

# Vers une modélisation du risque cybersécurité en soutien à la certification

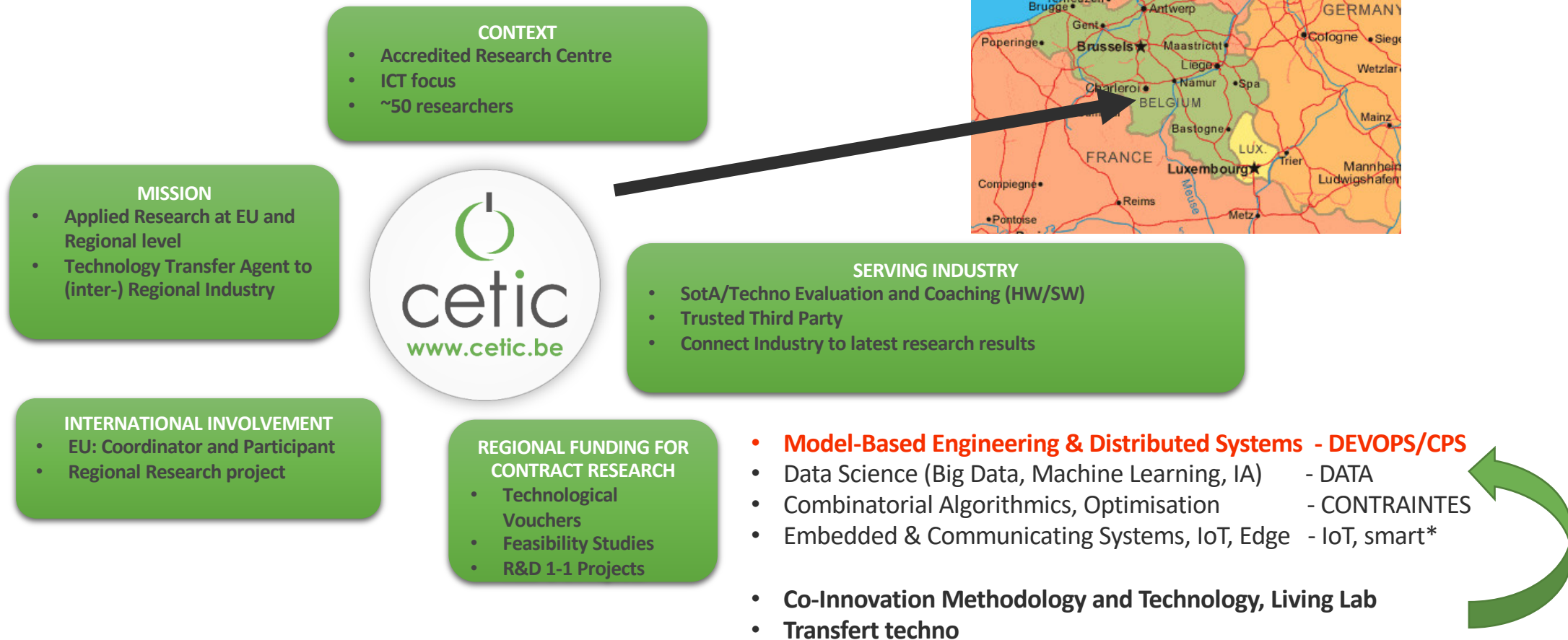
PER -Christophe Ponsard, Philippe Massonet

MBEDIS – Valery Ramon, Denis Darquennes

GT IE, 9 décembre 2021

# CETIC en bref – centre R&D appliquée

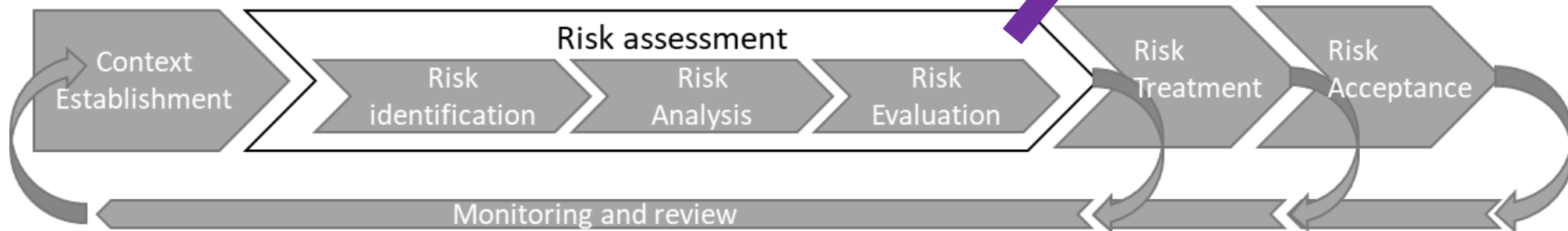
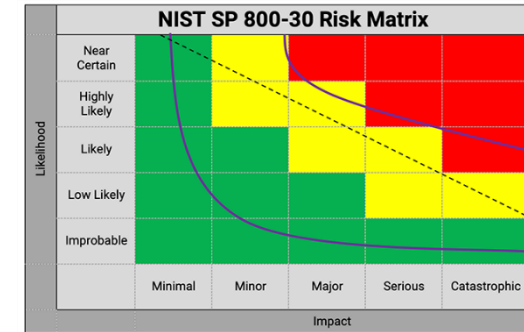
Fondé en 2001 par UCLouvain, UNamur, UMONS



Domaine: santé, logistique (ferroviaire/automotive), industrie 4.0, numérique  
Thématiques: safety, **cybersecurity**, privacy, sustainability,...

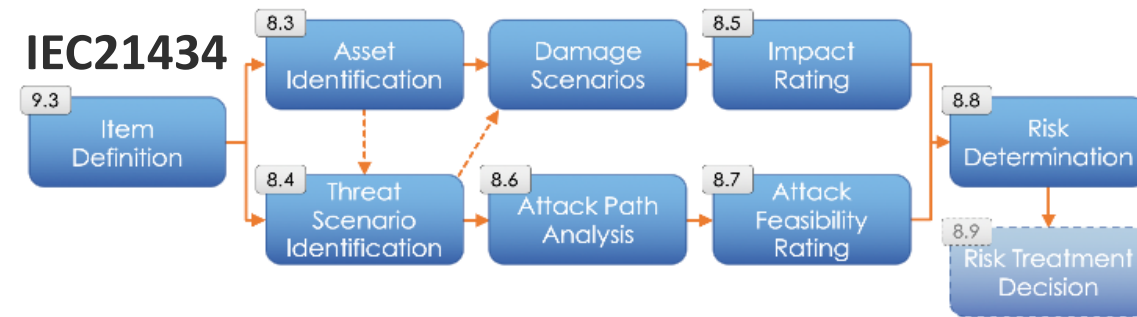
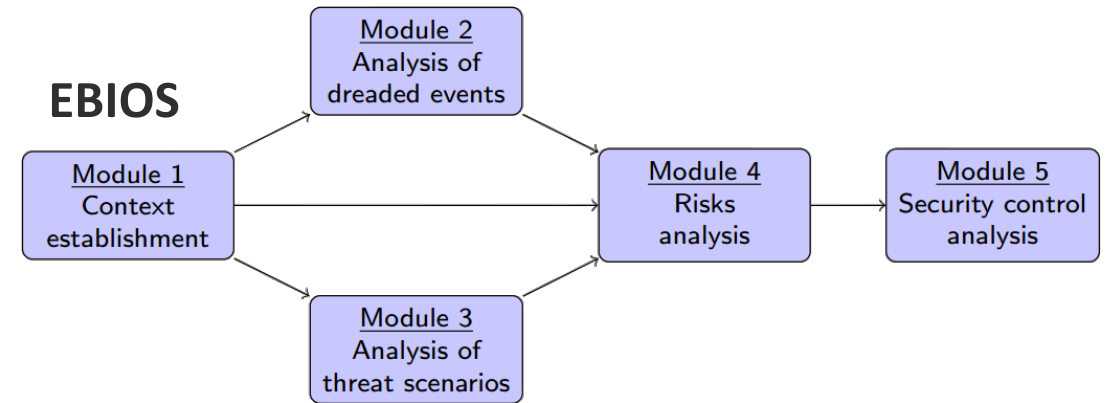
# Context – Risk Analysis Process

- Ubiquitous and interconnected computer systems
  - ➔ many useful functionalities for citizen/enterprises
  - ➔ increasing attack surface to cyber threats !
- Development of cyber security frameworks and standards
  - ISO27K (IT, 2005, 2013)
  - IEC 62443 (OT, 2010)
  - IEC 21434 (automotive, 2021)
- Follow a risk-based approach (ISO31000)
  - Also in other domains, e.g. safety



# Typical Risk Analysis Process

- **Risk = impact x feasibility**
- **Impact** → Business Domain
  - contains valuable assets (information, processes)
  - different properties to be protected (confidentiality, integrity and availability)
  - **Impact** analysis, e.g. on Safety/Financial/Operation/Privacy
- **Feasibility** → Infrastructure Domain
  - contains the support assets on which business assets rely
  - capture both IT and OT infrastructure
  - Identify attack scenarios, paths to determine **feasibility**





# Research Focus: Towards Model-Based Risk Analysis

- Typical approach document/table based
    - E.g. EBIOS (FR), Monarc (LU)
  - Define lists/trees of business/IT assets
  - Use typical threats for each component
  - Use simple attack paths (linear) with worst case estimation
- ➔ Qualitative: “good enough” for prioritisation
- ➔ HOWEVER: coarse-grained and limited ability to identify precise measures for risk reduction

## 4.1.5 Altération des données de sécurité

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Système du prestataire – Portail d'accès	Un administrateur fonctionnel interne ou un pirate modifie le référentiel des identités et des droits pour permettre l'accès au système à des personnes non autorisées.

N°	Evénement Redouté	Besoin	Sources de menaces	Impacts	Gravité
ER5	Altération des données de sécurité	Intègre	<ul style="list-style-type: none"> <li>• Pirate</li> <li>• Employé peu sérieux</li> <li>• Employé malveillant</li> </ul>	<ul style="list-style-type: none"> <li>• Perte de contrôle sur le système d'information externalisé</li> <li>• Impossibilité d'assurer le traitement</li> </ul>	3. Importante

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une altération	1	<ul style="list-style-type: none"> <li>• Pirate</li> <li>• Concurrent</li> <li>• Employé malveillant</li> </ul>	<ul style="list-style-type: none"> <li>• M13 RSX-USG Attaque du milieu sur un canal informatique</li> </ul>	<ul style="list-style-type: none"> <li>• Attaque de type Man in the Middle</li> </ul>	3. Forte
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une altération	1	<ul style="list-style-type: none"> <li>• Pirate</li> <li>• Employé du prestataire malveillant</li> </ul>	<ul style="list-style-type: none"> <li>• M13 RSX-USG Attaque du milieu sur un canal informatique</li> <li>• M11 LOG-MOD Modification d'un logiciel</li> </ul>	<ul style="list-style-type: none"> <li>• Attaque de type Man in the Middle</li> <li>• Changement des données du portail d'accès au cloud</li> </ul>	3. Forte
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une altération	1	<ul style="list-style-type: none"> <li>• Employé peu sérieux</li> </ul>	<ul style="list-style-type: none"> <li>• M21 PER-DEP Surcharge des capacités d'une personne</li> </ul>	<ul style="list-style-type: none"> <li>• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire</li> </ul>	1. Minime
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une altération	1	<ul style="list-style-type: none"> <li>• Employé peu sérieux</li> </ul>	<ul style="list-style-type: none"> <li>• M21 PER-DEP Surcharge des capacités d'une personne</li> </ul>	<ul style="list-style-type: none"> <li>• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire</li> </ul>	1. Minime

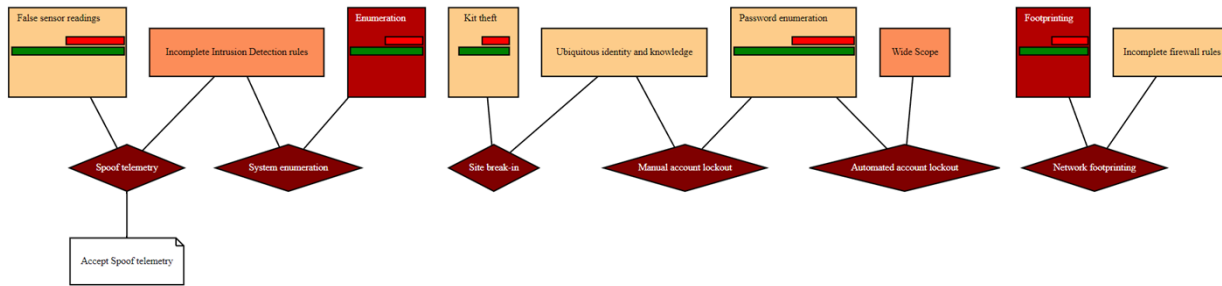
Menace	Vulnérabilités	Pré-requis	Vraisemblance
Attaque de type Man in the Middle	<ul style="list-style-type: none"> <li>• Possibilité de falsification du service appelé</li> <li>• Routage altérable</li> </ul>	<ul style="list-style-type: none"> <li>• Accès à la table de routage</li> <li>• Accès aux utilisateurs</li> </ul>	3. Forte
Changement des données du portail d'accès au cloud	<ul style="list-style-type: none"> <li>• Données du portail d'accès modifiables</li> <li>• Données du portail d'accès accessibles avec les droits adéquats</li> </ul>	<ul style="list-style-type: none"> <li>• Accès physique ou logique au portail d'accès</li> <li>• Connaissance de l'existence du portail d'accès</li> </ul>	3. Forte
Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	<ul style="list-style-type: none"> <li>• Manque de compétence du personnel</li> <li>• Négligence du personnel</li> </ul>	<ul style="list-style-type: none"> <li>• Partage de l'administration entre le personnel interne et le personnel du prestataire</li> </ul>	1. Minime

Niveau de risque avant application des mesures

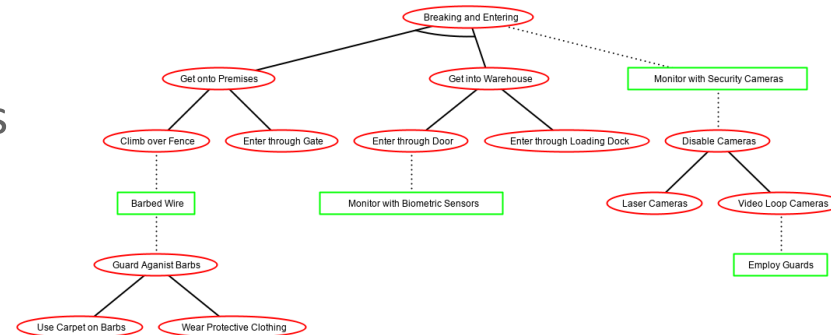
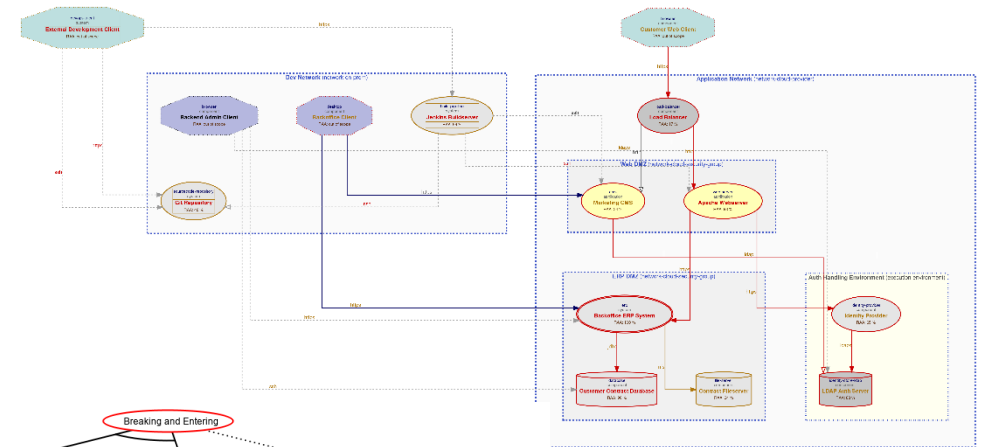
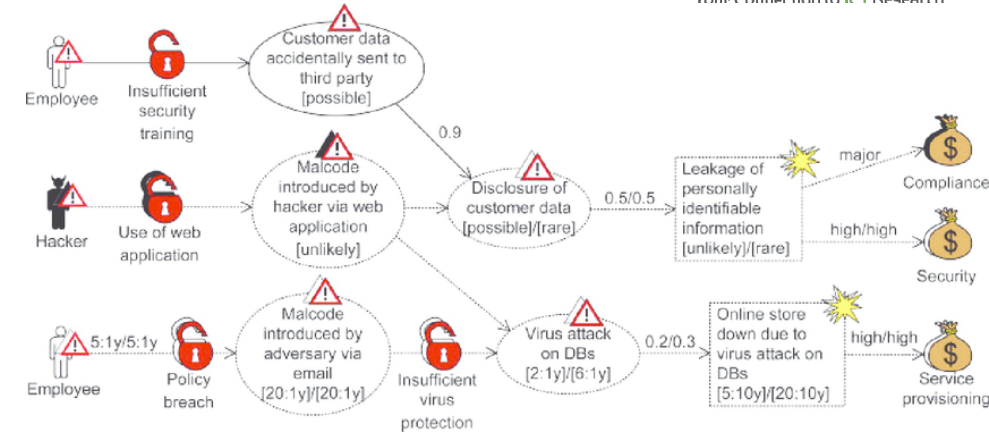
<b>Niveau de risque</b>	1. Négligeable	2. Limité	3. Significatif	4. Intolérable
<b>Gravité</b>	1. Négligeable	2. Limitée	3. Importante	4. Critique
<b>Vraisemblance</b>	1. Minime	2. Significative	3. Forte	4. Maximale

# Some Existing Approaches in Model-Based Risk Analysis

- organization, process level – also **negative**
  - (mis)-use-cases, UMLSec, CORAS
  - Goal-Oriented Requirements Engineering (i\*, KAOS, GSN...) e.g. Vulnerability Centric Framework, Formal Tropos, CAIRIS



- infrastructure and attacks
  - Infrastructure models, information flows
  - threat modelling
  - Attack (defense) trees (can connect to busines



# Research Question and Focus of this Talk

- Research Questions

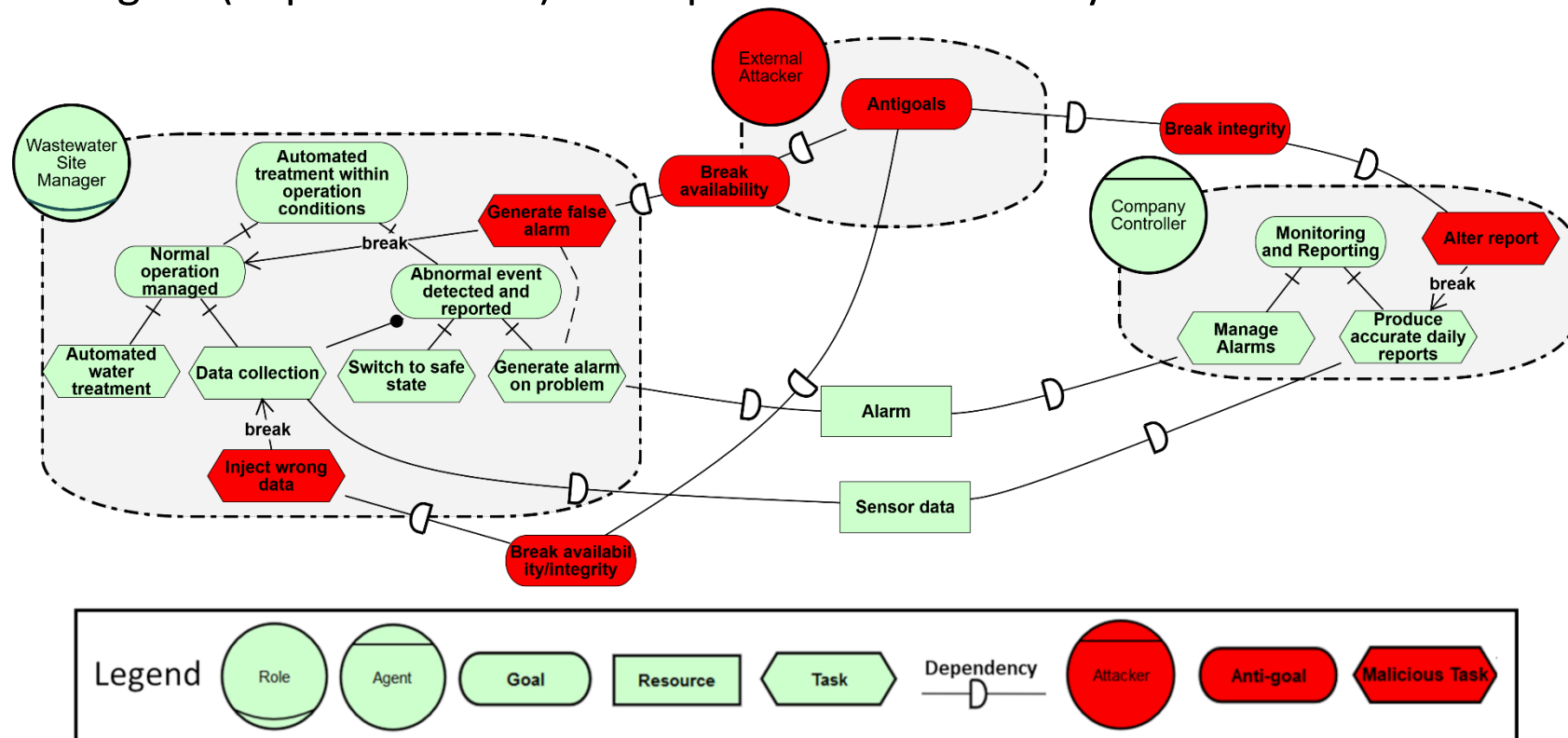
- *What is an interesting set of modelling notations for supporting risk analysis ?*
  - to capture both domain and infrastructure assets (business vs technical level)
  - reaching enough precision might also need to combine and map different models
- *How to provide a good automation level ?*
  - based on the models and related tools
  - here EBIOS until risk treatment phase
- *How to efficiently support certification processes ?*
  - *In a DevSecOps context*

- Talk structure:

- a modelling exercise combining generic i\* modelling for the business level and a standard infrastructure notation for the technical level
- application to automotive domain (ISO 21434)
- process modelling for speeding certification and enabling incremental certification (DevSecOps context)

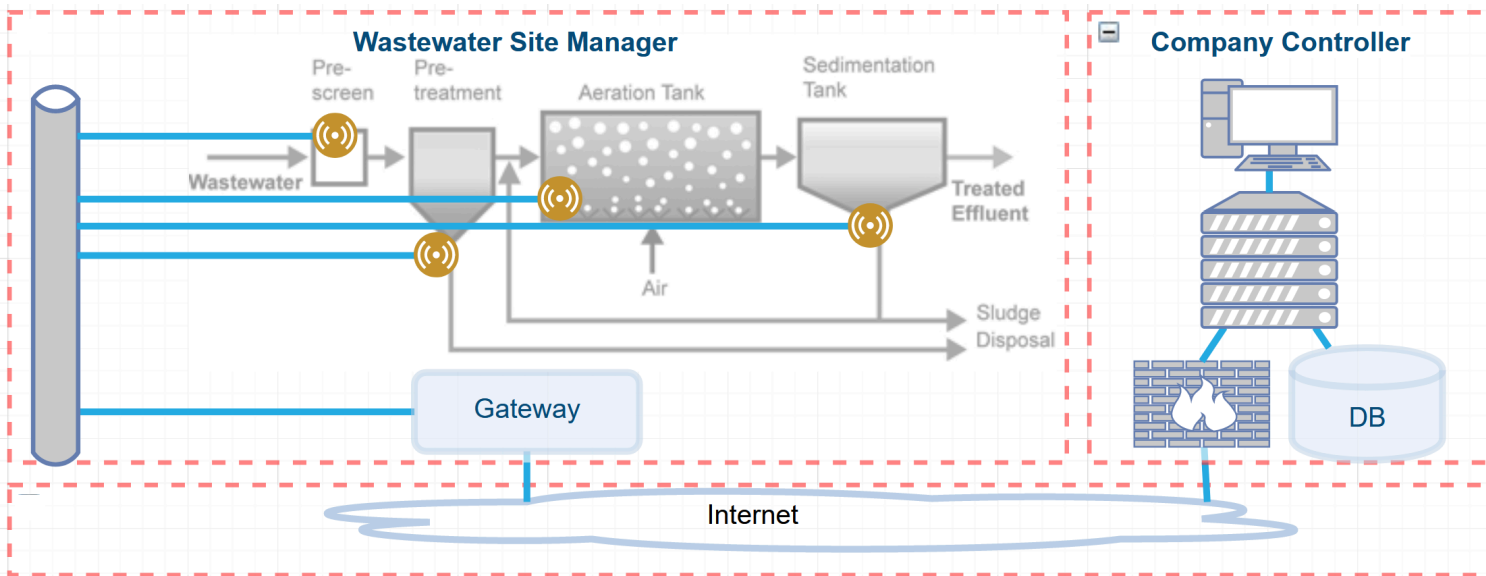
# Modelling Business Assets/Dreaded Event for Impact Assessment

- Using i\* strategic rationale diagram with piStar tooling (JSON format)
- Good mapping of EBIOS types (ORG, SYS, PER) → actors
- Clean structuring of business goals and processes per actor
- Identification of information flows
- Capturing threat sources as attacker agent (depicted in red) → inspired of vulnerability centric framework
  - Attacker motivations
  - Insider/outsider profiles
  - Specific goals and capabilities required for attack



# Modelling Infrastructure for Threat Scenario Analysis

- Using standard infra/network diagrams (IT/OT)
  - Prototyped with Irius Risk tool (XML format) , also possible with Threagile or pyTM
- Similar top-level containers as i\* actors → direct mapping
- Explicit modelling of communication channels → mapping inferred from linked parties
- Threat modelling can be used to identify vulnerabilities from this level
  - e.g. weak IoT protocol, unsecured communication channel,...
- Also capture specific protection agent (boundaries access control, monitoring, recovery...)



Severity	Likelihood	Impact	STRIDE	Function	CWE	Risk Category	Technical Asset
Elevated	Likely	High	Tampering	Development	CWE-79	Cross-Site Scripting (XSS)	Marketing CMS
Elevated	Likely	Medium	Elevation of Privilege	Architecture	CWE-306	Missing Authentication	Marketing CMS
Elevated	Likely	Medium	Elevation of Privilege	Architecture	CWE-306	Missing Authentication	Contract Fileserver
Elevated	Unlikely	High	Tampering	Operations	1008	Missing Cloud Hardening	
Elevated	Unlikely	High	Tampering	Operations	1008	Missing Cloud Hardening	Apache Webserver
Elevated	Unlikely	High	Tampering	Operations	1008	Missing Cloud Hardening	
Elevated	Unlikely	High	Tampering	Operations	1008	Missing Cloud Hardening	
Elevated	Unlikely	High	Tampering	Operations	1008	Missing Cloud Hardening	Contract Fileserver
Medium	Unlikely	High	Tampering	Development	CWE-434	Missing File Validation	Apache Webserver

# Automation Scripting

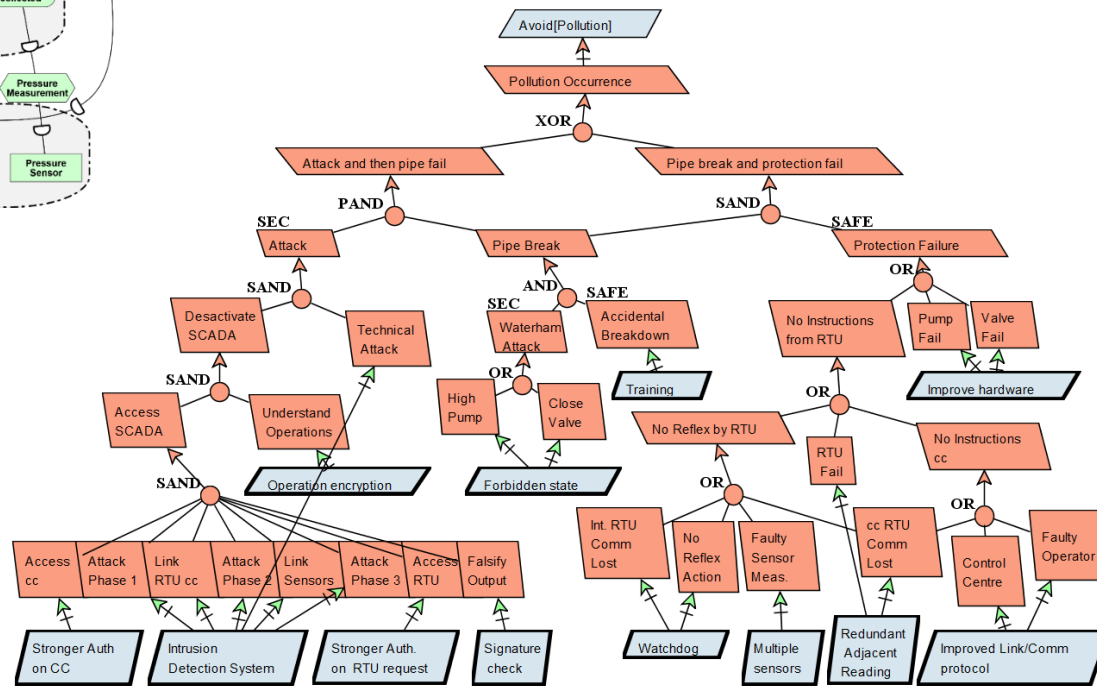
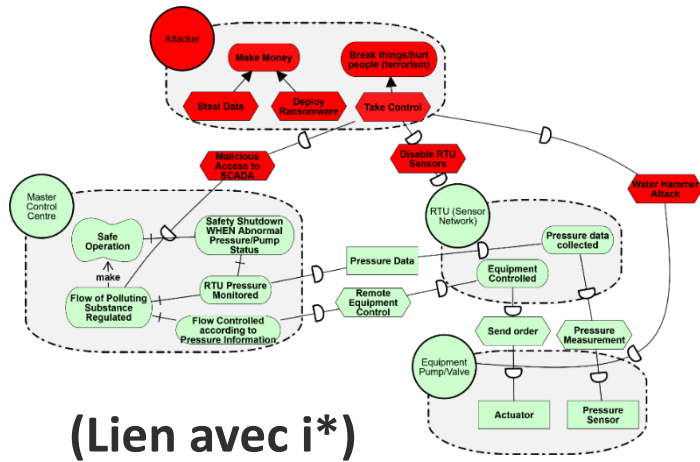
- The above models can be automatically processed through their JSON or XML output formats using Python
  - extract different security impact on business asset from the i\* strategic diagram based on exposure
    - process operation, potential safety impact
    - information confidentiality/integrity: financial, privacy depending on type
  - support IT/OT assets can be traced using the mapping
    - for each asset, the technical feasibility of the identified attack can be assessed.
    - technical information about existing vulnerabilities/exploitability provided by the infrastructure level tool
    - refining precise path level analysis to assess feasibility  
e.g. inject wrong data on (sensor 1a AND sensor 1b) OR bus OR gateway (implicit attack tree)
  - feasibility and impact information are then combined using the model structure to yield a good risk estimate
    - considering existing measure: redundant components (online/offline spares), secure channels, ...
    - specific rules for risk reduction: more or less formal (impact of hardware spare on natural failure → impact of training on phishing)

- Resulting risk matrix can then be generated and further analyzed for risk treatment phase

<b>I M P A C T</b>	<b>4. Critical</b>		Alarm unavailable	Report integrity lost	
	<b>3. Important</b>		Sensor data integrity lost		
			Sensor data unavailable		
	<b>2. Limited</b>		Report unavailable		
	<b>1. Negligible</b>		Sensor data unavailable		
		<b>1. Minimal</b>	<b>2. Significant</b>	<b>3. Strong</b>	<b>4. Maximal</b>
<b>LIKELIHOOD</b>					



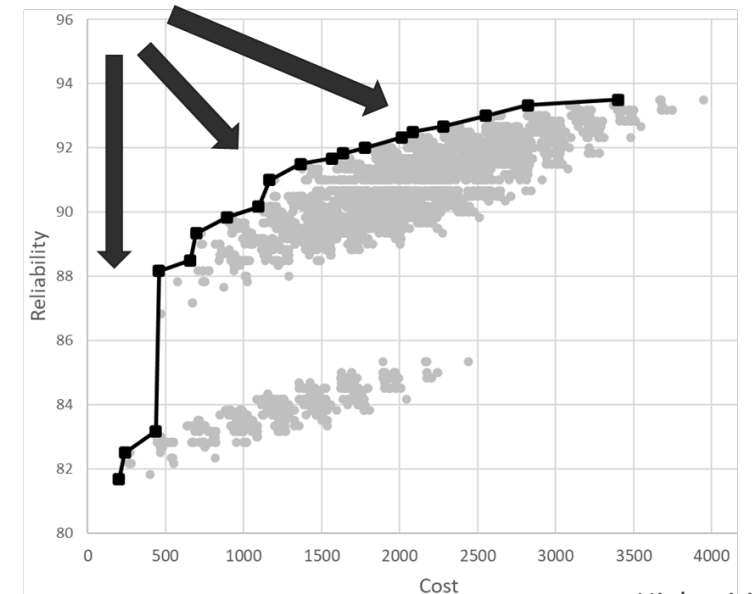
# Support for selecting counter-measures (cost/benefit)



Extension safety/security



Pareto front



Low mitigation Budget

High mitigation budget

# Preliminary Discussion and Comparison

- EBIOS experiment (current)
  - document/table-based template does not scale beyond a few primary assets and number of risks tend to grow quickly.
  - lack of precision even with good tooling due to rough mapping between assets and the systematic worst-case risk assessment rule
  - our (simple) modelling approach:
    - drives the investigation more reliably from business down to infrastructure level.
    - richer models → more accurate risk estimates although still qualitative.
  - beyond: EBIOS guidelines and knowledge base interesting to capture through GORE model patterns
- Secure Tropos: Socio-Technical System (STS) for modelling and reasoning about security requirements
  - precise modelling language capturing contracts constraining the interactions among STS actors
  - tooling for reasoning on the model and detecting possible conflicts
  - holistic analysis framework using 3 layers: business → software → infrastructure with 3 i\* models, mostly top-down
  - our modelling approach:
    - less reasoning capabilities but aims at more precise connections with infrastructure models
    - only two levels but infrastructure level is domain specific
- CORAS:
  - security risk modelling language customized for communication, documentation and analysis of security threat and risk scenarios
  - graphical and textual syntax + semantics but rather business level and directed towards protection by design
  - our modelling approach:
    - supports both business and infrastructure modelling
    - directed towards a matrix-based approach as in most cyber security standards
- CAIRIS:
  - very rich and complete, based on KAOS
  - our modelling approach: purposely more lightweight and focused on a specific methodology but anchored in similar GORE modelling

## Automotive Case study:

- KAOS modelling
- ISO21434 risk modelling approach (certification context) ≠ EBIOS (ISO27K)

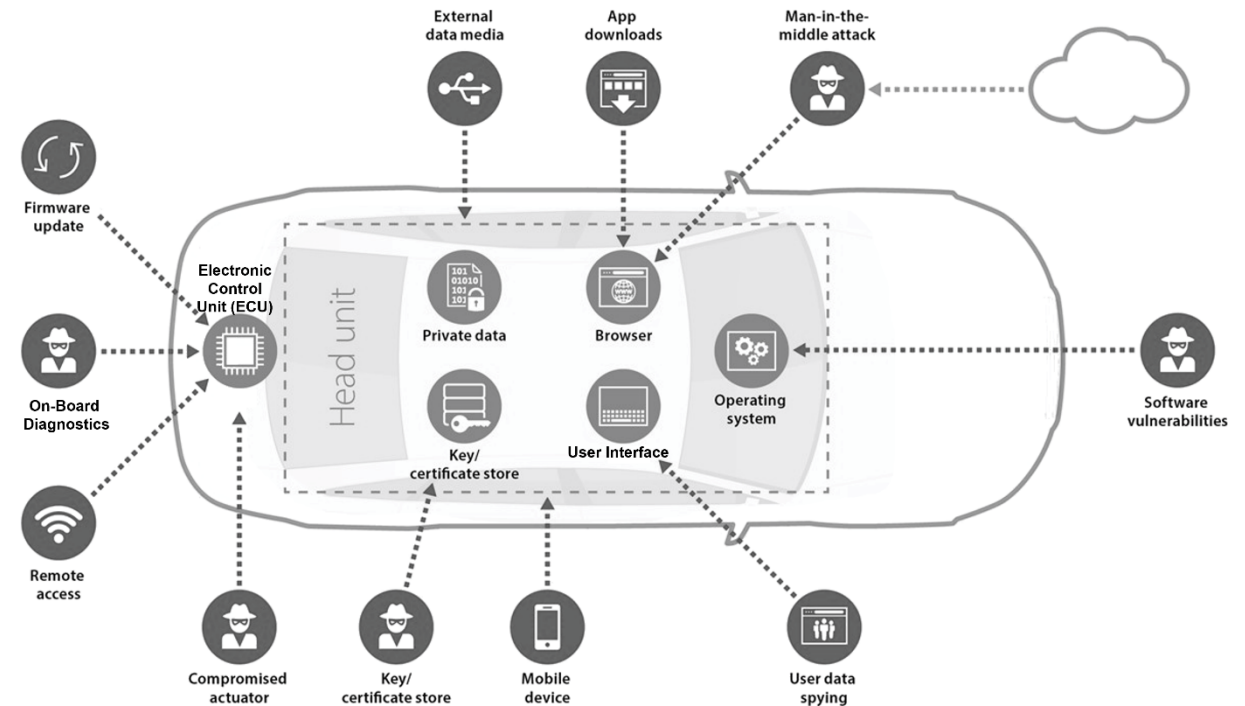
# Context – Automotive Cybersecurity

## Worrying situation

- Increasing attack surface due to software, connectivity
- Cybersecurity practice behind: J3061 “best practices”

## However improving

- emerging ISO21434
- good safety culture  
→ can also drive cybersecurity (and co-engineering)

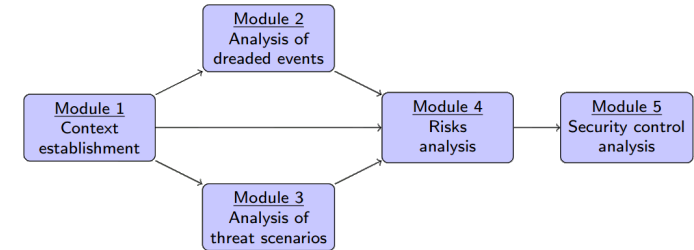
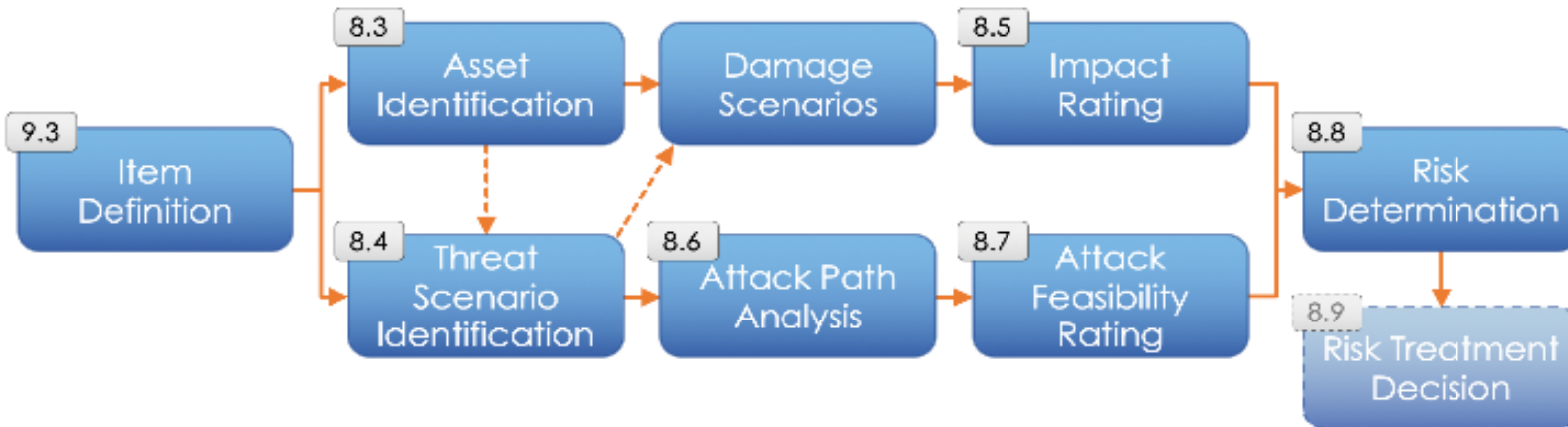
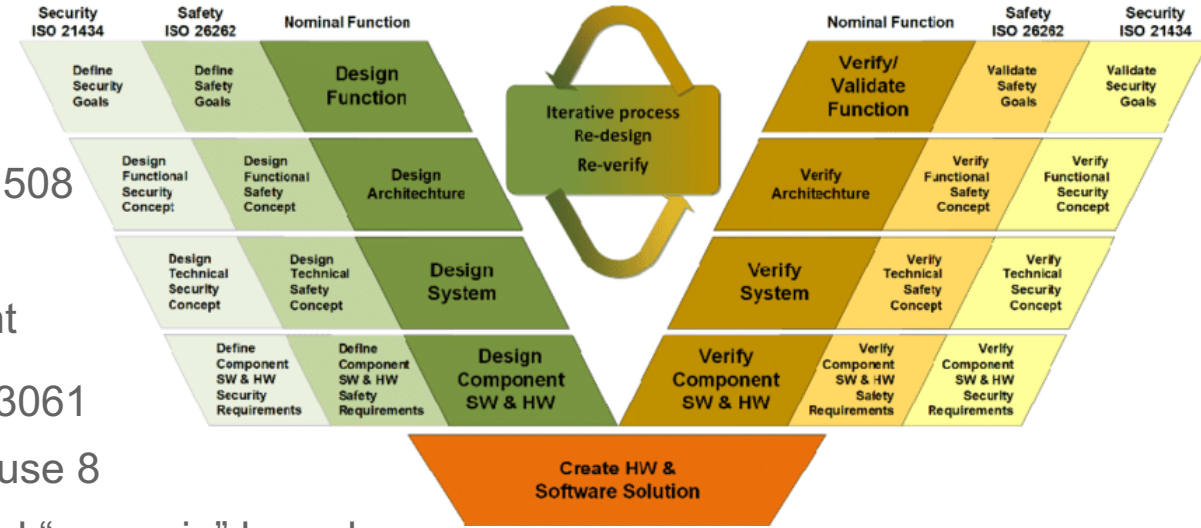


## Our research: can a model-based approach be interesting ?

- identification of key assets, safety and security properties and related risks.
- co-engineering practices through commonly adopted methods to integrate TARA with HARA.
- use of tool chain with analysis, transformation and document generation

# Existing ISO 26262 → safety and Emerging ISO 21434 → cyber security

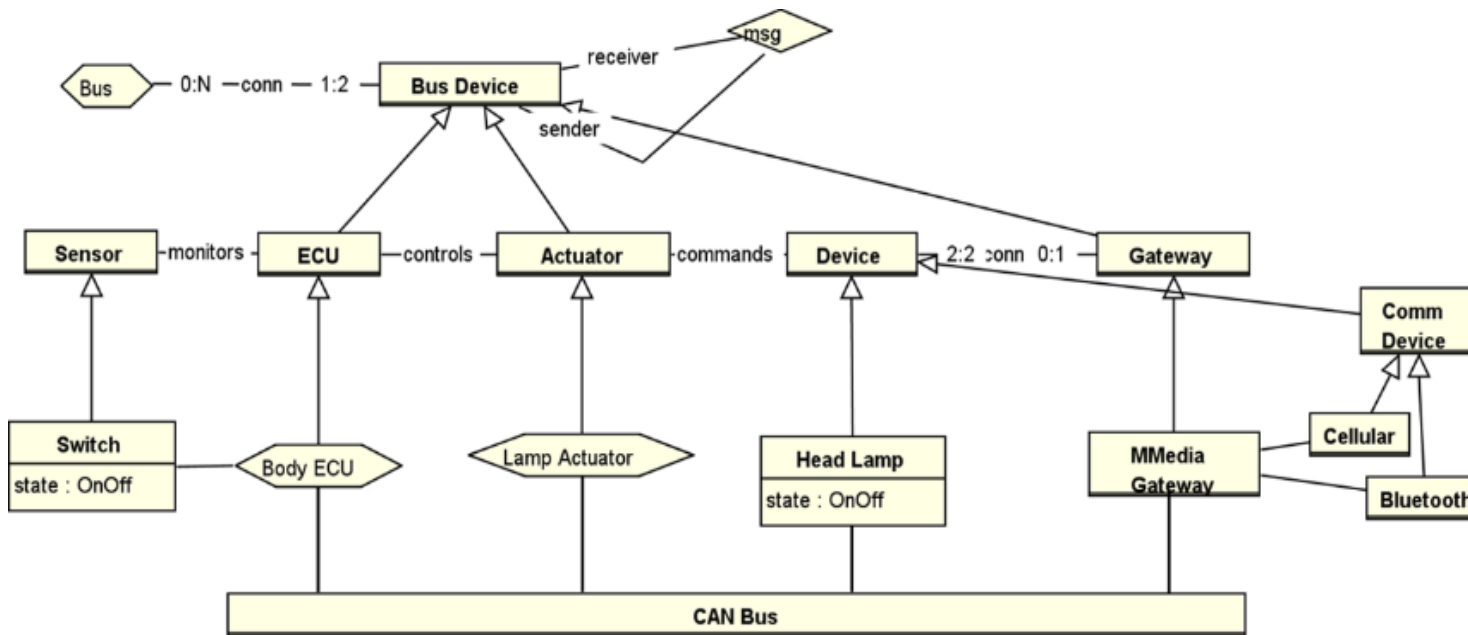
- Both risk-based grounded in ISO 31000 (PDCA loop)
- ISO 26262 older (2011) for safety based on IEC IEC 61508
  - Hazard Analysis and Risk Assessment (HARA)
  - only basic cyber security guidelines for development
- ISO 21434 – draft standard (due 2021) – superseding J3061
  - Threat Analysis and Risk Assessment (TARA) = clause 8
  - domain-level “damage” branch vs infrastructure-level “scenario” branch



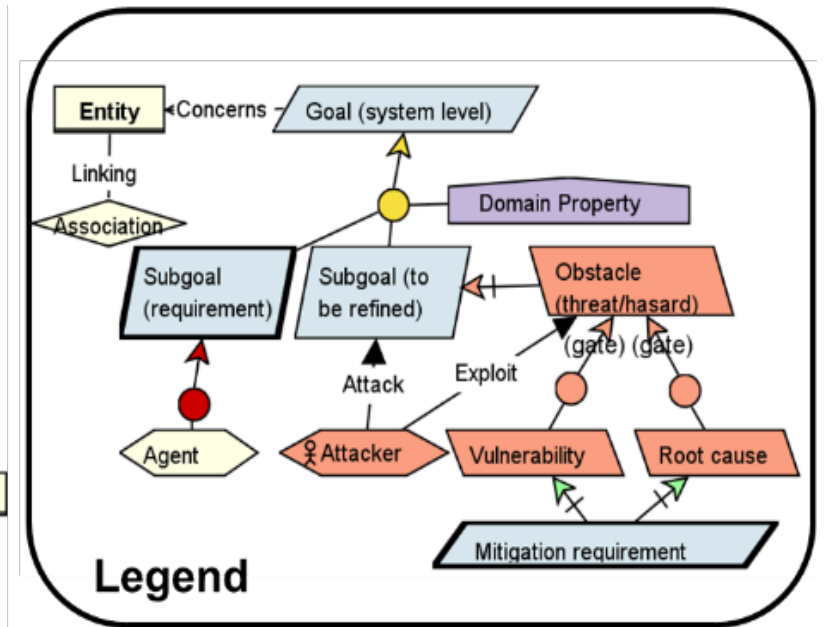
# Goal-oriented Models for Co-engineering illustrated on a partial case study (lighting system)

- Lighting system case used by the standard and other references
- KAOS notations: goal-oriented (among other candidates such as GRL, i\*)

## Context – asset identification (8.3)



## Relevant KAOS notations

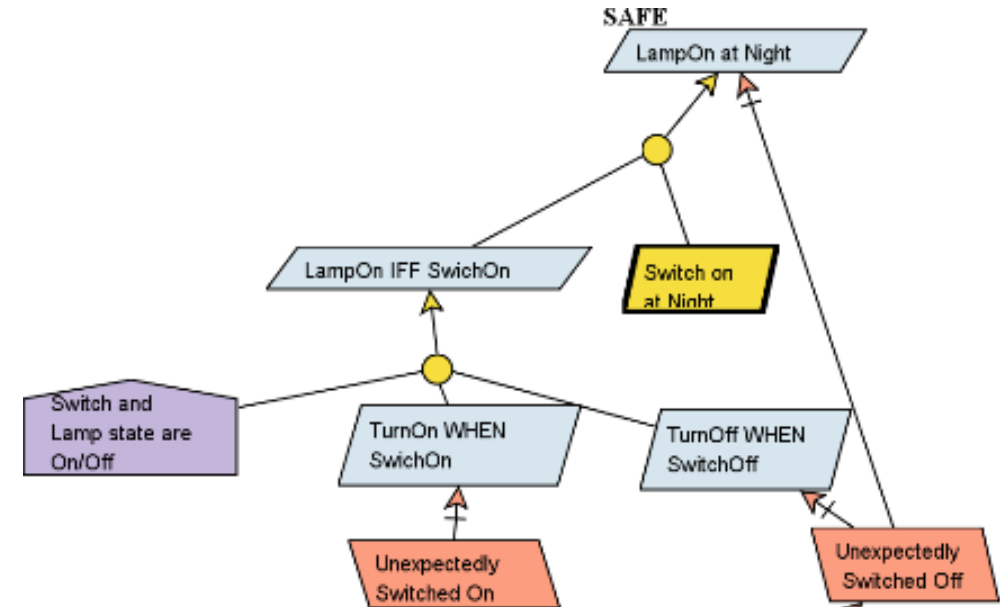




# Damage scenario and impact rating branch (8.5)

## Method: challenge CIA dimensions → root obstacles & impact

- Confidentiality: not relevant (public information)
- Integrity: obstacles related to **unexpectedly turning lights off** or on  
→ can have a major safety impact if at night !  
(other dimensions: financial, reputation)
- Availability: obstacles related to impossibility of turning lights on or off  
→ ...



# Threat scenario and attack path analysis (8.4/6/7)

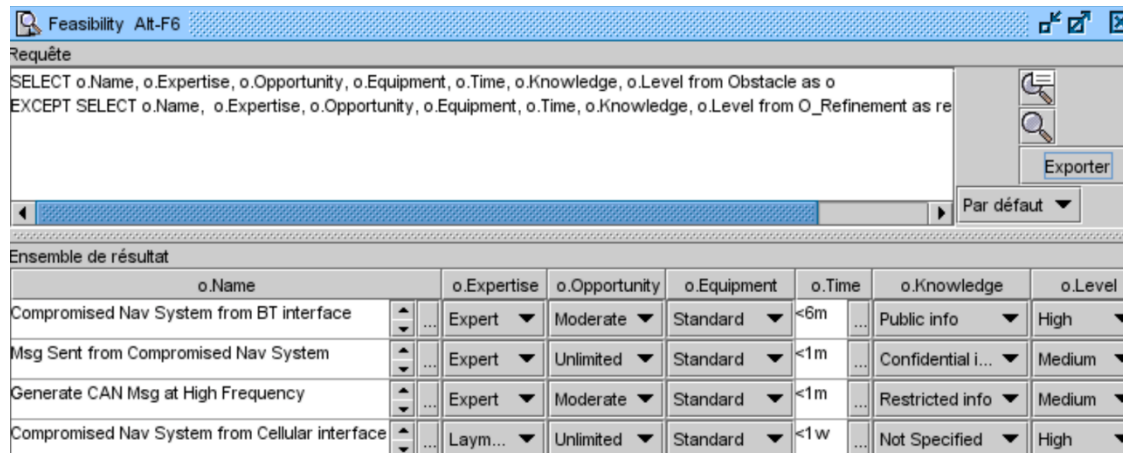
## Threat scenario (8.4) and attack path analysis (8.6)

→ method: develop obstacle analysis  
(top-down or bottom-up from vulnerabilities)

## 8.7 Attack feasibility rating

→ method: use assessment model  
(expertise/opportunity/equipment/knowledge/level)

Using: model query, edition and processing



Feasibility Alt-F6

Requête

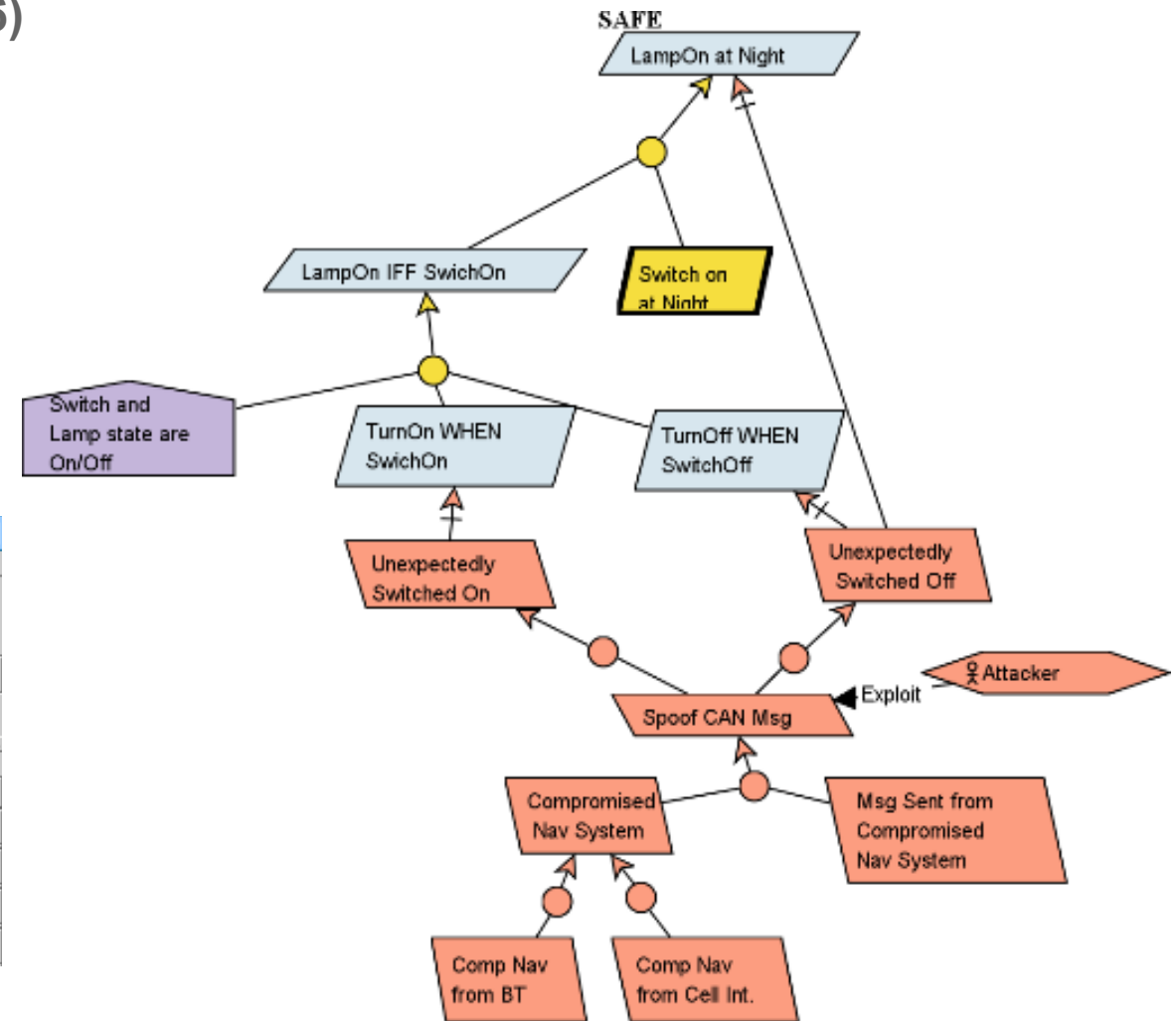
```
SELECT o.Name, o.Expertise, o.Opportunity, o.Equipment, o.Time, o.Knowledge, o.Level from Obstacle as o  
EXCEPT SELECT o.Name, o.Expertise, o.Opportunity, o.Equipment, o.Time, o.Knowledge, o.Level from O_Refinement as re
```

Exporter

Par défaut

Ensemble de résultat

o.Name	o.Expertise	o.Opportunity	o.Equipment	o.Time	o.Knowledge	o.Level
Compromised Nav System from BT interface	Expert	Moderate	Standard	<6m	Public info	High
Msg Sent from Compromised Nav System	Expert	Unlimited	Standard	<1m	Confidential i...	Medium
Generate CAN Msg at High Frequency	Expert	Moderate	Standard	<1m	Restricted info	Medium
Compromised Nav System from Cellular interface	Laym...	Unlimited	Standard	<1w	Not Specified	High



# Resulting risk matrix and Next Steps

- **8.8 Risk determination: risk matrix**
  - ➔ Generated from the model
  - ➔ Prioritization strategy
- **8.8 Risk treatment** – not detailed here

	Very Low	Low	Medium	High
Severe			<b>unexpectedly turning lights off</b>	
Major			R2	
Moderate		R4		
Negligible		R3	R1	

## Conclusion: MBSE helps

- in systematic risk identification
- more objective assessment
- enables automation

## Further work

- support mitigation phase
- check scalability/modularity
- safety-security co-engineering
- conformance process

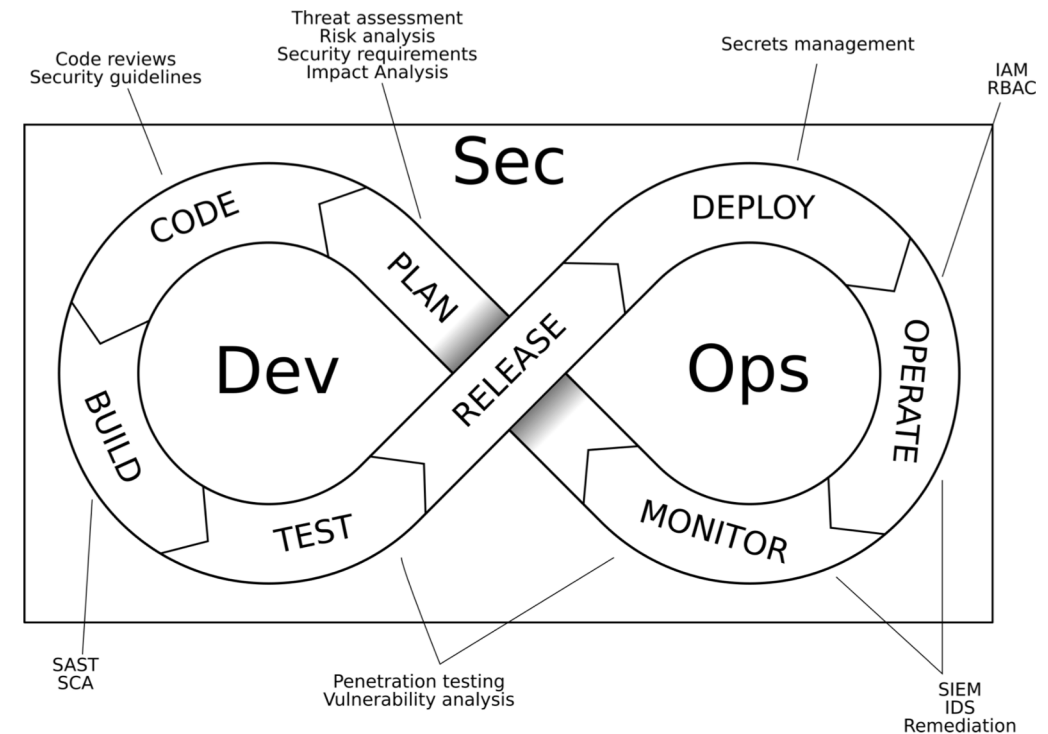
# Process modelling

- in DevSecOps context
- for speeding certification and enabling incremental certification

# Challenge and Opportunities

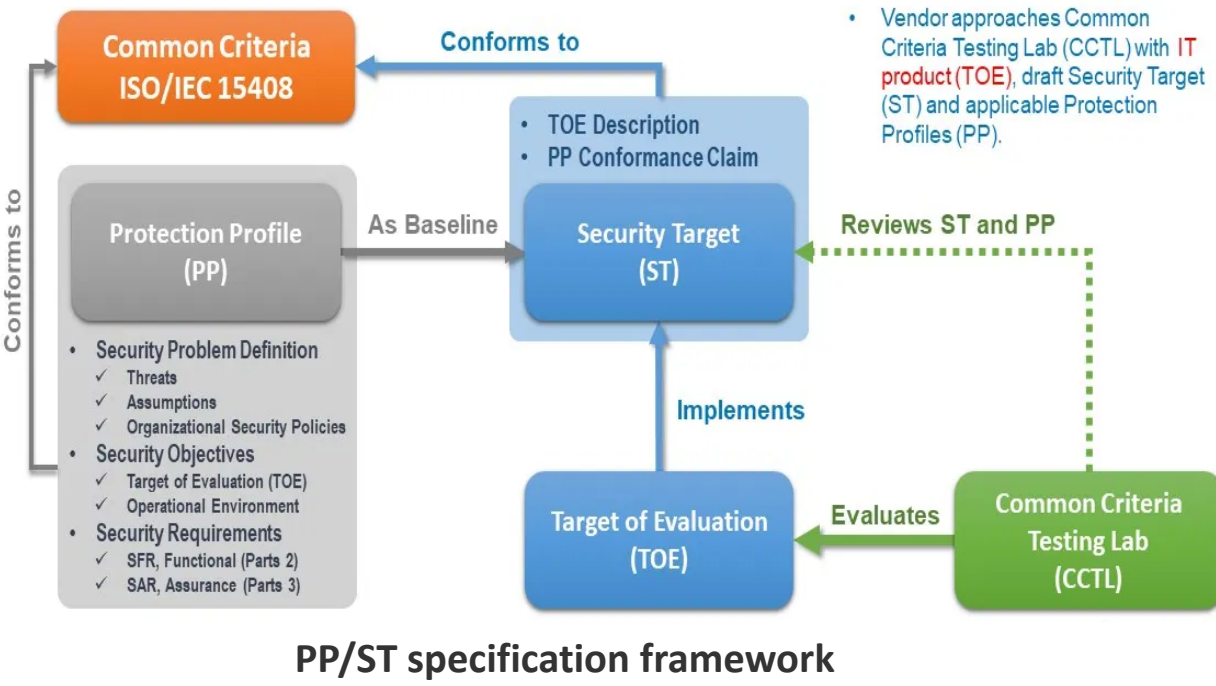
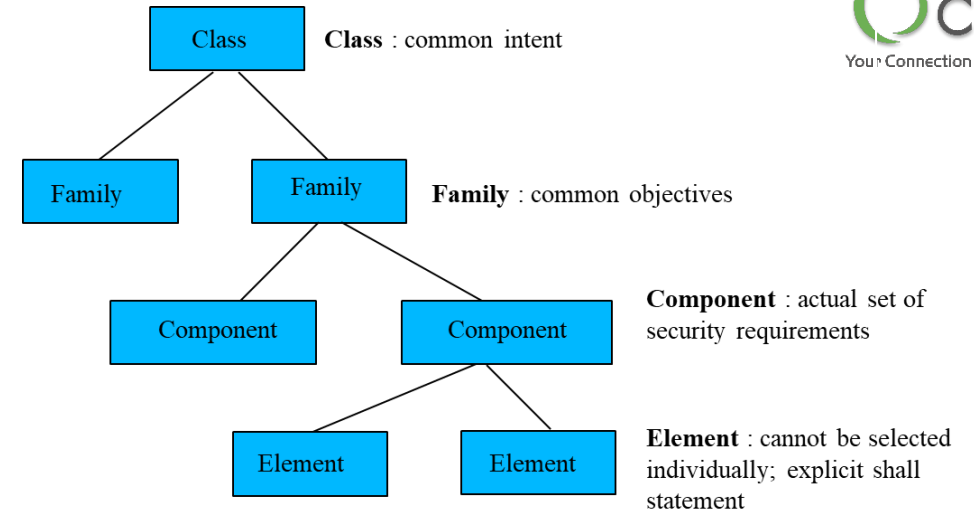
- Security challenged
  - fast evolution of threat landscape [days]
  - heavyweight certification schemes – e.g. Common Criteria (months)

- DevSecOps Opportunity
  - DevOps: focused on producing quality code, quickly and reliably – not focused on security
  - DevSecOps augment DevOps with security procedures to ensure continuous security assessment.

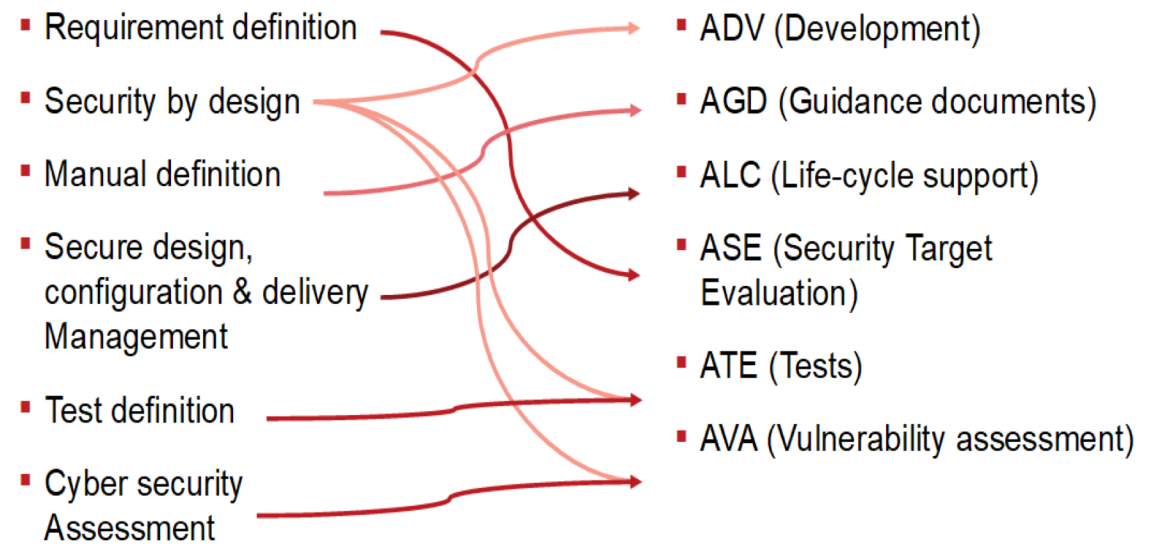


# Modeling certification processes

## Common Criteria



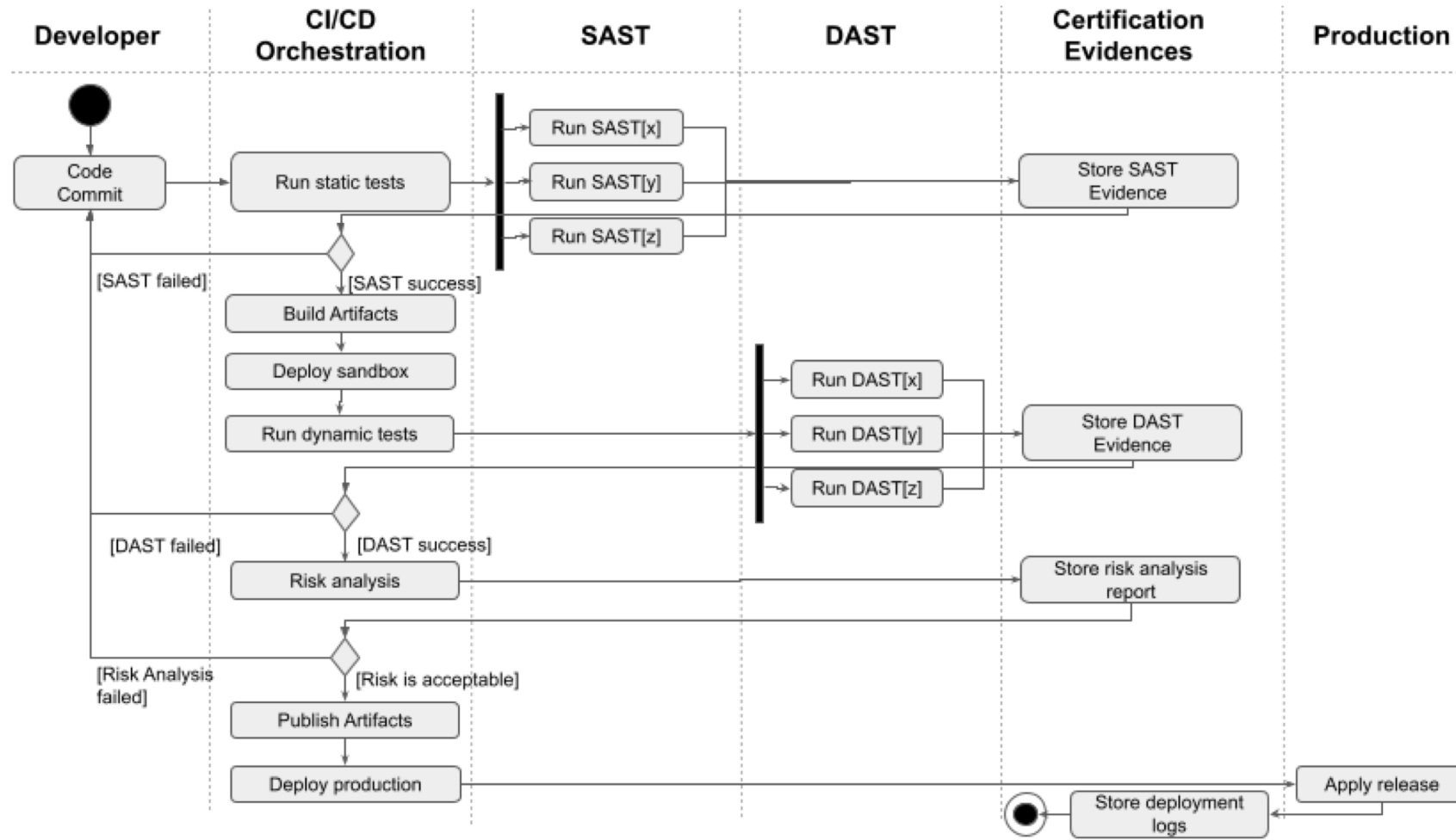
PP/ST specification framework





# Modeling certification processes

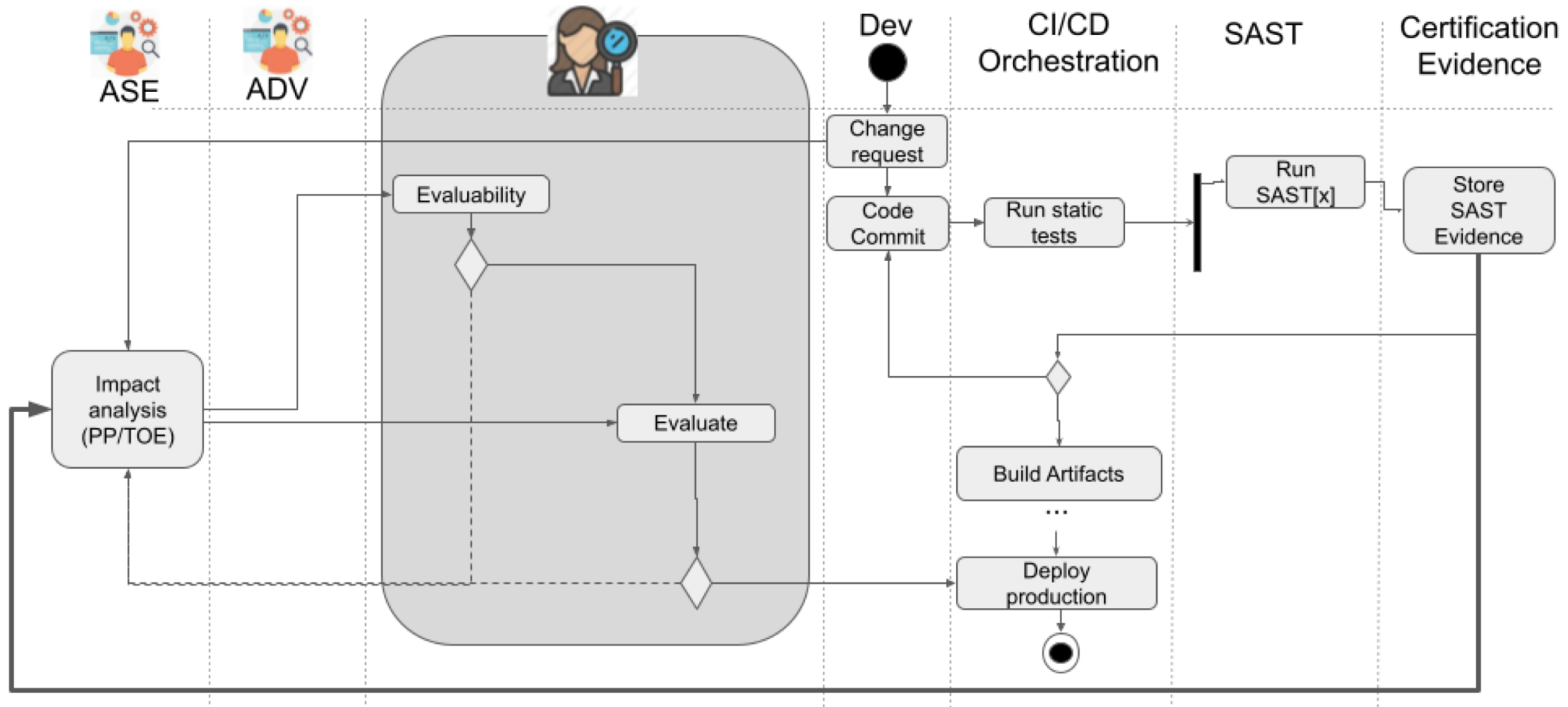
## DevSecOps



DevSecOps process activity diagram - code, build, test, release, deploy

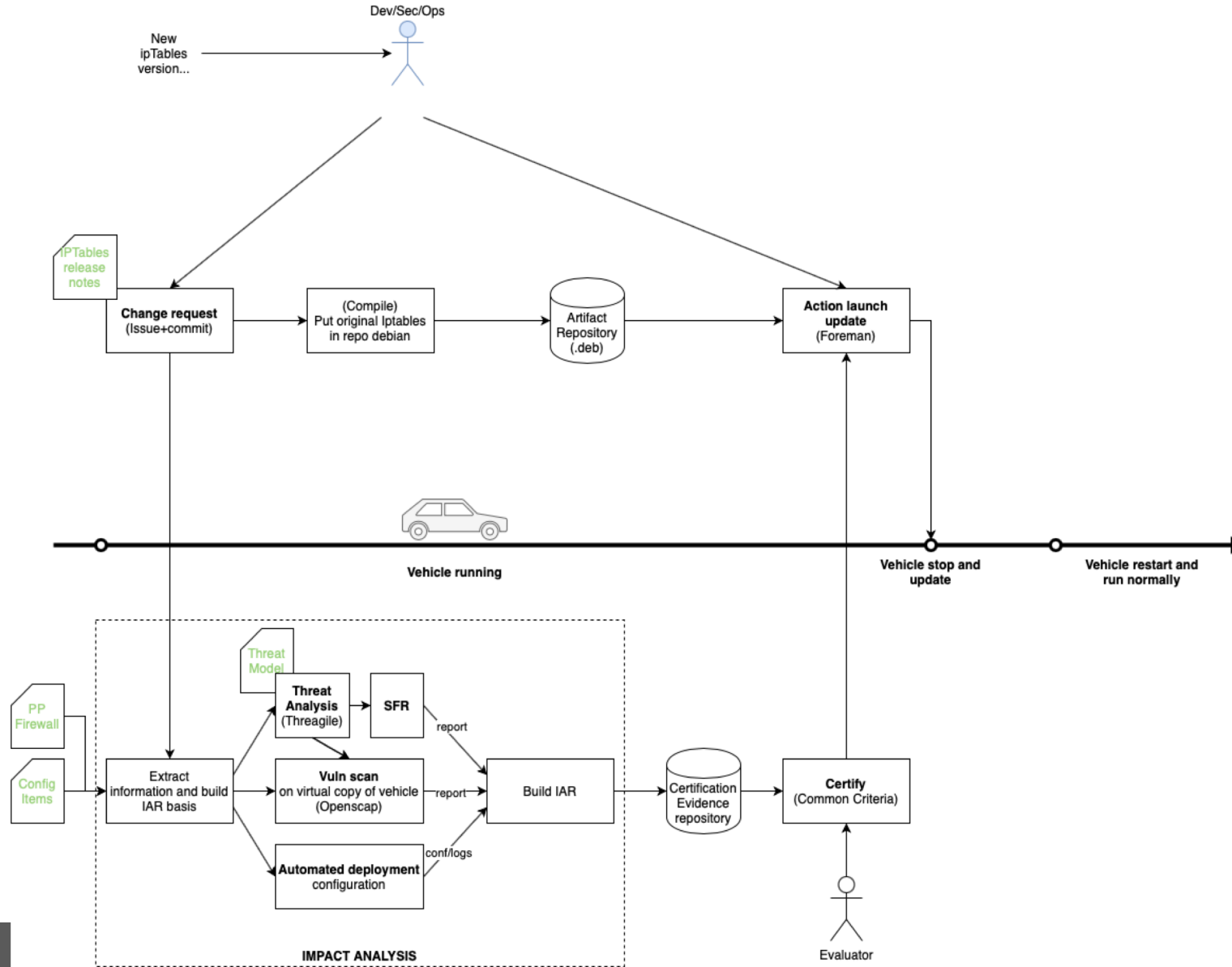
# Modeling certification processes

## Composing incremental certification and DevSecOps



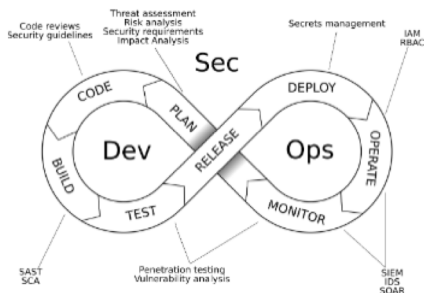
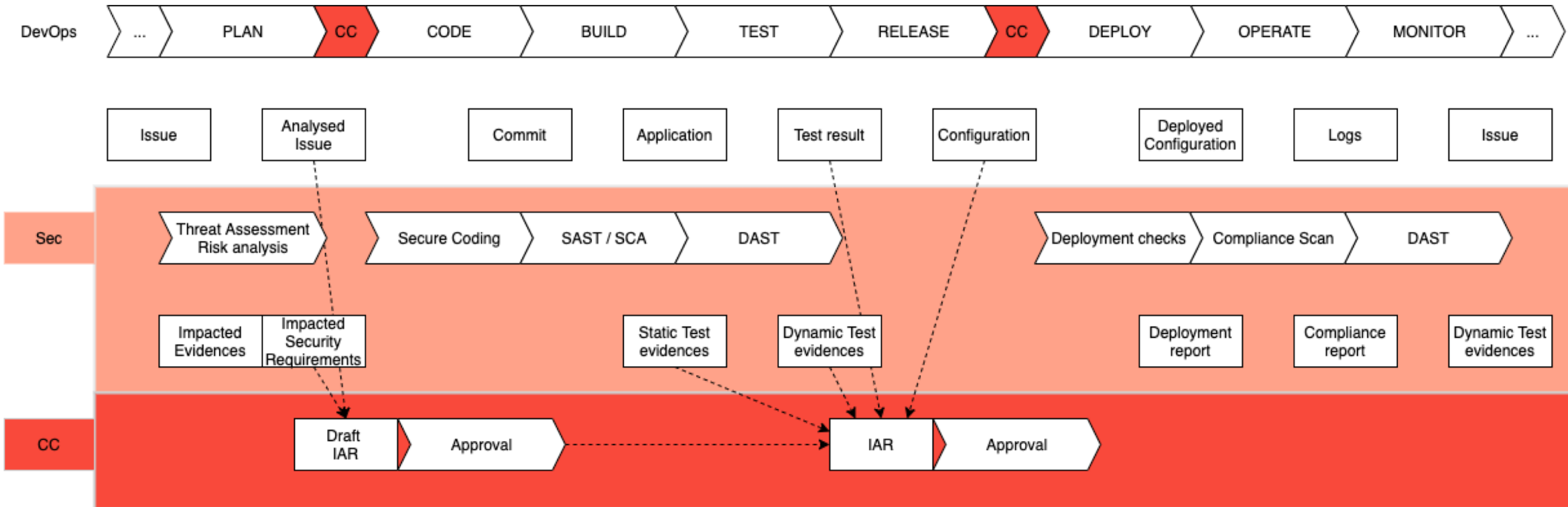
Composed certification and DevSecOps activity diagram - Impact Analysis

# Illustration of benefits with DevSecOps for Common Criteria impact analysis: vehicle firewall update case study



# Illustration of benefits with DevSecOps for Common Criteria impact analysis

## Implementation of DevSecOps process for impact analysis



### Impact Analysis Report content :

- **Step 1** (Identify Certified TOE) : Configuration artifact from previous cycle
- **Step 2** (Identify and describe changes) : Analysed Issue & Impacted Security Requirements  
⇒ Draft Impact Analysis Report
- **Step 3** (Determine impacted developer evidence) : All evidences are available from the devsecops process
- **Step 4** (Perform required modifications to developer evidence) : Idem Step 3  
⇒ Impact Analysis Report
- **Step 5** (Conclude) : Manual conclusion

# Illustration of benefits with DevSecOps for Common Criteria impact analysis

## Examples of tables : Firewall changes to be implemented

ID	Summary	Description
2	xtables-monitor: fix rule printing	trace_print_rule does a rule dump. This prints unrelated rules in the same chain. Instead the function should only request the specific handle. Furthermore flush output buffer afterwards so this plays nice when output is not a terminal.
3	xtables-monitor: fix packet family protocol	This prints the family passed on the command line (which might be 0). Print the table family instead.
4	nft: Optimize class-based IP prefix matches	Payload expression works on byte-boundaries leverage this with suitable prefix lengths.
5	nft: Fix selective chain compatibility checks	Since commit 80251bc2a56ed ("nft: remove cache build calls") chain parameter passed to nft_chain_list_get() is no longer effective. Before it was used to fetch only that single chain from kernel when populating the cache. So the returned list of chains for which compatibility checks are done would contain only that single chain. Re-establish the single chain compat checking by introducing a dedicated code path to nft_is_chain_compatible() doing so.

References: IPTables 1.8.7 changelog and issue tracker

[https://www.netfilter.org/projects/iptables/files/changes-iptables-](https://www.netfilter.org/projects/iptables/files/changes-iptables-1.8.7.txt)

[1.8.7.txt](https://www.netfilter.org/projects/iptables/files/changes-iptables-1.8.7.txt)

# Illustration of benefits with DevSecOps for Common Criteria impact analysis

## Examples of tables : Security Functional Requirements (SFR)

These requirements are extracted from the Protection Profile resulting from the full Common Criteria certification performed on the system.

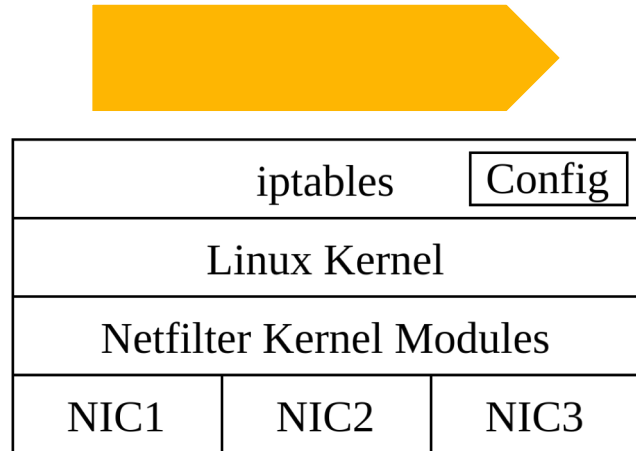
Tag	SFR Description
FDP_ACF.1.1	The TSF shall enforce the access control to objects based on security attributes.
FDP_ACF.1.2	The TSF shall enforce rules to determine if an operation among controlled subjects and controlled objects is allowed.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on additional rules.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules.
FDP_IFF.4.1	The TSF shall enforce the information flow control to limit the capacity of illicit information flows to a maximum capacity.
FDP_IFF.4.2	The TSF shall prevent the following types of illicit information flow : tcp shell or http shell.
PMM_IF.1.1	The TOE shall maintain an outgoing heart-beat data flow with other platooning vehicles as specified below: From TOE to VCS (and then to another vehicle TOE). Messages transmitted shall contain the following data computed from the TOE vehicle sensors/algorithms: Vehicle unique identifier - Vehicle speed - Direction - Geo-Position - Timestamp.
PMM_IF.3.1	The TOE shall maintain an incoming flow with other vehicles informing the TOE vehicle about emergency brake maneuvers as specified below: From (another vehicle TOE to vehicle) VCS to TOE. Messages transmitted shall contain the following data: Unique identifier of the vehicle to which the emergency brake has been issued - Emergency brake identifier - Timestamp - Digitally signed certificates.



# Illustration of benefits with DevSecOps for Common Criteria impact analysis

Examples of tables : Traceability SFR - Components to Traceability SFR - Impacted Components

SFR - Components Traceability	
Name	Tag
SafeSecPMM	PMM_IF.1.1
SafeSecPMM	PMM_IF.3.1
iptables	FDP_ACF.1.1
netfilter	FDP_ACF.1.3
netfilter	FDP_ACF.1.4
netfilter	FDP_IFF.4.1
netfilter	FDP_IFF.4.2
iptables	FDP_ACF.1.2



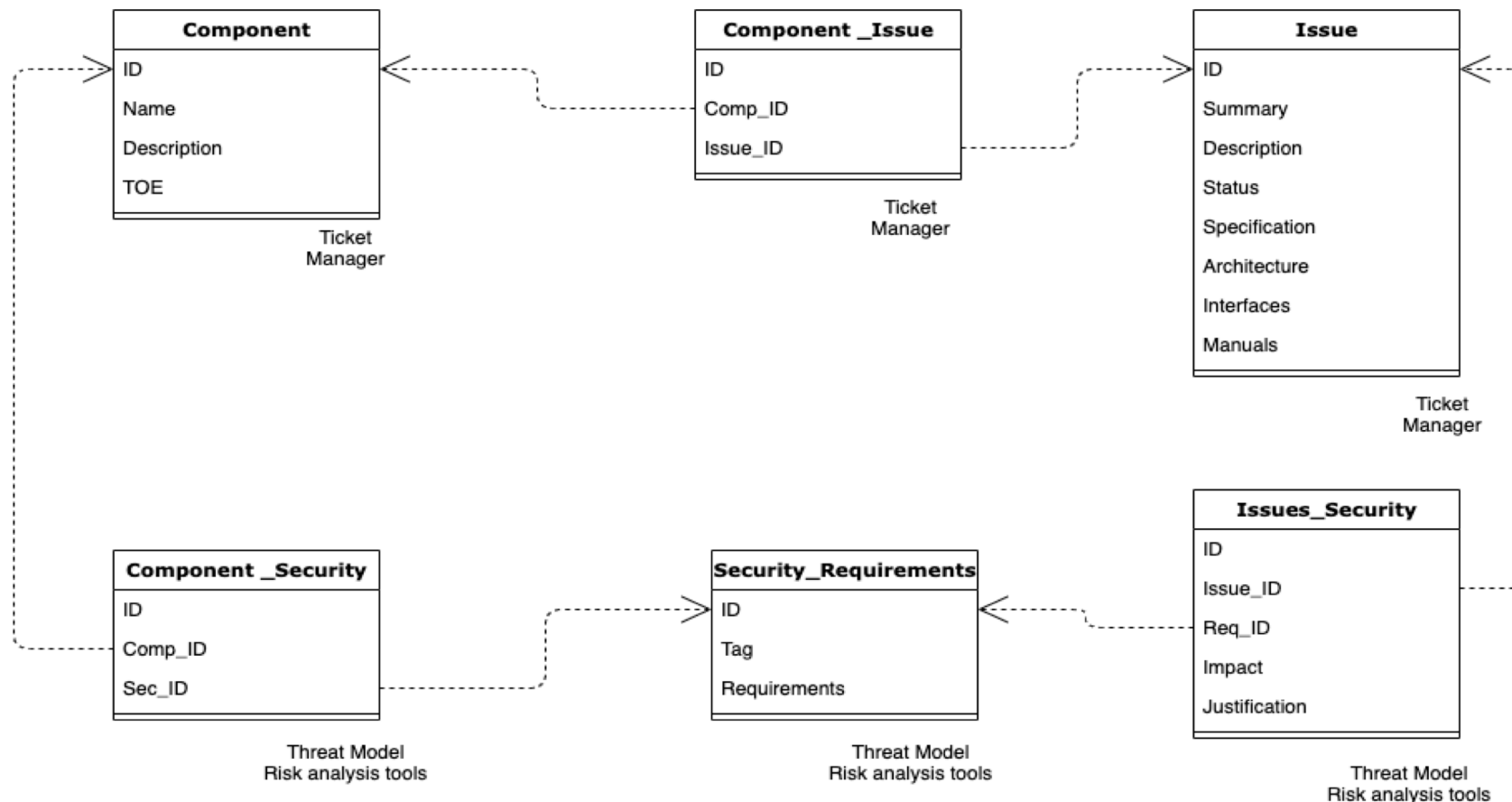
SFR - Impacted Components Traceability	
Name	Tag
iptables	FDP_ACF.1.1
netfilter	FDP_ACF.1.3
netfilter	FDP_ACF.1.4
netfilter	FDP_IFF.4.1
netfilter	FDP_IFF.4.2
iptables	FDP_ACF.1.2

# Illustration of benefits with DevSecOps for Common Criteria impact analysis - Examples of tables : Impact Analysis Results

ID	Tag	Impact	Justification
2	FDP_ACF.1.2	False	The changes to the code of the component do not affect the requirement as it concerns only display.
2	FDP_ACF.1.1	False	The changes to the code of the component do not affect the requirement as it concerns only display.
3	FDP_ACF.1.2	False	The changes to the code of the component do not affect the requirement as the requirement is not satisfied by this component.
3	FDP_ACF.1.1	False	The changes to the code of the component do not affect the requirement as it concerns only display.
4	FDP_ACF.1.3	True	The changes impact the component and the implementation of the requirement
4	FDP_ACF.1.4	True	The changes impact the component and the implementation of the requirement
4	FDP_IFF.4.1	True	The changes impact the component and the implementation of the requirement
4	FDP_IFF.4.2	True	The changes impact the component and the implementation of the requirement
5	FDP_ACF.1.3	False	The change to the code of the component do not affect the requirement as it is a compatibility change for checks.
5	FDP_ACF.1.4	False	The change to the code of the component do not affect the requirement as it is a compatibility change for checks.
5	FDP_IFF.4.1	False	The change to the code of the component do not affect the requirement as it is a compatibility change for checks.
5	FDP_IFF.4.2	False	The change to the code of the component do not affect the requirement as it is a compatibility change for checks.

# Illustration of benefits with DevSecOps for Common Criteria impact analysis

Examples of tables : DataBase Scheme with information sources



Good evidence of benefits of model-based approach for

- risk analysis process
- a global security focused lifecycle (including DEV & OPS)

Especially

- Completeness
- Precision
- Reactivity/incrementality

Next steps

- Build a more integrated toolset
- Validate on enterprise/industry cases
  - On-going comparative validation with a pool of about 30 learners from enterprise context (post-graduate cursus)



Your Connection to ICT Research

Aéropole de Charleroi-Gosselies  
Avenue Jean Mermoz 28  
6041 Charleroi - Belgique



twitter.com/@CETIC  
twitter.com/@CETIC\_be



linkedin.com/company/cetic



info@cetic.be



+32 71 159 362

[www.cetic.be](http://www.cetic.be)

# Questions?

Christophe Ponsard

*R&D&I Coordinator*

+32 472 56 90 99

christophe.ponsard@cetic.be