEC – Q006
AEC - Q100

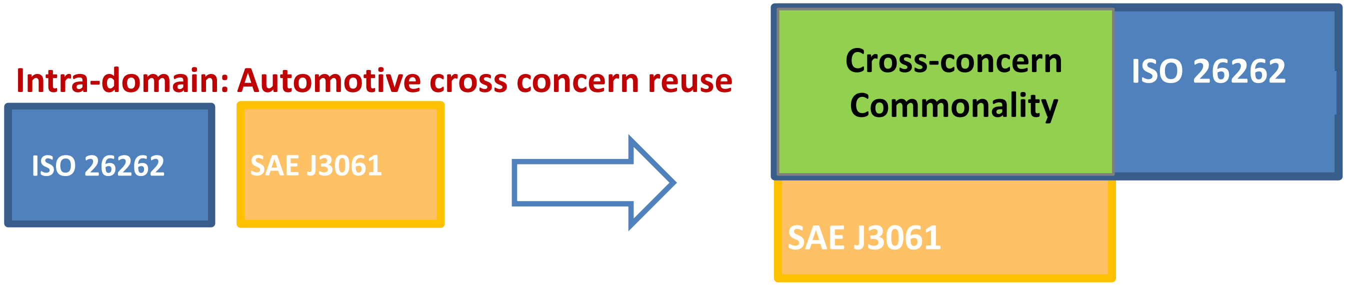
RTCA DO-254

Cross-domain Commonality

ISO 26262
AEC – Q006
AEC - Q100

RTCA DO-254

Intra-domain: Automotive cross concern reuse


ISO 26262

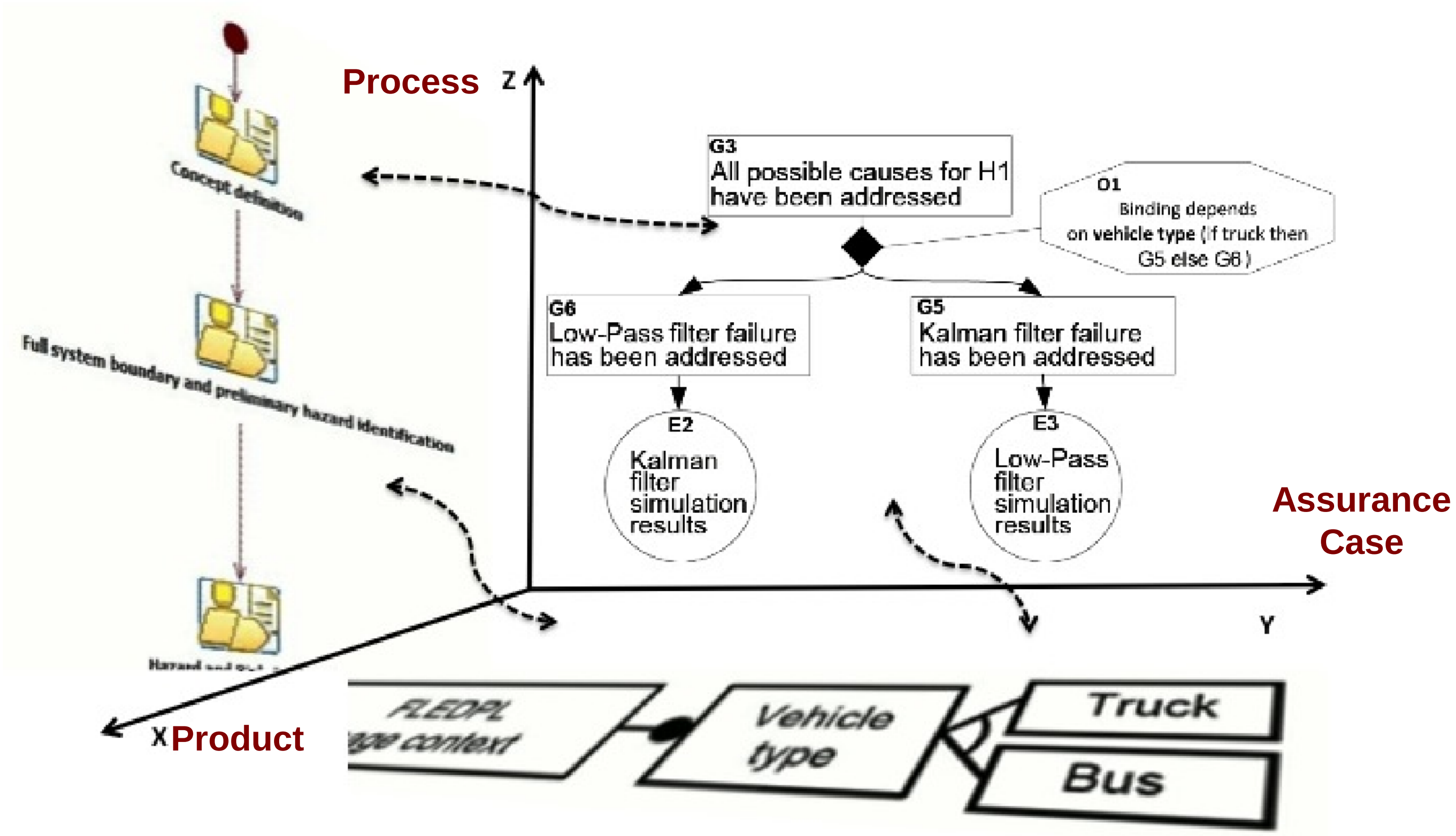
SAE J3061

Cross-concern Commonality

ISO 26262

SAE J3061

Anti-Sysiphus


Process
Z
Concept definition
Full system boundary and preliminary hazard identification
Hazard and ris...
G3
All possible causes for H1 have been addressed
O1
Binding depends on vehicle type (if truck then G5 else G6)
G6
Low-Pass filter failure has been addressed
G5
Kalman filter failure has been addressed
E2
Kalman filter simulation results
E3
Low-Pass filter simulation results
Assurance Case
Y
X
Product
FLEDPL
...age context
Vehicle type
Truck
Bus

AMASS Prototypes

Three prototyping dimensions:

1. **Conceptual/Research Development**: development of solutions from a conceptual perspective.
2. **Tool Development**: development of tools implementing conceptual solutions.
3. **Case Study Development**: development of industrial case studies using the conceptual and tooling solutions.

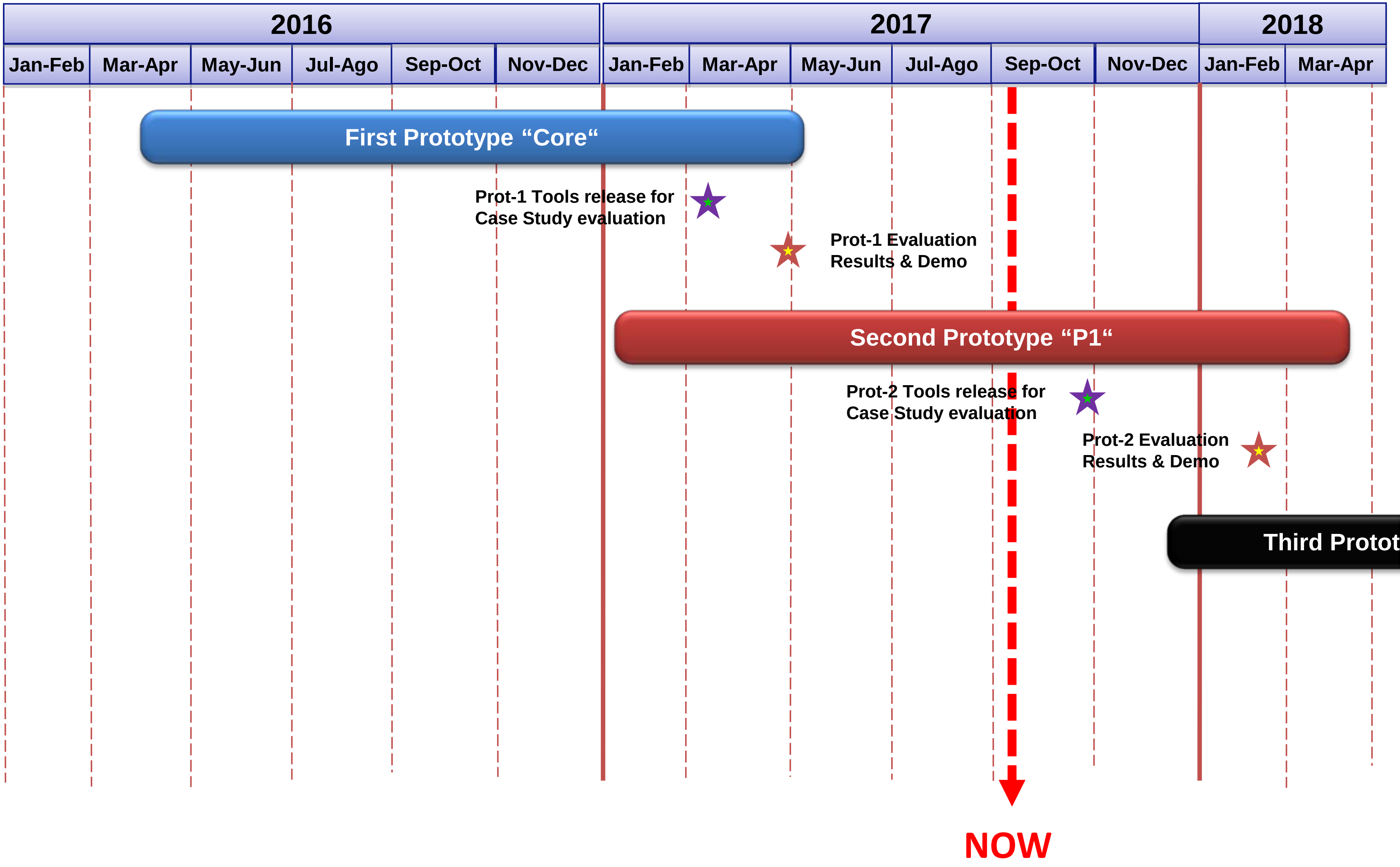
Prototype iterations has three phases:

a) **Prototype Development:** Involves the three dimensions above-mentioned

b) **Prototype Evaluation:** Results evaluated by research questions, tool objectives and case goal achievements.

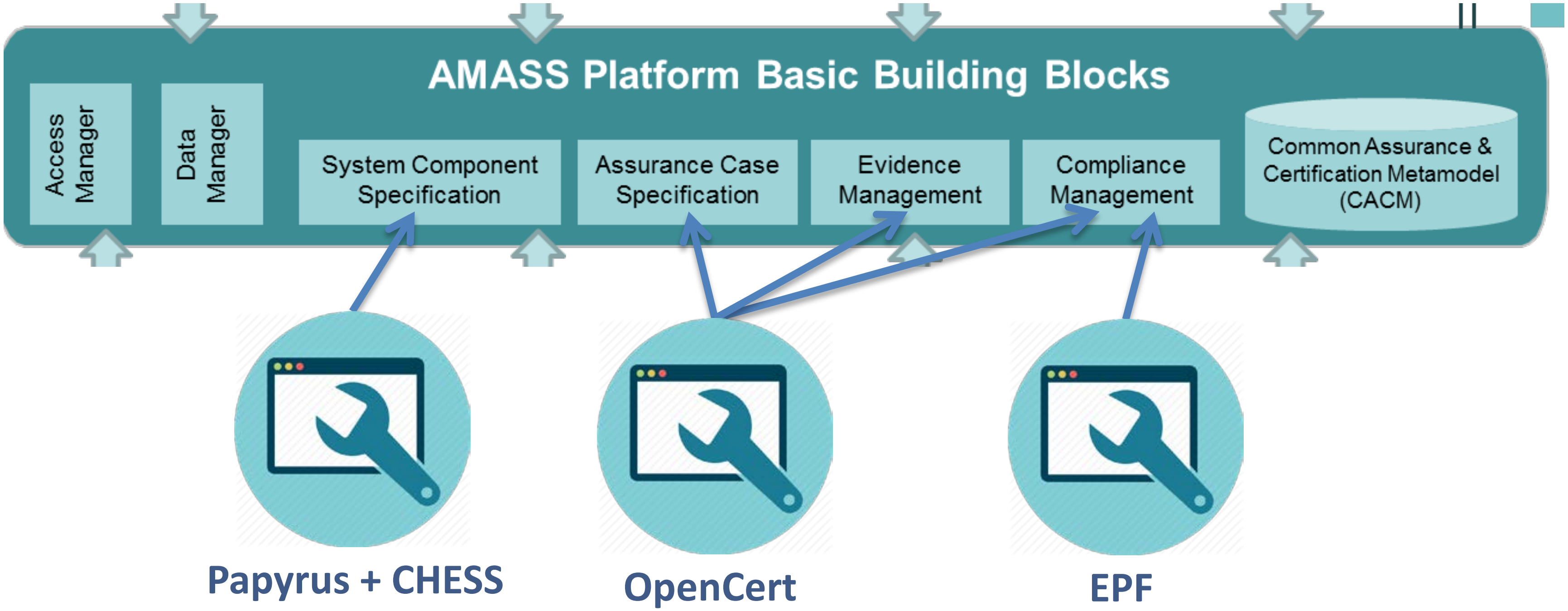
c) **Prototype Refinement:** Changes to the AMASS approach as recommended by the Evaluation phase

Prototype Schedule (First and Second Prototype)

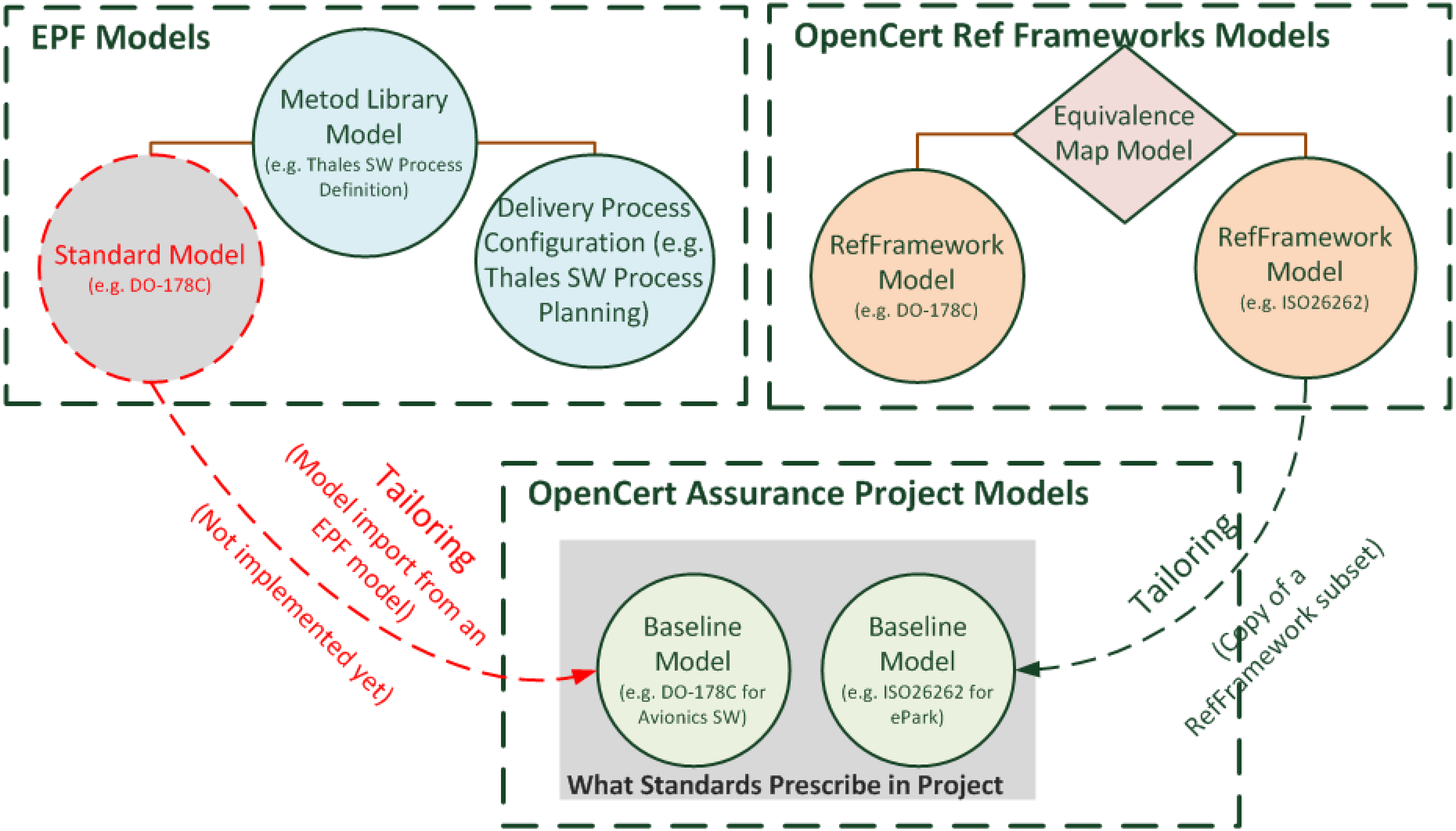


Prototype Core: Baseline Tools

- ❖ Functional description in D2.2: AMASS Reference Architecture (a)
- ❖ Prototype Core has been built upon 3 pre-existing toolsets:
  1. Tools from Papyrus and CHESS projects (Eclipse/PolarSys)
  2. Tools from pre-existing OpenCert project (Eclipse /PolarSys)
  3. Tools from EPF (Eclipse Process Framework) project (Eclipse)

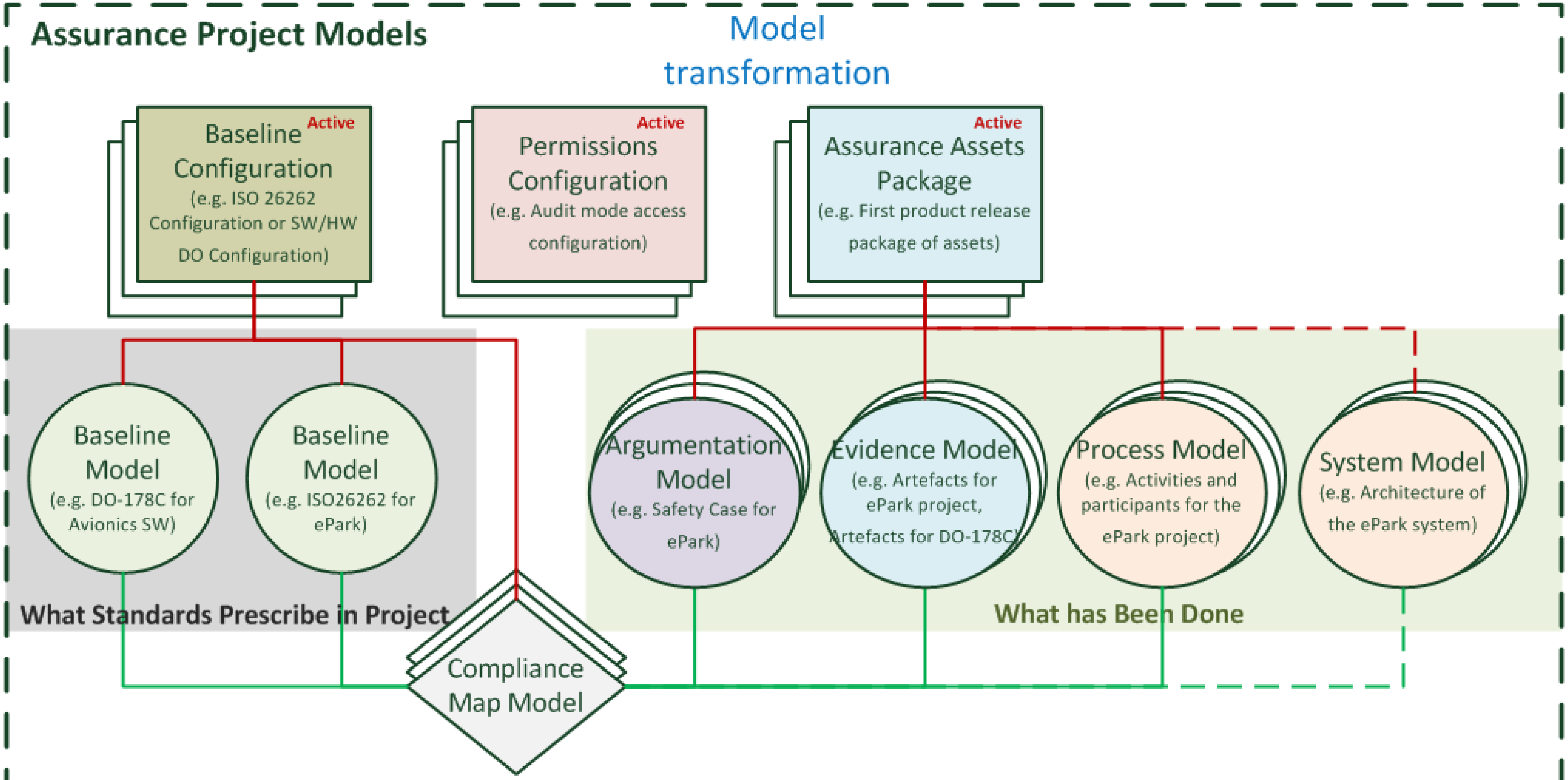

AMASS Platform Basic Building Blocks
Access Manager
Data Manager
System Component Specification
Assurance Case Specification
Evidence Management
Compliance Management
Common Assurance & Certification Metamodel (CACM)
Papyrus + CHESS
OpenCert
EPF

AMASS Platform: Standards & Process Models


EPF Models
Metod Library Model
(e.g. Thales SW Process Definition)
Standard Model
(e.g. DO-178C)
Delivery Process Configuration (e.g. Thales SW Process Planning)
OpenCert Ref Frameworks Models
Equivalence Map Model
RefFramework Model
(e.g. DO-178C)
RefFramework Model
(e.g. ISO26262)
Tailoring
(Model import from an EPF model)
(Not implemented yet)
OpenCert Assurance Project Models
Baseline Model
(e.g. DO-178C for Avionics SW)
Baseline Model
(e.g. ISO26262 for ePark)
What Standards Prescribe in Project
Tailoring
(Copy of a RefFramework subset)

*Tailoring EPF Standard models into Baseline models has not implemented yet.

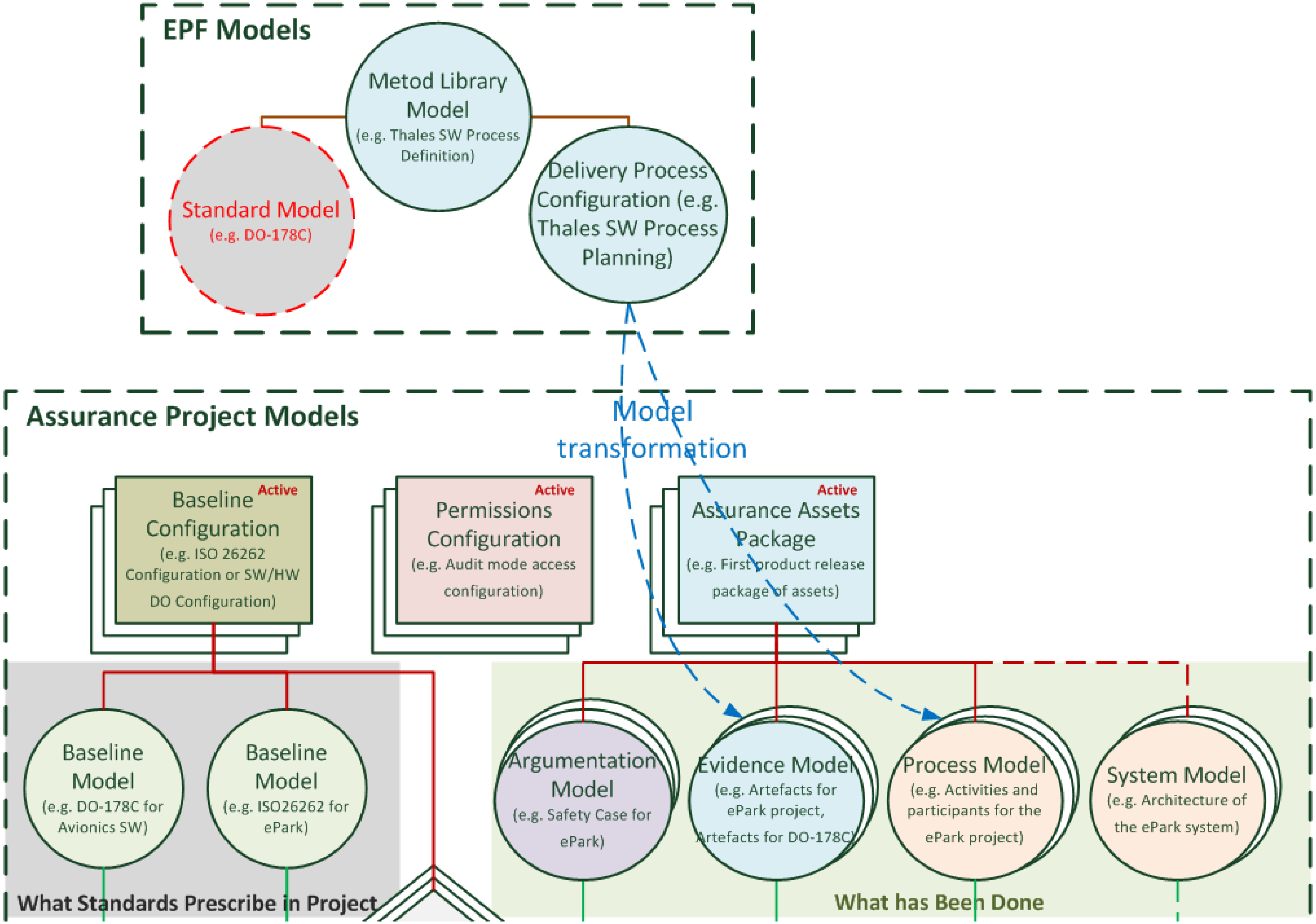
AMASS Platform: Assurance Project Models



Assurance Project Models
Model transformation
Baseline Configuration
Active
(e.g. ISO 26262 Configuration or SW/HW DO Configuration)
Permissions Configuration
Active
(e.g. Audit mode access configuration)
Assurance Assets Package
Active
(e.g. First product release package of assets)
Baseline Model
(e.g. DO-178C for Avionics SW)
Baseline Model
(e.g. ISO26262 for ePark)
What Standards Prescribe in Project
Argumentation Model
(e.g. Safety Case for ePark)
Evidence Model
(e.g. Artefacts for ePark project, Artefacts for DO-178C)
Process Model
(e.g. Activities and participants for the ePark project)
System Model
(e.g. Architecture of the ePark system)
What has Been Done
Compliance Map Model

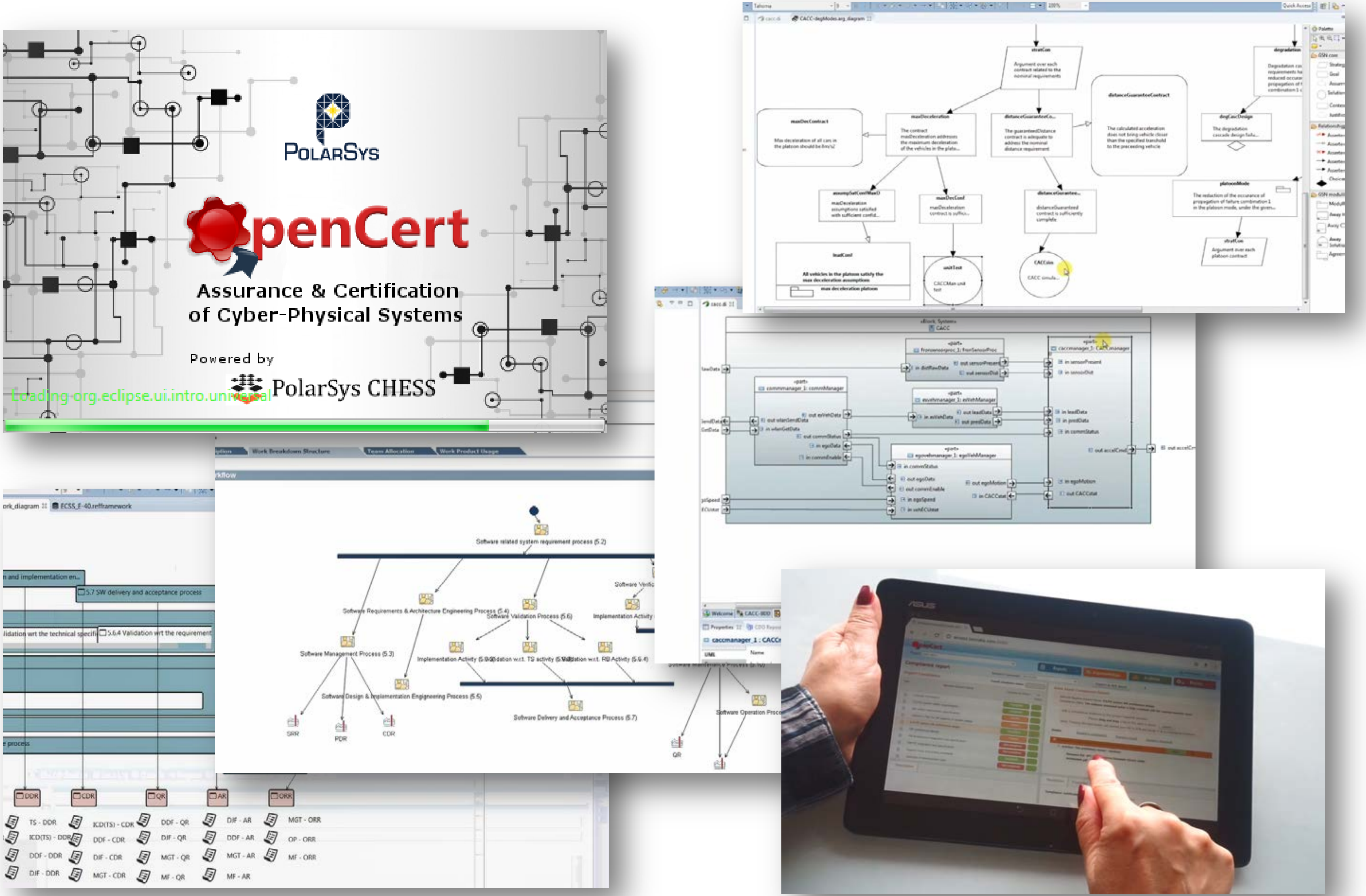
*System Models are edited in Papyrus + CHESS. Its links have not been created yet.

AMASS Platform: Importing EPF Models



EPF Models
Metod Library Model (e.g. Thales SW Process Definition)
Standard Model (e.g. DO-178C)
Delivery Process Configuration (e.g. Thales SW Process Planning)
Model transformation
Assurance Project Models
Active
Baseline Configuration (e.g. ISO 26262 Configuration or SW/HW DO Configuration)
Active
Permissions Configuration (e.g. Audit mode access configuration)
Active
Assurance Assets Package (e.g. First product release package of assets)
Baseline Model (e.g. DO-178C for Avionics SW)
Baseline Model (e.g. ISO26262 for ePark)
Argumentation Model (e.g. Safety Case for ePark)
Evidence Model (e.g. Artefacts for ePark project, Artefacts for DO-178C)
Process Model (e.g. Activities and participants for the ePark project)
System Model (e.g. Architecture of the ePark system)
What Standards Prescribe in Project
What has Been Done

Prototype Core: Video


PolarSys
OpenCert
Assurance & Certification of Cyber-Physical Systems
Powered by
PolarSys CHESS
Loading org.eclipse.ui.intro.universal
Work Breakdown Structure
Team Allocation
Work Product Usage
Workflow
Software related system requirement process (5.2)
Software Requirements & Architecture Engineering Process (5.4)
Software Validation Process (5.6)
Implementation Activity
Software Management Process (5.3)
Software Design & Implementation Engineering Process (5.5)
Software Delivery and Acceptance Process (5.7)
Software Operation Process
SRR
PDR
CDR
QR
5.7 SW delivery and acceptance process
5.6.4 Validation wrt the requirement
DDR
CDR
QR
AR
ORR
TS - DDR
ICD(TS) - DDR
DDF - DDR
DJF - DDR
ICD(TS) - CDR
DDF - CDR
DJF - CDR
MGT - CDR
DDF - QR
DJF - QR
MGT - QR
MF - QR
DJF - AR
DDF - AR
MGT - AR
MF - AR
MGT - ORR
OP - ORR
MF - ORR
ECSS_E-40.refframework
stratCon
maxDecContract
maxDeceleration
distanceGuaranteeCo...
distanceGuaranteeContract
degradation
degCaccDesign
platoonMode
assumpSatConfMaxD
maxDecConf
distanceGuarantee...
leadConf
unitTest
CACCsim
CACC
commmanager_1: commManager
caccmanager_1: CACCmanager
evehmanager_1: evVehManager
egovehmanager_1: egoVehManager
ASUS
Compliance report

Thank you for your attention!

?