



AMASS

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

WP4: Multiconcern Assurance Progress and Achievements

First EAB Workshop
Trento, 11 September, 2017

Thomas Gruber
WP4 Leader



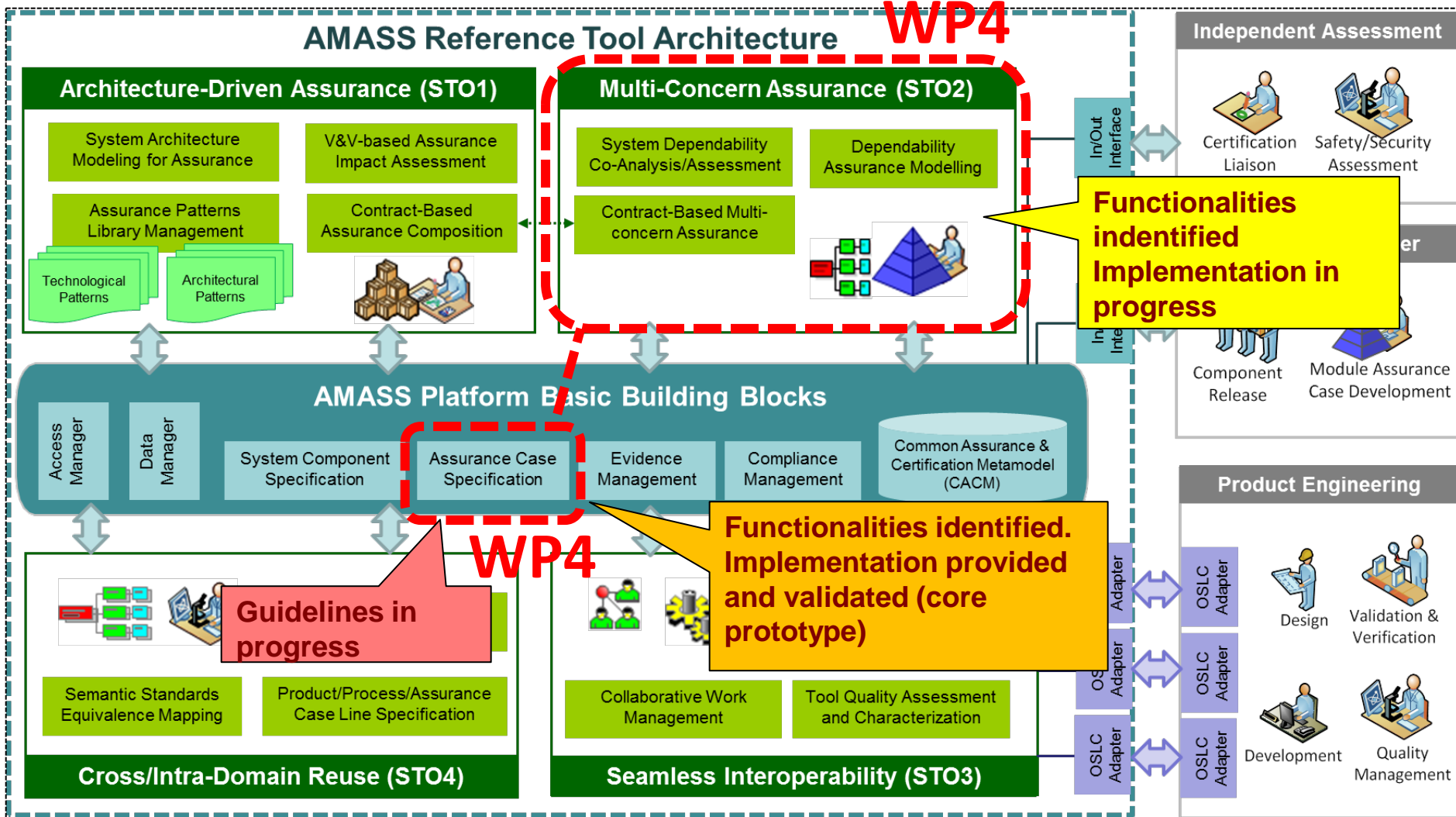
WP4 Objectives

Provide research foundation & technologies for extended system safety assurance, including: **security**, reliability, availability and performance.

Main specific objectives:

1. Determine **needs and constraints** for the approach to be developed
2. Provide a **conceptual framework** covering the information needs for multi-concern assurance
3. **Refine safety-focussed CCL meta-models & vocabulary** to include wider assurance concerns relevant to the case studies in the target domain
4. **Enrich** the AMASS meta-model **CACM**.
5. Develop an **assurance case framework** which is capable of
 - **supporting** the **composition** of system components
 - adequately **dealing with trade-offs** between complementary and competing assurance concerns (in multi-dimensional way, not simply pairwise)
 - **supporting multiple views** of **assurance data** and **argument**.

Multi-concern Assurance in the ARTA



Assessment of Applicable Standards

Avionics and ATM Domain Standards	Status	Reliability	Availability	Maintainability	Safety	Security	Performance	Robustness
IEC 61508	publ.				x			
RTCA DO-278A:	publ.				x			
RTCA DO-178B/C:	publ.				x			x
RTCA DO-326A	publ.				x	x		x
RTCA DO-355	publ.				x	x		
RTCA DO-356	publ.				x	x		x
RTCA DO-297	publ.	x	x	x	x	x	x	x
RTCA DO-330	publ.				x			x
RTCA DO-331	publ.				x			x
RTCA DO-331	publ.				x			x
RTCA DO-331	publ.				x			x
SAE-ARP 4754/4754A	publ.				x			
RTCA DO-254	publ.				x		x	x
ARP 4761	publ.				x			

Railway Domain Standards	Status	Reliability	Availability	Maintainability	Safety	Security	Performance	Robustness
IEC 61508	publ.				x			
EN 50126	publ.	x	x	x	x			
EN 50128	publ.	x	x	x	x			
EN 50129	publ.	x	x	x	x			
EN 50159	publ.				x			
DIN/VDE V 0831-104	publ.					x		

Automotive Domain Standards	Status	Reliability	Availability	Maintainability	Safety	Security	Performance	Robustness
ISO 26262 V1	publ.				x			
ISO 26262 V2	work i.p.				x	x		
SAE J3061	publ.					x		
NWIP Autom. Cybersecurity	work i.p.					x		
NWIP SotIF	work i.p.	x	x		x		x	
ETSI ITS Stds.	publ.					x		
ISO/IEC 27001	publ.					x		
ISO/IEC 15408	publ.					x		
IEC 61508	publ.				x			
SAE J3101	work i.p.					x		

Industrial Automation Domain Standards	Status	Reliability	Availability	Maintainability	Safety	Security	Performance	Robustness
IEC 61508	publ.				x			
ISO/TS 15066:2016	publ.				x			
ISO 10218-1:2011	publ.				x			
IEC 62443	publ.					x		
IEEE 1686	publ.					x		
IEC 62351	publ.					x		

Space Domain Standards	Status	Reliability	Availability	Maintainability	Safety	Security	Performance	Robustness
ECSS-Q40	publ.				x			
ECSS-Q30	publ.	Dependability						
ECSS-Q80	publ.	SW Product Assurance						

Quality Attributes Treated

- Scope varies from domain to domain
- Safety strongly supported
- Security is recognized except in the Space domain
- Especially in the automotive domain much work towards treating complex ADAS & Cybersecurity

State of the Art in Multiconcern Assurance - Standards

- Standardization activities to include safety & security have proceeded:
 - **Industrial domain:** IEC 62443 "Industrial communication networks – Network and system security" is in force.
 - **Railway:** Security Guideline DIN VDE V 0831-104 based on IEC 62443 (Planned to be issued as IEC standard).
 - **Automotive:** In addition to functional safety oriented ISO26262, SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" is used. Currently ISO 26262 Ed.2 is being elaborated, Annex F on security is planned. Wrt. autonomous driving, the SOTIF "Safety of the intended Functionality" subgroup has been founded (-> ADAS) and joint SAE / ISO Working Group started the development of an automotive security standard.

State of the Art in Multiconcern Assurance – other Projects

- Predecessor Artemis projects **OPENCROSS** and **p+nSafeCer** focused on safety only.
- Artemis project **SESAMO** investigated MB safety and security assessment and used dedicated tool chain (Medini Analyse & CHESS) to specify critical architecture parts.
- **CONCERTO** project: MB, component-oriented toolset (CHESS), WCET and schedulability analysis; Dependability Profile (RAMS but also Human Factors).
- **MERgE** - Model-Based Safety & Security Assessment approach – Sa/Se views in Safety Architect
- **EMC2**
 - Safety and security assurance processes combined (HARA, TARA, STAMP-SEC, FMVEA)
 - Objectives:
 - Establish Multi-Core technology in all relevant Embedded Systems domains
 - Enable mixed-criticality applications.
 - Focus on multi-core platform for multiple domains ensuring safety and security for critical applications.
 - Key achievements for safety and security:
 - Integrate Safety&Security Engineering to handle the impact of security on safety
 - Conditional runtime certification (safety checks of dynamic system compositions)



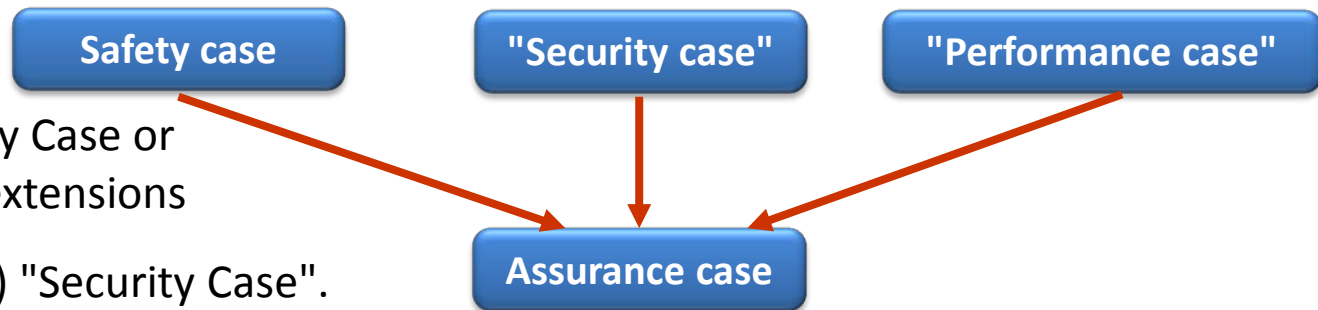
Scope of Multiconcern Assurance in AMASS

AMASS deals with

- Security-Aware Safety Case or
- Dependability Case extensions

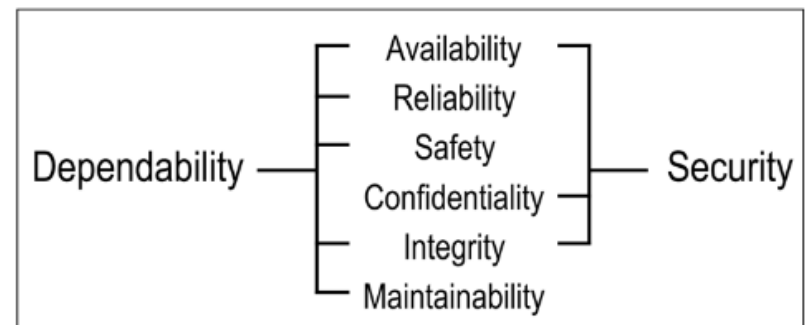
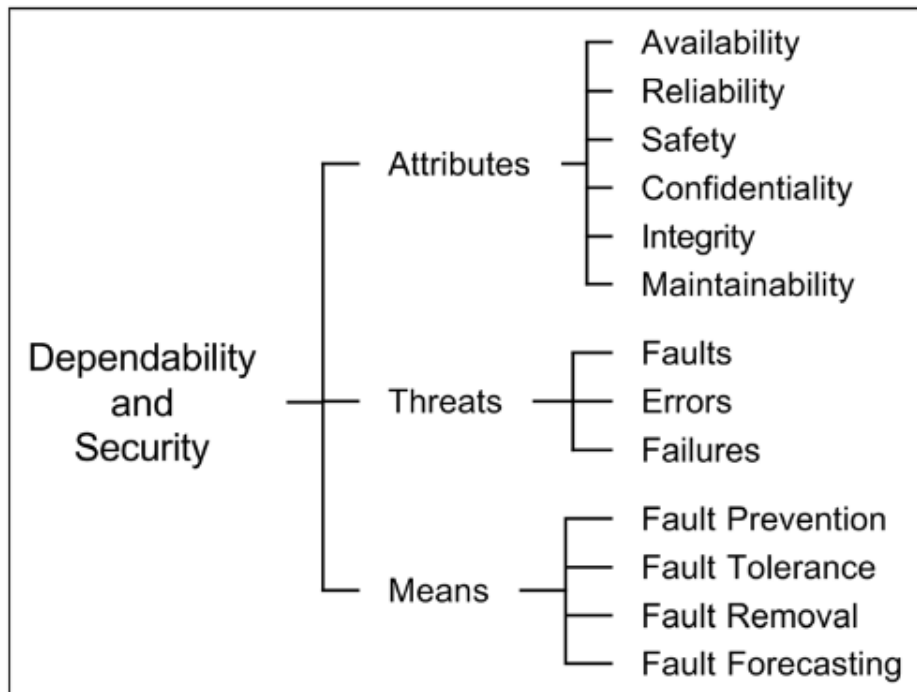
No fully-fledged (kind of) "Security Case".

- Safety case is an established concept, security case is new => start from safety and extend

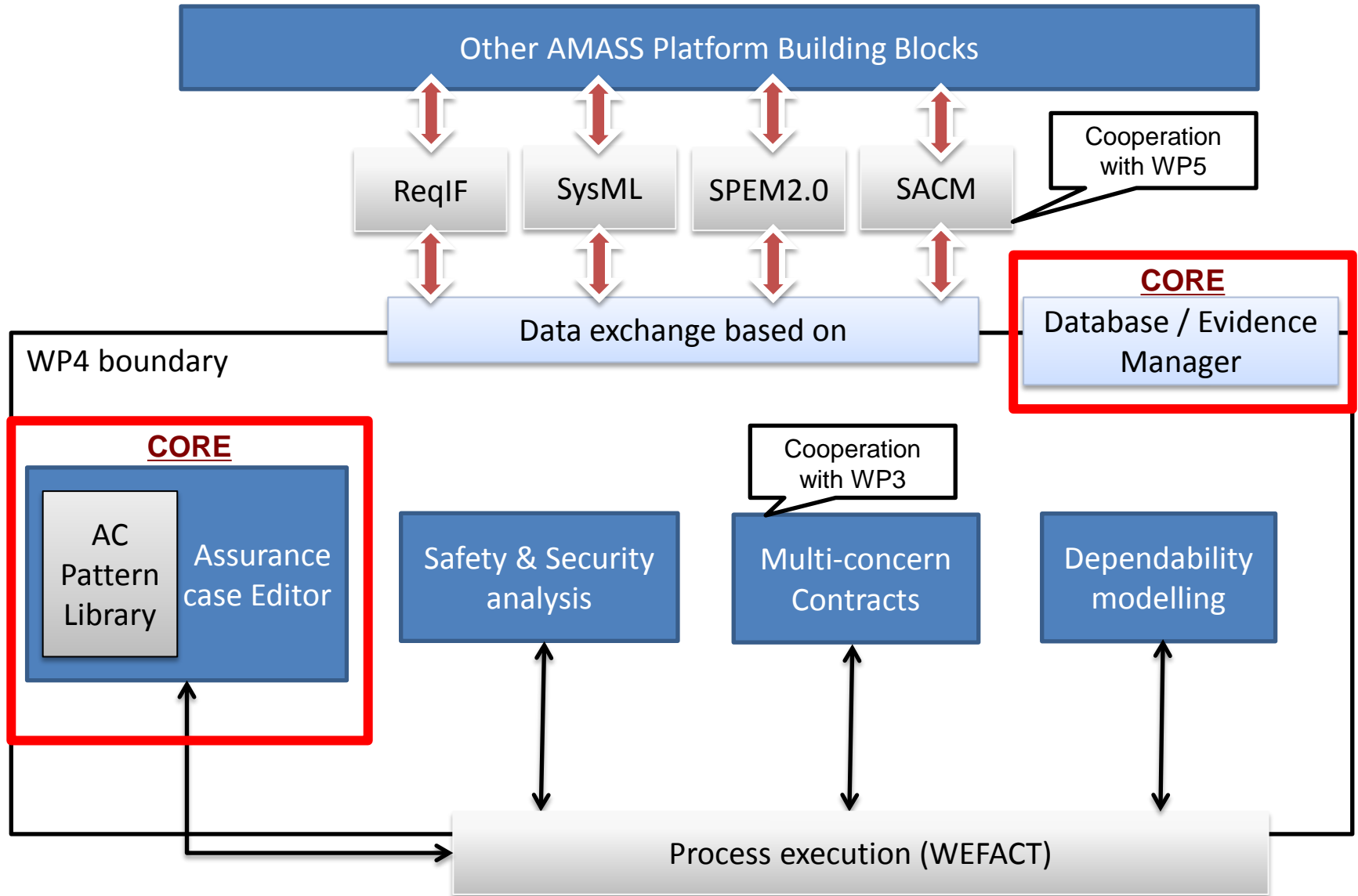


Relevant quality attributes for AMASS:

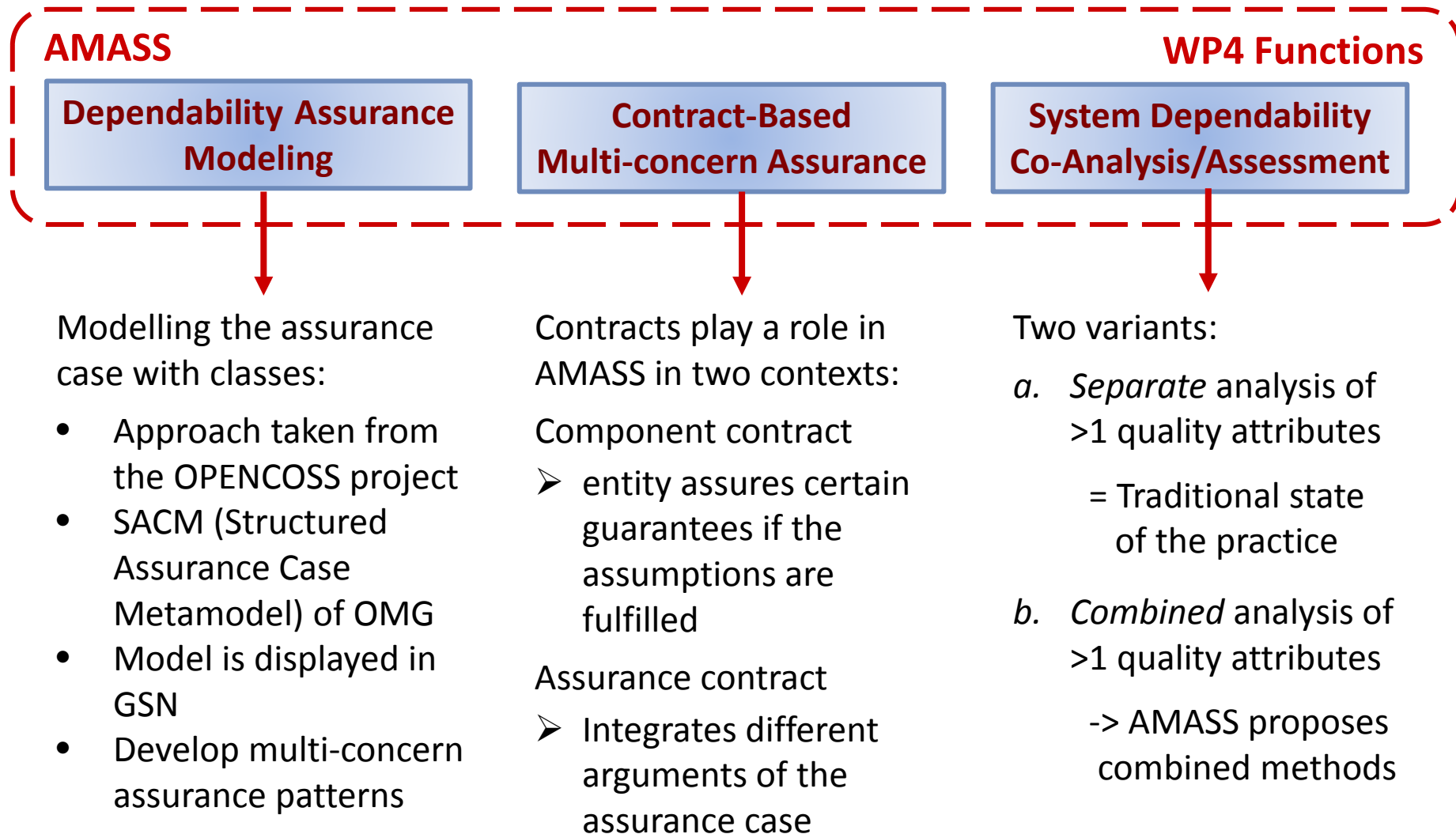
- Algirdas Avizienis' and Jean-Claude Laprie's taxonomy (2004)
- Plus more, e.g. robustness
- AMASS takes a generic approach and is open for any attribute
- Most important: Safety & Security!



WP4 - Overview



AMASS Functions to be Provided by WP4



Concepts: Relations between Claims wrt. Quality Attributes

Dependency relationship.

- The claim A of one attribute depends on the fulfillment of claim B of another attribute.
- E.g. a fail-safe claim (safety) depends on safety system not tampered (security).

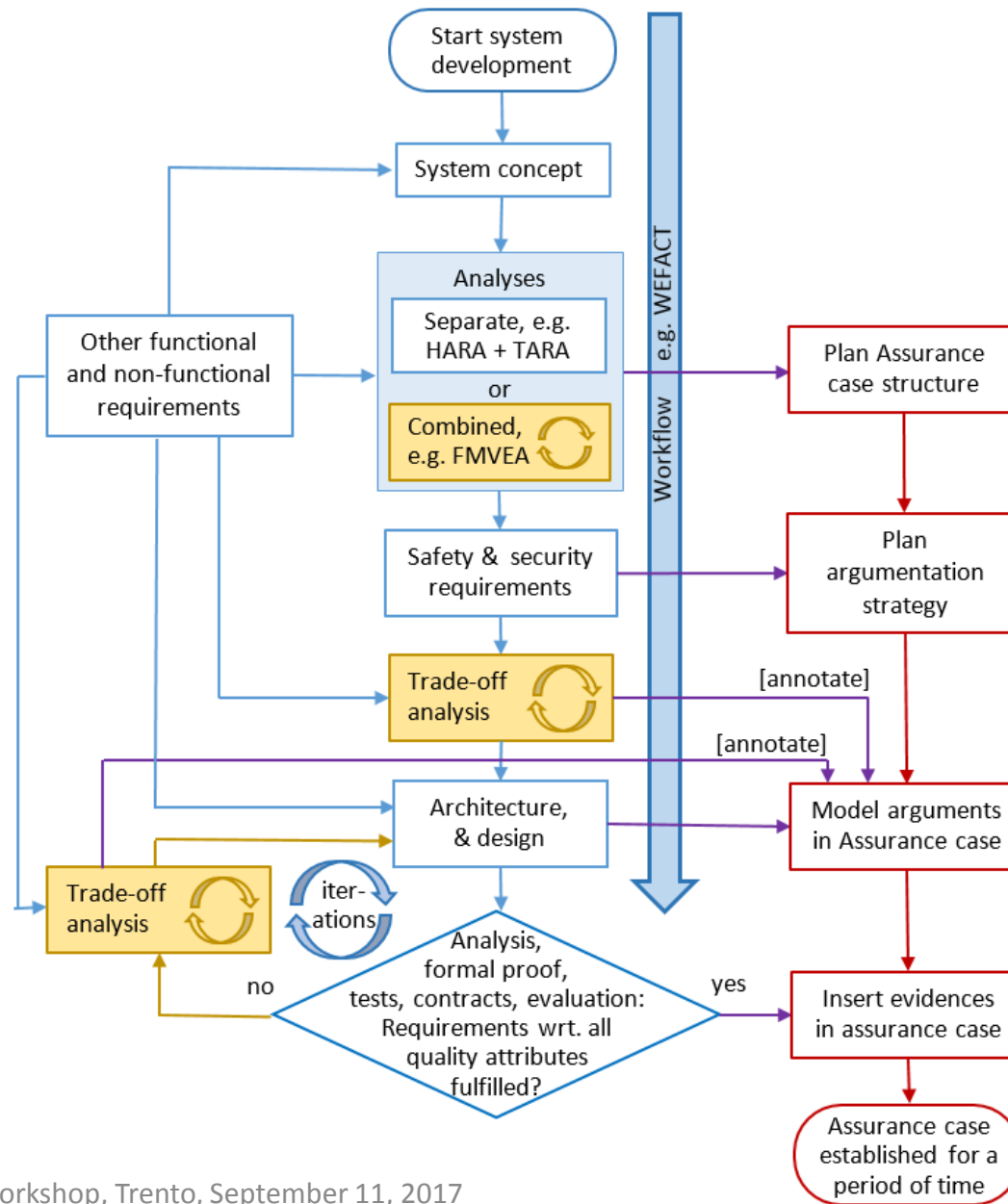
Conflicting relationship.

- The assurance measure of attribute A is in conflict with the assurance measure of attribute B.
- E.g. “strong password or blocking a terminal after several failed login attempts” (security) conflicts with “emergency shutdown” (safety).
- Resolution of such a conflict needs to be noted in the Assurance Case.

Supporting relationship.

- Assurance measure of attribute A is also applicable to assurance of attribute B
=> one assurance measure can be used to replace two separate ones.
- E.g., encryption can be used for both confidentiality (security) and to check data integrity instead of checksum (safety).
=> This means two goals can be addressed by one argumentation.

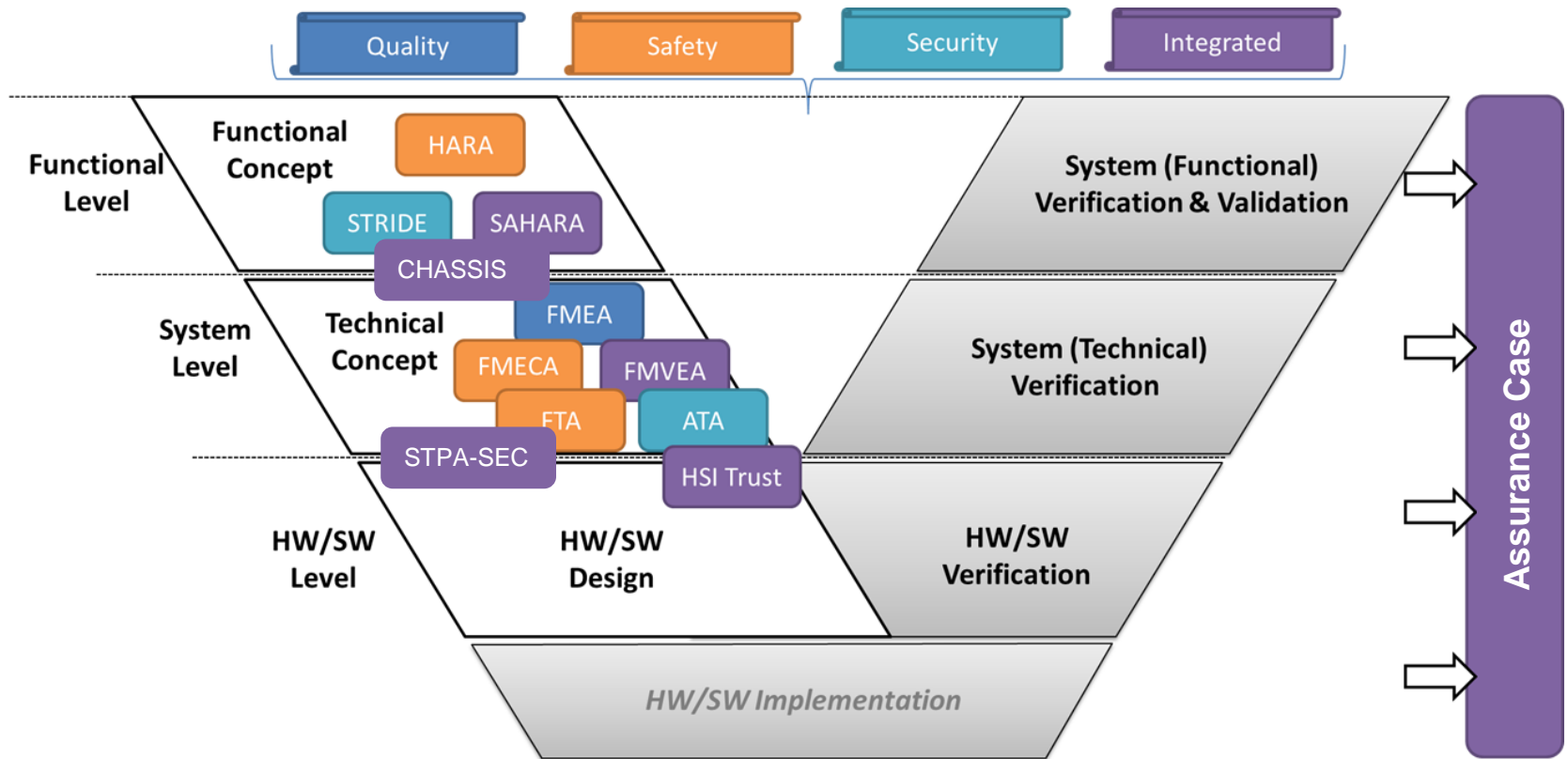
Multiconcern Assurance Processes in the System Lifecycle



WP4 – Concepts: Co-analysis

Mapping of methods to specific development phase

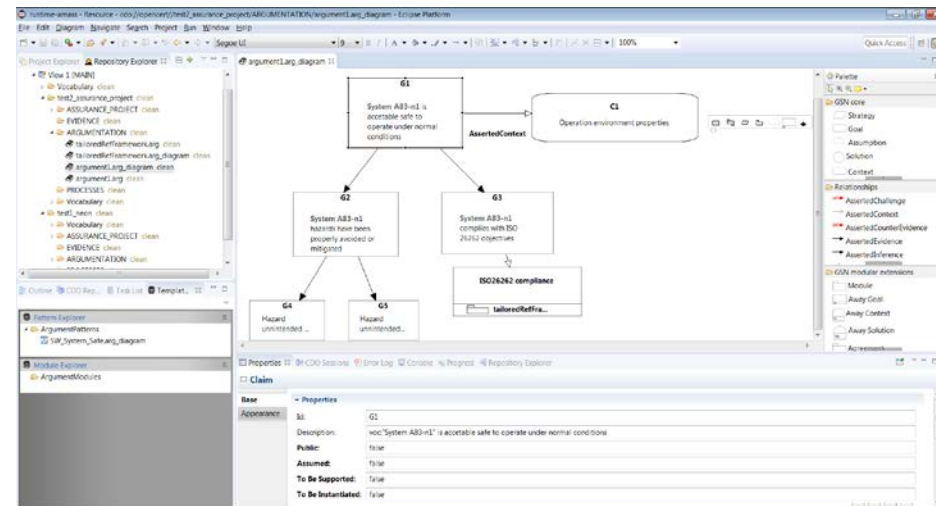
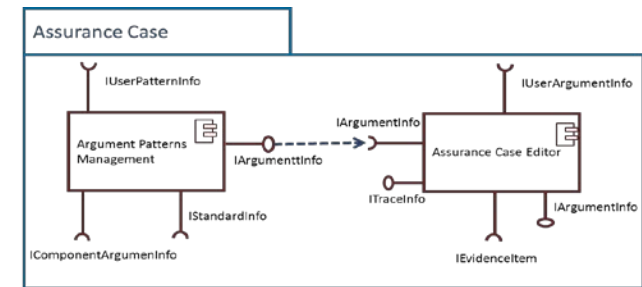
- Support consideration of multiple attributes during all phases



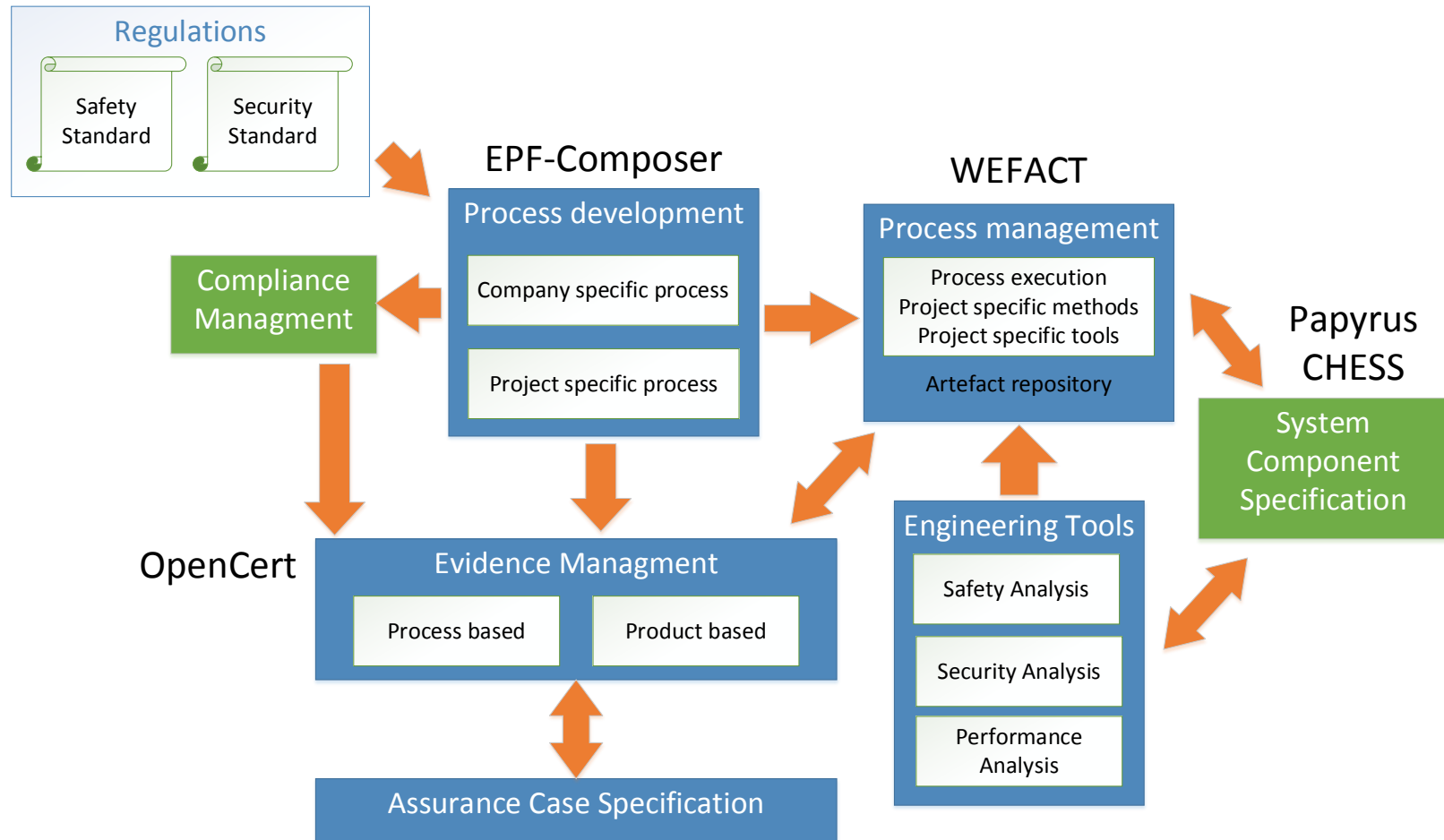
Focus is on consideration of safety impacts due to security incidents

WP4 – ARTA Functionalities to Achieve STO2

- Prototype Core:
 - Basic Building Block "Assurance Case Specification"
 - Extended OPENCROSS Assurance Case Editor from OpenCert including pattern library
 - Internally using SACM (Structured Assurance Case Metamodel) of OMG
 - GSN diagrams in the GUI
 - relevant for industry
 - Released as open source tool with documentation and user manual as D4.4 on Jan.31st, 2017



WEFACT – Integration Concept



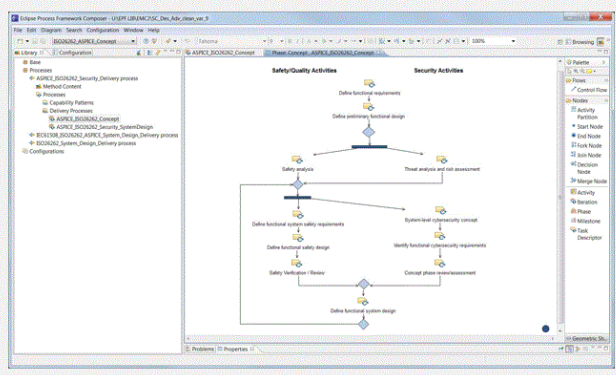
Process-related Co-Assessment with WEFACT

- Requirements from standards wrt. multiple concerns modelled in EPF
- Process model imported in WEFACT and executed for automated multiconcern assessment

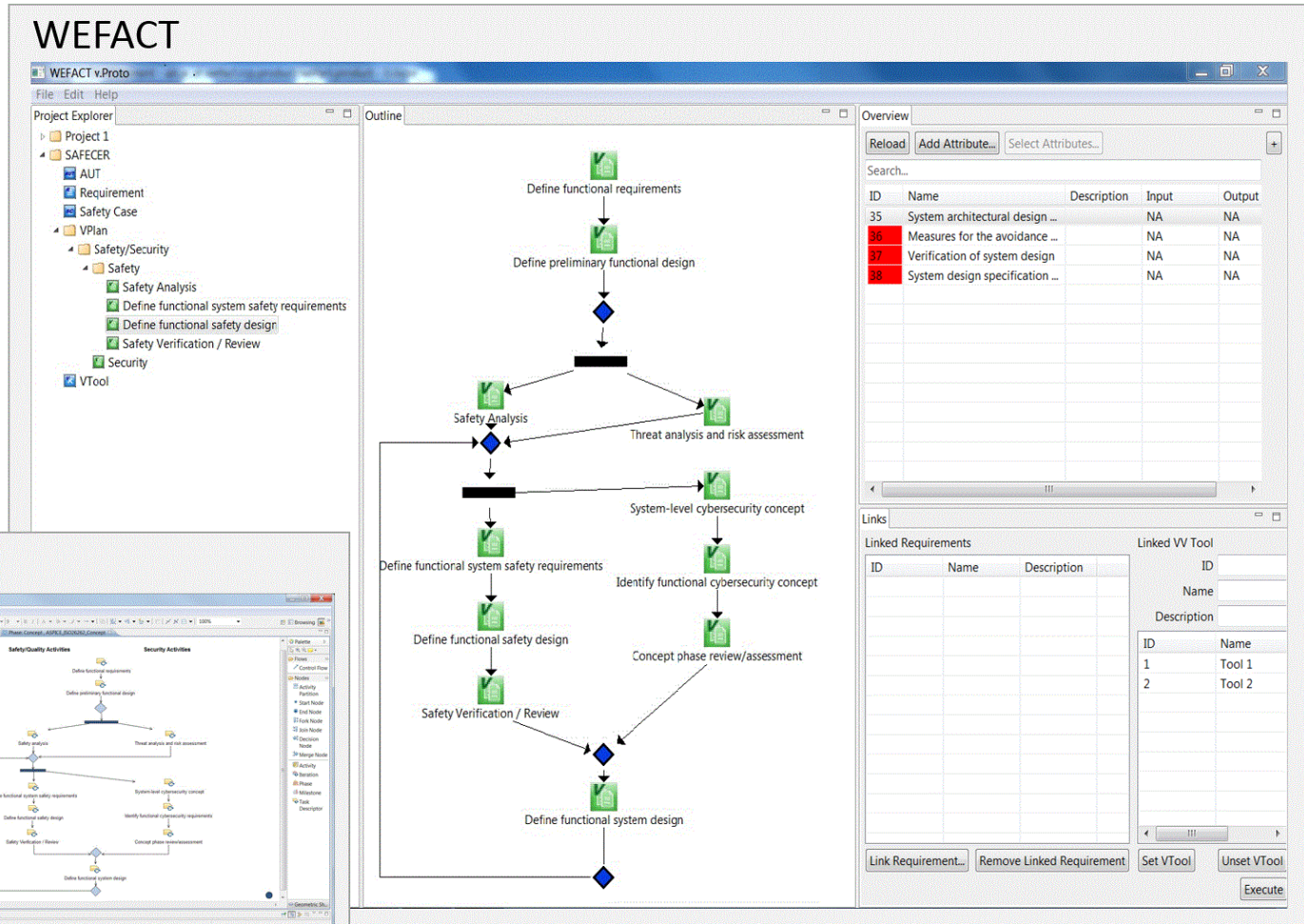
Process
Model
Import



EPF-C



WEFACT



Main Achievements Year 1

- Applicable standards identified for different quality attributes in several domains
- State of the art for co-engineering in standards and industrial practice including existing methods investigated and published in D4.1, released on Sept. 30th, 2016
- Concept for co-engineering developed and Multiconcern Assurance tools and methods for second iteration of ARTA proposed & documented in D4.2
- Definition of first multi-concern patterns
- WP4 contribution to the first iteration of the ARTA – the OpenCert Assurance case editor – released with D4.4

Next Steps in WP4

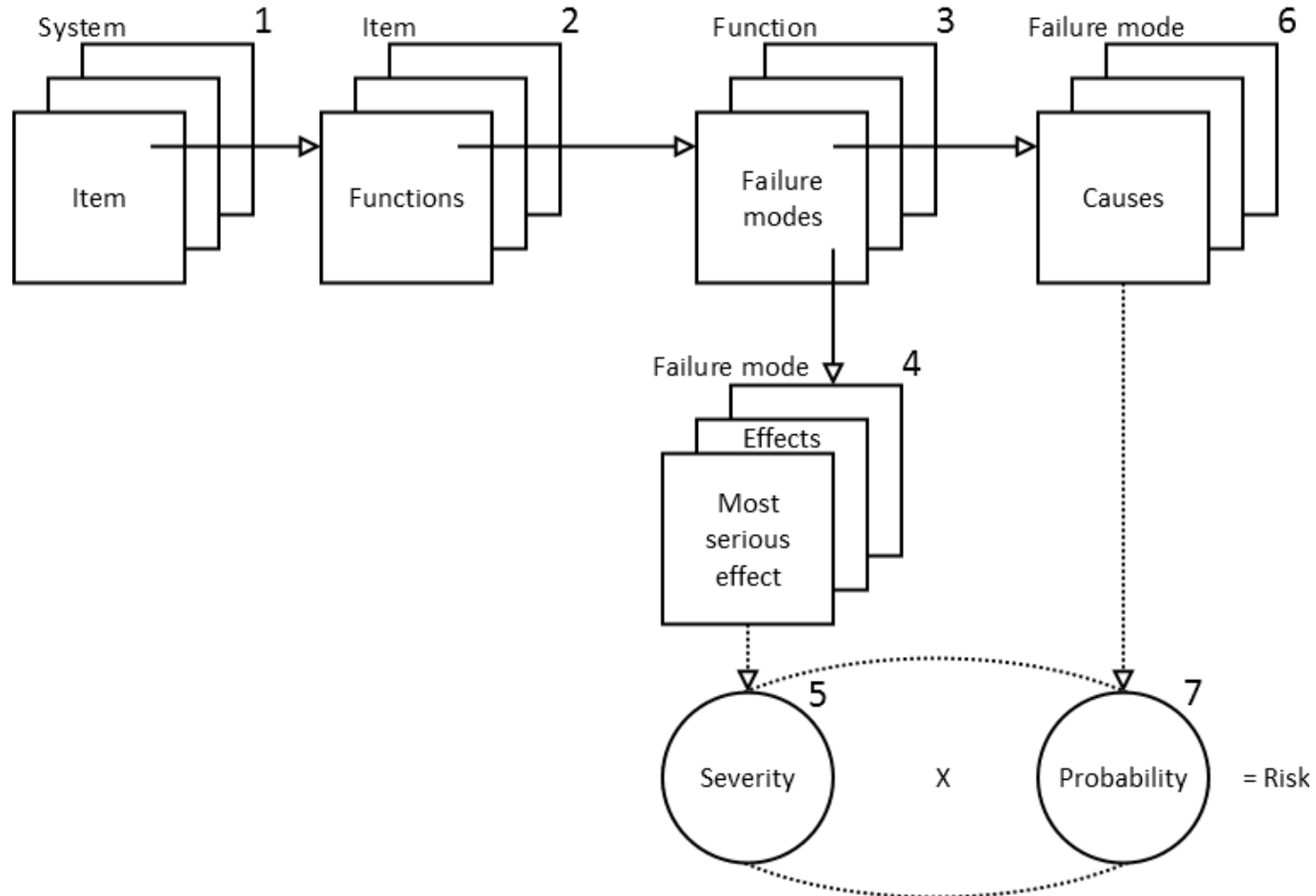
- Release of D4.2
 - Definition of concepts for multiconcern assurance:
 - dependability assurance modelling,
 - system dependability co-analysis/assessment, and
 - contract-based multiconcern assurance
- Definition of Guidelines
 - To be started next in T4.4
- Support for the AMASS second prototype
 - Work started in T4.3, to implement the developed concepts

Thank you for your attention!

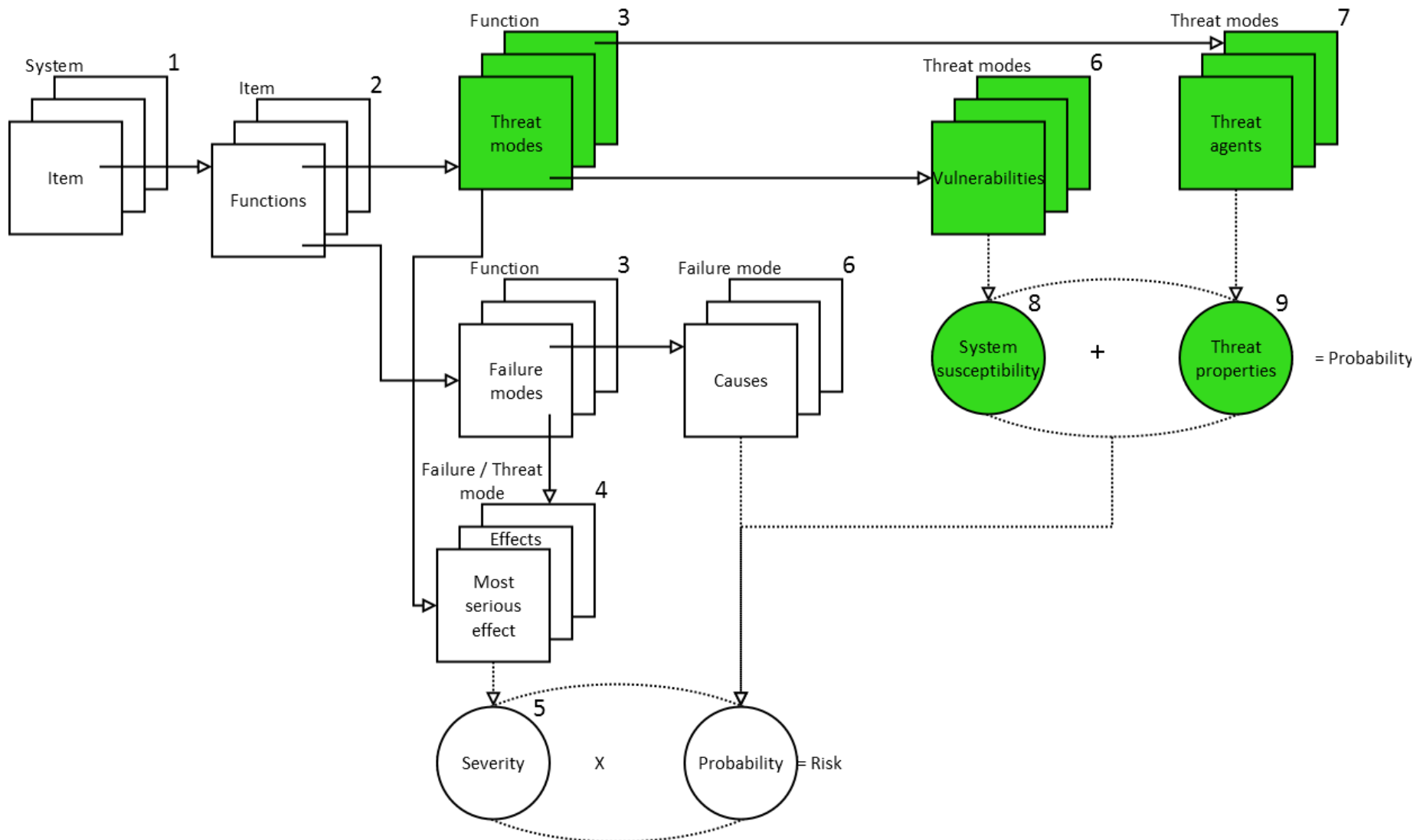


Backup

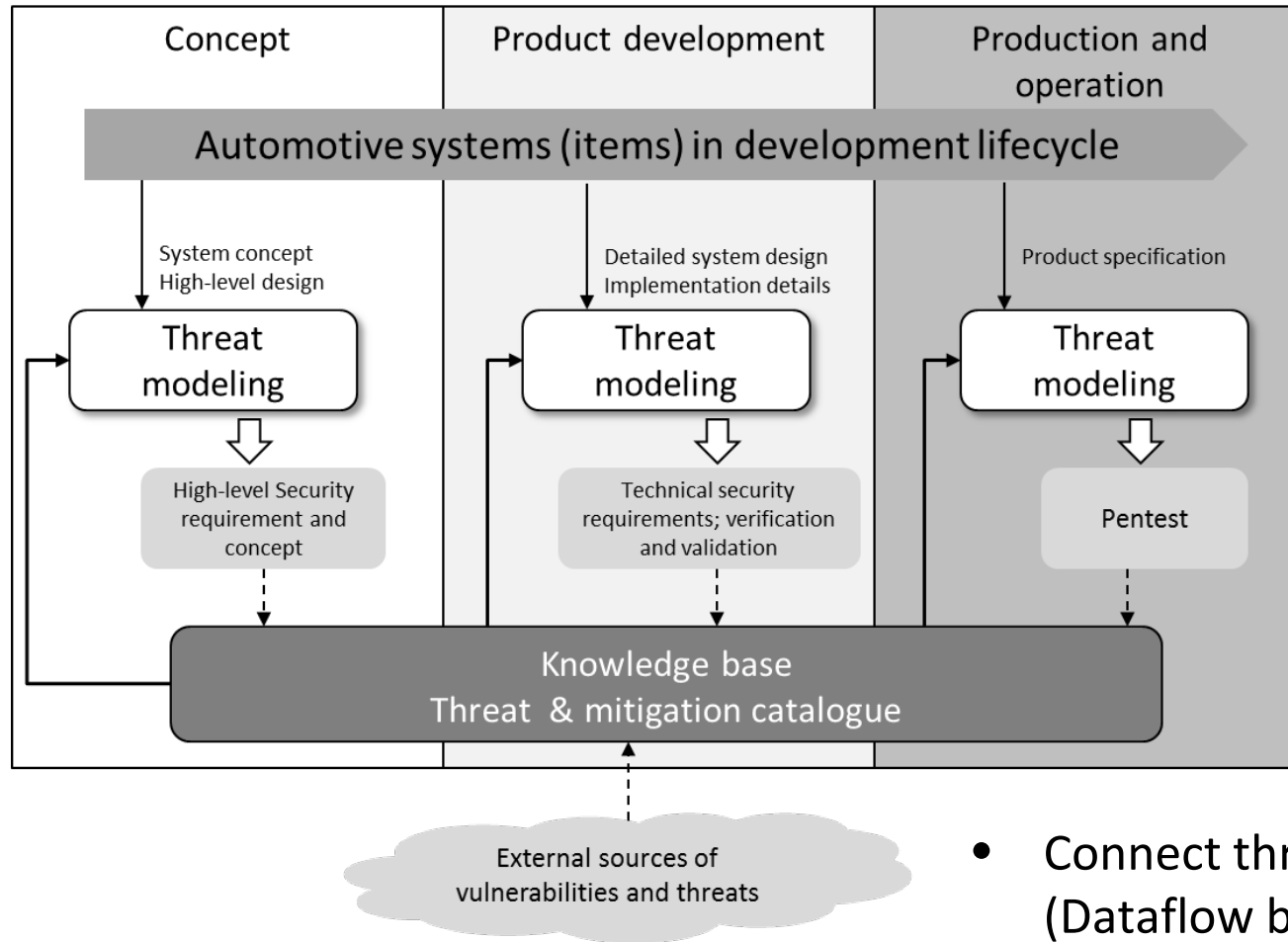
FMEA Analysis Process



Extended Analysis Process in FMVEA

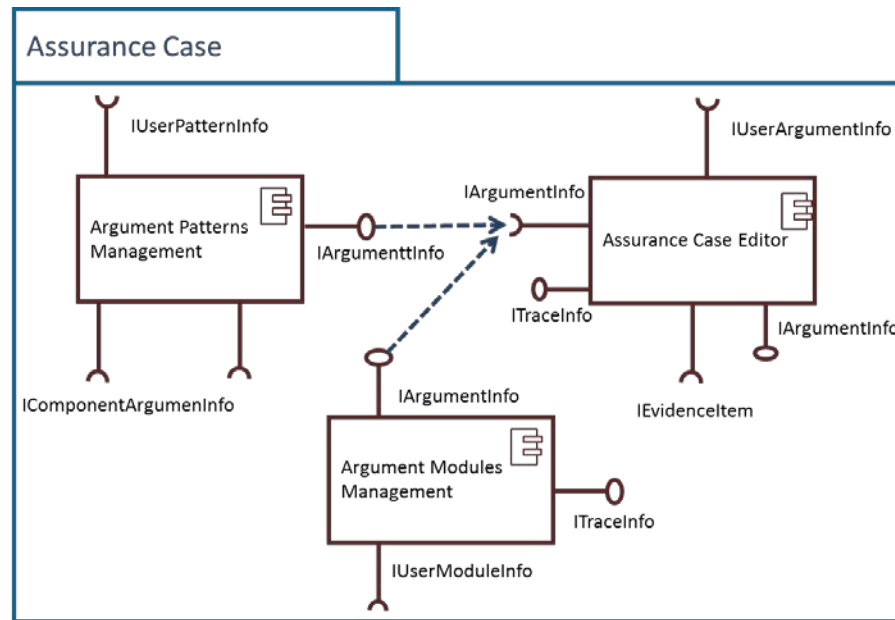


Security Part in FMVEA is Based on STRIDE / Threat Modeling



- Connect threat modeling (Dataflow based) with system functions and potential hazards => direct identification of hazards caused by threats

WP4 – ARTA Functionalities to Achieve STO2

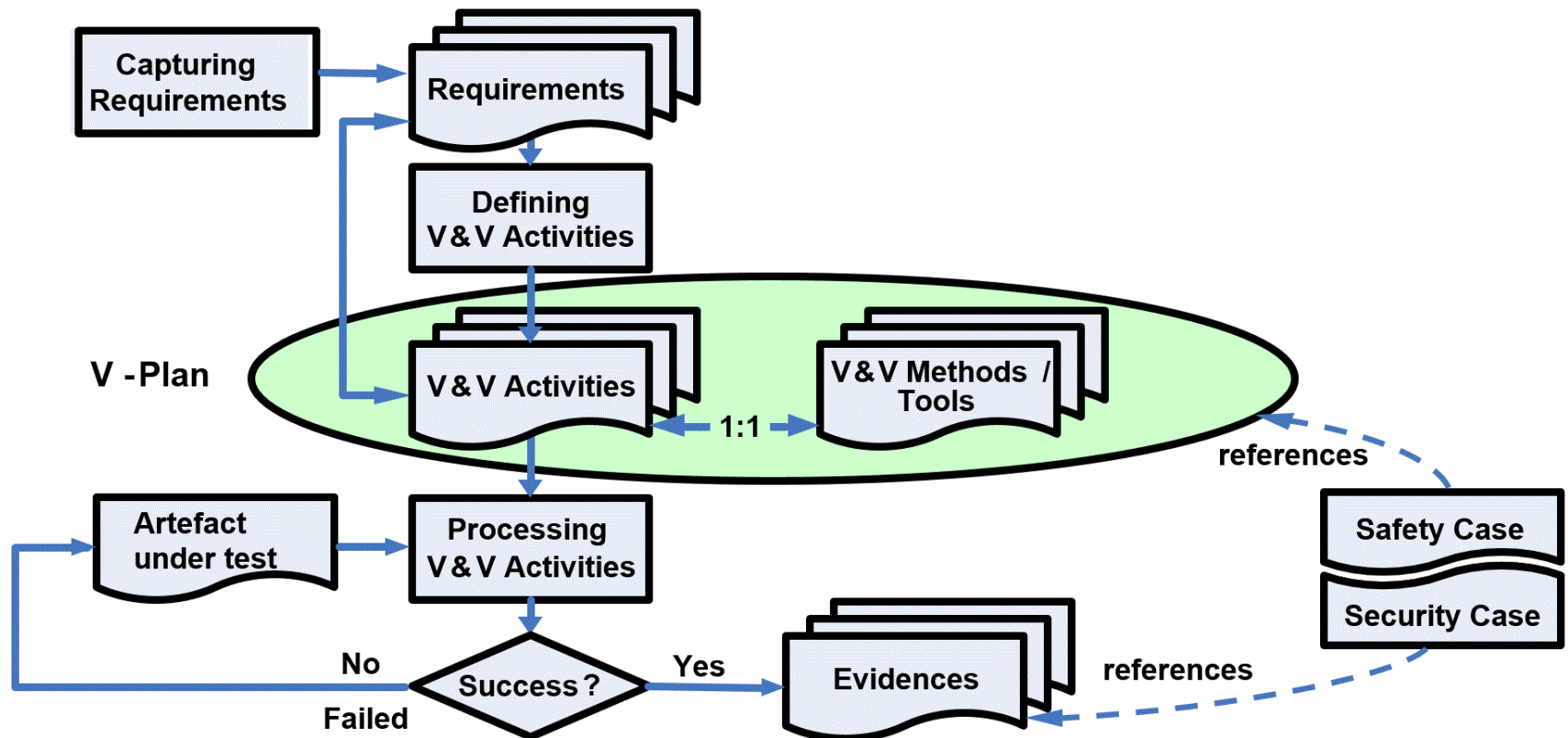


WEFACT Assurance Workflow Tool

- Prototype WEFACT V2 under development
- Eclipse RCP application using MySQL DB
- Basics incl. EPF import implemented
- First results presented in Sevilla plenary
- Roles/users and report generator to be done
- In terms of AMASS: affects multiconcern assurance workflow and evidence management (WP5)

WEFACT – Basic Workflow Concept

- Requirements-based assurance - as far as possible automated
- Various tool bindings, can treat deliberate quality attributes
- Results are evidenced for the assurance case
- This example depicts the workflow for safety and security co-assurance



- WEFACT is a workflow engine which is currently re-implemented in Eclipse
- Can import process from EPF
- Interconnect process steps with tools
 - Different levels from Command line call to OSLC
- Exchange requirements with tools