



# 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

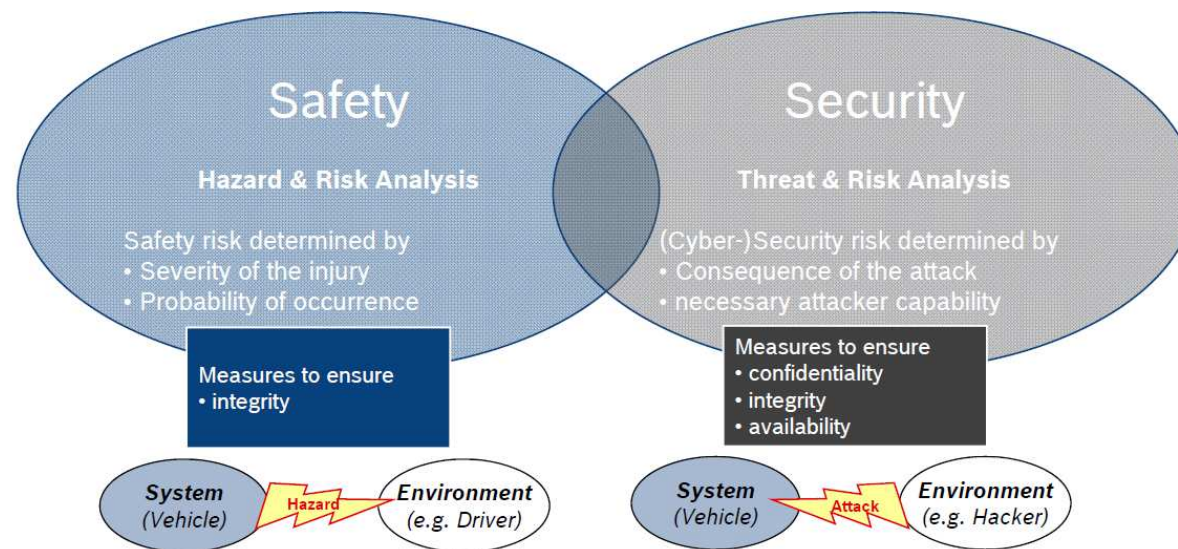
Ada-Europe, Warsaw  
February 11-14, 2019

XX  
Virtual Vehicle Research Center



# Safety and Security Co-Engineering for Road Vehicles

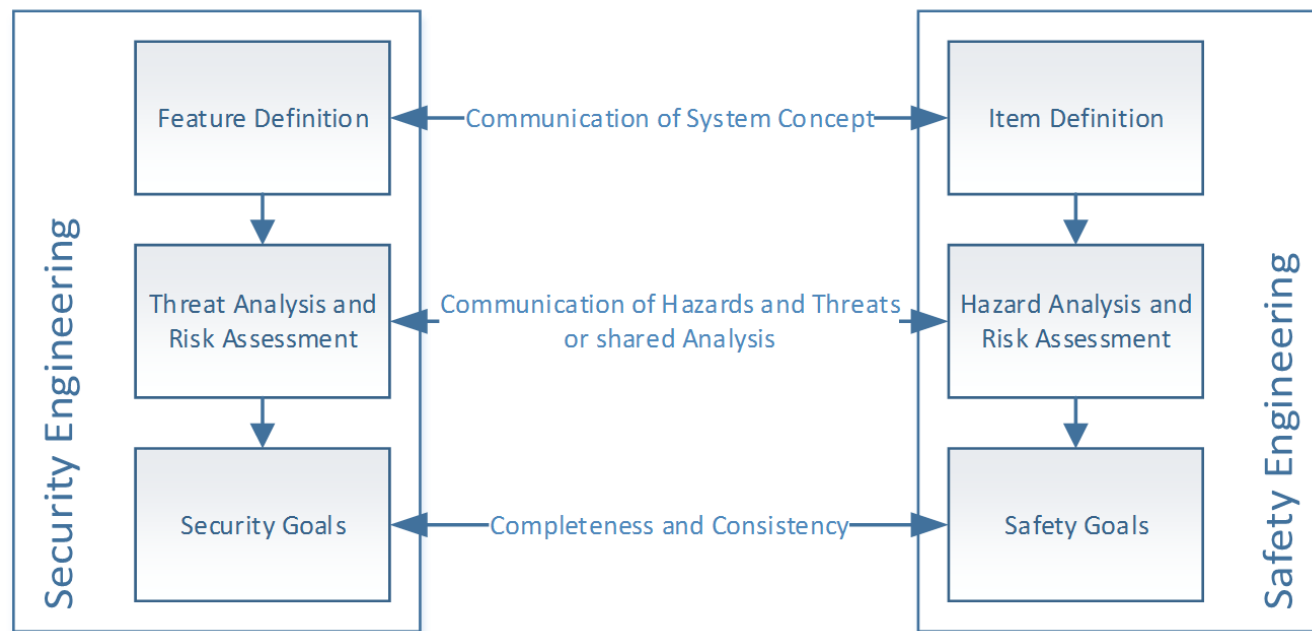
- Safety vs. Security
- Safety protects people from the machine
  - Prevent errors in the system that can lead to harm person
- Security protects the machine from people
  - Prevent human intervention in the system that can lead to all types of damage (Safety, Financial, Law, Image,...)



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

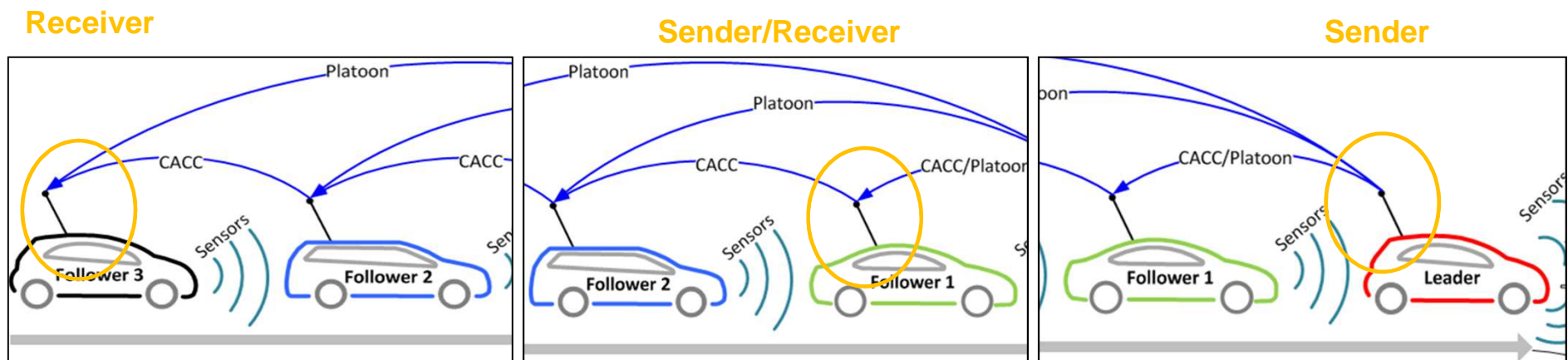
- Safety and Security aspects of radio connection

## Safety

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

## Security

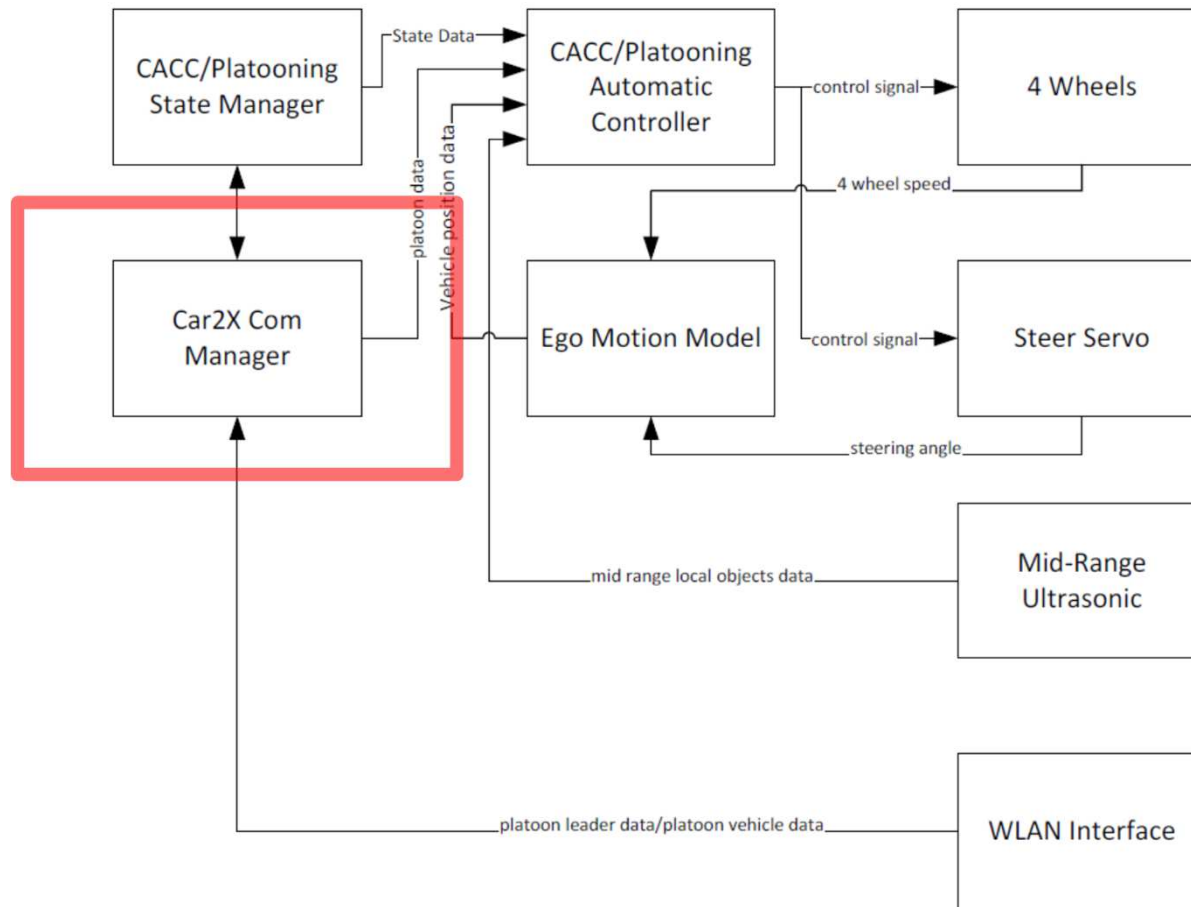
- Feature Definition
- TARA
- Cybersecurity Goals
- Cybersecurity Requirements
- FMVEA



# Usage Scenario

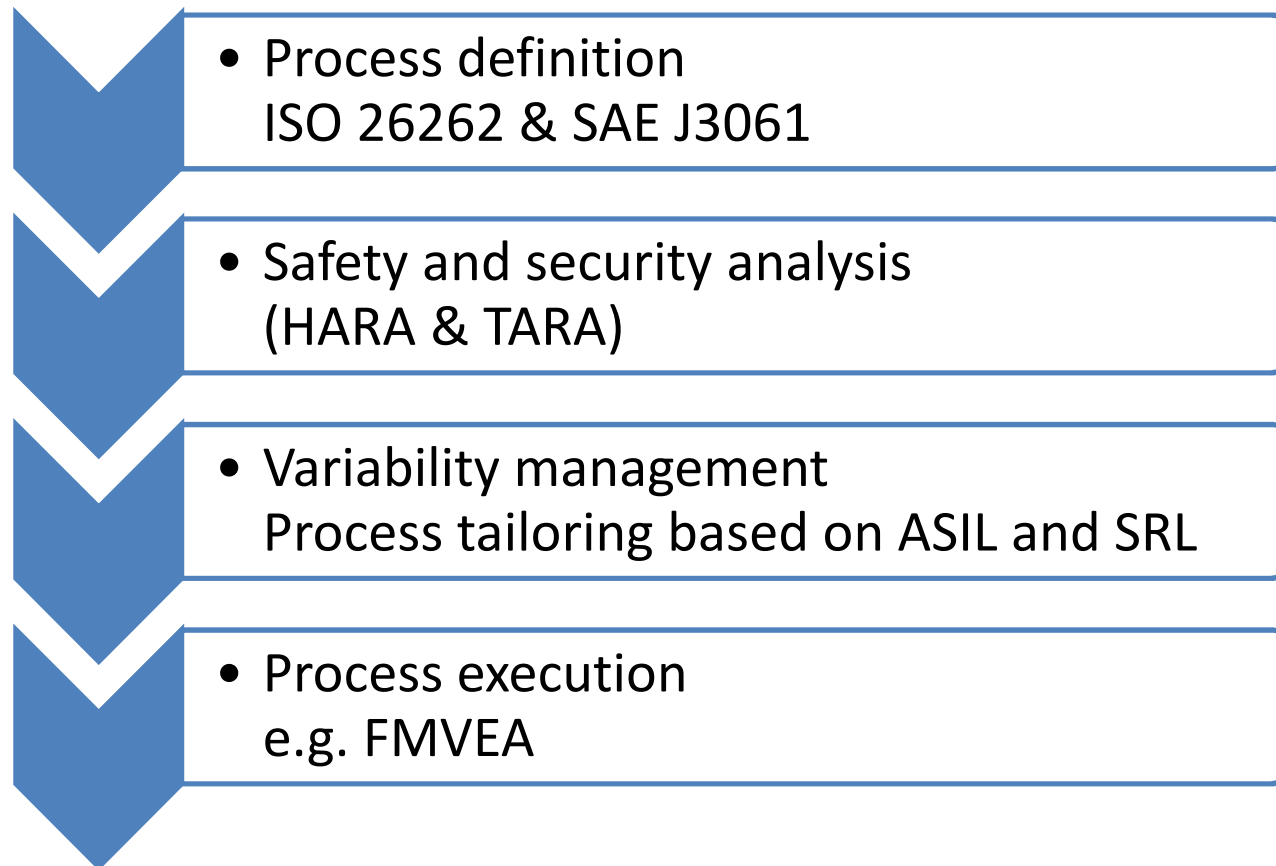
## Verification of the system design

### Car2X Communication Manager Unit



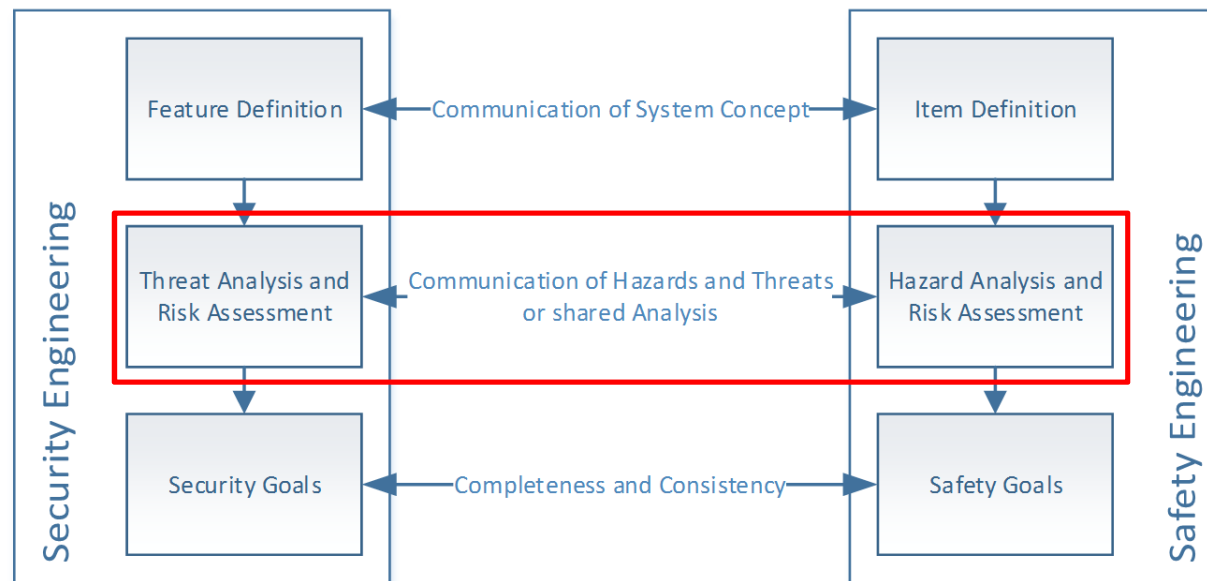
Source: Berner&Mattner

# 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



## SURFACE VEHICLE RECOMMENDED PRACTICE

J3061™

JAN2016

Issued 2016-01

Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

INTERNATIONAL  
STANDARD

ISO  
26262-3

Road vehicles — Functional

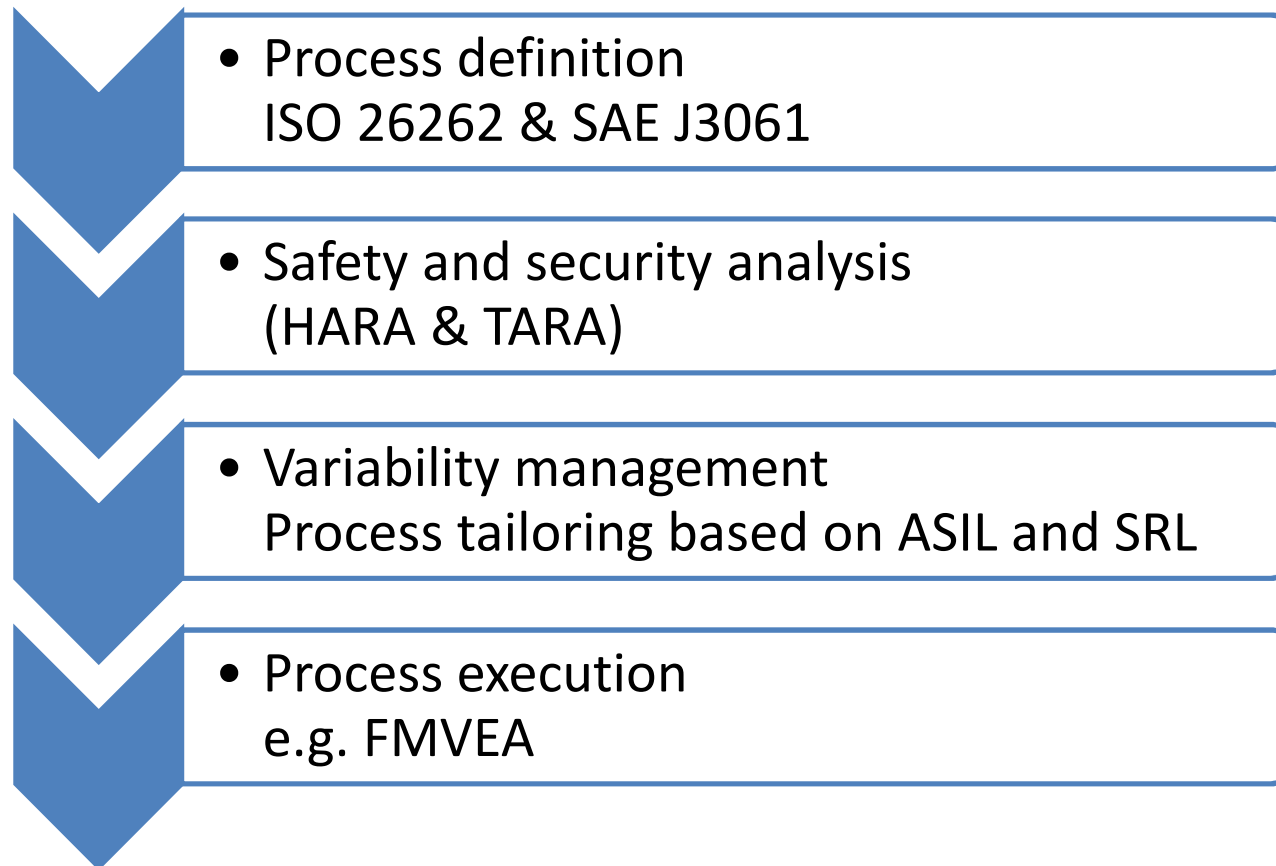
Part 3:  
Concept phase

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

Attack Path	Severity	Controllability	Elapsed Time	Expertise	Knowledge of TOE	Window of Opportunity	Equipment	Attack Potential	Attack Probability	Risk Level	Security Goal
[E] [E03] Block WLAN signal	S2	C3	1 - (<= one week)	0 - Layman	0 - Public	4 - Moderate	0 - Standard	Basic	Highly likely	R7+	[G002] Prevent block of WLAN Connection
[E] [E03] Block WLAN signal	S2	C3	1 - (<= one week)	0 - Layman	0 - Public	4 - Moderate	0 - Standard	Basic	Highly likely	R7+	[G002] Prevent block of WLAN Connection
[E] [E04] Get access to WLAN channel selection	S2	C3	4 - (<= one month)	6 - Expert	0 - Public	1 - Easy	4 - Specialised	Moderate	Possible	R6	[G001] Prevent manipulation of WL Connection
[E] [E05] Manipulate WLAN channel selection	S2	C3	4 - (<= one month)	6 - Expert	0 - Public	1 - Easy	4 - Specialised	Moderate	Possible	R6	[G001] Prevent manipulation of WL Connection
[E] [E04] Get access to WLAN channel selection	S2	C3	4 - (<= one month)	6 - Expert	0 - Public	1 - Easy	4 - Specialised	Moderate	Possible	R6	[G001] Prevent manipulation of WL Connection
[E] [E05] Manipulate WLAN channel selection	S2	C3	4 - (<= one month)	6 - Expert	0 - Public	1 - Easy	4 - Specialised	Moderate	Possible	R6	[G001] Prevent manipulation of WL Connection
[E] [E06] Get access to WLAN channel	S2	C3	4 - (<= one month)	6 - Expert	7 - Sensitive	4 - Moderate	4 - Specialised	Beyond high	Remote	R4	[G001] Prevent manipulation of WL Connection
[E] [E07] Manipulate path information	S2	C3	4 - (<= one month)	6 - Expert	7 - Sensitive	4 - Moderate	4 - Specialised	Beyond high	Remote	R4	[G001] Prevent manipulation of WL Connection
[E] [E06] Get access to WLAN channel	S2	C3	4 - (<= one month)	6 - Expert	7 - Sensitive	4 - Moderate	4 - Specialised	Beyond high	Remote	R4	[G001] Prevent manipulation of WL Connection
[E] [E16] Manipulate start/ (emergency) stop signal	S2	C3	4 - (<= one month)	6 - Expert	7 - Sensitive	4 - Moderate	4 - Specialised	Beyond high	Remote	R4	[G001] Prevent manipulation of WL Connection



# Process flow

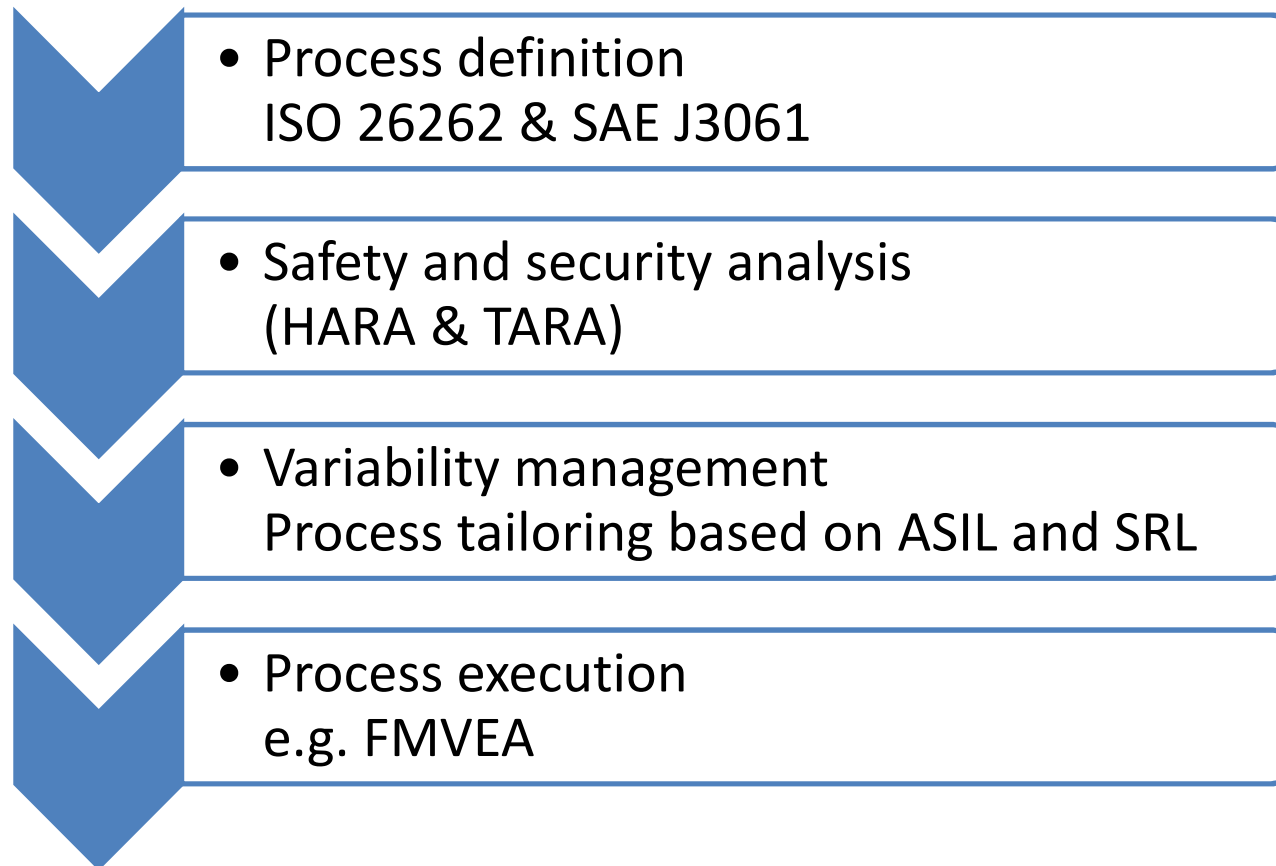


# TARA for specific usage scenario in medini analyze tool

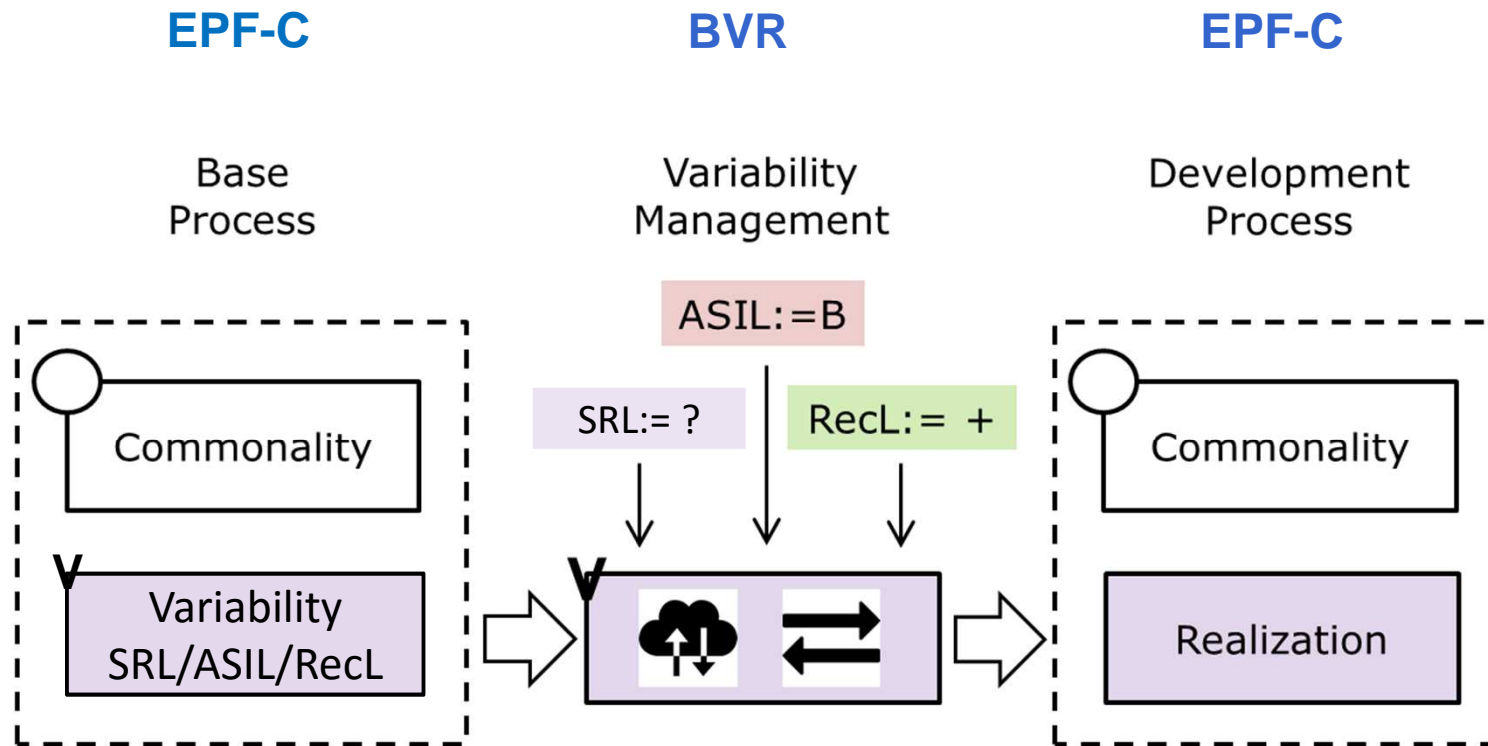
The screenshot shows the 'medini analyze' application window. The main area displays a 'Scenario Analysis' table for the 'AMASS' project. The table has the following columns: Attack Path, Severity, Controllability, Elapsed Time, Expertise, Knowledge of TOE, Window of Opportunity, Equipment, Attack Potential, Attack Probability, Risk Level, and Security Goal. The table contains several rows of data, including attack paths like '[E03] Block WLAN signal', '[E04] Get access to WLAN channel selection', and '[E06] Get access to WLAN channel'. The interface also includes a 'Model Browser' on the left and a 'List View' at the bottom.

Attack Path	Severity	Controllability	Elapsed Time	Expertise	Knowledge of TOE	Window of Opportunity	Equipment	Attack Potential	Attack Probability	Risk Level	Security Goal
[E] [E03] Block WLAN signal	S2	C3	1 - (<= one week)	0 - Layman	0 - Public	4 - Moderate	0 - Standard	Basic	Highly likely	R7+	[G002] Prevent block of WLAN Connection
[E] [E03] Block WLAN signal	S2	C3	1 - (<= one week)	0 - Layman	0 - Public	4 - Moderate	0 - Standard	Basic	Highly likely	R7+	[G002] Prevent block of WLAN Connection
[E] [E04] Get access to WLAN channel selection	S2	C3	4 - (<= one month)	6 - Expert	0 - Public	1 - Easy	4 - Specialised	Moderate	Possible	R6	[G001] Prevent manipulation of WLAN Connection
[E] [E05] Manipulate WLAN channel selection											[G001] Prevent manipulation of WLAN Connection
[E] [E04] Get access to WLAN channel selection	S2	C3	4 - (<= one month)	6 - Expert	0 - Public	1 - Easy	4 - Specialised	Moderate	Possible	R6	[G001] Prevent manipulation of WLAN Connection
[E] [E05] Manipulate WLAN channel selection											[G001] Prevent manipulation of WLAN Connection
[E] [E06] Get access to WLAN channel	S2	C3	4 - (<= one month)	6 - Expert	7 - Sensitive	4 - Moderate	4 - Specialised	Beyond high	Remote	R4	[G001] Prevent manipulation of WLAN Connection
[E] [E07] Manipulate path information											[G001] Prevent manipulation of WLAN Connection
[E] [E06] Get access to WLAN channel	S2	C3	4 - (<= one month)	6 - Expert	7 - Sensitive	4 - Moderate	4 - Specialised	Beyond high	Remote	R4	[G001] Prevent manipulation of WLAN Connection
[E] [E16] Manipulate start/ (emergency) stop signal											[G001] Prevent manipulation of WLAN Connection

# Process flow



# Variability Management with BVR

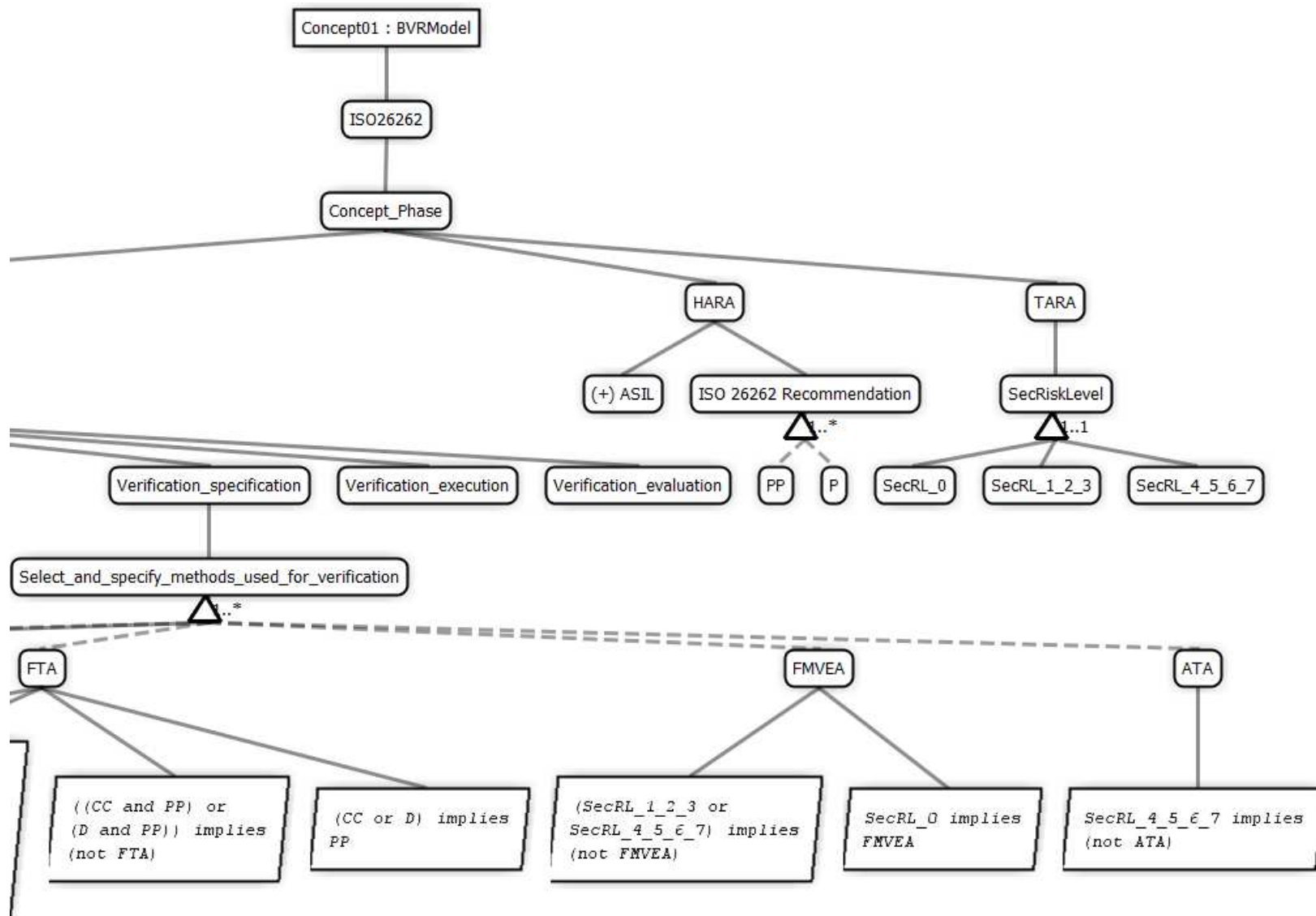


- Remove unwanted activities
- Add new project specific activities
- Decision is based on parameters

Process tailoring

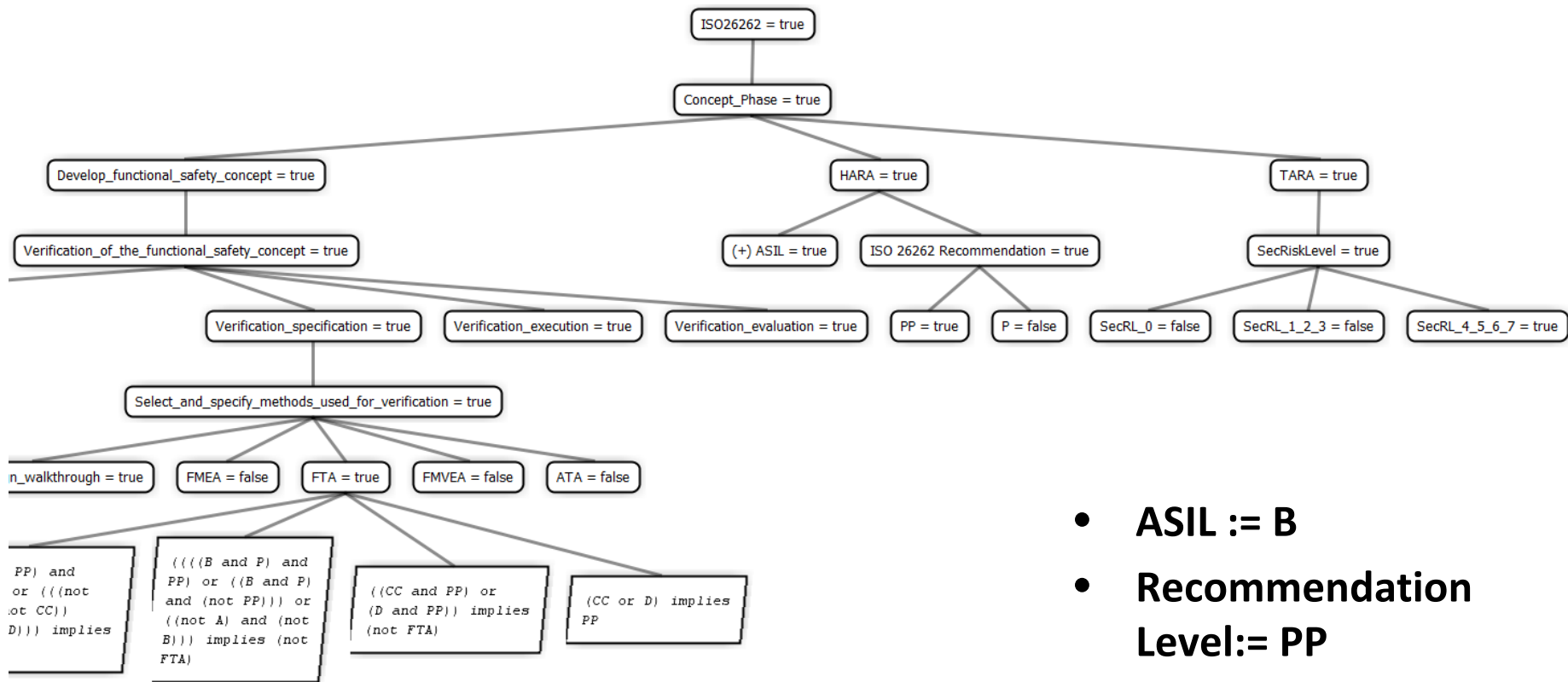


# Variability Management – Vspec Diagram



# 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

The screenshot shows the Eclipse IDE interface for Variability Management. The left pane is titled 'Variation points Bindings' and contains a table with the following data:

Variation points	VSpec	Kind	Fragment
FragmentSubstituti...	FTA	Replacement	Null
		Placement	FTA

The right pane shows the 'model.xml' tree view with the following structure:

- platform:/resource/org.eclipse.amass.process.reuse/ohb-libran
- Resource Manager \_ArhqYXIGEee\_DaV-qsuHxw
- Process Component Verification of the functional safety con
  - Method Element Property pkg\_loadCheck
  - Method Element Property me\_edited
  - Process Package Verification planning
    - Process Package Verification methods**
      - Activity Verification methods
      - Task Descriptor system\_design\_walkthrough
      - Task Descriptor fmea
    - Task Descriptor fta**
      - Method Element Property me\_references
      - Descriptor Description fta,\_A0LmwHwwEeeD
  - Activity Verification planning
  - Task Descriptor define\_the\_content\_of\_the\_work\_prodi



# Applicable Development Process in EPF-C

Base process

Project specific  
development process

Presentation Name	Index
Verification_System_Design_2	0
Verification planning activities	1
Define content of the work products to be verified	2
Define the methods used for verification	3
Verification specification activities	4
Select and specify methods to be used for verification	5
Verification methods	6
FTA	7
ATA	8
FMVEA	9
FMEA	10
Execution activities	11
Execute Verification	12
Evaluation activities	13
Evaluate verification	14

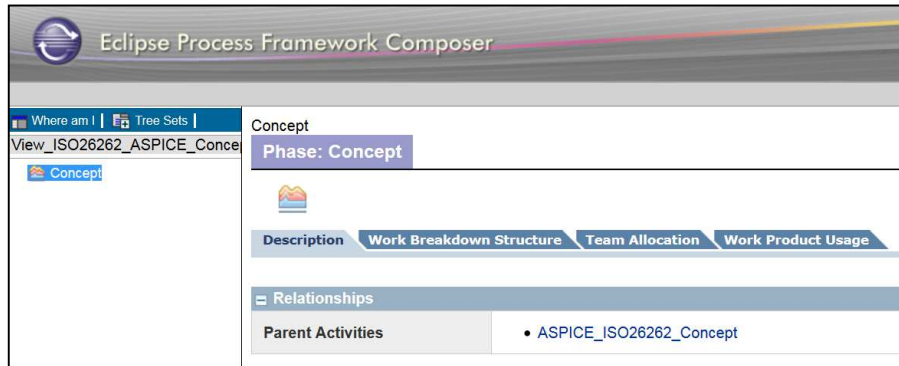
Presentation Name	Index
Verification_System_Design_2	0
Verification planning activities	1
Define content of the work products to be verified	2
Define the methods used for verification	3
Verification specification activities	4
Select and specify methods to be used for verification	5
Verification methods	6
ATA	7
FMVEA	8
FMEA	9
Execution activities	10
Execute Verification	11
Evaluation activities	12
Evaluate verification	13



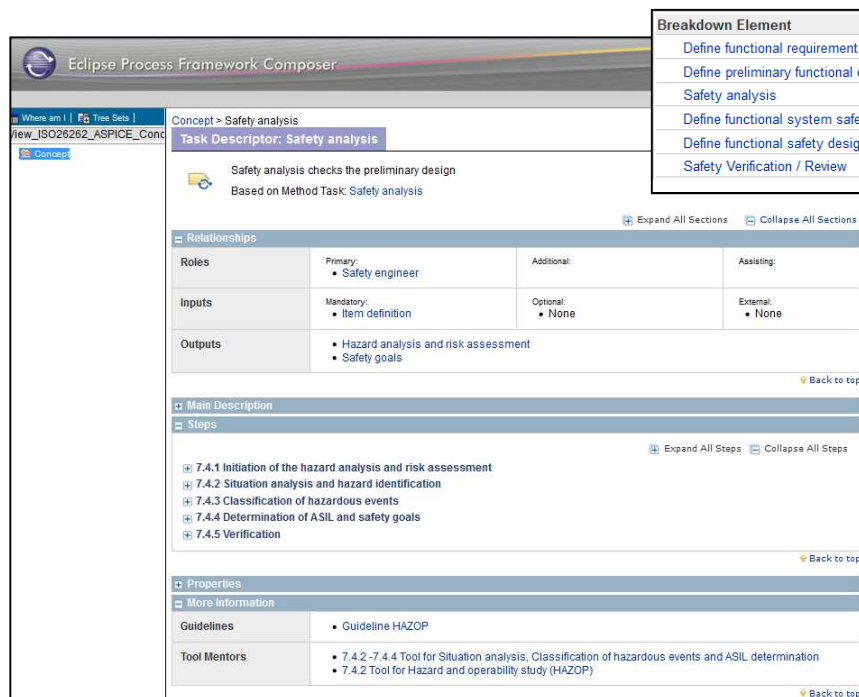


# Project specific process

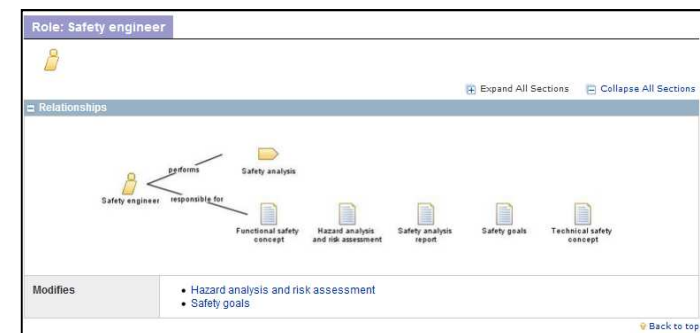
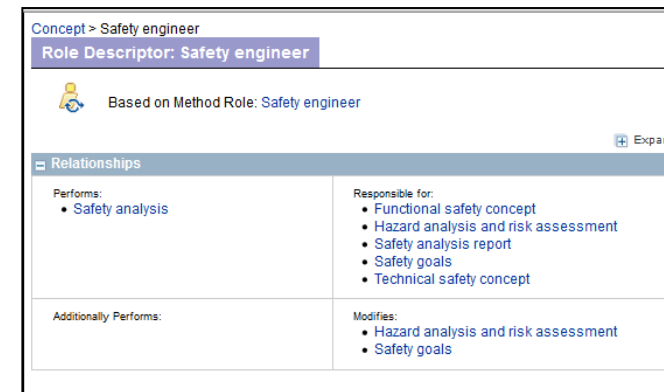
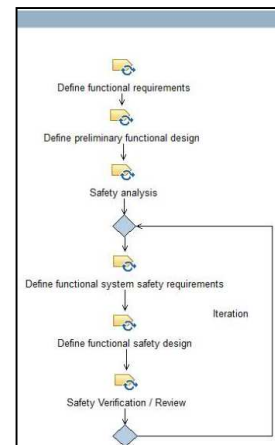
- Project specific process (Tool: Eclipse Process Framework Composer)



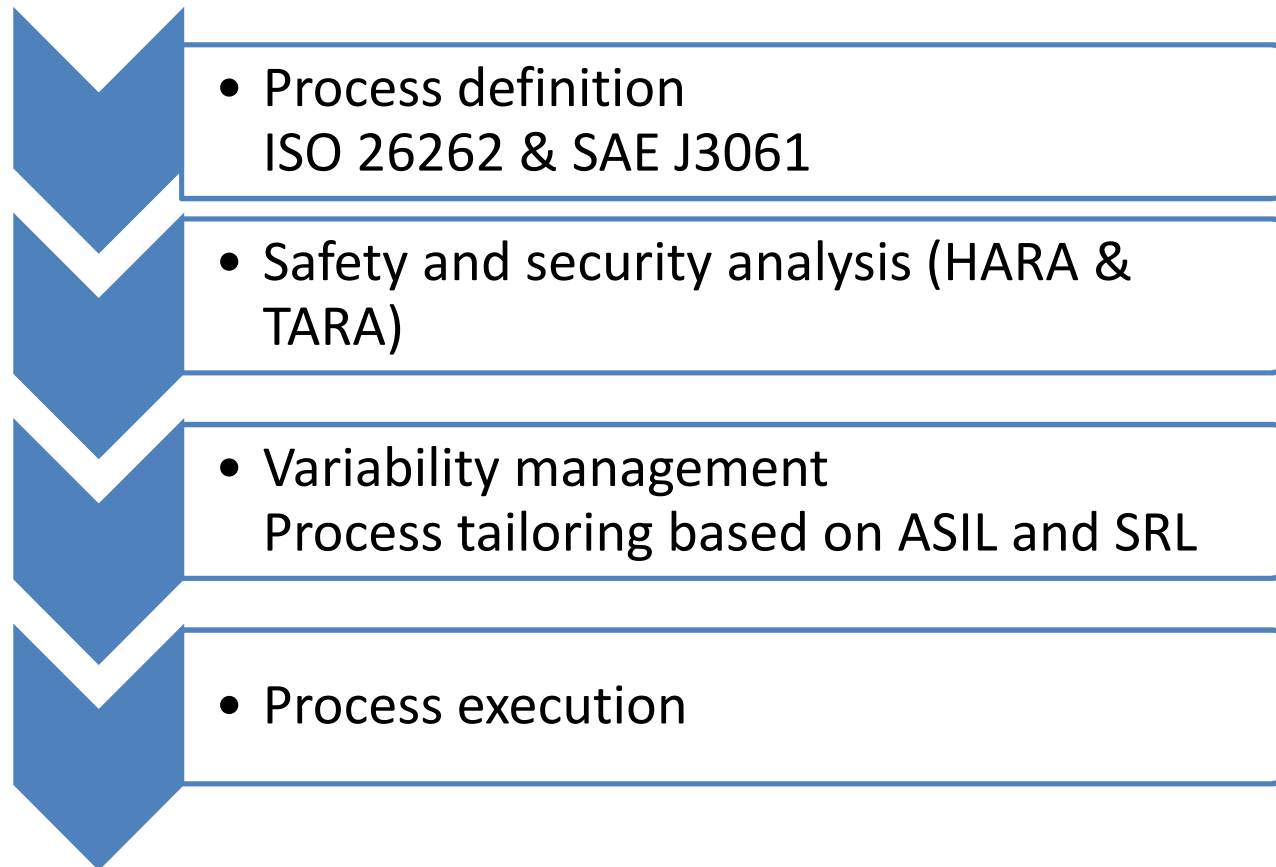
- Process description
  - Phase/Activity/Task
  - Delivery (Input/Output)
- Visualization (Breakdown)
  - Relations between elements
- Roles



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

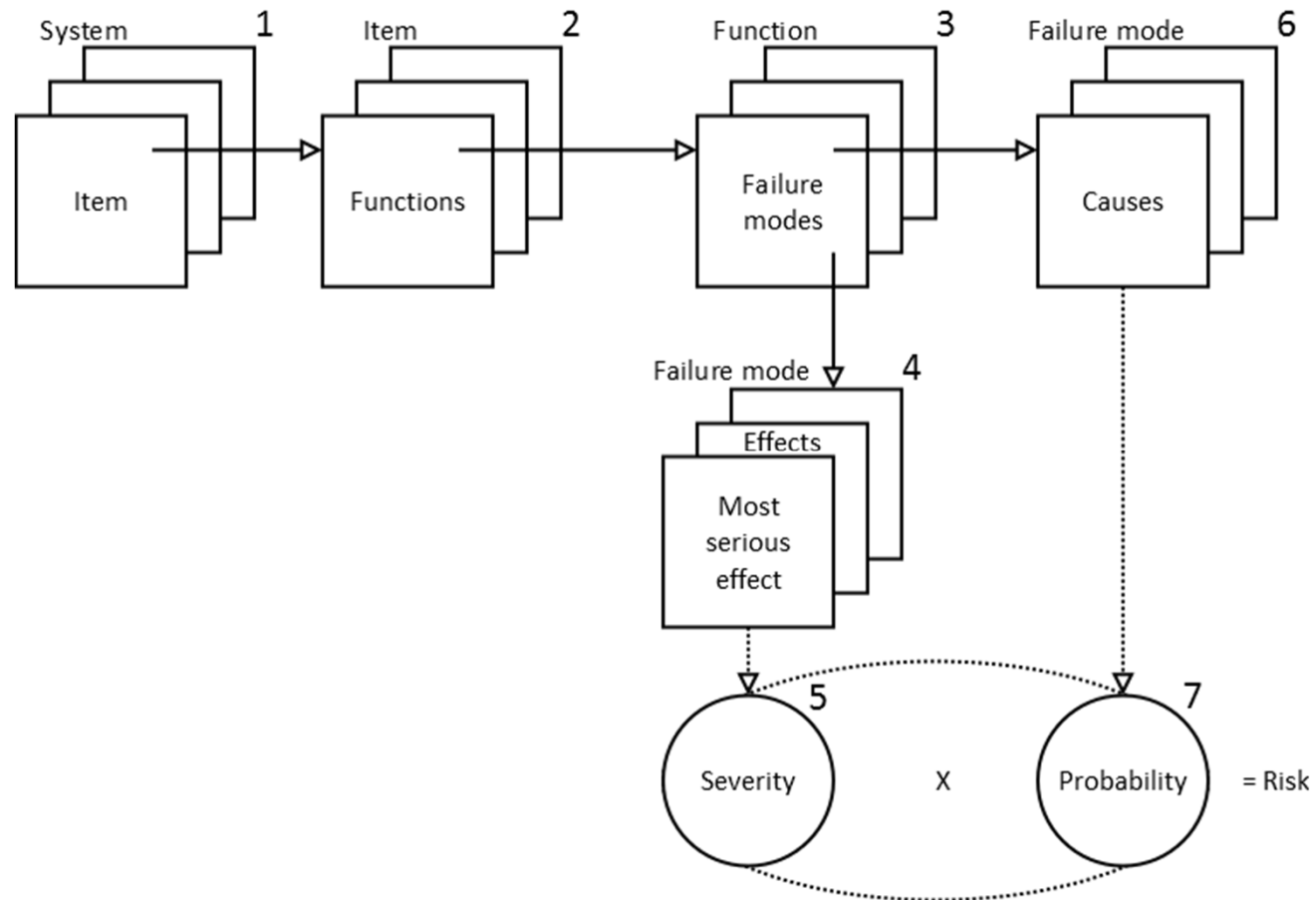


# Process flow



# FMEA - safety

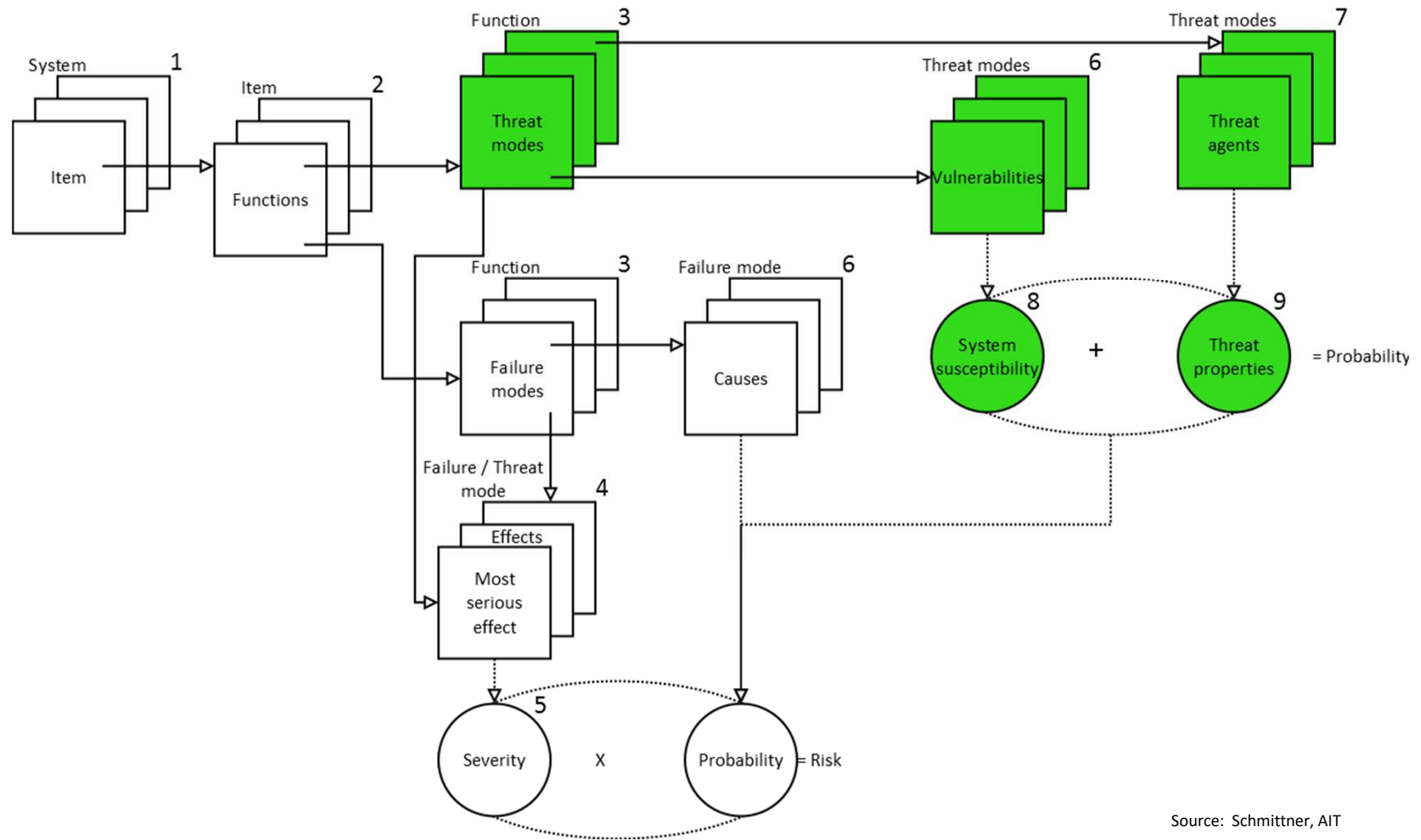
- FMEA Cause Effect Chain for safety



Source: Schmittner, AIT

# FMVEA – safety & security

- FMEA Cause Effect Chain for Security



# 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!**

