AMASS

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

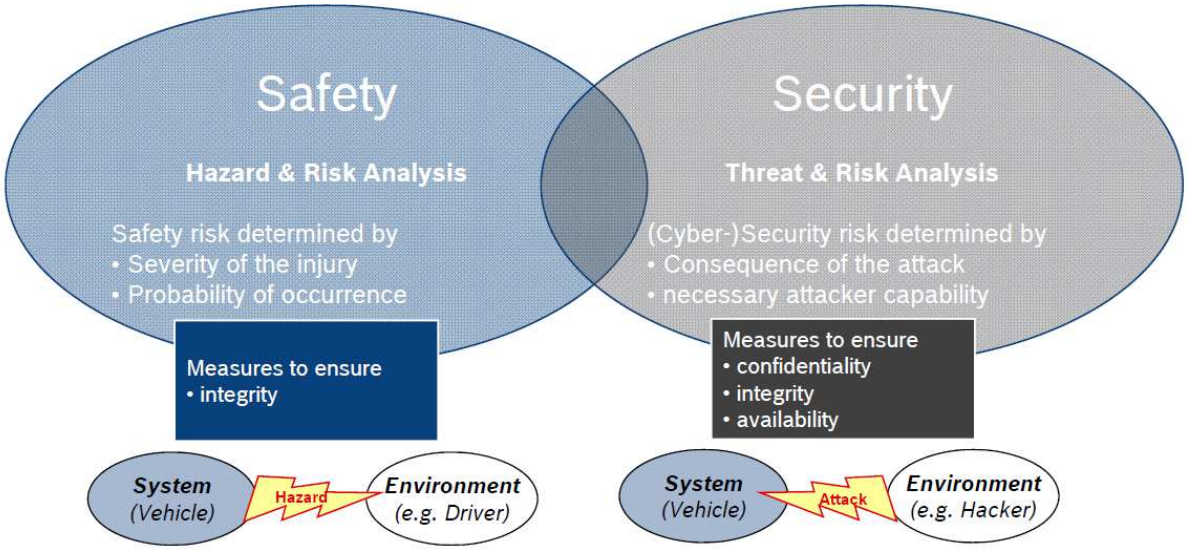
Co-engineering of security and safety life-cycles for engineering security-informed safety-critical automotive systems in compliance with SAE J3061 and ISO 26262

Ada-Europe, Warsaw
February 11-14, 2019

XX
Virtual Vehicle Research Center

Safety and Security Co-Engineering for Road Vehicles

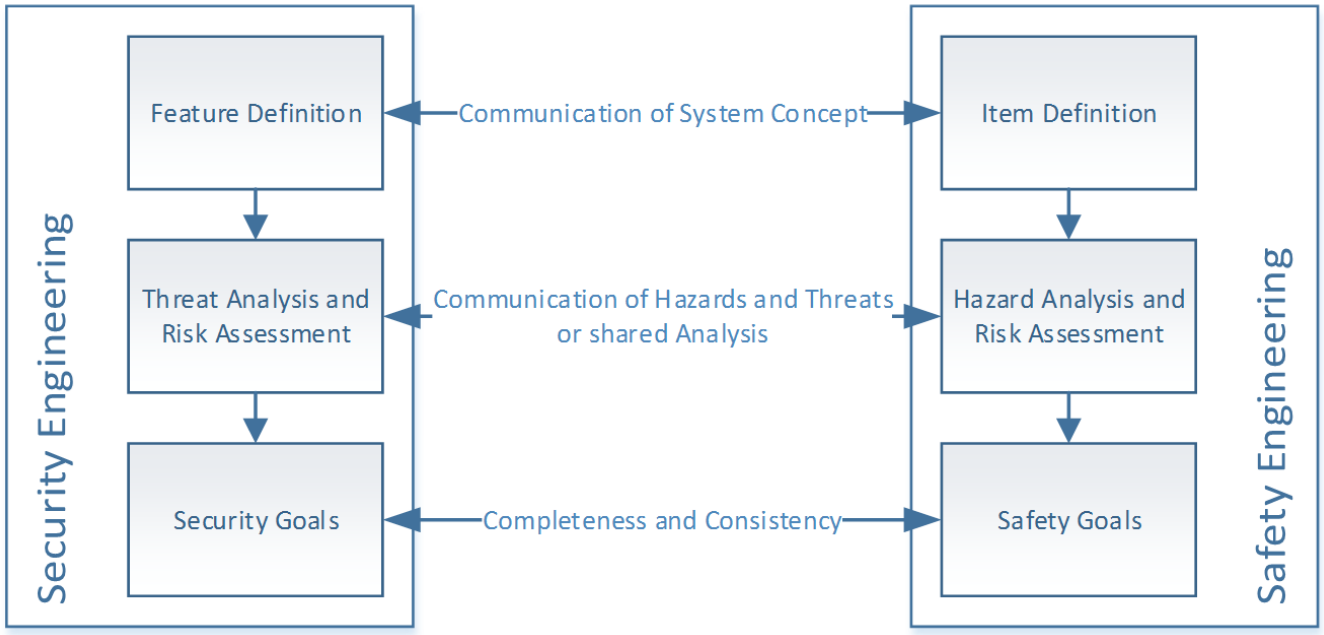
- Safety vs. Security
- Safety protects people from the machine
  - Prevent errors in the system that can lead to harm person
- Security protects the machine from people
  - Prevent human intervention in the system that can lead to all types of damage (Safety, Financial, Law, Image,...)



Source: Safety_meets_Security 2018 Klarmann_Gebauer

Process Definition based on two Standards

- Identification of commonality and variability (safety perspective)
  - ISO 26262 (safety)
  - SAE J3061 (security)



Source: AIT

Usage Scenario

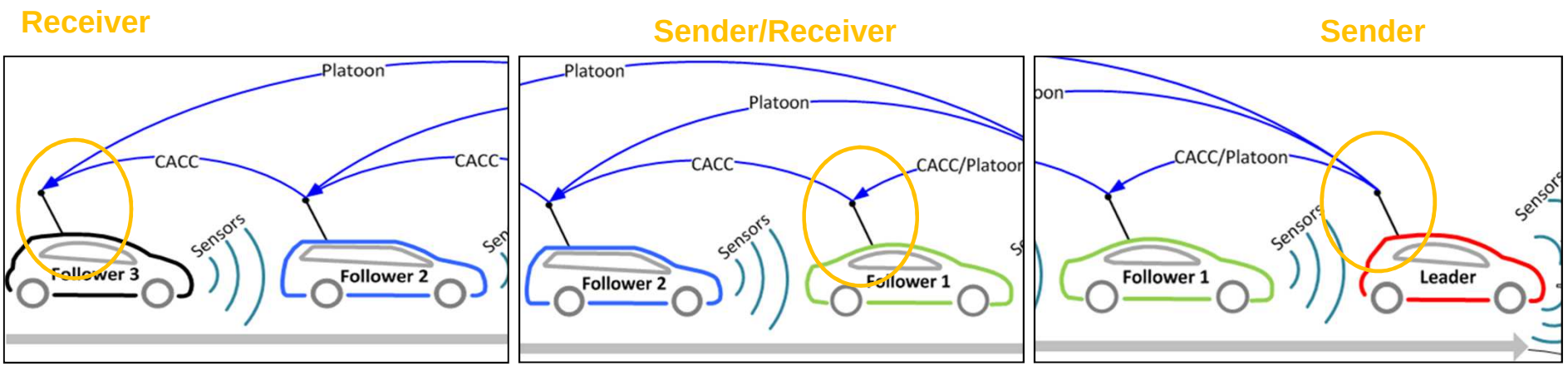
- Safety and Security aspects of radio connection

Safety

- Item Definition
- HARA
- Safety Goals
- Functional Safety Requirements
- FMEA

Security

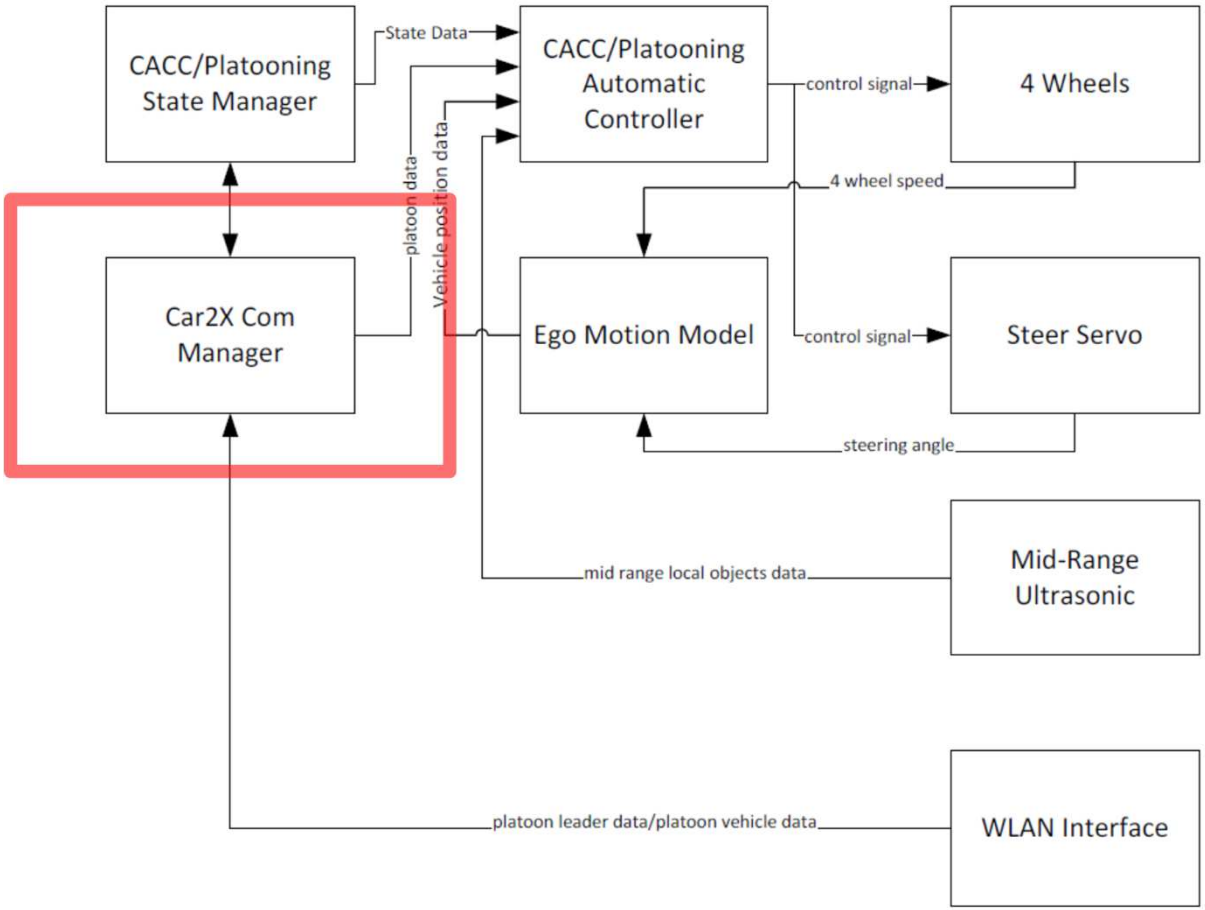
- Feature Definition
- TARA
- Cybersecurity Goals
- Cybersecurity Requirements
- FMVEA



Usage Scenario

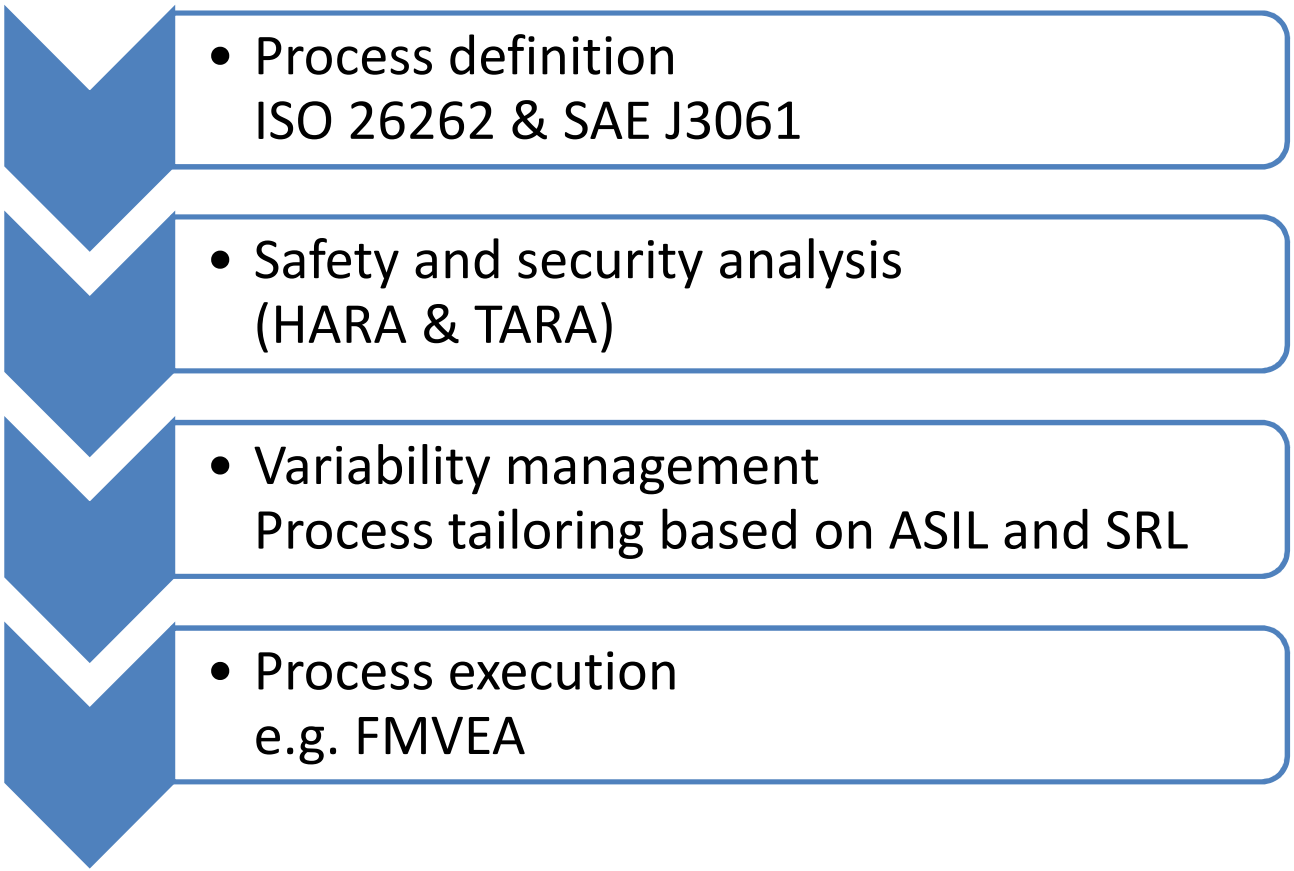
Verification of the system design

Car2X Communication Manager Unit



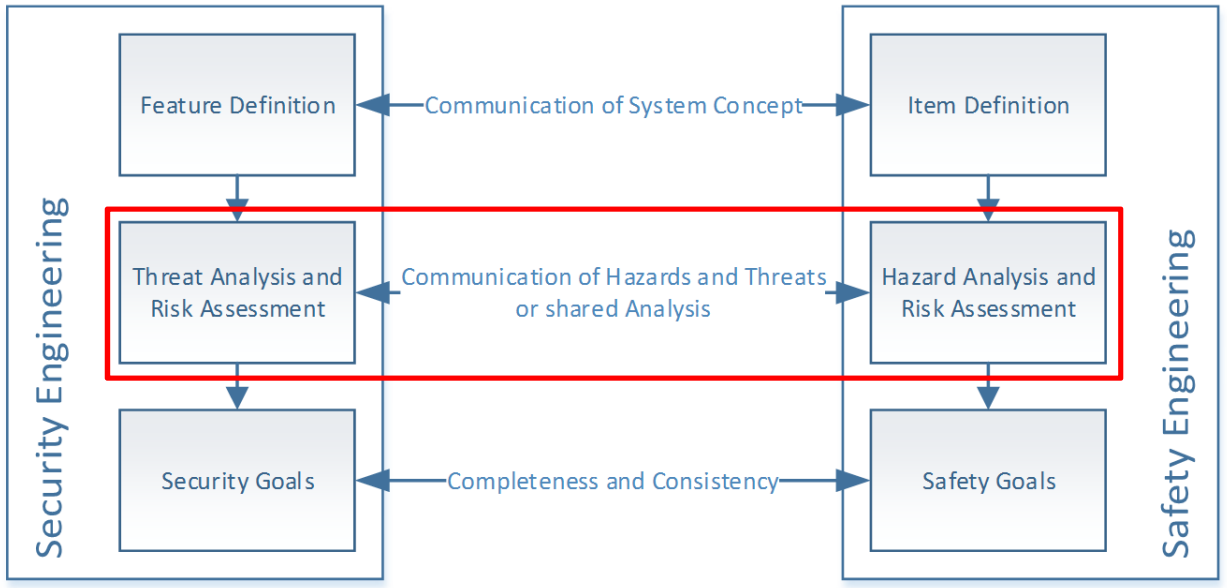
Source: Berner&Mattner

Process flow



Process Development - Safety Security Co-engineering

- Identification of co-engineering activities
  - based on ISO 26262 and SAE J3061
- Interaction between safety and security
  - Identification of interaction points
- Development of base process
  - Output: general process model



Source: AIT

Safety Security Analysis – elaboration of ASIL and SRL

SAE INTERNATIONAL

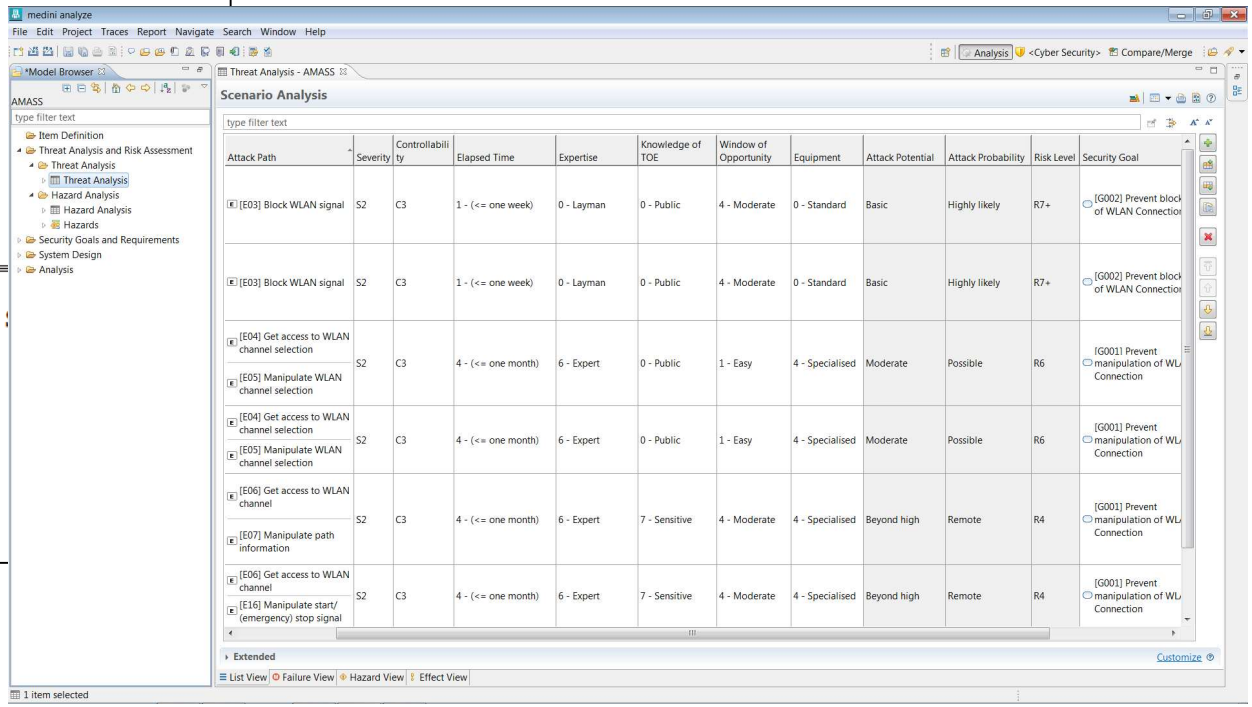
SURFACE VEHICLE RECOMMENDED PRACTICE	J3061™	JAN2016
	Issued 2016-01	
Cybersecurity Guidebook for Cyber-Physical Vehicle Systems		

INTERNATIONAL STANDARD **ISO 26262-3**

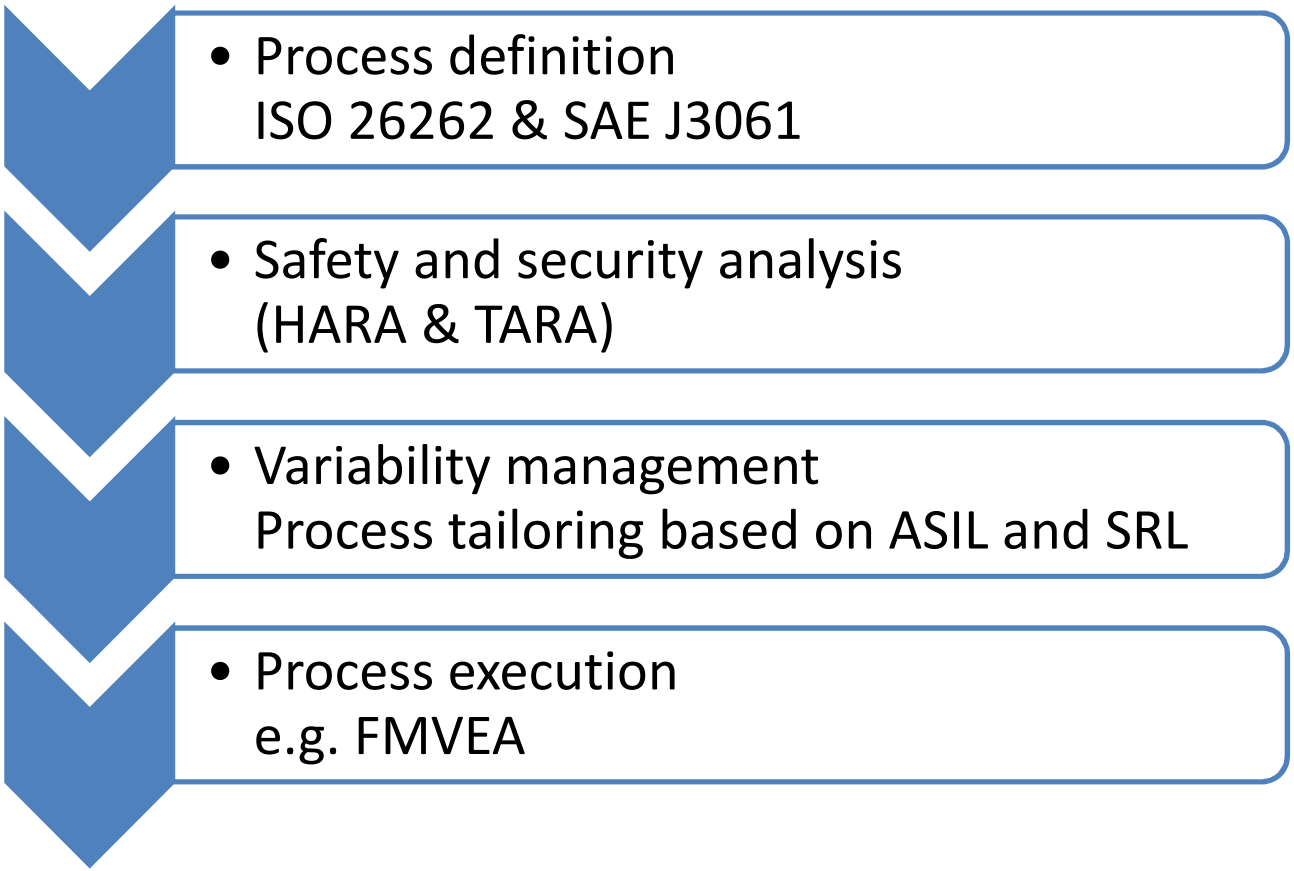
Road vehicles — Functional

Part 3:
Concept phase

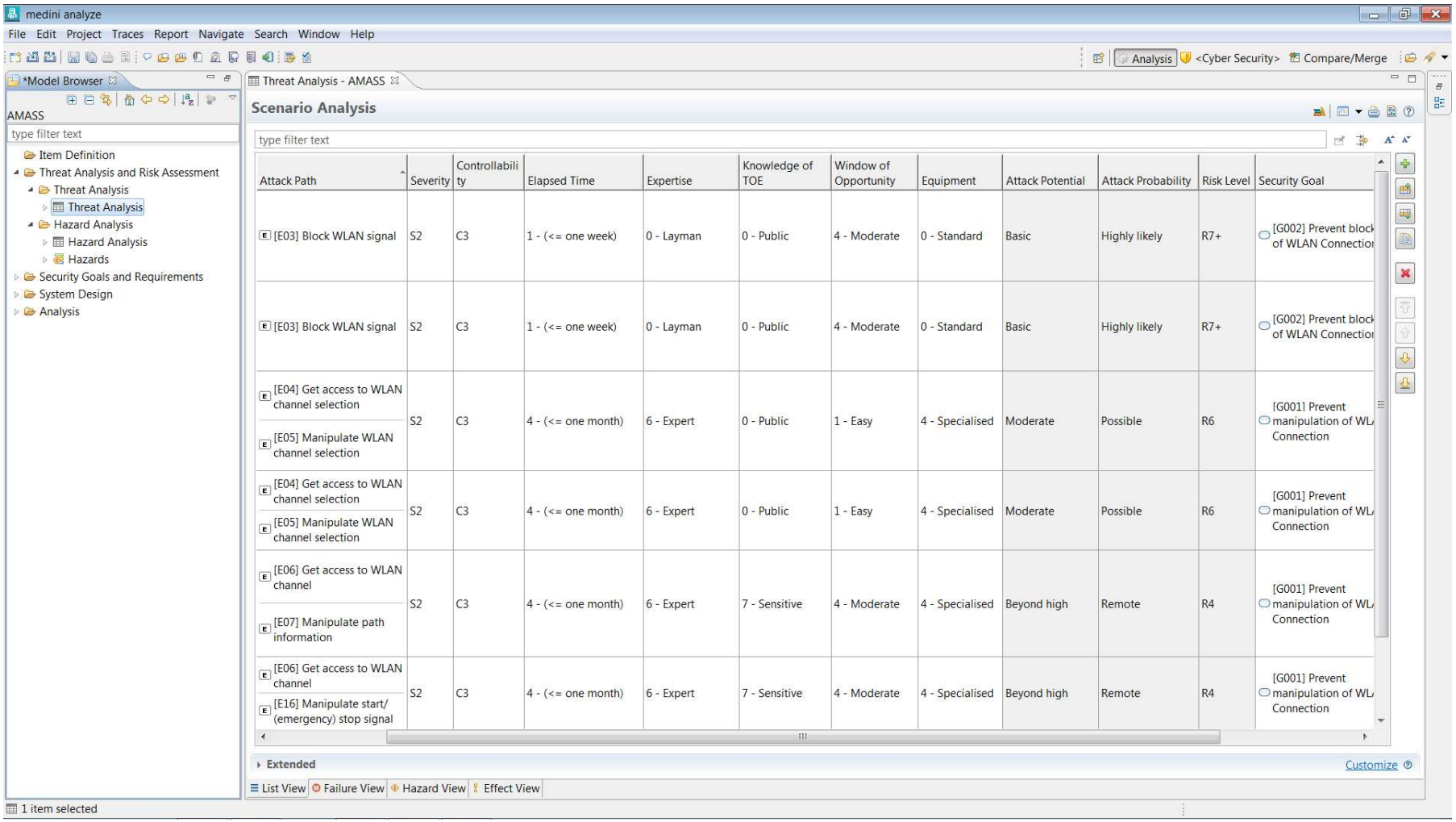
Véhicules routiers — Sécurité fonctionnelle —
Partie 3: Phase de projet



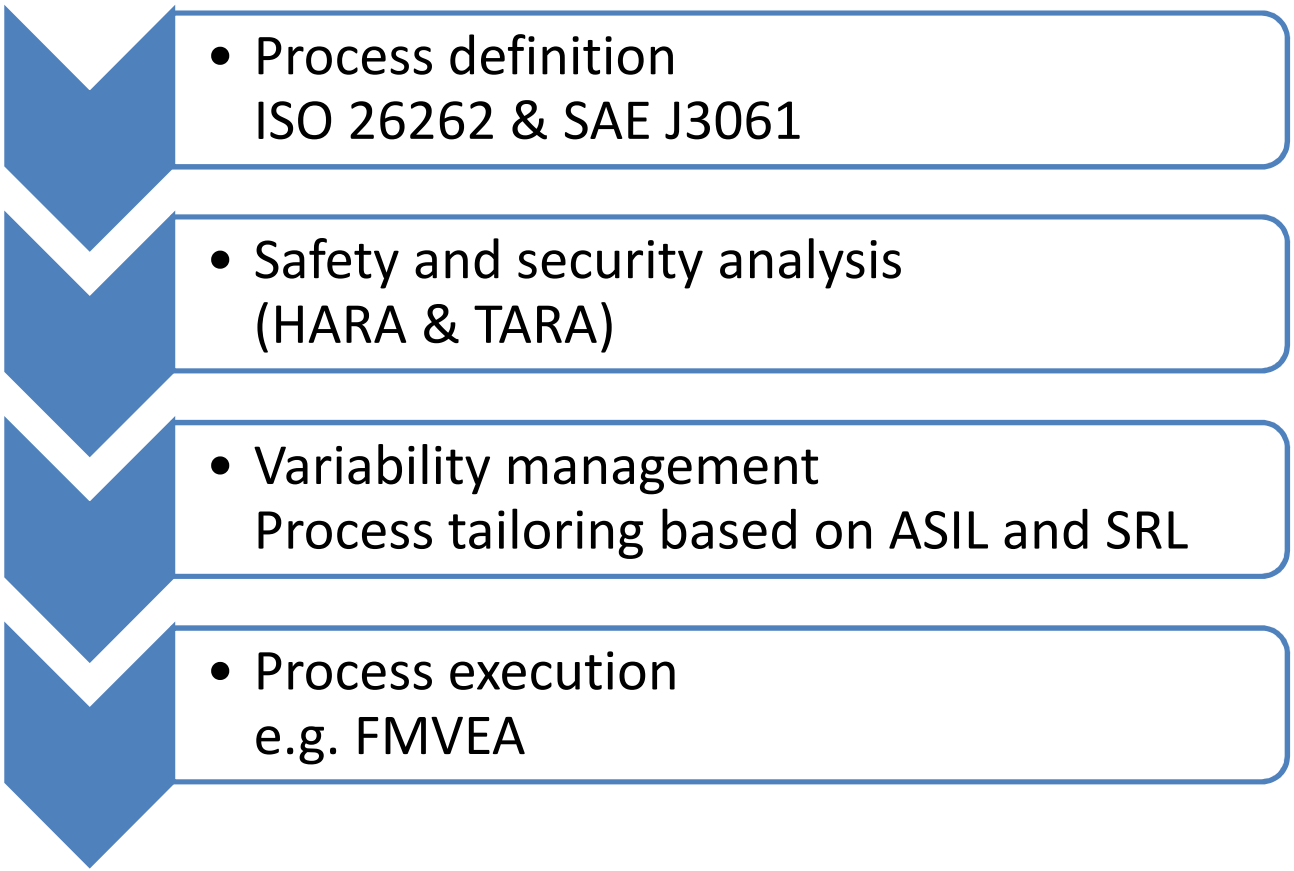
Process flow



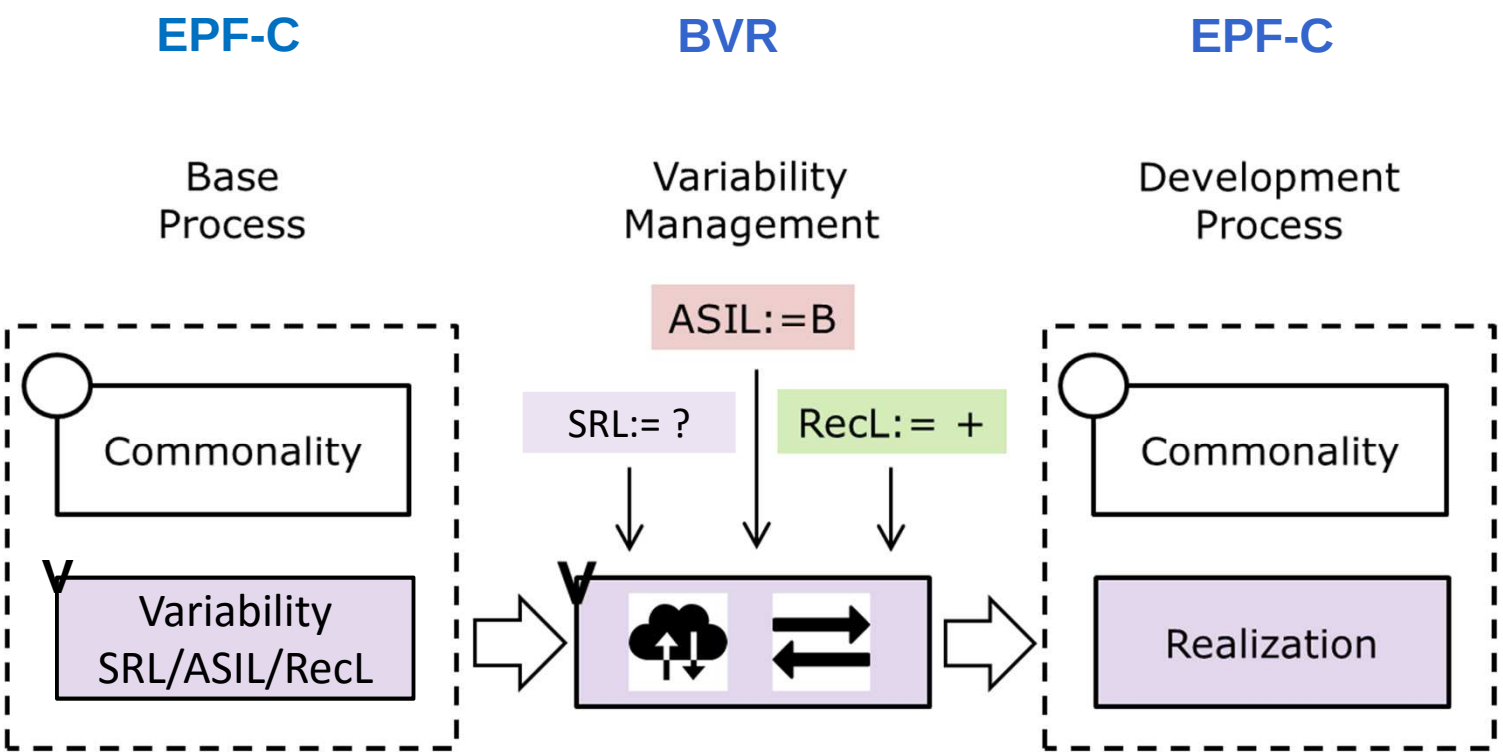
TARA for specific usage scenario in medini analyze tool



Process flow



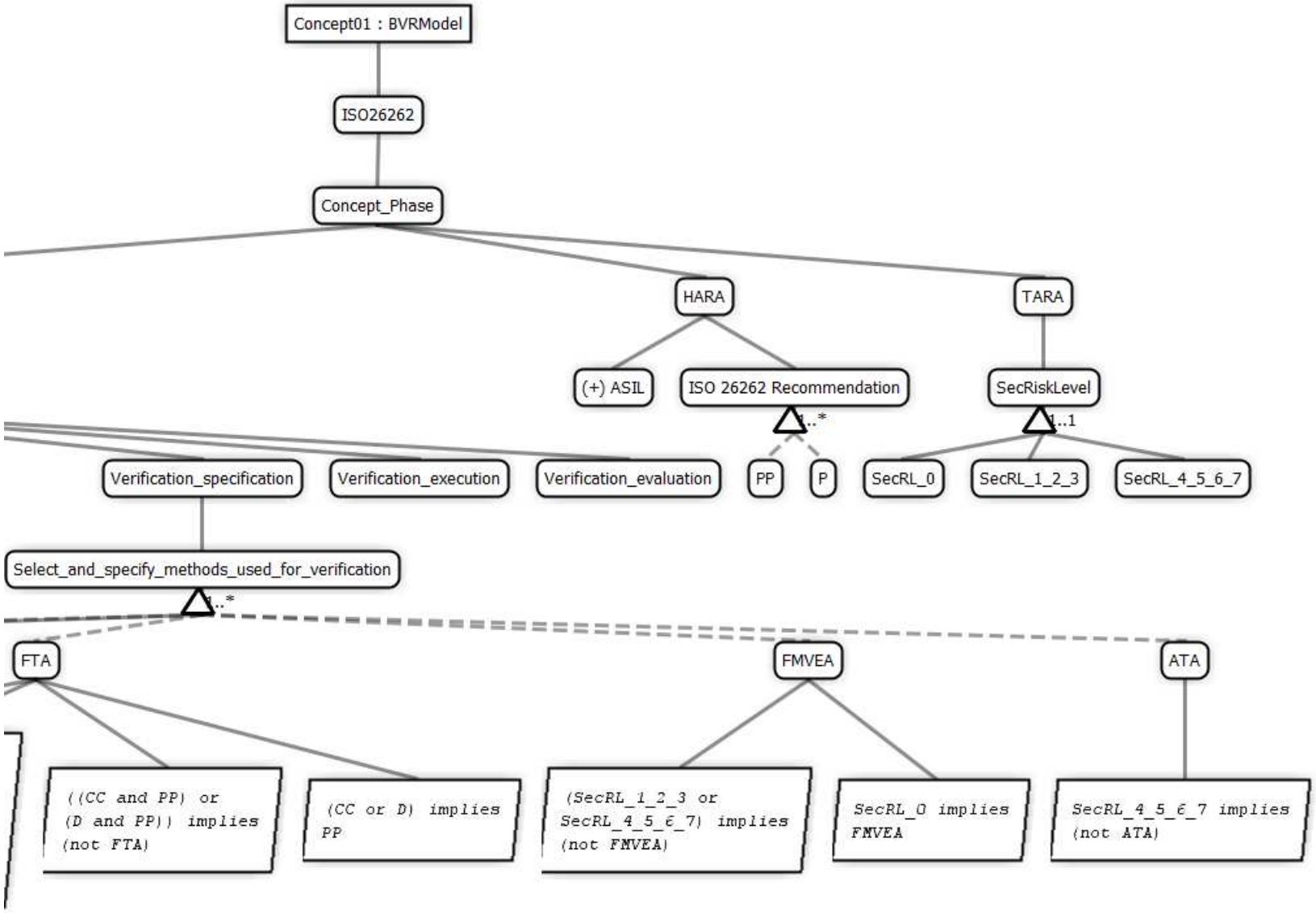
Variability Management with BVR



- Remove unwanted activities
- Add new project specific activities
- Decision is based on parameters

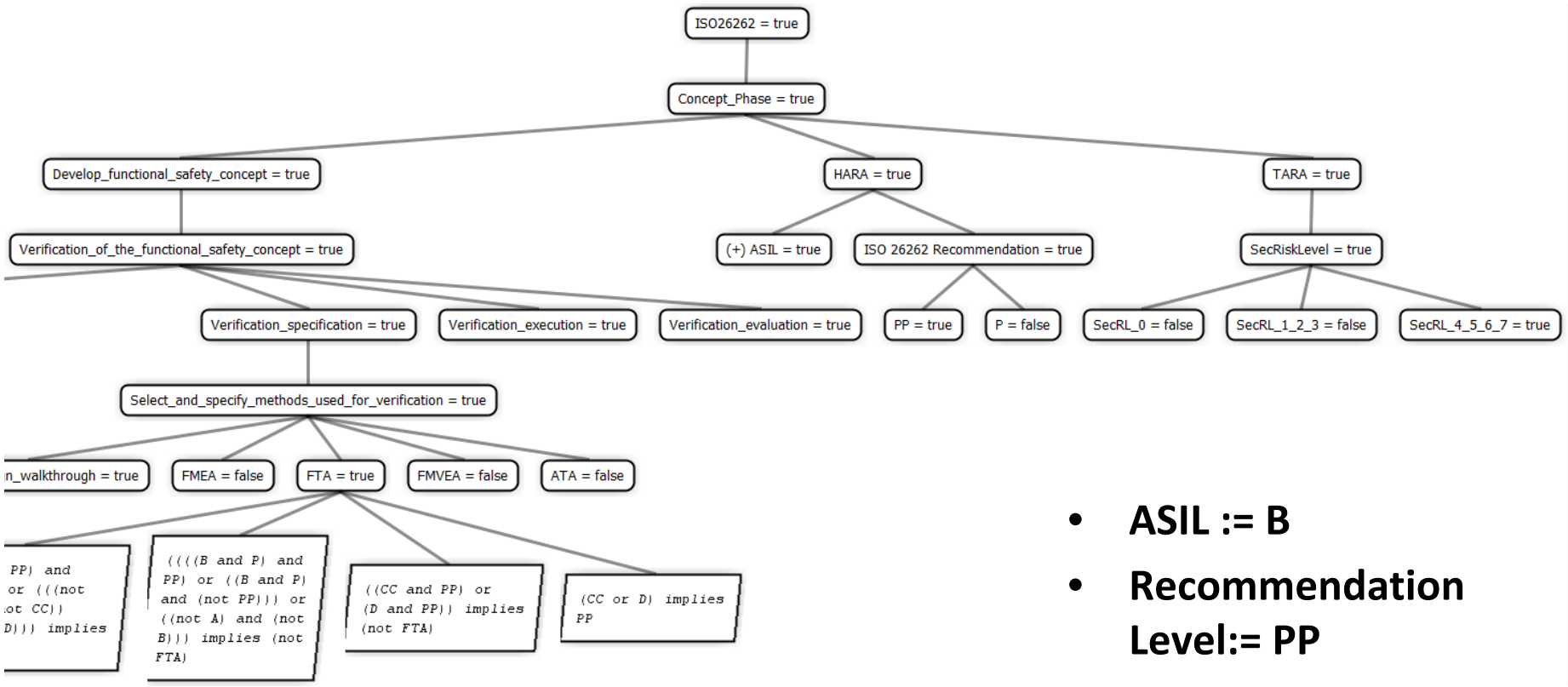
Process tailoring

Variability Management – Vspec Diagram



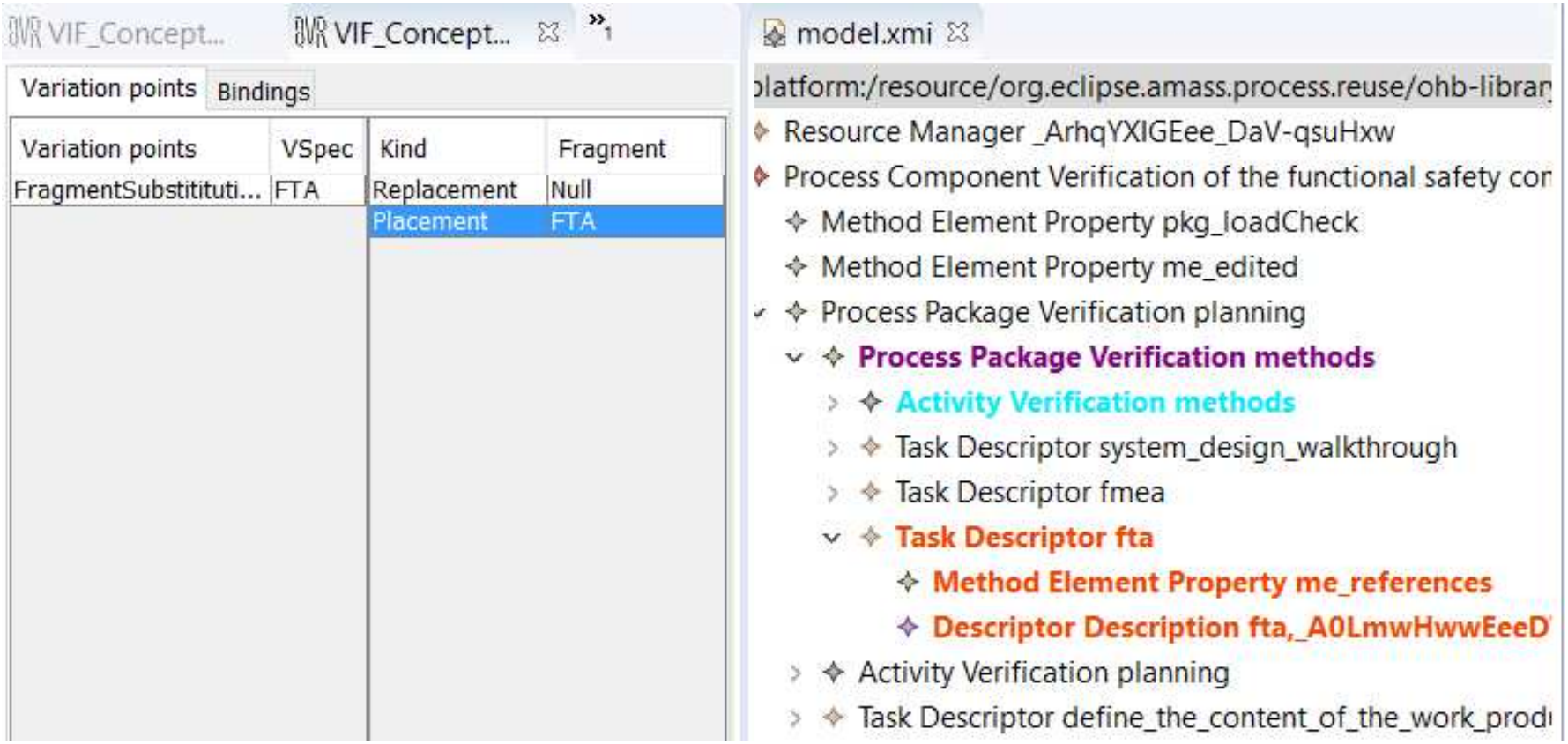
Variability Management – Resolution Diagram

- BVR Tool evaluates constraints and parameters
  - If FTA:= true, it will be removed



- **ASIL := B**
- **Recommendation Level:= PP**

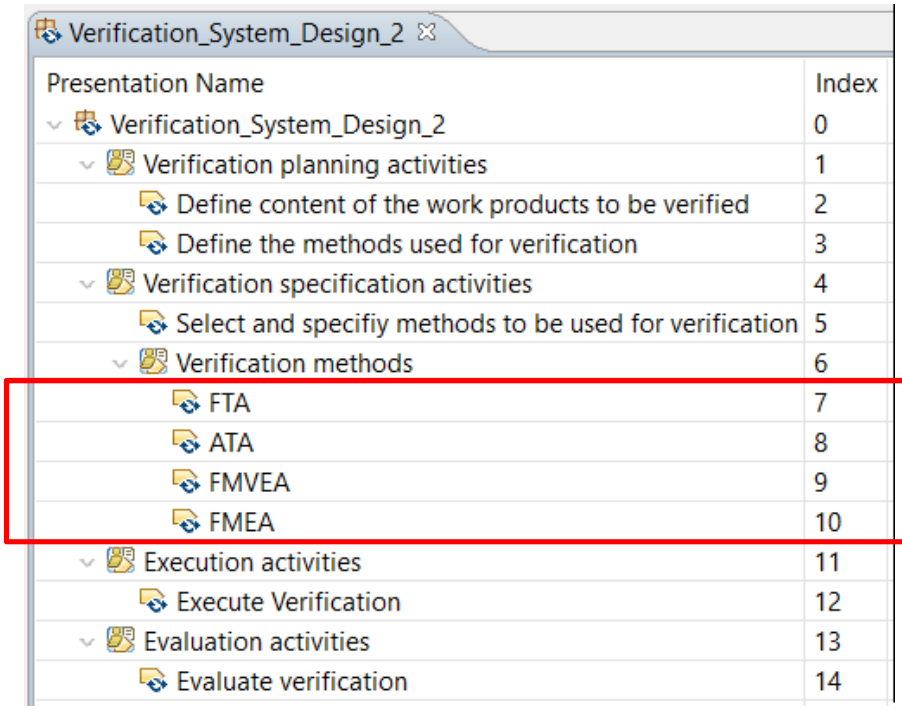
Variability Management – Realization Diagram

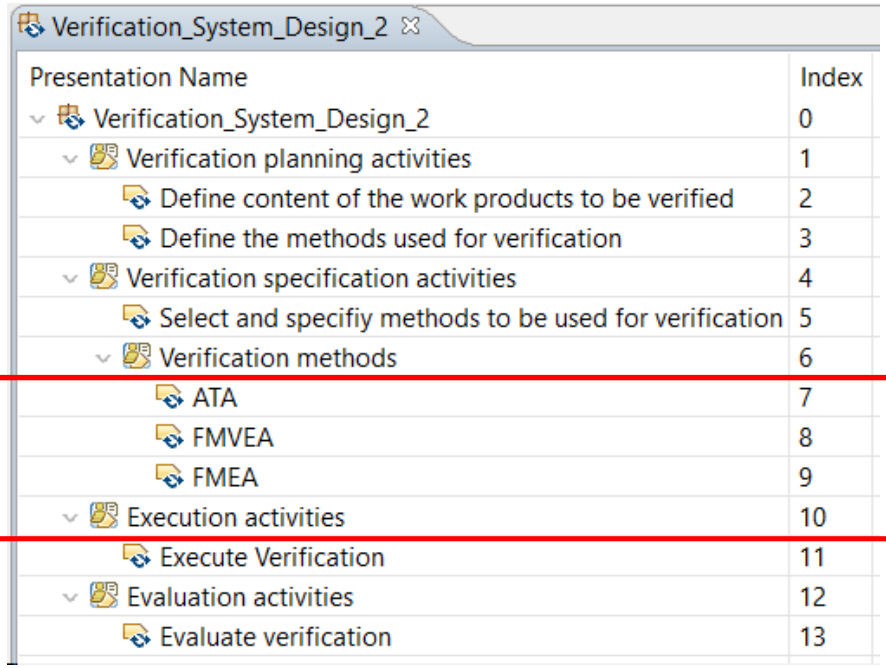


Applicable Development Process in EPF-C

Base process

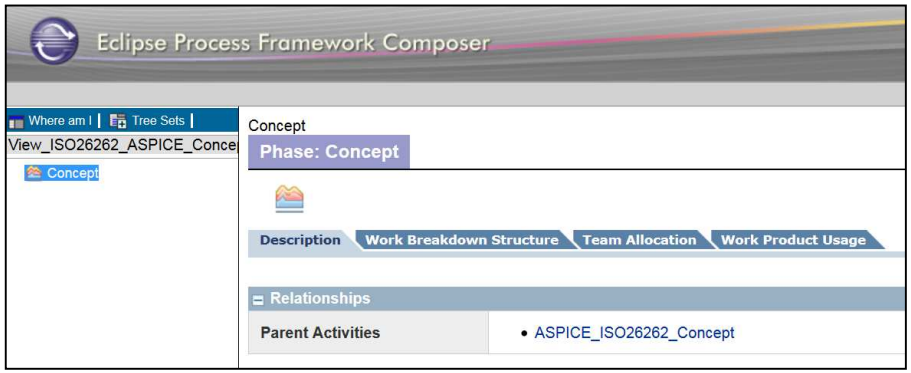
Project specific development process



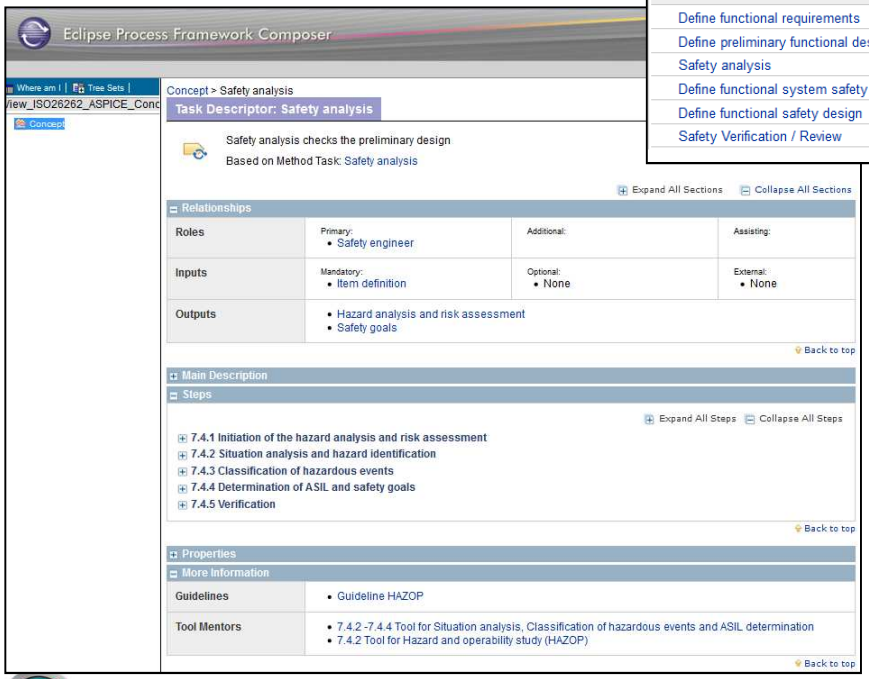


Project specific process

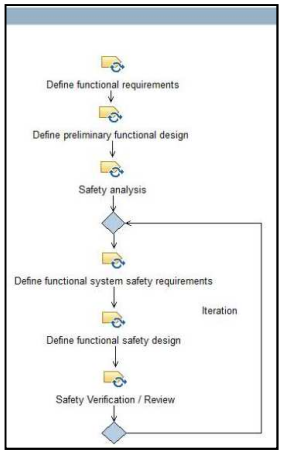
- Project specific process (Tool: Eclipse Process Framework Composer)

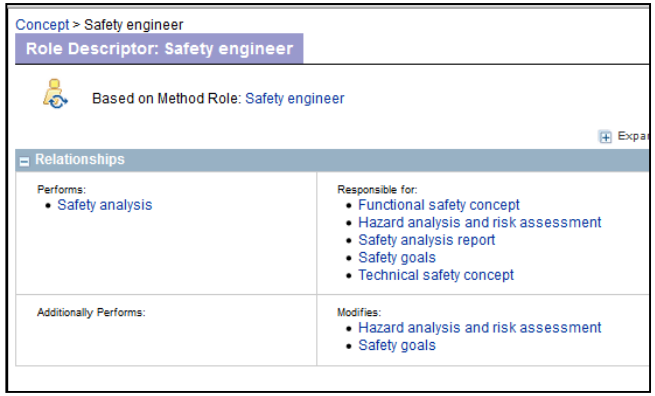


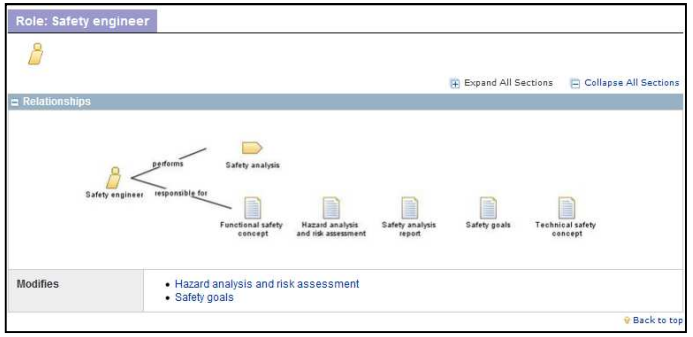
- **Process description**
  - **Phase/Activity/Task**
  - **Delivery (Input/Output)**
- **Visualization (Breakdown)**
  - **Relations between elements**
- **Roles**



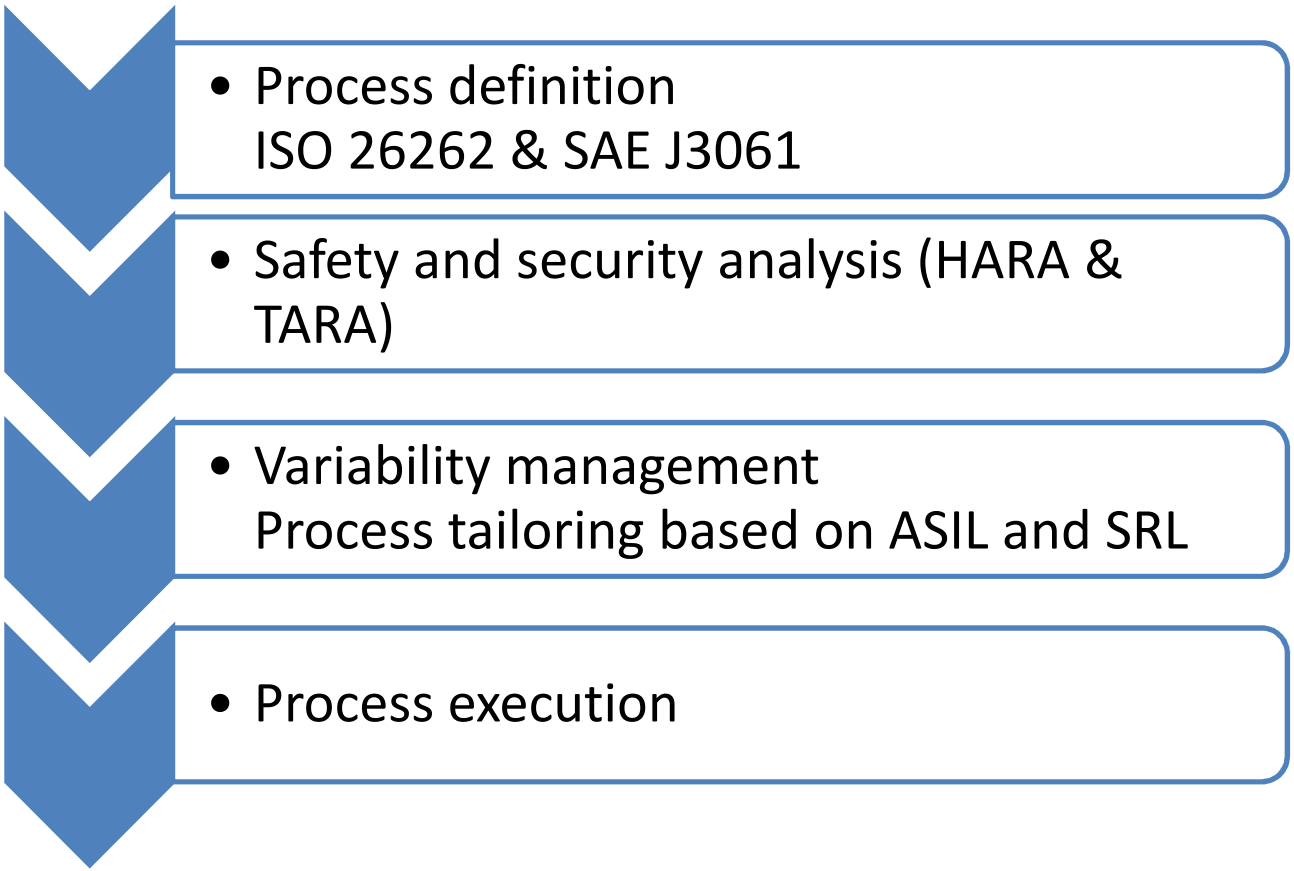
Breakdown Element	Steps	Index	Predecessors
Define functional requirements		2	
Define preliminary functional design		3	2
Safety analysis		4	3
Define functional system safety requirements		5	
Define functional safety design		6	5
Safety Verification / Review		7	6





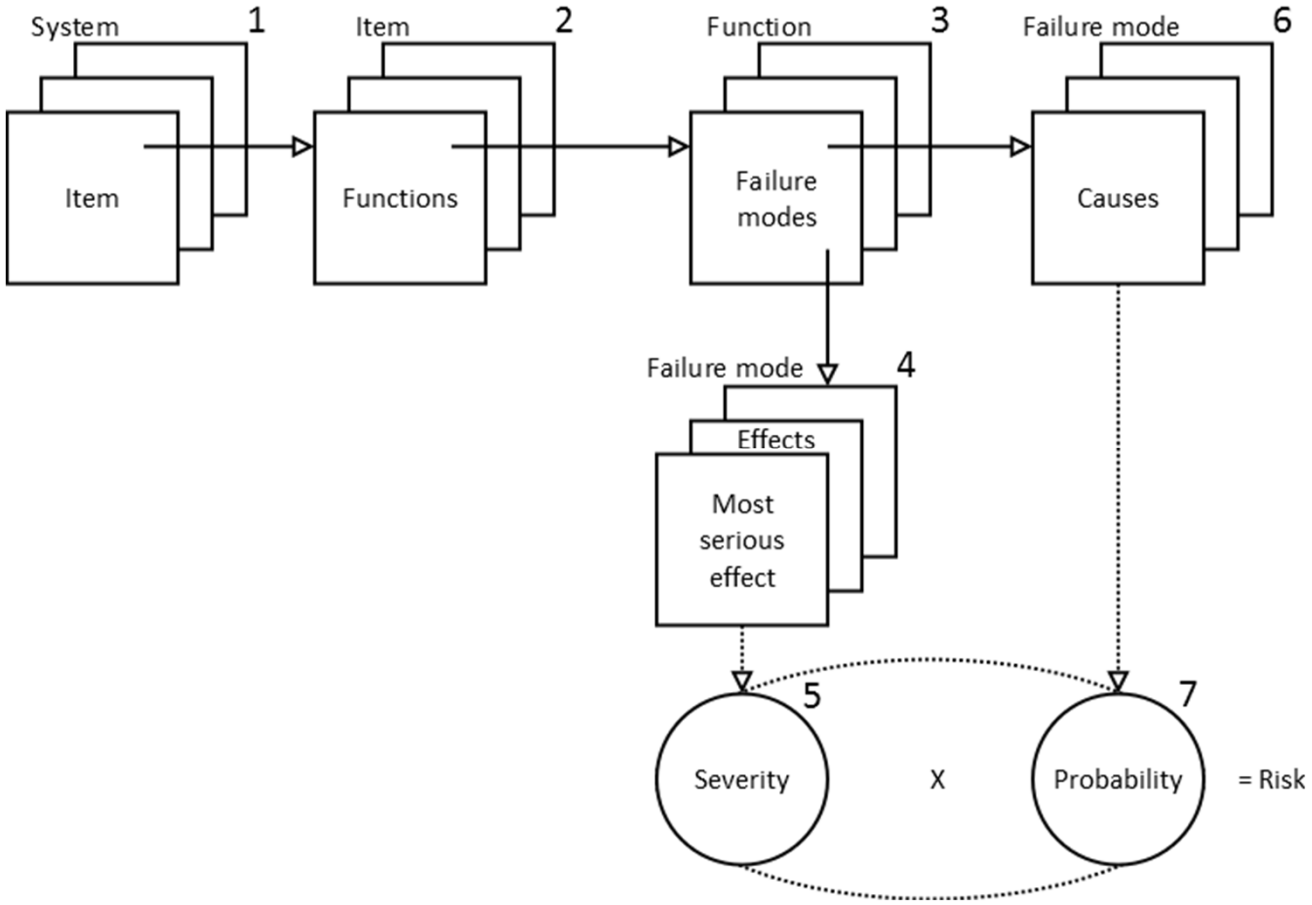


Process flow



FMEA - safety

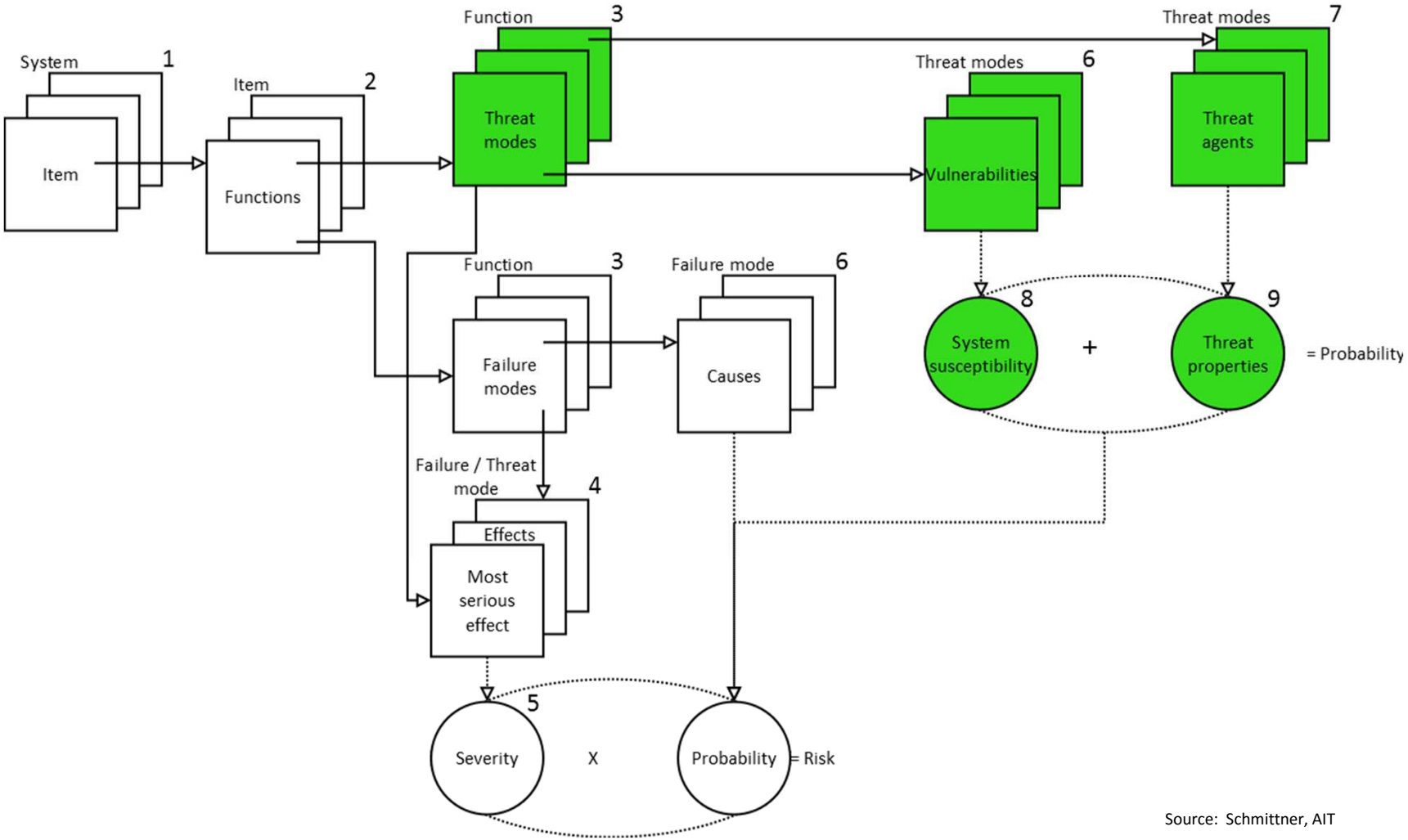
- FMEA Cause Effect Chain for safety



Source: Schmittner, AIT

FMVEA – safety & security

- FMEA Cause Effect Chain for Security



Source: Schmittner, AIT

FMVEA - Example

FMVEA Car2X Communication Manager Unit

	ID	Vulnerability	Threat mode	Threat effect	System status	System effect	Severity	System susceptibility	Threat properties	Attack probability
Car2X Com Manager	1	No device verification, man in the middle attack with physical access to device or connection	Attacker is pretending to be the device	Intercept configuration changes and data	Normal operation	System is no longer reliable	Catastrophic	4	Hacker: 3	7

Conclusion

- ISO/SAE aligned standard is currently under development (Methodology and best practice)
- Methodology is not approved
- Tool support not optimal
  - Co-engineering, process development
  - Co-analysis
- Further research is necessary to achieve a reliable assessment of security risks

Thank you for your attention!