ECSEL Joint Undertaking

European Commission

AMASS

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

AMASS Usage Scenario 4: Safety and Security Co-Assessment

2nd EAB Workshop
Västerås, September 17, 2018

Thomas Gruber
WP4 Leader
AIT Austrian Institute of Technology

Introduction

- Co-assessment is a central prerequisite for efficient assurance of safety and security (& other concerns):
  - Traditionally, co-engineering is supported by applying separate, safety specific and security specific tools.
  - For a few years, combined approaches have been a topic in research and are now producing first tools as results.
- Using separate tools has drawbacks:
  - results may (and mostly do) influence the assumptions for applying the other one.
  - An additional analysis of the mutual influences between the quality attributes (Supporting/Conflicting/Dependency Impact Relationship) and of the trade-offs between them is necessary.
  - At least one additional iteration of the (concern-specific, parallel) assurance steps is required to integrate the trade-off analysis results.

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).

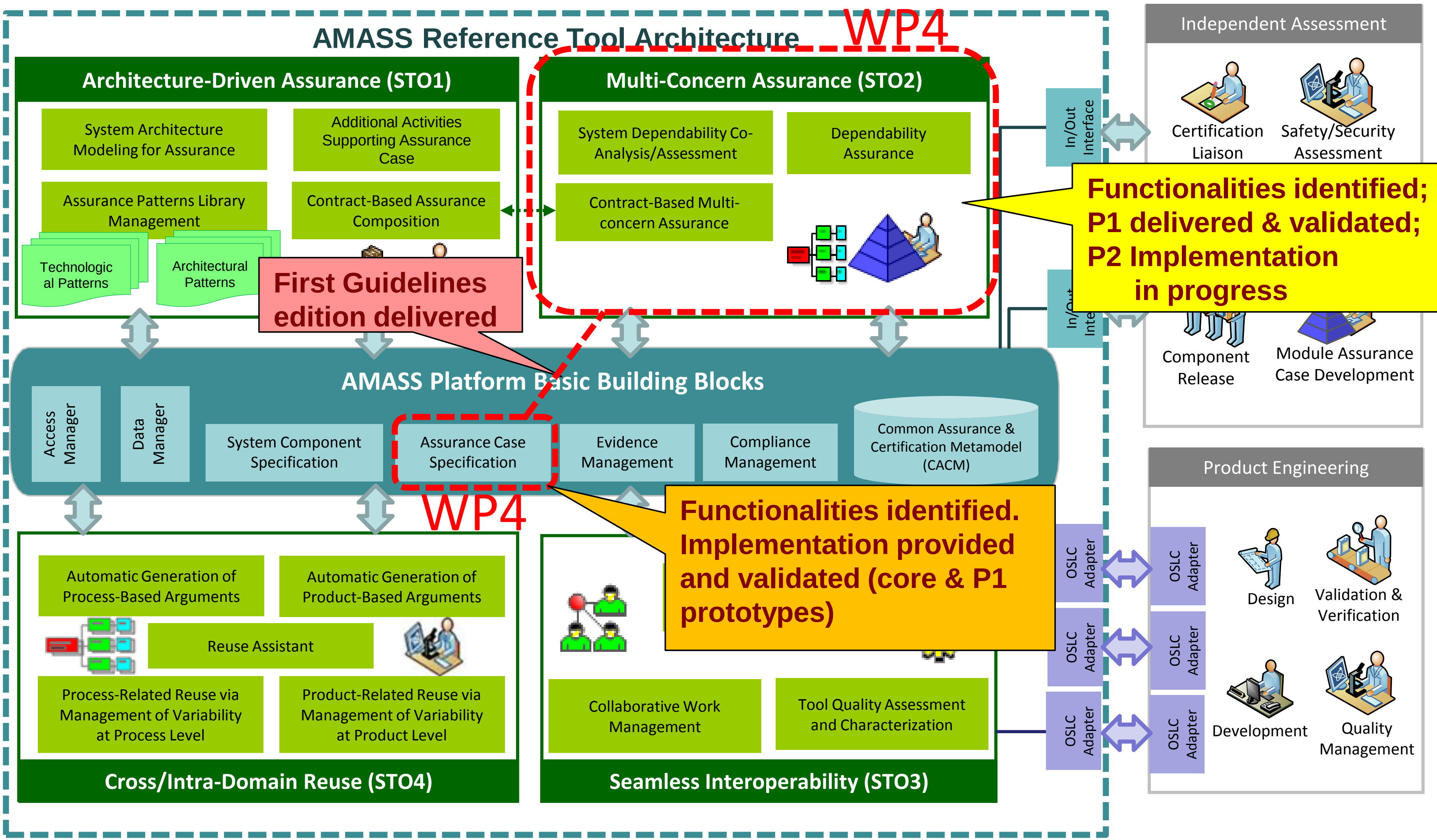
Conflicting relationship.

- 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.

ARTA: Building Blocks for Multiconcern Assurance



How Standards deal with Co-Engineering

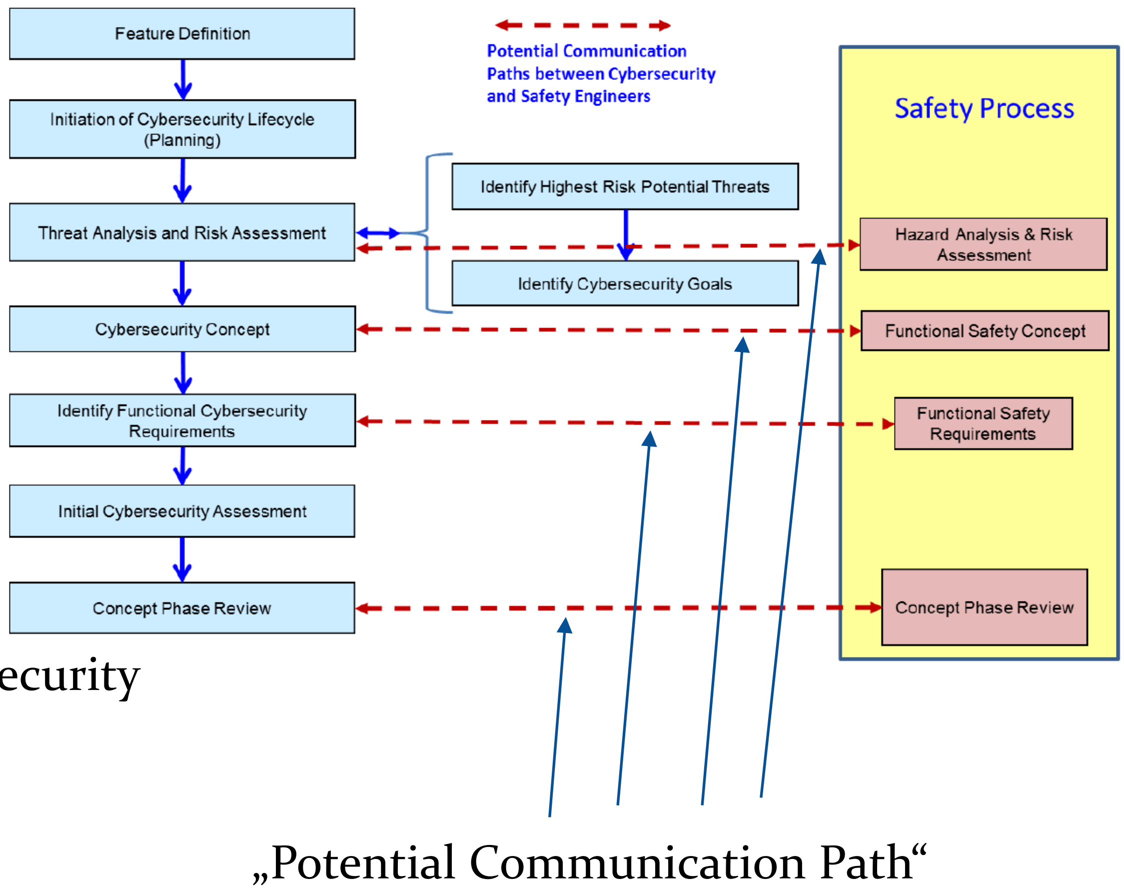
SAE-J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

Guidebook and not a standard

Only available for a few months, then back to Work in Progress

Multiple methods proposed, but no consistent approach (e.g. risk rating differs on used method)

Process copied from ISO26262
Alignment is needed but cybersecurity needs to include later stages



How Standards deal with Co-Engineering

ISO/SAE 21434 WD Road Vehicles - Cybersecurity Engineering

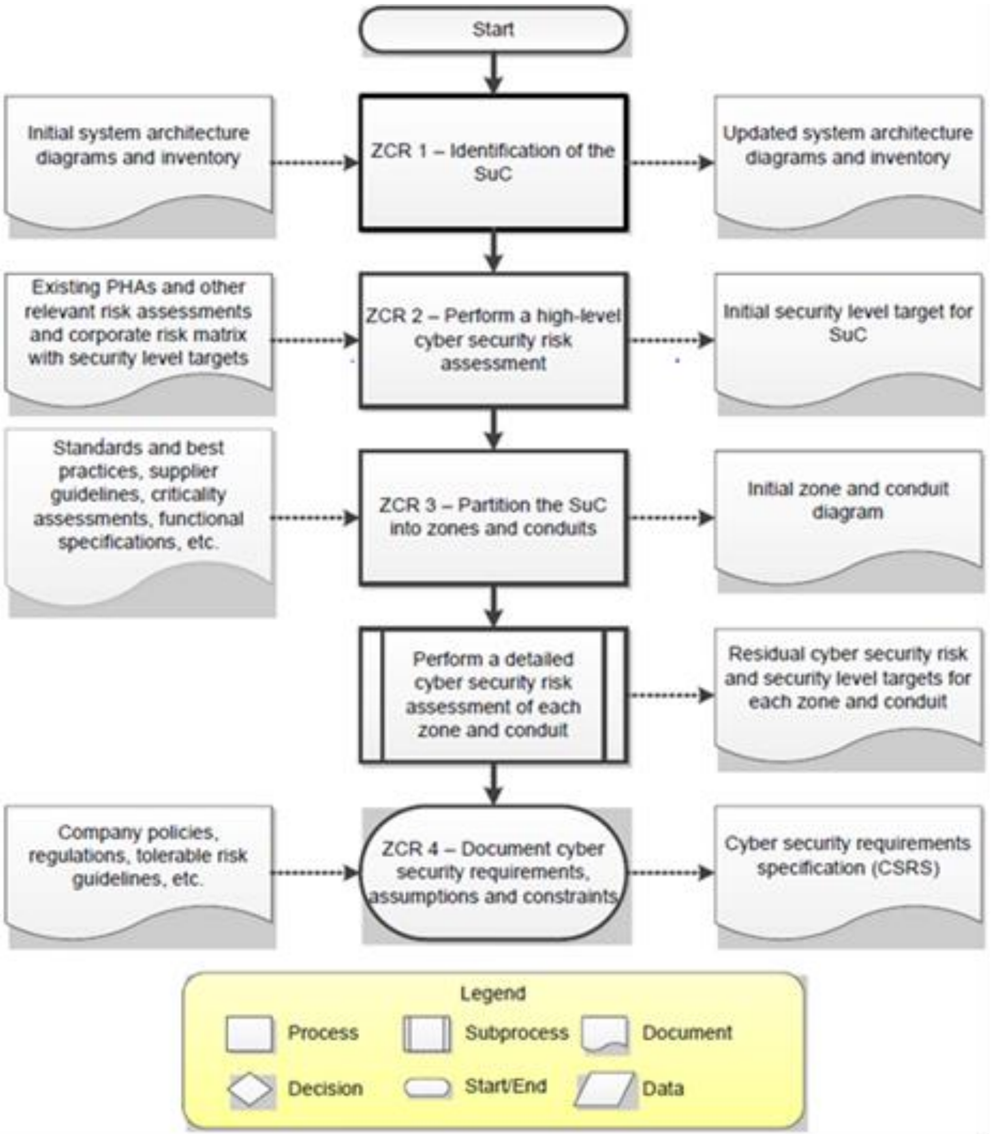
- Based on SAE-J3061 but much more detailed guidance
- Scope:
  - Requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (concept, design, development), production, operation, maintenance, and decommissioning.
  - A framework that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk among stakeholders
  - applicable to road vehicles that include electrical and electronic (E/E) systems, their interfaces and their communications
  - Standard does not prescribe specific technology or solutions related to cybersecurity
  - Engineering rigor depends on CAL (Cybersecurity Assurance Level)

How Standards deal with Co-Engineering

IEC62443 Industrial communication networks – Network and system security

Security

Lifecycle



How Standards deal with Co-Engineering

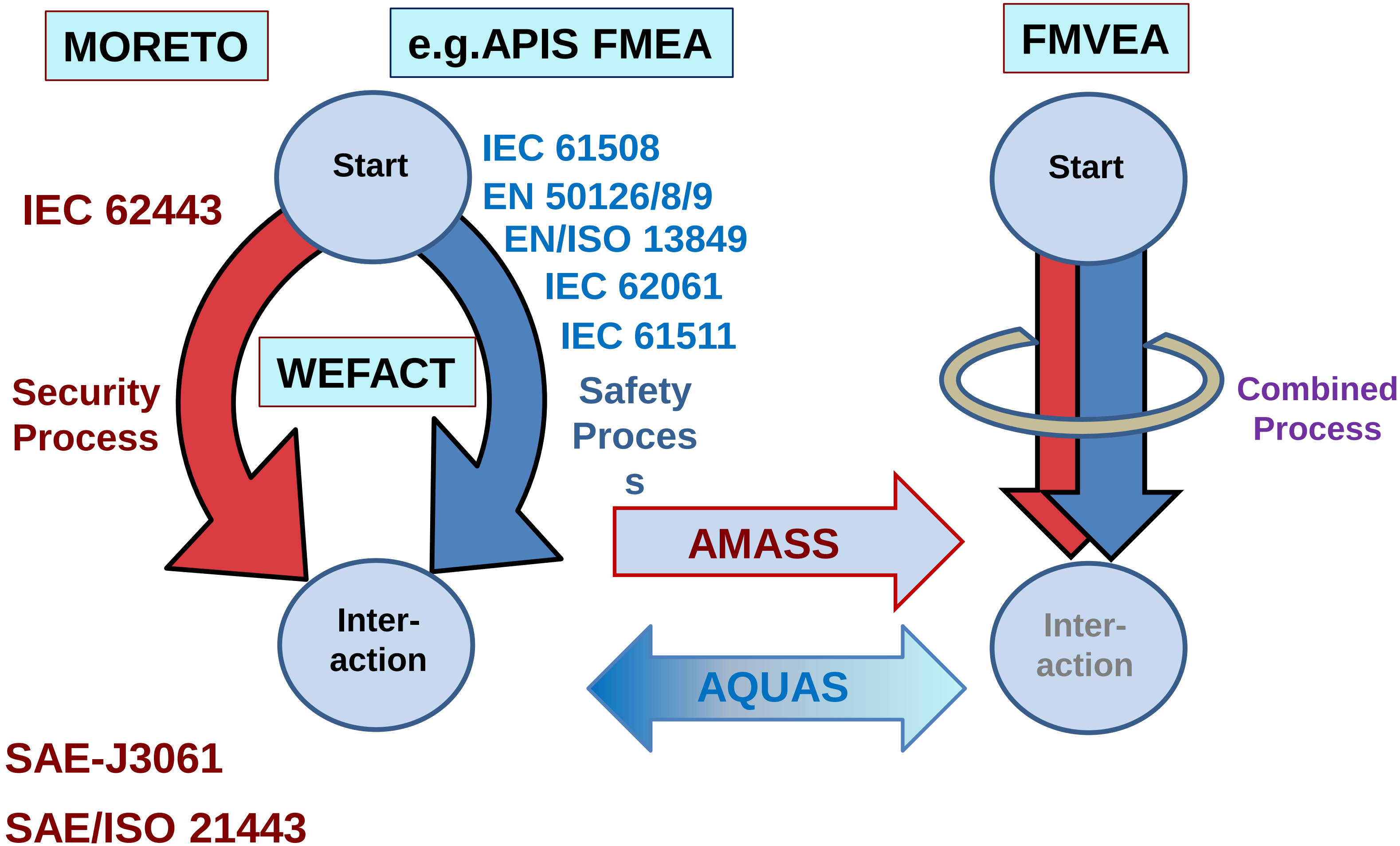
IEC 62443 Industrial communication networks - Network and system security:

Mapping between safety and security lifecycles

Lifecycle Phase		*Functional Safety*	*IACS Cybersecurity*
Risk Analysis	Target of Evaluation	• Equipment under control (EUC)	• Zones and Conduits based on logical grouping of assets
	Failure Likelihood	• Random failures due to operational and environmental stresses • Systematic failures due to errors during safety life cycle	• Threats: Internal, external or combination • Vulnerabilities due to ○ component or system design flaws ○ making non-validated changes ○ not following security practices and procedures ○ Threats exploiting vulnerabilities Lead to failure
	Consequence Severity	• Impact on environment, health and safety of personnel and the general public	• Loss of availability and/or data integrity has direct impact and loss of confidentiality has indirect impact on functional safety
	Risk Categorization	• Based on likelihood and severity; risk may be quantified	• Based on likelihood and severity; risk is currently qualitative • Risk categorization for every security requirement; • multi-dimensional problem • Assigned to Zone with target SL for each zone/conduit
	Risk Mitigation Measures	• Relies on independent protection layers concept • Safeguards reduce likelihood of consequence evaluated • identifies integrity requirements for safeguards; for SIF assigns target SIL	• Relies on security countermeasures within conduits connected to the Zone, and defense in depth concept • Countermeasures reduce likelihood • identifies requirements for countermeasures to meet the Zone Target SL for each threat vector
Implementation of Measures		• Safety manual for components • Quantitative SIL verification for SIF	• Security manual for components • Verification through different Levels of testing for target SL
Operation and Maintenance		• Restrict access to IACS components to competent personnel with necessary access privileges • Periodic testing of measures • Demand rate and component failures to be monitored • Awareness and training	• Restrict access to IACS components to competent personnel with necessary access privileges • Periodic testing of measures • Frequent reviews to identify new vulnerabilities and • take appropriate action, if necessary • Awareness and training • Cyber risk reassessment after each software or hardware change
Management System		• Defines requirements for competency, training, verification, testing, audit, MOC, and documentation	Defines requirements for competency, training, verification, testing, audit, MOC, and documentation

Two Ways to Realize Co-Engineering

Using separate tools | Using one combined tool



The real challenge is the trade-off analysis

Co-Engineering Processes

- 2 ways of realizing co-engineering
- AMASS prefers efficient combined tools
- Other projects rely on separated ones, e.g. AQUAS, whose interaction point approach is similar to „potential communication paths“ in SAE-J3061 „Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”
- Standardization for safety and security is still separate. In the case study we used:
- For safety
  - IEC 61508 Functional Safety of Electrical / Electronic / Programmable Electronic safety-related systems
- For security
  - IEEE 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, and
  - *IEC 62443 Industrial communication networks – Network and system security*

Multiconcern Assurance Scenario Overview

- Developing an Industrial Automation domain CPS in Case Study 1: Industrial and Automation Control Systems (IACS)
- Different tools are used for system analysis and requirements generation (so far MORETO, in the 3rd project year FMVEA)
  - FMVEA is included in the recent delivery of the 3rd AMASS platform iteration P2 as an external tool.
- The AMASS Platform is used for assurance & certification-specific activities:
  - Security analysis and security requirements allocation in compliance with the requirements of IEEE 1686-2013 “IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities” and IEC 62443 “Industrial communication networks - Network and system security“
  - Combined safety and security analysis in compliance with IEC 61508 and IEC 62443 avoiding iterations due to conflicts detected in the trade-off analysis
- The company aims to be able manage safety and security analysis; risk assessment based on a common model in the AMASS Platform

Higher-level objectives & expected gains

- **O2:** define a ***multi-concern assurance*** approach to ensure not only safety and security, but also other dependability aspects such as availability, robustness and reliability.
- **Metrics**
  - Effort for assurance and certification
  - Effectiveness in failure/threat identification capabilities
  - Number of requirements fed back into the model
  - time needed for separate safety and security engineering process and the co-engineering process
  - architectural/design modifications saved by combined safety/security co-engineering
- **G1:** to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50% (STO1&2).

Intro to MORETO & WEFACT/FMVEA Scenarios

- Case Study 1: Industrial Automation domain: Industrial and Automation Control Systems (IACS)
- Usage Scenario 2: Perform safety and security co-assessment
- **Timeline:**

Platform Iteration	**1st Iteration - Pcore**	**2nd Iteration – P1**	**3rd Iteration – P2**
Tool	**MORETO (Eclipse)**	**MORETO (Enterprise Architect)**	**FMVEA (Browser)** **(+WEFACT (Eclipse))**
Safety Standards	**-**	**-**	**IEC 61508**
Security Standards	**IEEE 1686** **IEC 62443**[1)]	**IEEE 1586** **IEC 62443**	**IEC 62443**

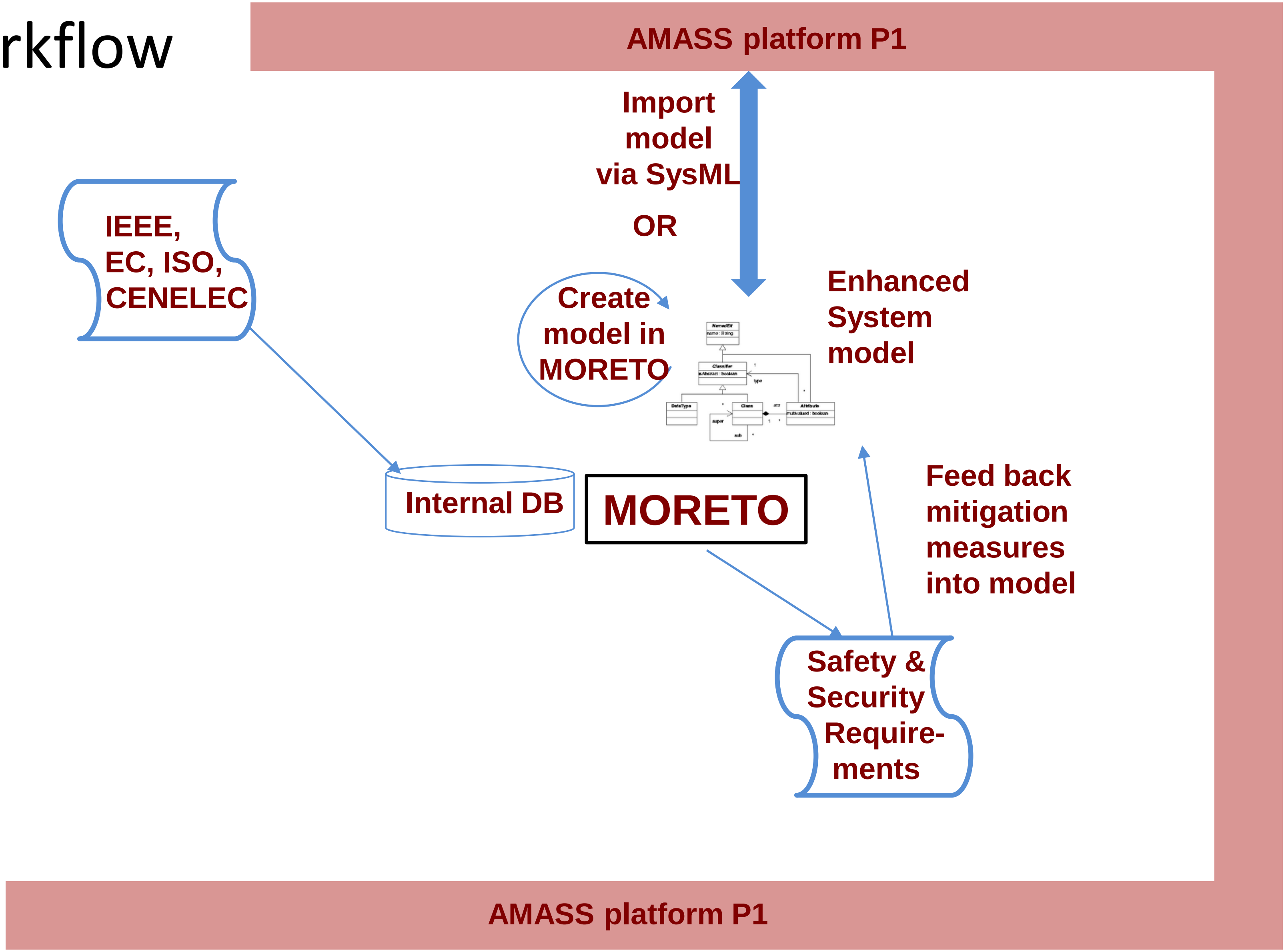
1) Not yet for RTU

Scenario in 2nd Iteration P1

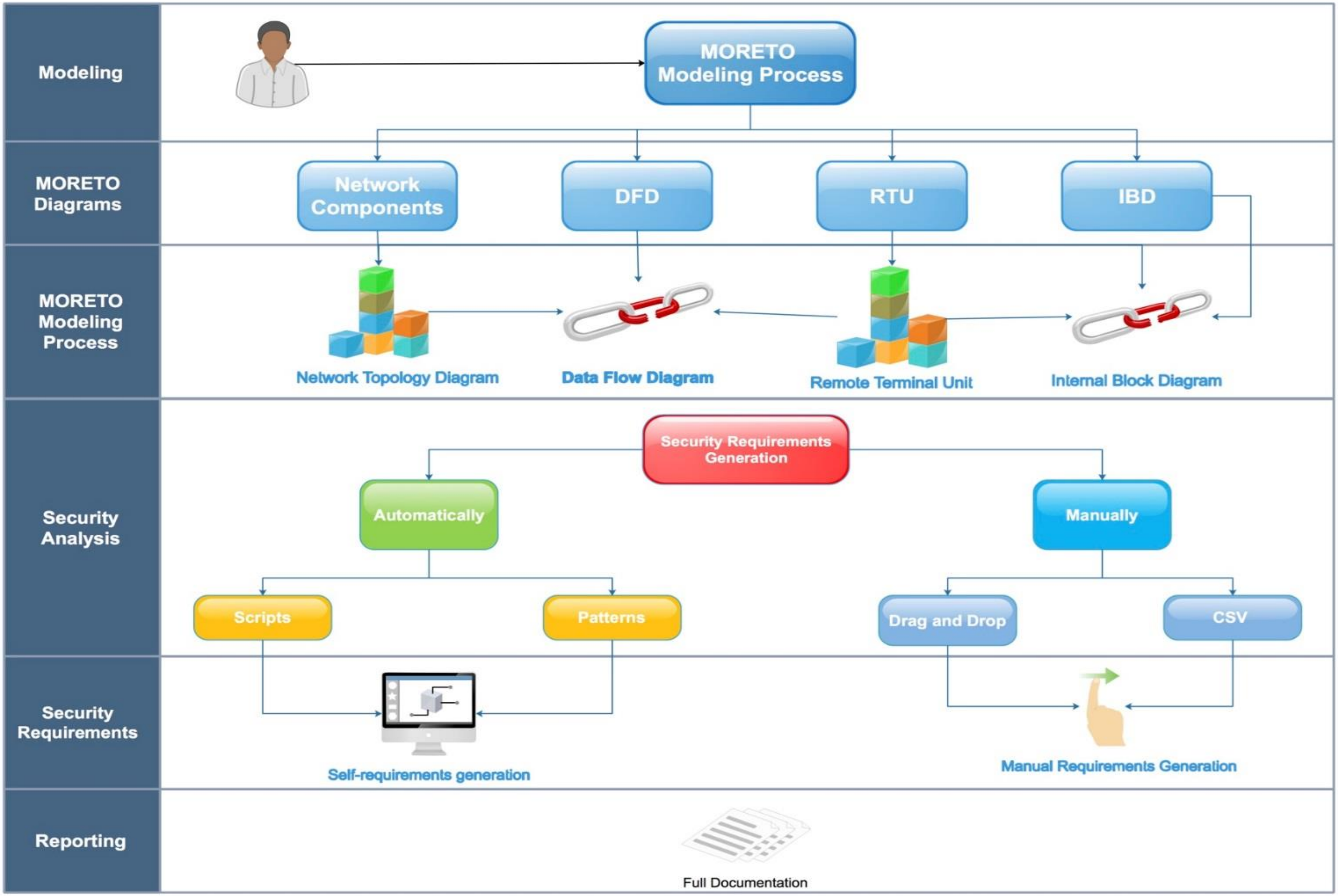
- Design System in MORETO model editor or import SysML model
- Add security relevant properties including already present security controls into model
- Start requirements generation
- Feed back corresponding security controls into the model (with IEC 62443: corresponding to SL-T (Target security level)

Scenario in the 2nd Iteration P1 with MORETO

- Workflow



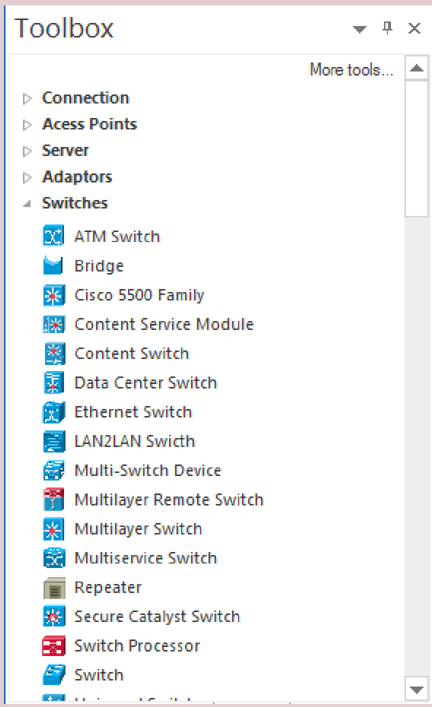
MORETO Workflow



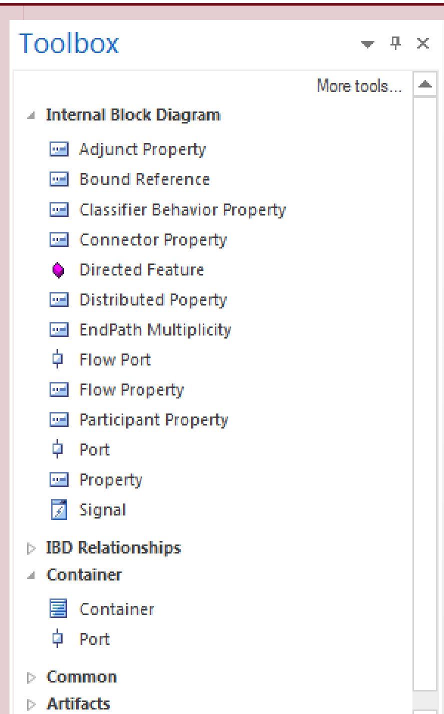
MORETO Design

4 different diagrams for the system modeling process:

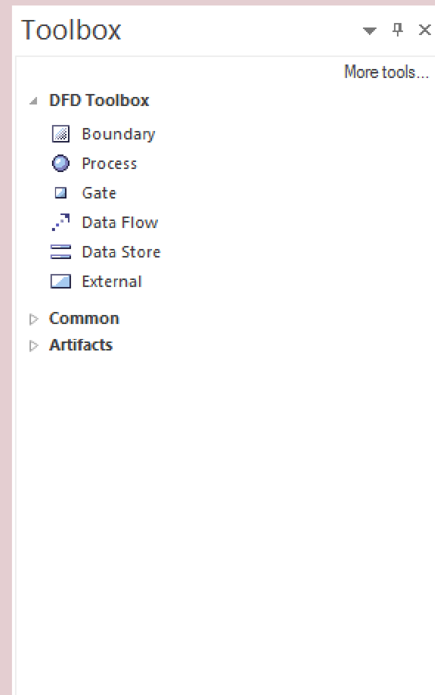
Block Definition Diagram (BDD) for network elements



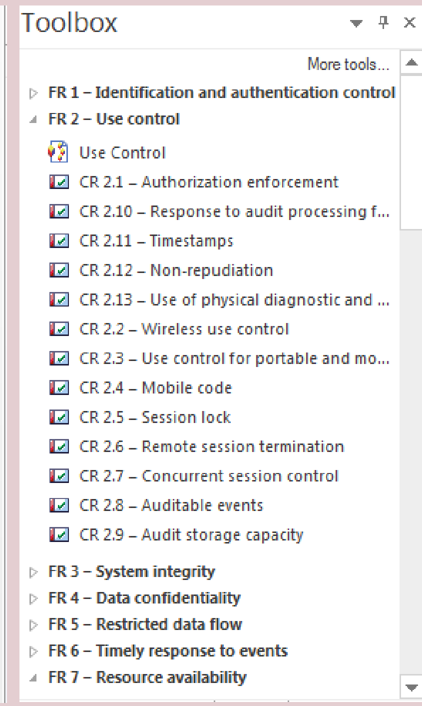
Internal Block Diagram (IBD) for detailed modeling



Dataflow Diagram (DFD) for Threat Modeling

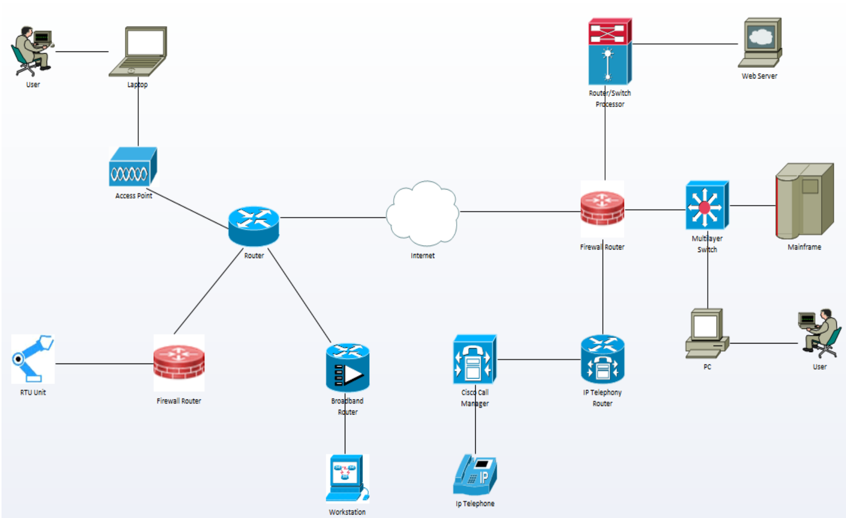


Requirement diagram for security requirements

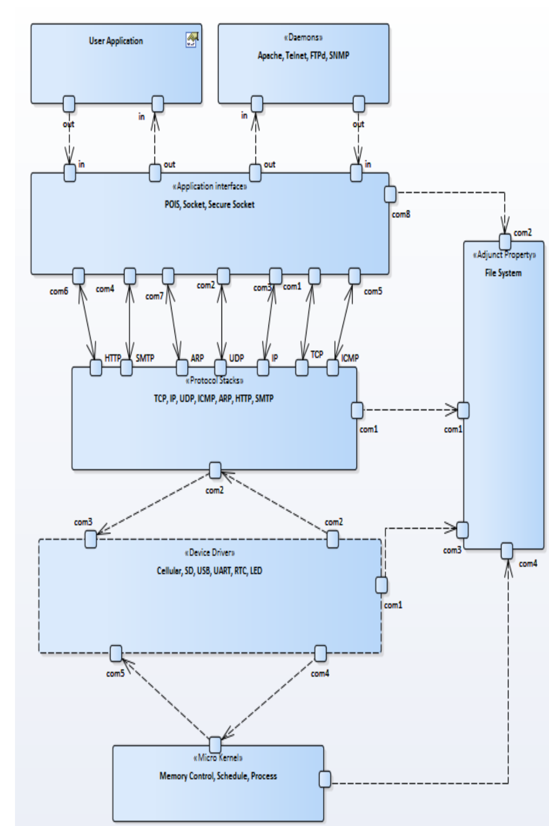


External / Intermediate / Internal Layer

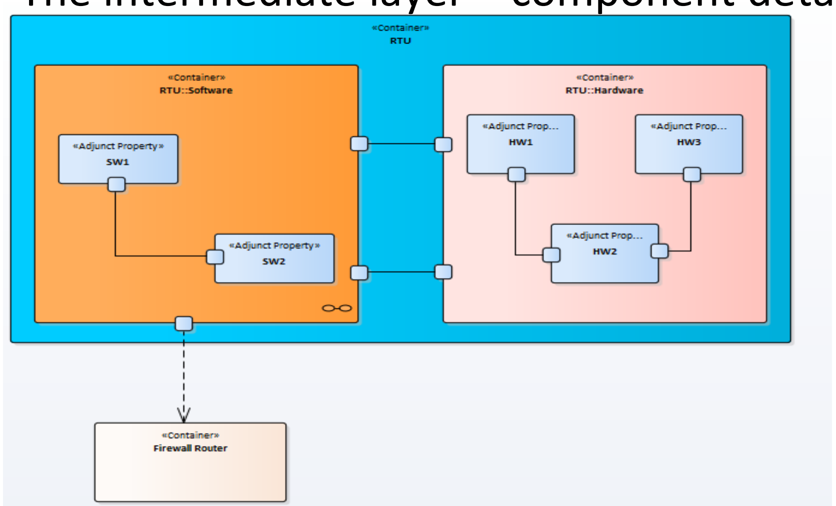
The external layer = network architecture



The interal layer = further details about components

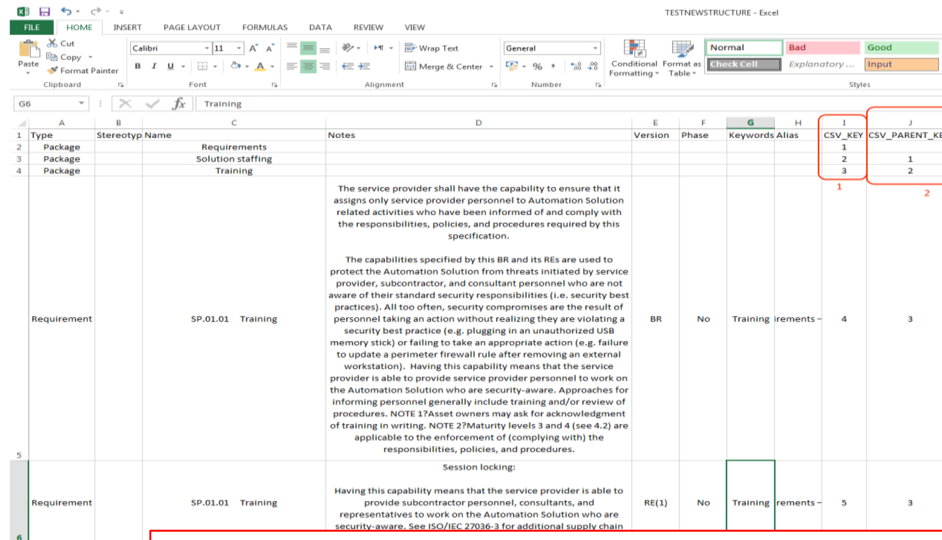


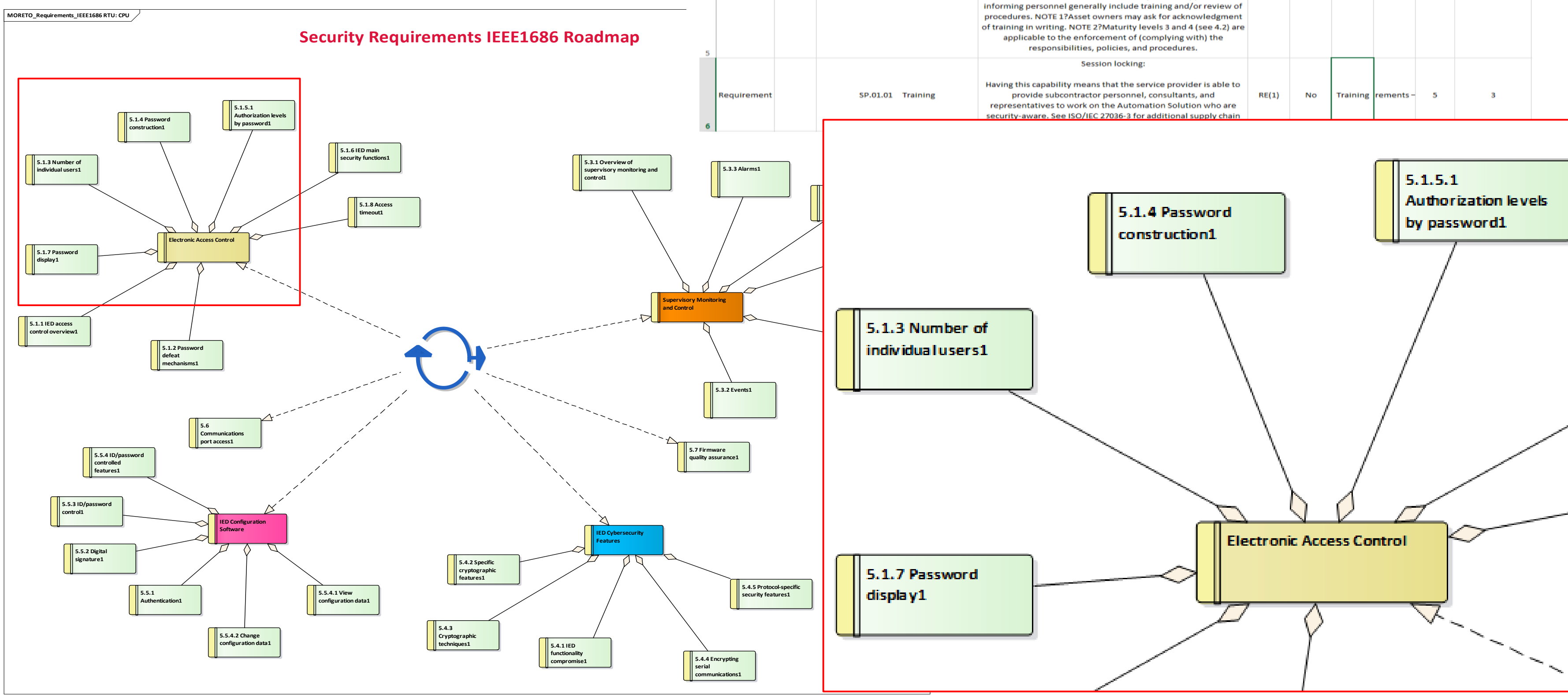
The intermediate layer = component details



Requirements Generation

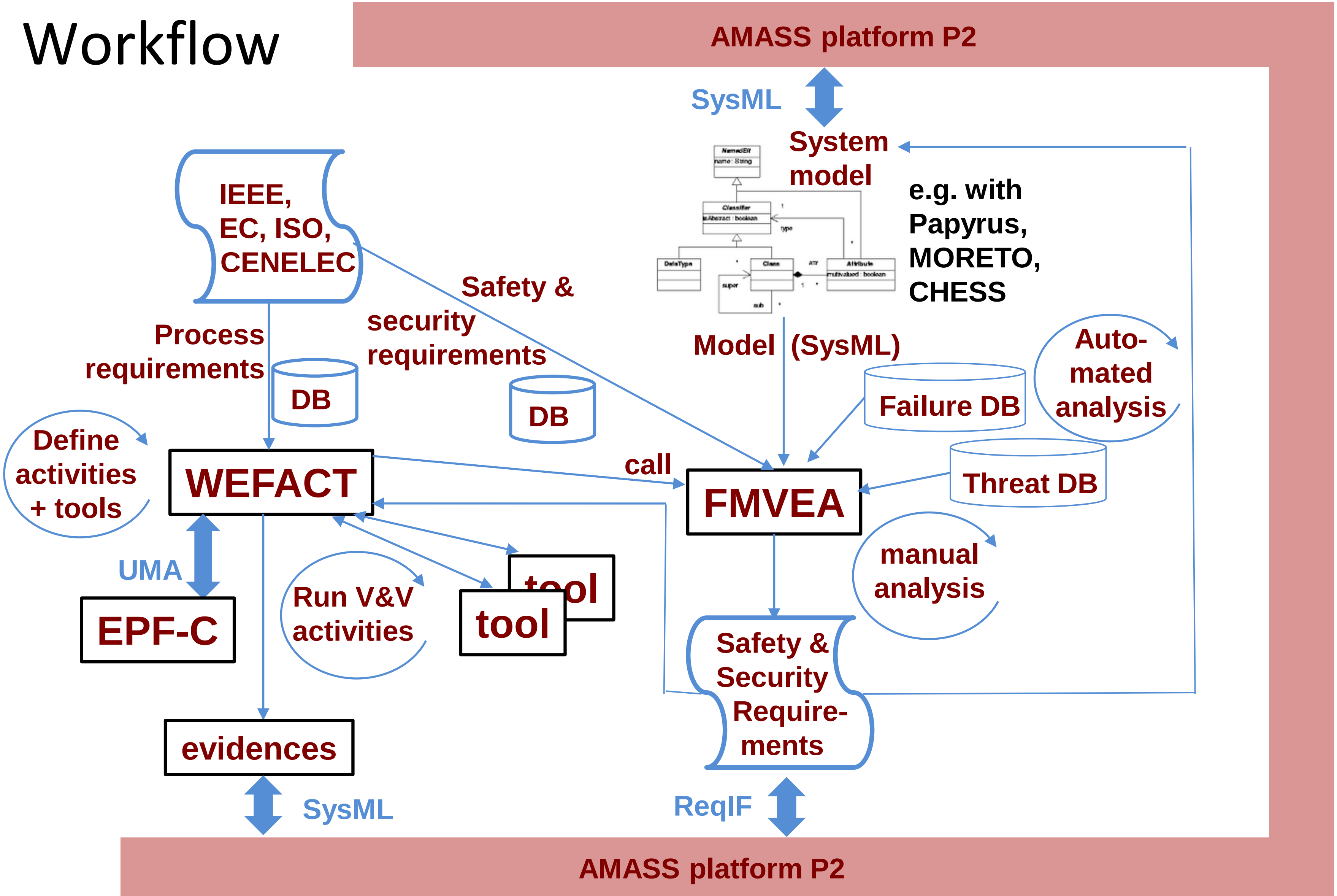
- **Manual Mode:**
  - With Drag and Drop, or
  - Importing a CSV File
- **Automated mode:**
  - With patterns
  - With Scripts





WEFACT and FMVEA Presentation

- Workflow

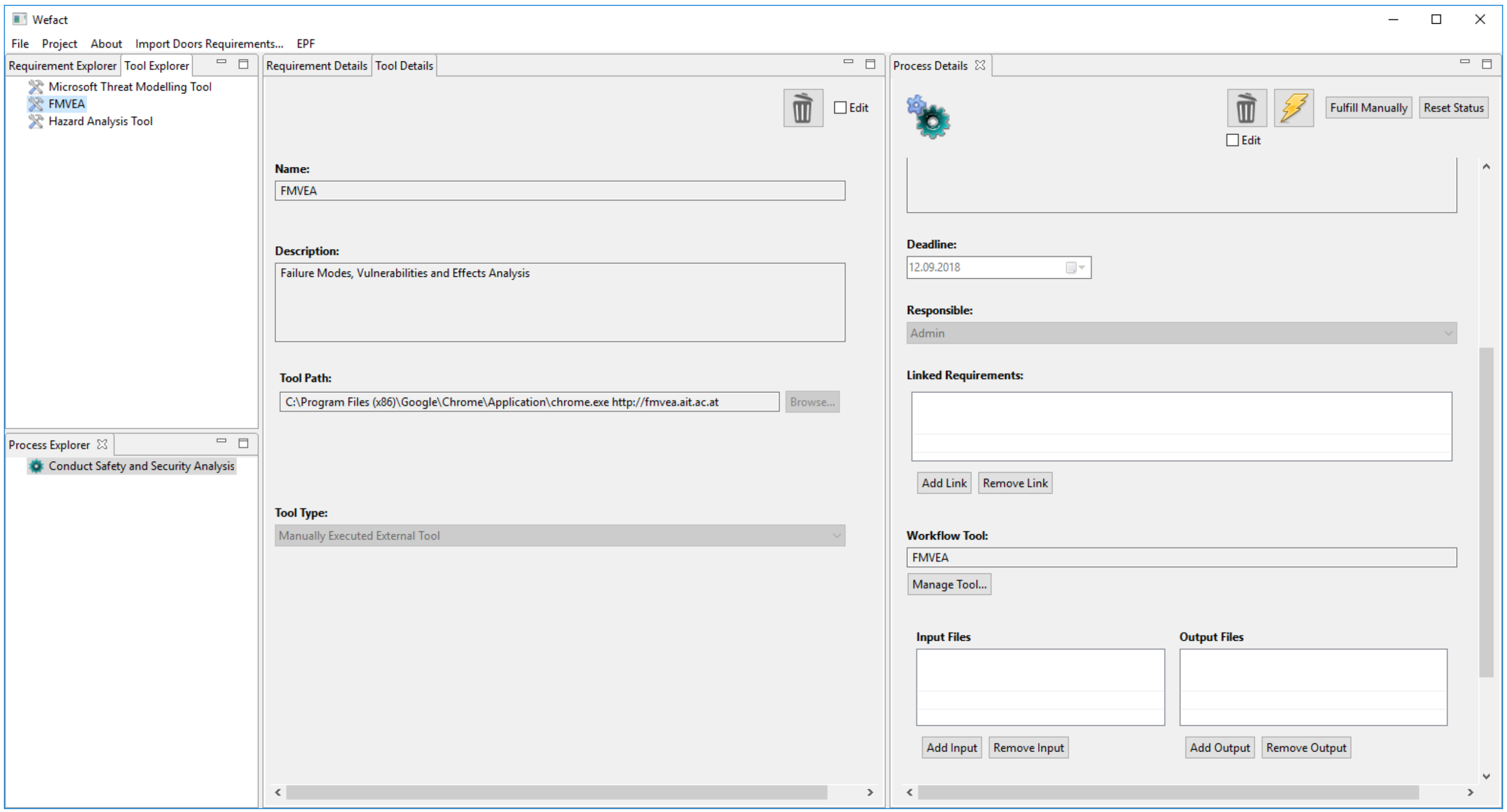


Activities in Iteration 3

- The WEFACT workflow engine executes the tool FMVEA
- The user creates the system model with dependability-relevant properties in FMVEA or imports a SysML model and enhances it with the required properties.
- The user can add rules in FMVEA or re-uses a previously created threat and failure database with these rules. In the case study, the rules correspond to the requirements of the applied standard.
- The database is applied to the system model yielding respective safety and security requirements.
  - In the case study we focus on safety and security, but these rules are not restricted to these quality attributes. The user could as well include multiple concerns, e.g. add a performance requirement like a WCET or a maximum memory usage.
- Two outputs:
  - These security requirments are fed back into the model manually and/or automatically.
  - The requirements are mported in WEFACT to crerate the executable assurance processes which create the evidences

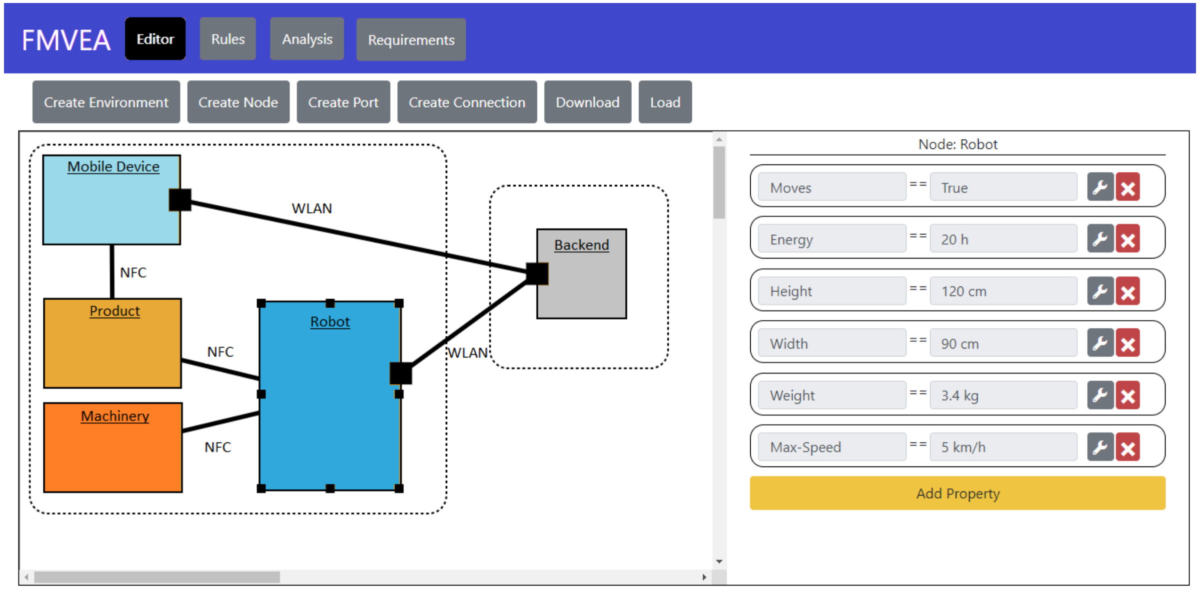
WEFACT Lifecycle Activity for HARA/TARA

- Eclipse RCP application WEFACT is started
- Its process model (edited in WEFACT or imported from EPF-C in UMA dialect format) has associated lifecycle activities.
- In the Lifecycle the HARA/TARA phase is reached by the workflow
- The process starts the FMVEA tool



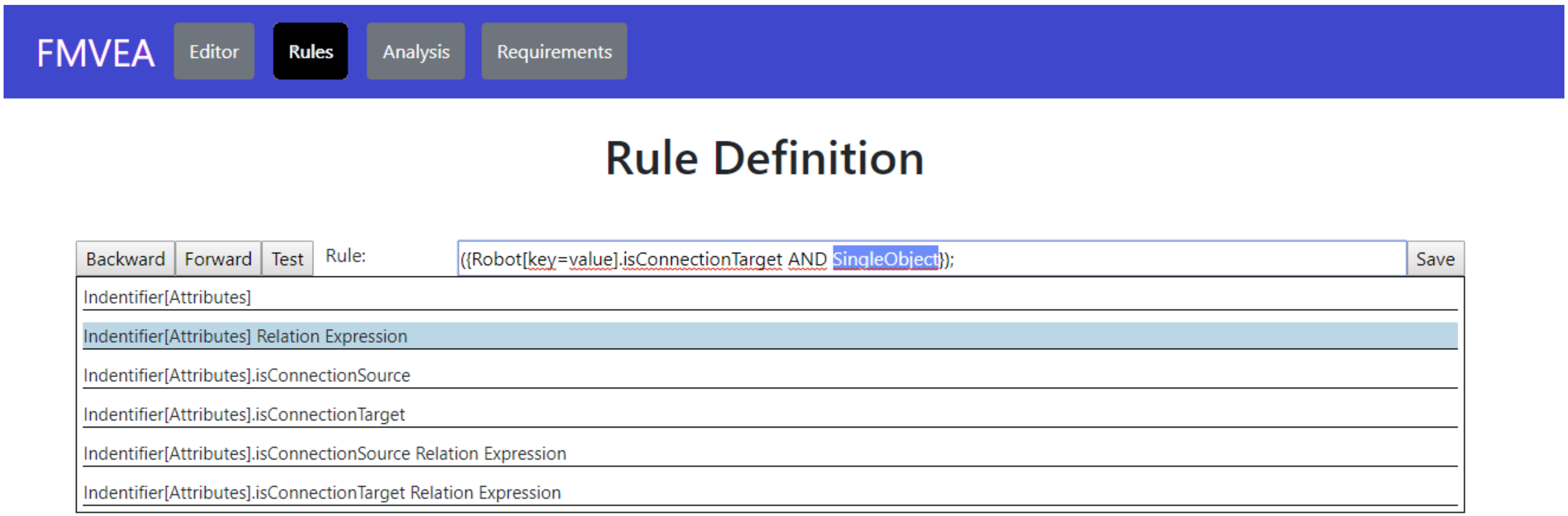
FMVEA Starts with the Model Editor

- Model (with dependability relevant properties) can be edited in FMVEA tool or imported eg. from Papyrus/CHESS via SysML



Safety/Security Rules Are Defined or Re-Used from DB

- FMVEA allows do define rules



- Or to use a previously created database,
  e.g. realizing the rules of a specific standard

Automated Rule-based Safety/Security Analysis

- FMVEA applies its rules on model elements and thereby performs the FMVEA safety and security analysis.

FMVEA | Editor | Rules | **Analysis** | Requirements

Analysis Results

#	Affected Element	Threat	Likelihood	Impact	Risk
1	NFC	Robot recieves wrong information from NFC communication from machinery	2	F1	2
2	WIFI	Eavesdropping of wifi Signal	2	C4	20
3	Robot	Behaviour is not under control	5	F3	5

- Requirements generated according to the rules

FMVEA | Editor | Rules | Analysis | **Requirements**

Requirements

#	Affected Element	Requirement	Description	SL
1	WIFI	The WIFI Communication shall be encrypted	Encrypt the WIFI with appropriate algorithm.	4
		Limit the range of the WIFI signal	Restrict the area where the WIFI signal is active.	4
2	NFC	Integrate a sensor for product validation	Install a Sensor on Robot to detect wrong information from machinery.	1
		The Robot shall alarm when it detects irregularities	After the robot received wrong information from the machinery he was able to detect the error and then reports the error.	1
3	Robot	The Robot shall have emergency shutdown	Robot needs emergency stop which is always active. (Physical)	2
		The Robot shall only operate in a restricted area	Restrict the movement of the robot with physical borders.	2

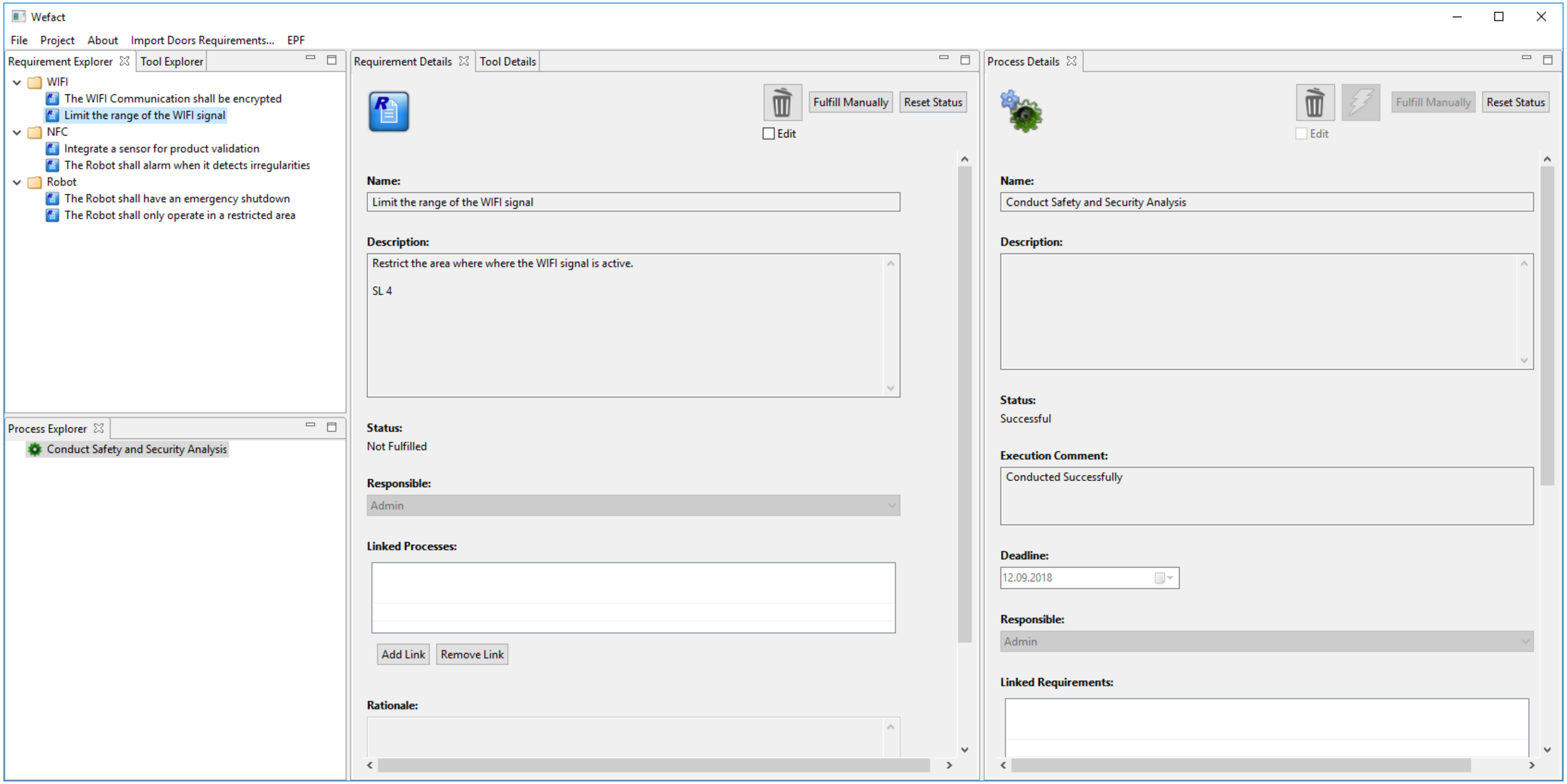
- Export function to open format ReqIF

FMVEA in an Excel File

- This shows a sheet for a manual FMVEA analysis -> Effort intensive

Element	Threat / Failure Mode	STRIDEF(ailure)	Direct Effect	System Effect	Impact	Cause	Likelihood	Risk	Comments
NFC Zone	Manipulated data	Tampering with data, Denial of Service	Machinery recieves wrong information from NFC communication from robot	Machine stops (wrong data detected)	F2	Insider attack	2	4	
			Robot recieves wrong information from NFC communication from machinery	Robot stops and alarms (wrong data detected)	F1	Insider attack	2	2	
			Robot recieves wrong information from NFC communication from product	Robot stops and alarms (wrong data detected)	F1	Insider attack	2	2	No clarification of how the robot behaves, we decided that the robot should stop. But this may result in the worst financial impact.
	Jamming	Denial of Service	Jamming of NFC Signal	Machinery and Robot stop because weak or anomalous signal is detected.	F3	Jammer signal reaches factory	5	15	
	Eavesdropping	Information Disclosure	Eavesdropping of NFC Signal	Cannot detect eavesdropping.	C4	Signal reaches the receiver's antenna	5	20	Countermeasure: Use authenticated encryption with key that was exchanged in a safe environment beforehand.
Wi-fi Zone	Manipulated data	Tampering with data, Denial of Service	Robot receives wrong instructions via wifi.	Robot does not work properly.	O2	Attack	5	10	
			Mobile device receives wrong instructions via wifi	Mobile device does not work properly. Mobile device may configure NFC tags of products wrongly.	O2	Attack	5	10	
			Backend receives wrong information from wifi.	Backend recognizes wrong information. Initiates reconfiguration of operators.	O2	Attack	5	10	Detected
				Backend does not recognize wrong information.	O3	Man in the middle attack	5	15	Not detected
	Jamming	Denial of Service	Jamming of wifi Signal	No information can be transmitted via wifi.	F3	Jammer signal reaches factory	5	15	
	Eavesdropping	Information Disclosure	Eavesdropping of wifi Signal	Cannot detect eavesdropping.	C4	Signal reaches the receiver's antenna	5	20	Countermeasure: Use authenticated encryption with key that was exchanged in a safe environment beforehand.
Mobile Device	Wrong configuration is written on NFC tag by the mobile device	Tampering with data	We assume that the robot does not find the (correct) product because the product received a wrong NFC tag from the mobile device.	The robot cannot execute its command as it cannot find the associated NFC tag.	F2	Insider Attack	3	6	
Robot	Manipulated configuration of the robot	Denial of Service	Behaviour is not under control	Unexpected behaviour of the robot.	F3	Insider attack	5	15	
Entire System	High Altitute Electromagnetic Pulse (HEMP)	Denial of Service	Electronic devices are damaged	Production is stopped completely, multiple devices harmed, devices may work wrongly, unecpected incidents	4	Atttack	1	4	

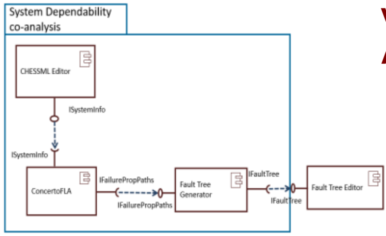
- Requirements lead to security controls whose presence/correctness must be assured.
- This leads back to WEFACT activities which implement the executable assurance processes for these new requirements



Scenario Outcome (expected in P2)

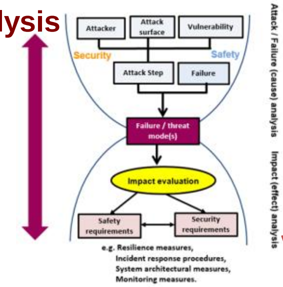
- Reduced effort for assurance and certification through automation and co-assessment
- Effectiveness in failure/threat identification capabilities by following standards
- Update of the model according to the requirements created
- time needed for separate safety and security engineering process is significantly reduced when applying the combined co-engineering process
- Iterations for deriving requirements for architectural or design modifications reduced by combined safety/security co-engineering

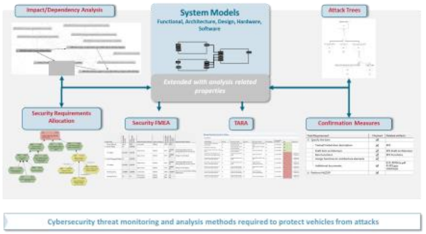
Y2 Achievements: Delivery for P2 on August 31st, 2018



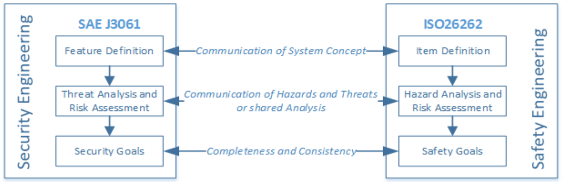
System dependability co-analysis via ConcertoFLA

FMVEA- Failure Modes, Vulnerabilities & Effects Analysis

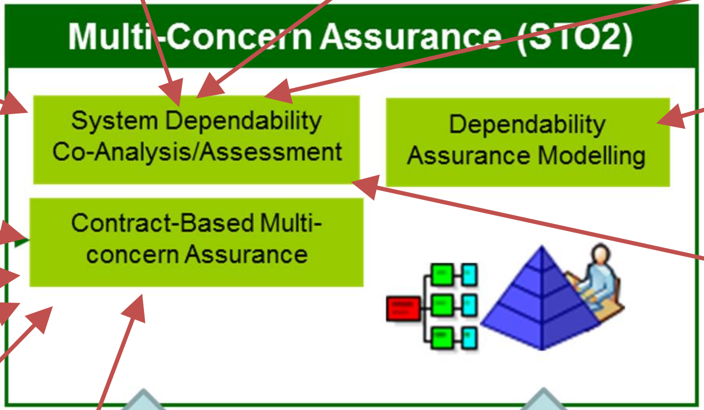


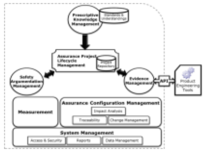


External tool
Medini Analyzer



SiSoPLE for enabling process-related co-assessment



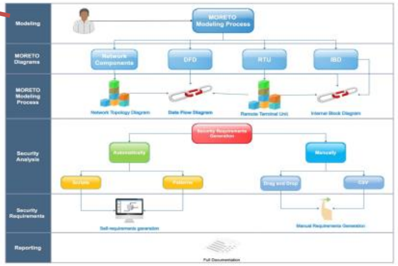


P1 ✓
openCert Assurance Case Editor

Contract-based trade-off analysis In parameterized architectures

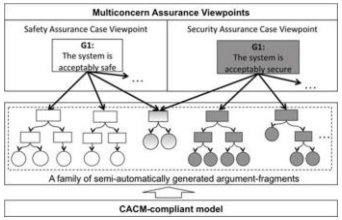
Abstract functions in the contracts specification

Contract-based trade-off analysis with Analytical Network Process

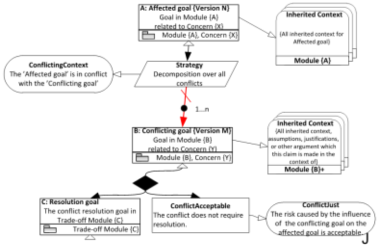


External MORETO Security analysis and requirements generation tool

multiconcern contracts in assurance via argument-fragment generation



General extensions To contract based multi-concern assurance

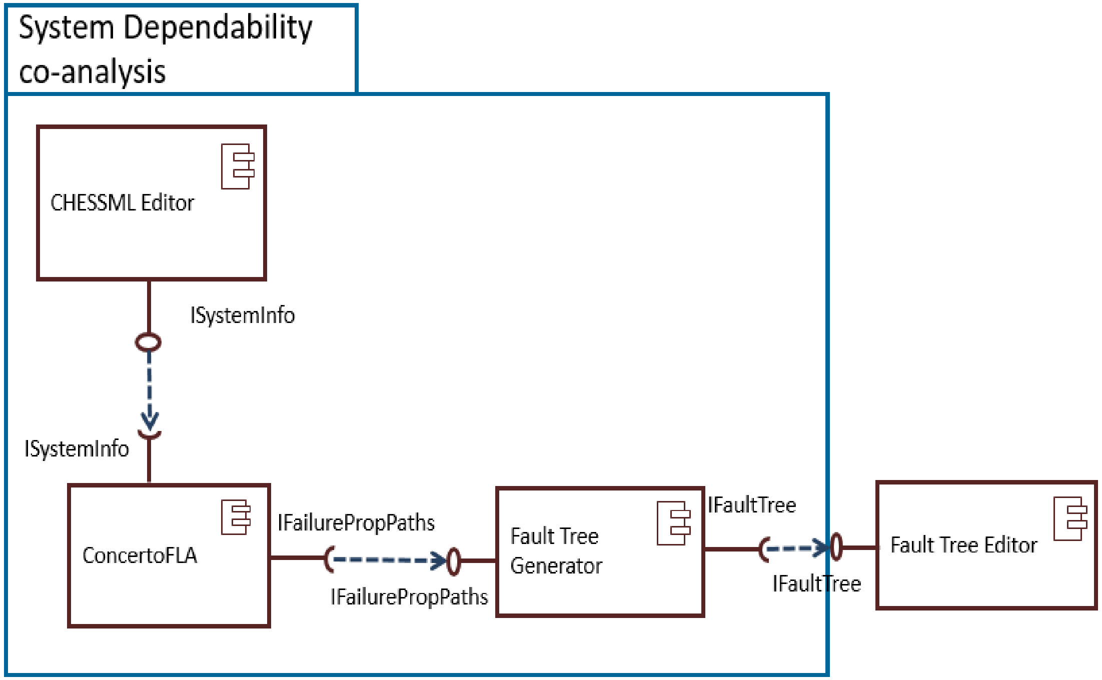


Many functional extensions delivered in:

D4.6 Prototype for multi-concern assurance (c)

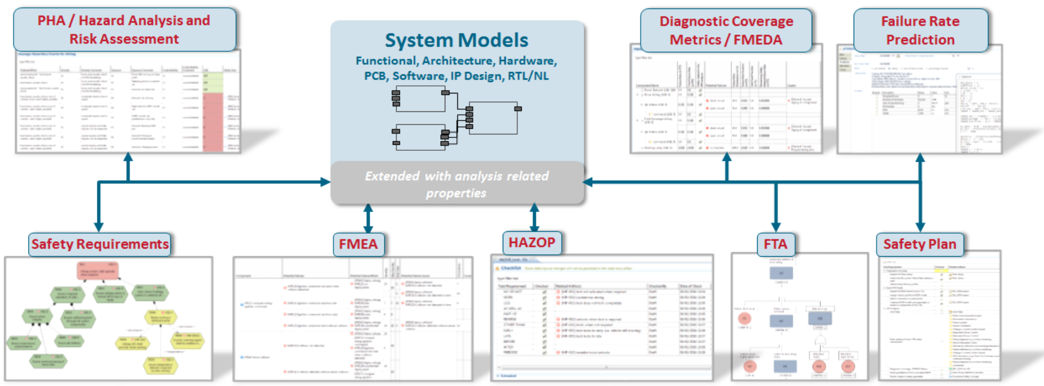
System Dependability Co-analysis via ConcertoFLA

- A compositional technique to qualitatively assess the dependability of component-based systems. Users can
- decorate CHESSML models with dependability-related information
- execute Failure Logic Analysis (FLA) techniques (based on Failure Propagation Transformation Calculus (FPTC) and using the FlaMM meta model), and
- calculate the failure behaviour of a component based system at system-level, based on the specification of the failure behaviour of the individual components
- get results back-propagated onto the original model.



Medini Analyzer

medini analyze – a Model based and System oriented Solution



Model-based approach ensures unrivalled level of consistency, traceability and efficiency

Safety Analyzer available for a long time

Features:

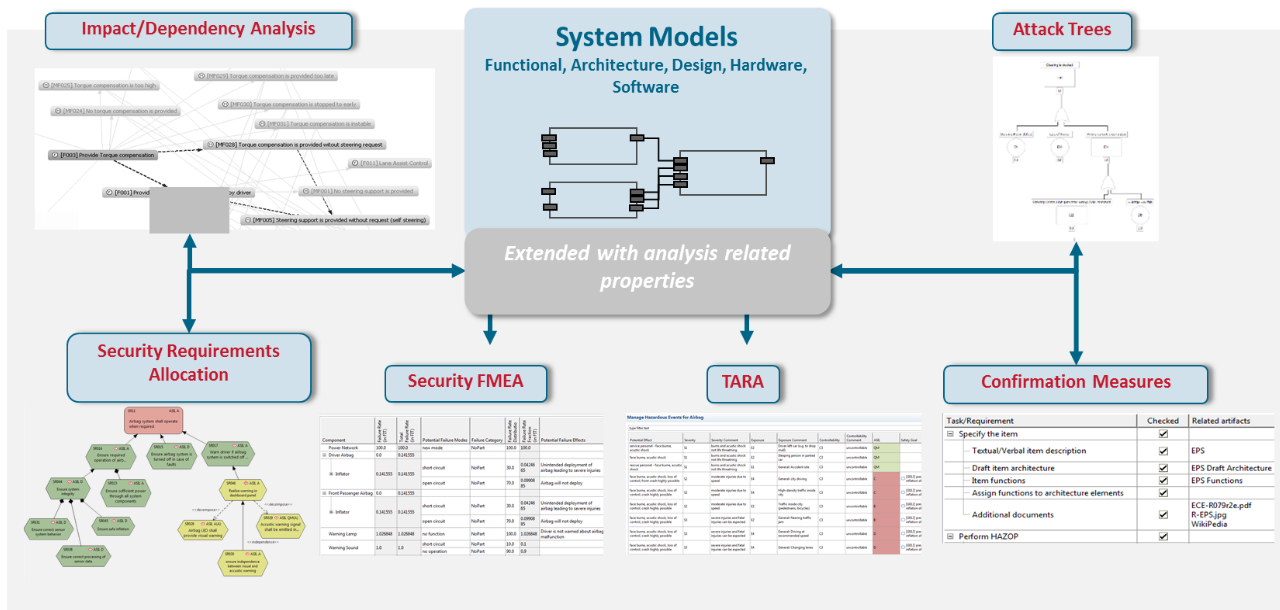
- Eclipse based
- PHA, HARA, FMEA, FMEDA, FTA, HAZOP, Safety requirements & plans

SESAMO: prototype for security analysis

Cybersecurity analysis now available as a mature comercial tool

Features:

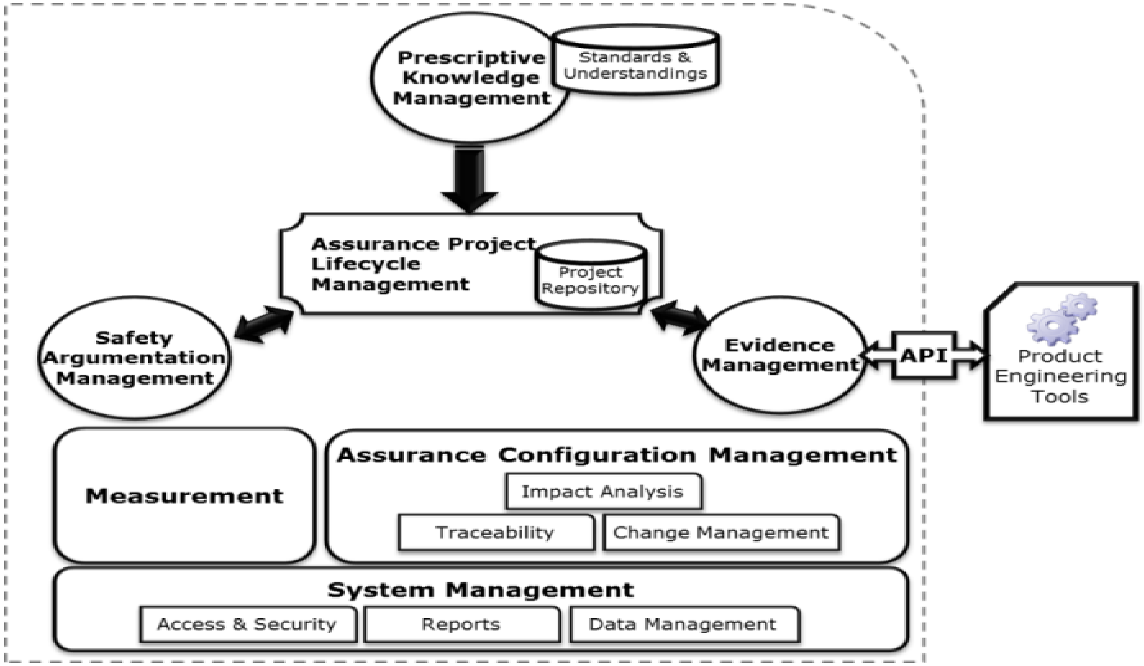
- Attack trees, TARA, Security FMEA, Security requirements allocation, confirmation measures
- AMASS integration via
- SCADE Architect



Cybersecurity threat monitoring and analysis methods required to protect vehicles from attacks

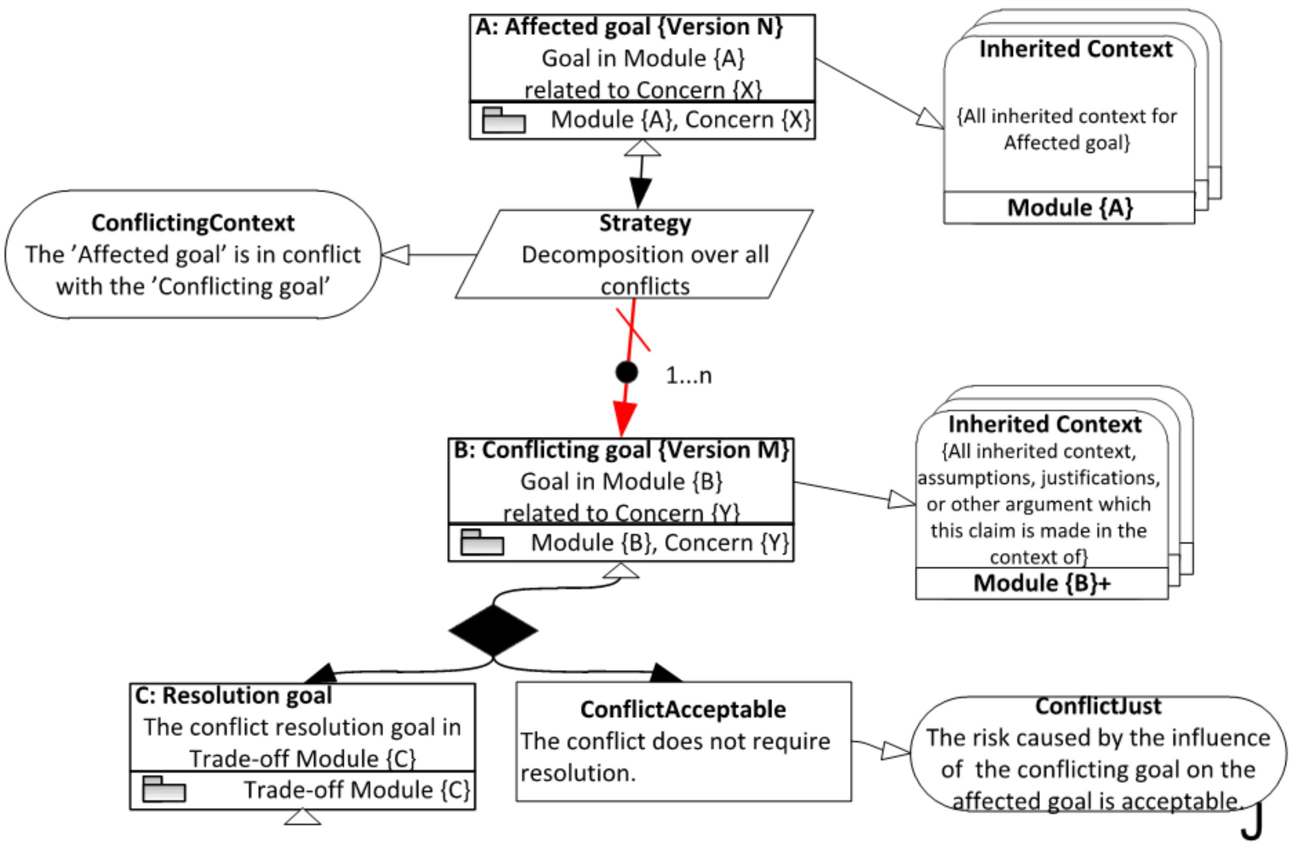
openCert Assurance Case Editor

- Edit in graphical GSN syntax, internal data in SACM,
- Support multiconcern argumentation
- Argument patterns,
- Assurance case contracts
- Implements Basic Building block „Assurance case specification“
- Delivered in Pcore and P1



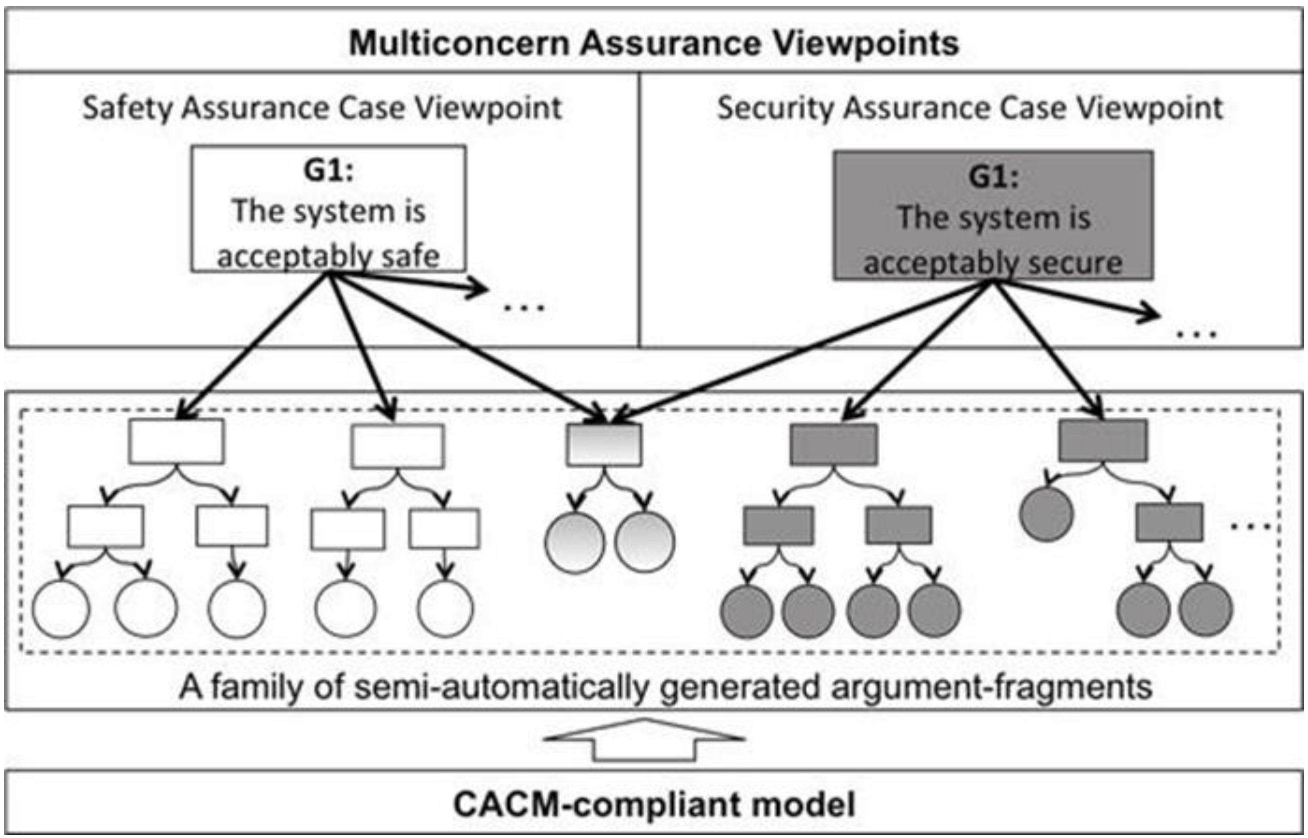
General Extensions to Contract-based Multi-concern Assurance

- Extensions in CHESS for contract-based trade-off analysis
- Model treats conflicts between dependability attribute-specific goals

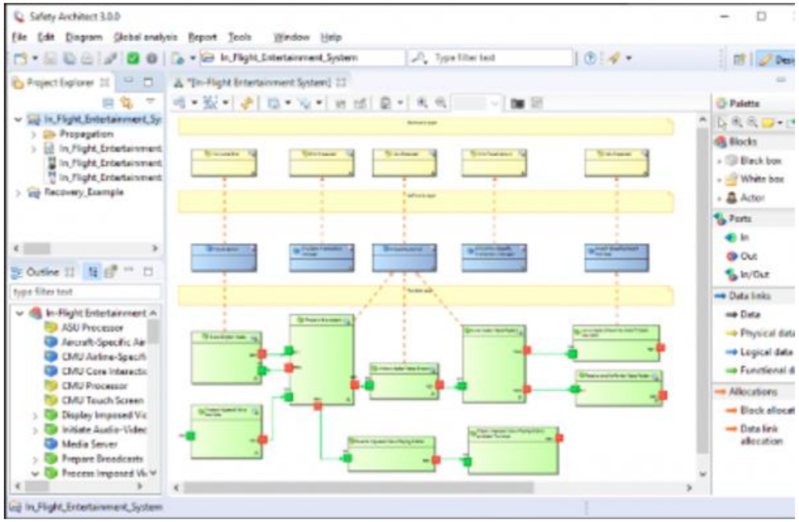


Multiconcern Contracts in Assurance via Argument-Fragment Generation

- Out of defined processes for generating evidences, corresponding arguments for the assurance case can be generated.
- Feature strongly related to WP6 and therefore descried there.



Extended Safetey Architect



- All4Tec commercial tool
- Supports FMEA, FTA with automatic detection ofthe FE (feared events),
- extended during the MERgE ITEA and French Clarity Project to support Safety and Security Co-Analysis
- For describing failure and threat propagation, Safety Architect provides safety view, security view & merged view
- dysfunctional analysis techniques applied for automatic fault or attack tree generation
- interfaces with many system engineering tools, such as Capella, System Architect, Papyrus, and the AMASS platform

AMT 2.0 – Analogue Mixed Signal Monitoring

- Apart from Contract-Based Multiconcern Assurance (STO2), tool is also related to Architecture-driven Assurance (STO1)
- deploy methods for monitoring and diagnosing Cyber-Physical System (CPS) models in Simulink
- translating informal system specifications into formal specification expressed in the extended Signal Temporal Logic (STL)
- Tool integrates existing monitoring techniques at AIT to the Simulink environment (CS3 in P2)
- Novel methods developed for system diagnosis and error localization in the Simulink models upon the detection of the specification violations.

Conclusion

- Guidance from standards getting slowly improved
- Other projects take partly comparable approaches
- Progress based on CS1, US2 demonstrated
- Integrating heterogeneous external tools essential
- Coupling workflows of single-concern tools necessary
- Few combined (integrated) tools available