Challenges for **Interference Analysis** *of* **Quality Attributes**
during Systems **Evolution**
BENEVOL 2020

Safety and Security Interference Analysis in the Design Stage

Jabier Martinez, Jean Godot, Alejandra Ruiz, Abel Balbis, and Ricardo Ruiz Nolasco

Tecnalia, Basque Research and Technology Alliance (BRTA), Derio, Spain
All4Tec, Laval, France
Thales Alenia Space, Madrid, Spain
RGB Medical Devices, Madrid, Spain

3 December 2020
BENEVOL 2020
Previously DECSoS workshop at SAFECOMP 2020

Safety and Security Co-Engineering

- Safety and security experts aim to reduce risks (from their own focus) to acceptable values
  - by integrating the needed barriers and measures within the components of the system.
- However, preventing both safety and security could cause conflicting situations
  - e.g., the introduction of a security method could cause a time delay which is in contradiction with a safety requirement

Safety and Security Co-Engineering

Evolving independently

- Highly specialized knowledge, skills, terminology
- Forced to show compliance to standards, jurisdictions,and regulations focusing only on one aspect
    - Imposing the life-cycle, activities, methods, terminology conventions that they should follow, and the expected artefacts that they should produce

Safety and Security Co-Engineering

Safety and security separation led to

- Redundant efforts *
- Late identification of conflicts and trade-offs in safety and security requirements.
    - The costs of not identifying issues related to safety and security concerns during early phases of the product life-cycle can be very significant

* Preliminary safety-security co-engineering process in the industrial automation sector.
Alejandra Ruiz, Javier Puelles, Jabier Martinez, Thomas Gruber, Martin Matschnig, Bernhard Fischer:
In: ERTS 2020, 10th European Congress on Embedded Real Time Systems (2020)

Aggregated Quality Assurance of Systems

We investigated Co-Engineering techniques for Safety, Security and Performance (SSP) of critical and complex embedded systems

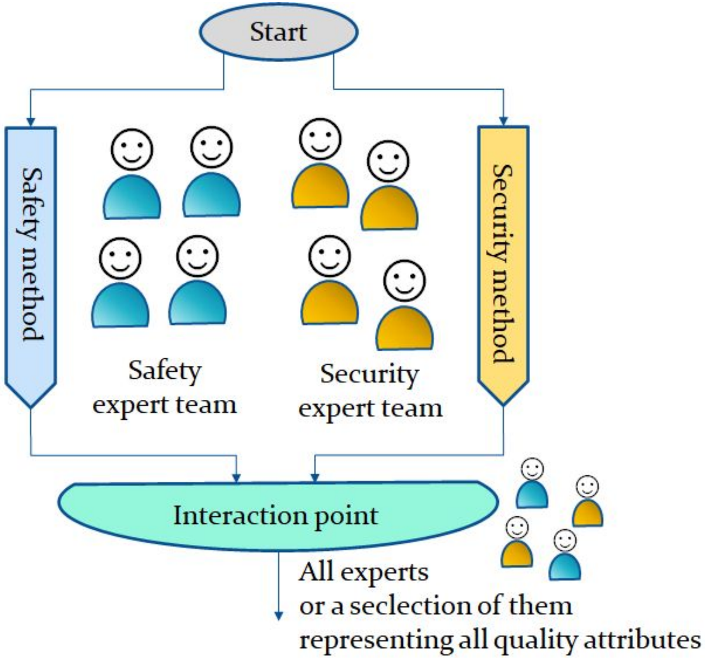
→ Co-Engineering into mainstream practices

H2020-ECSEL grant agreement 737475

Safety and Security Co-Engineering

Interaction Points

- Points in time (i.e. at different stages of a product life cycle), at which a holistic view on the system is taken to establish whether the system is "good enough". Direct interaction between experts and/or tool supported.
- A set of activities of system analysis. Combined analysis dealing with more than one quality attribute.



https://aquas-project.eu/documents/ D.3.2 Combined Safety, Security and Performance Analysis and Assessment Techniques – Preliminary

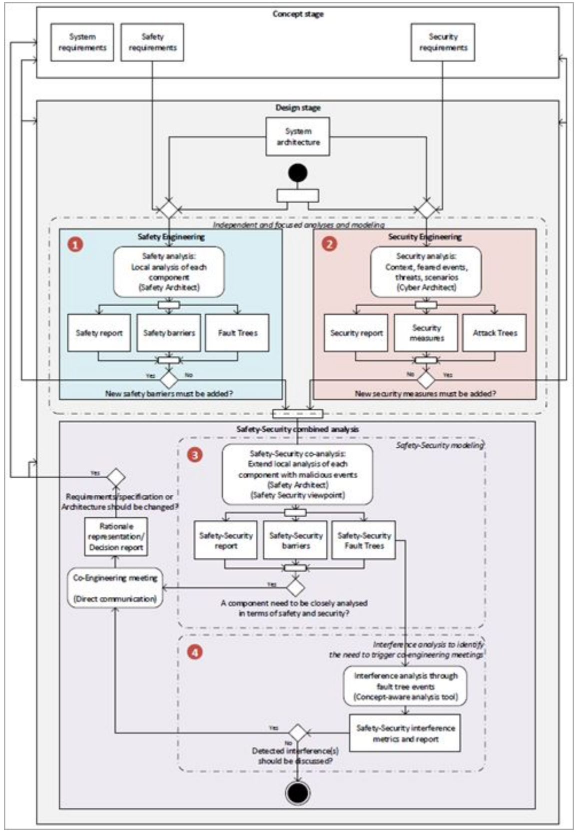
Safety and Security Co-Engineering

What triggers trade-off meetings ?

- They may either be
  - Scheduled
  - Triggered… when?
    - → a sufficient critical mass of interference need to be treated
- How this may be measured?

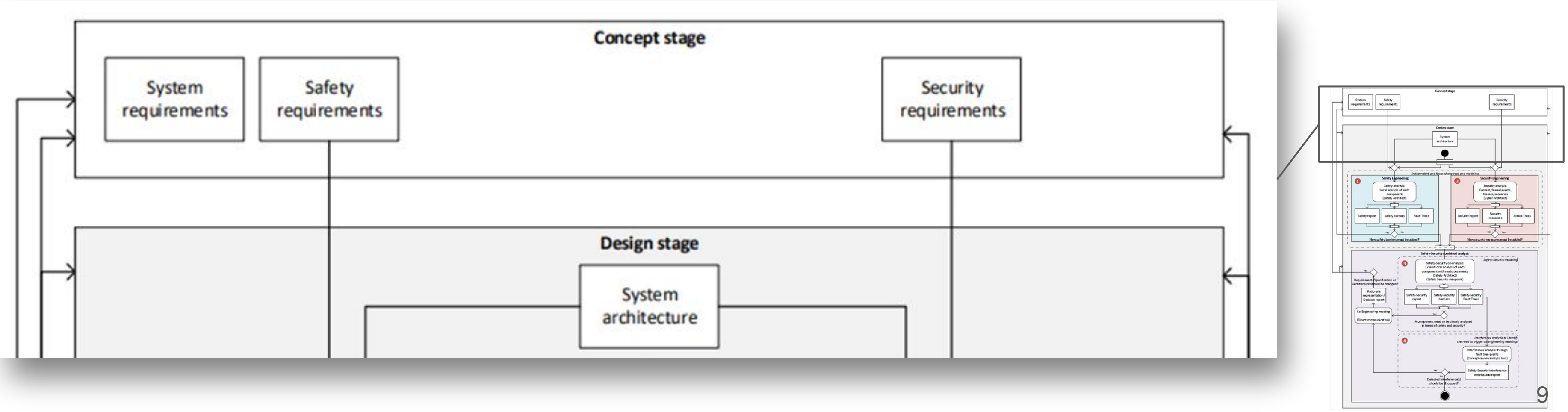
Safety-security co-analysis in the design stage with interference analysis

- A reusable process for safety security co-engineering in the design stage
  - Instantiated in two case studies
- With interference analysis support to trigger co-engineering meetings and conceptual/design refinements


Concept stage
System requirements
Safety requirements
Security requirements
Design stage
System architecture
Independent and focused analyses and modeling
1
Safety Engineering
Safety analysis: Local analysis of each component (Safety Architect)
Safety report
Safety barriers
Fault Trees
Yes
No
New safety barriers must be added?
2
Security Engineering
Security analysis: Context, feared events, threats, scenarios (Cyber Architect)
Security report
Security measures
Attack Trees
No
Yes
New security measures must be added?
Safety-Security combined analysis
Safety-Security modeling
3
Safety-Security co-analysis: Extend local analysis of each component with malicious events (Safety Architect) (Safety Security viewpoint)
Safety-Security report
Safety-Security barriers
Safety-Security Fault Trees
Yes
A component need to be closely analysed in terms of safety and security?
Co-Engineering meeting (Direct communication)
Rationale representation/ Decision report
Yes
Requirements/specification or Architecture should be changed?
4
Interference analysis to identify the need to trigger co-engineering meetings
Interference analysis through fault tree events (Concept-aware analysis tool)
Safety-Security interference metrics and report
Yes
No
Detected interference(s) should be discussed?

Safety-security co-analysis in the design stage with interference analysis

- Concept stage and initial system architecture is available



Concept stage

System requirements

Safety requirements

Security requirements

Design stage

System architecture

Independent and focused analyses and modeling

1 Safety Engineering

Safety analysis: Local analysis of each component (Safety Architect)

Safety report

Safety barriers

Fault Trees

Yes No

New safety barriers must be added?

2 Security Engineering

Security analysis: Context, feared events, threats, scenarios (Cyber Architect)

Security report

Security measures

Attack Trees

No Yes

New security measures must be added?

Safety-Security combined analysis

Safety-Security modeling

3

Safety-Security co-analysis: Extend local analysis of each component with malicious events (Safety Architect) (Safety Security viewpoint)

Safety-Security report

Safety-Security barriers

Safety-Security Fault Trees

Yes

A component need to be closely analysed in terms of safety and security?

Yes

Requirements/specification or Architecture should be changed?

Rationale representation/ Decision report

Co-Engineering meeting (Direct communication)

4

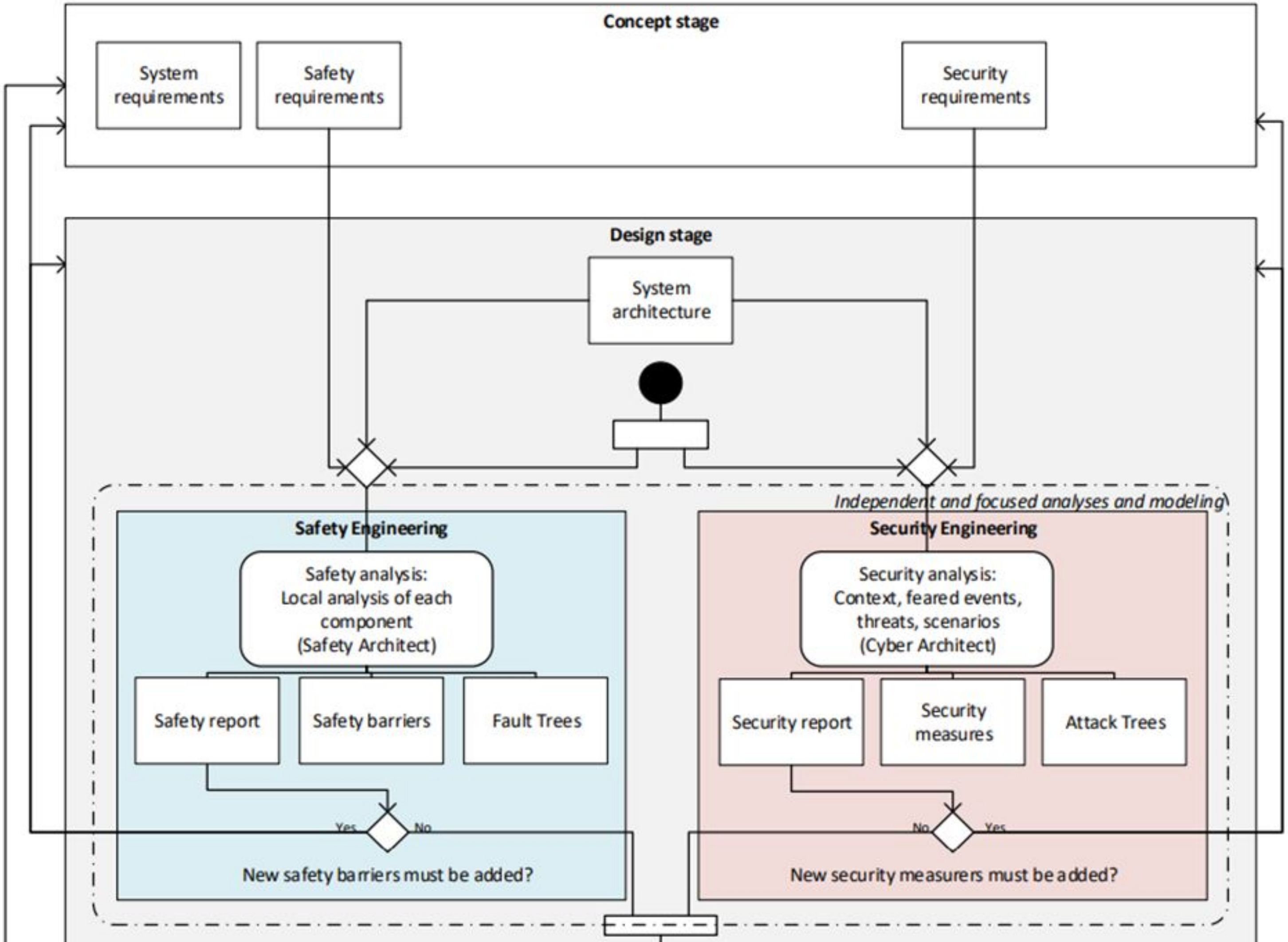
Interference analysis to identify the need to trigger co-engineering meetings

Interference analysis through fault tree events (Concept-aware analysis tool)

Safety-Security interference metrics and report

Yes No

Detected interference(s) should be discussed?



Concept stage

System requirements

Safety requirements

Security requirements

Design stage

System architecture

Independent and focused analyses and modeling

Safety Engineering

Safety analysis: Local analysis of each component (Safety Architect)

Safety report

Safety barriers

Fault Trees

Yes

No

New safety barriers must be added?

Security Engineering

Security analysis: Context, feared events, threats, scenarios (Cyber Architect)

Security report

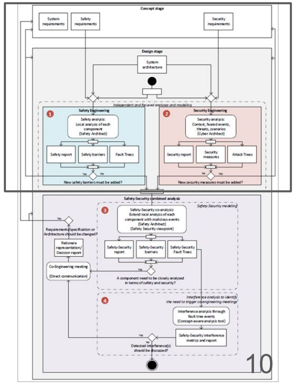
Security measures

Attack Trees

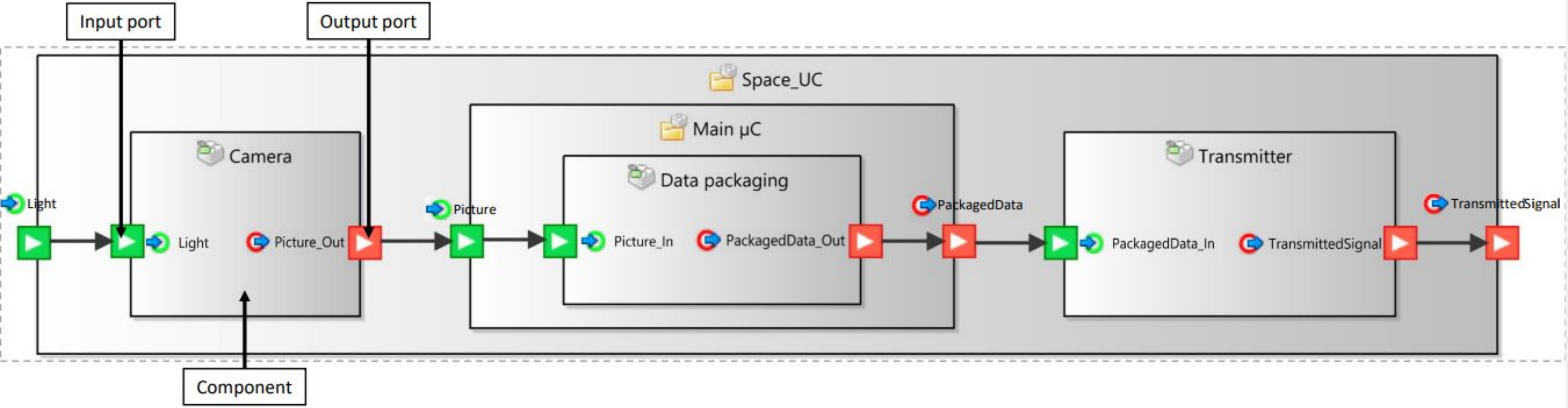
No

Yes

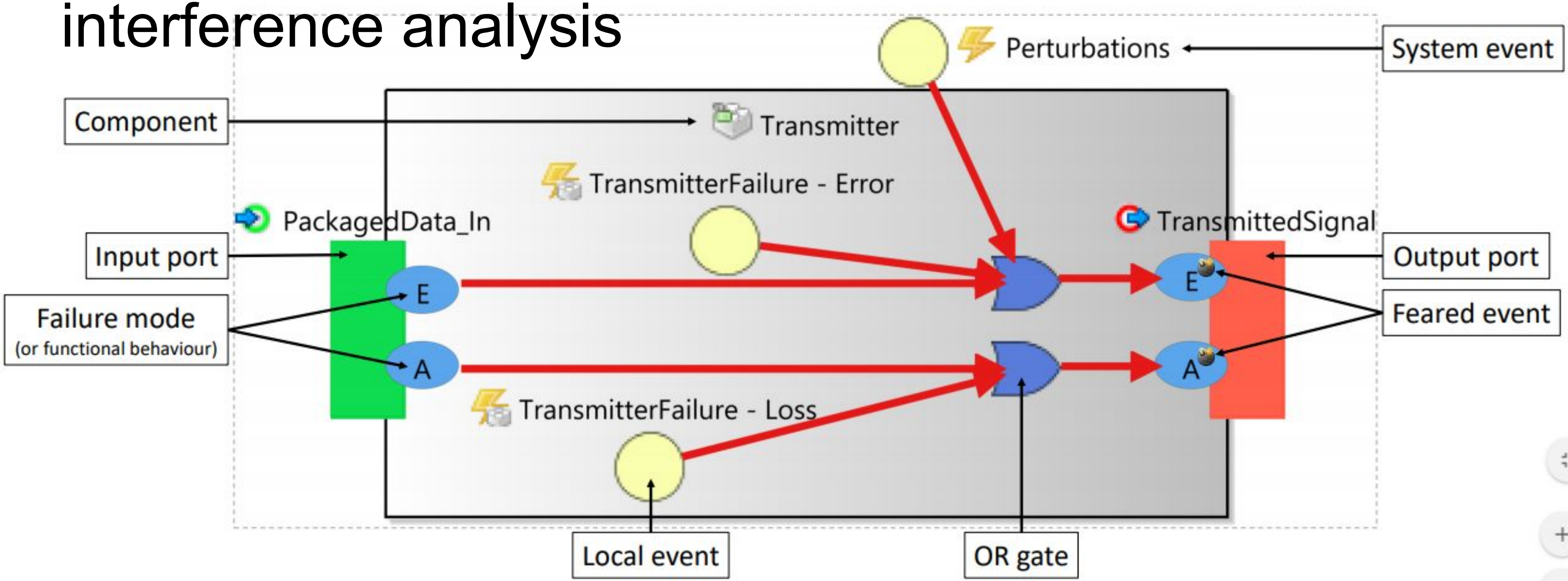
New security measurers must be added?



Safety-security co-analysis in the design stage with interference analysis



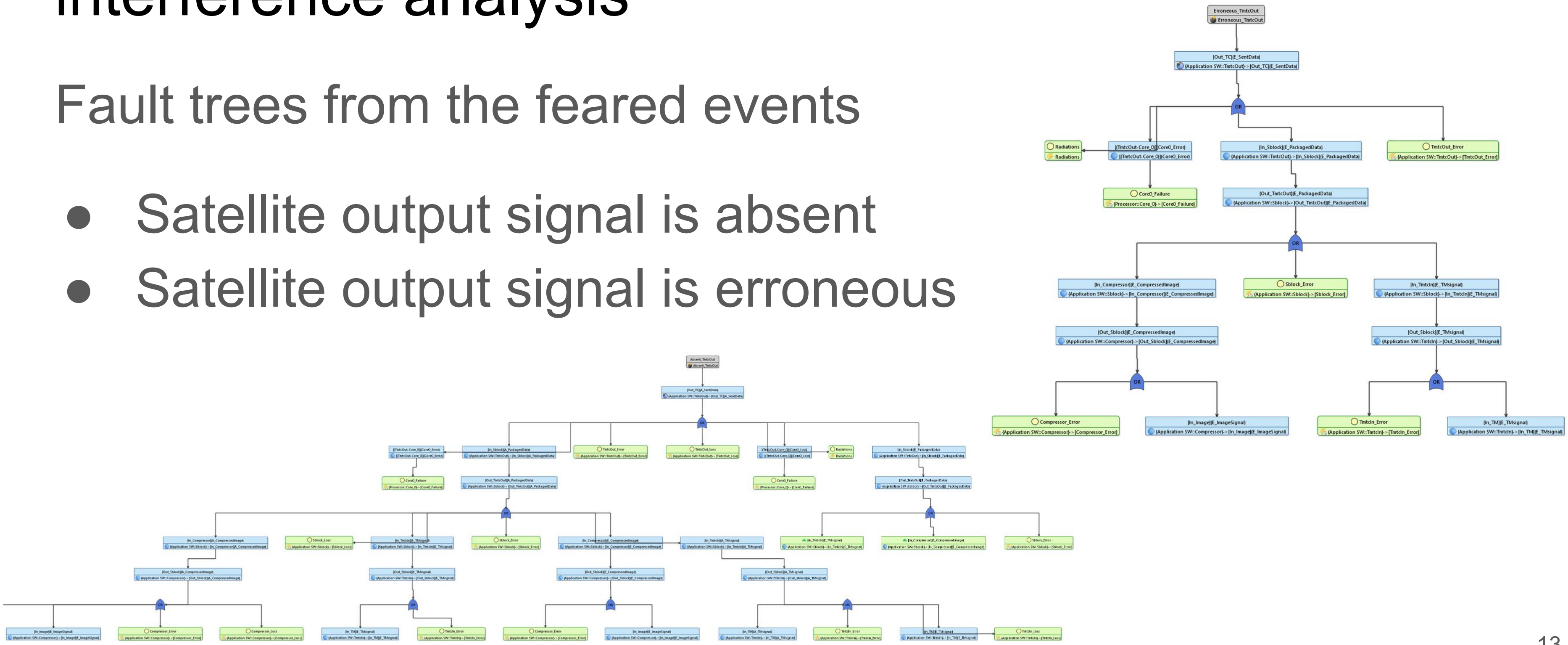
Safety-security co-analysis in the design stage with interference analysis



Safety-security co-analysis in the design stage with interference analysis

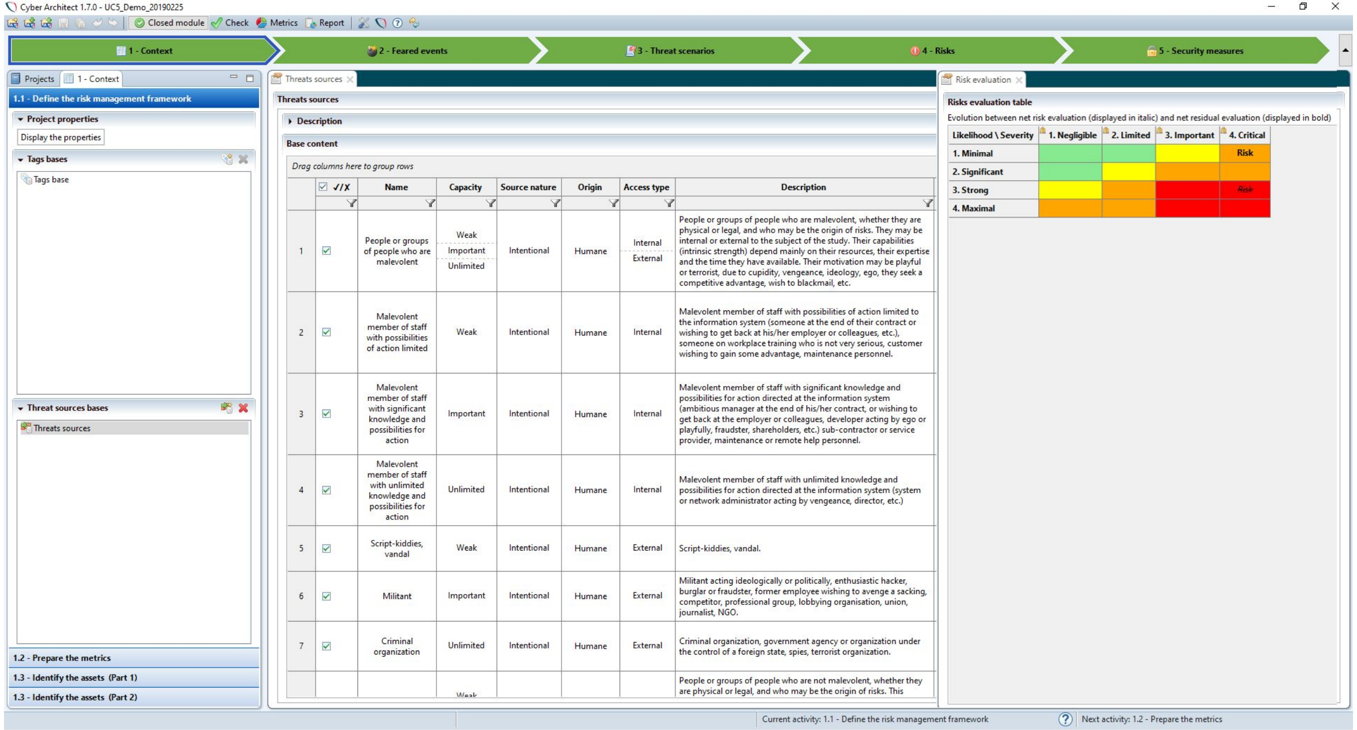
Fault trees from the feared events

- Satellite output signal is absent
- Satellite output signal is erroneous



Erroneous_TmtcOut
Erroneous_TmtcOut
[Out_TC](E_SentData)
{Application SW::TmtcOut}->[Out_TC](E_SentData)
OR
Radiations
Radiations
[(TmtcOut-Core_0)](Core0_Error)
[(TmtcOut-Core_0)](Core0_Error)
[In_Sblock](E_PackagedData)
{Application SW::TmtcOut}->[In_Sblock](E_PackagedData)
TmtcOut_Error
{Application SW::TmtcOut}->[TmtcOut_Error]
Core0_Failure
{Processor::Core_0}->[Core0_Failure]
[Out_TmtcOut](E_PackagedData)
{Application SW::Sblock}->[Out_TmtcOut](E_PackagedData)
OR
[In_Compressor](E_CompressedImage)
{Application SW::Sblock}->[In_Compressor](E_CompressedImage)
Sblock_Error
{Application SW::Sblock}->[Sblock_Error]
[In_TmtcIn](E_TMsignal)
{Application SW::Sblock}->[In_TmtcIn](E_TMsignal)
[Out_Sblock](E_CompressedImage)
{Application SW::Compressor}->[Out_Sblock](E_CompressedImage)
[Out_Sblock](E_TMsignal)
{Application SW::TmtcIn}->[Out_Sblock](E_TMsignal)
OR
OR
Compressor_Error
{Application SW::Compressor}->[Compressor_Error]
[In_Image](E_ImageSignal)
{Application SW::Compressor}->[In_Image](E_ImageSignal)
TmtcIn_Error
{Application SW::TmtcIn}->[TmtcIn_Error]
[In_TM](E_TMsignal)
{Application SW::TmtcIn}->[In_TM](E_TMsignal)
Absent_TmtcOut
Absent_TmtcOut
[Out_TC](A_SentData)
{Application SW::TmtcOut}->[Out_TC](A_SentData)
OR
[(TmtcOut-Core_0)](Core0_Error)
[(TmtcOut-Core_0)](Core0_Error)
[In_Sblock](A_PackagedData)
{Application SW::TmtcOut}->[In_Sblock](A_PackagedData)
TmtcOut_Error
{Application SW::TmtcOut}->[TmtcOut_Error]
TmtcOut_Loss
{Application SW::TmtcOut}->[TmtcOut_Loss]
[(TmtcOut-Core_0)](Core0_Loss)
[(TmtcOut-Core_0)](Core0_Loss)
Radiations
Radiations
[In_Sblock](E_PackagedData)
{Application SW::TmtcOut}->[In_Sblock](E_PackagedData)
Core0_Failure
{Processor::Core_0}->[Core0_Failure]
[Out_TmtcOut](A_PackagedData)
{Application SW::Sblock}->[Out_TmtcOut](A_PackagedData)
Core0_Failure
{Processor::Core_0}->[Core0_Failure]
[Out_TmtcOut](E_PackagedData)
{Application SW::Sblock}->[Out_TmtcOut](E_PackagedData)
OR
OR
[In_Compressor](A_CompressedImage)
{Application SW::Sblock}->[In_Compressor](A_CompressedImage)
Sblock_Loss
{Application SW::Sblock}->[Sblock_Loss]
[In_TmtcIn](E_TMsignal)
{Application SW::Sblock}->[In_TmtcIn](E_TMsignal)
Sblock_Error
{Application SW::Sblock}->[Sblock_Error]
[In_Compressor](E_CompressedImage)
{Application SW::Sblock}->[In_Compressor](E_CompressedImage)
[In_TmtcIn](A_TMsignal)
{Application SW::Sblock}->[In_TmtcIn](A_TMsignal)
[In_TmtcIn](E_TMsignal)
{Application SW::Sblock}->[In_TmtcIn](E_TMsignal)
[In_Compressor](E_CompressedImage)
{Application SW::Sblock}->[In_Compressor](E_CompressedImage)
Sblock_Error
{Application SW::Sblock}->[Sblock_Error]
[Out_Sblock](A_CompressedImage)
{Application SW::Compressor}->[Out_Sblock](A_CompressedImage)
[Out_Sblock](E_TMsignal)
{Application SW::TmtcIn}->[Out_Sblock](E_TMsignal)
[Out_Sblock](E_CompressedImage)
{Application SW::Compressor}->[Out_Sblock](E_CompressedImage)
[Out_Sblock](A_TMsignal)
{Application SW::TmtcIn}->[Out_Sblock](A_TMsignal)
OR
OR
OR
OR
[In_Image](E_ImageSignal)
{Application SW::Compressor}->[In_Image](E_ImageSignal)
Compressor_Error
{Application SW::Compressor}->[Compressor_Error]
Compressor_Loss
{Application SW::Compressor}->[Compressor_Loss]
[In_TM](E_TMsignal)
{Application SW::TmtcIn}->[In_TM](E_TMsignal)
TmtcIn_Error
{Application SW::TmtcIn}->[TmtcIn_Error]
Compressor_Error
{Application SW::Compressor}->[Compressor_Error]
[In_Image](E_ImageSignal)
{Application SW::Compressor}->[In_Image](E_ImageSignal)
[In_TM](A_TMsignal)
{Application SW::TmtcIn}->[In_TM](A_TMsignal)
TmtcIn_Error
{Application SW::TmtcIn}->[TmtcIn_Error]
[In_TM](E_TMsignal)
{Application SW::TmtcIn}->[In_TM](E_TMsignal)
TmtcIn_Loss
{Application SW::TmtcIn}->[TmtcIn_Loss]

Safety-security co-analysis in the design stage with interference analysis


Cyber Architect 1.7.0 - UC5_Demo_20190225
Closed module
Check
Metrics
Report
1 - Context
2 - Feared events
3 - Threat scenarios
4 - Risks
5 - Security measures
Projects
1 - Context
1.1 - Define the risk management framework
Project properties
Display the properties
Tags bases
Tags base
Threat sources bases
Threats sources
1.2 - Prepare the metrics
1.3 - Identify the assets (Part 1)
1.3 - Identify the assets (Part 2)
Threats sources
Description
Base content
Drag columns here to group rows
Risk evaluation
Current activity: 1.1 - Define the risk management framework
Next activity: 1.2 - Prepare the metrics

Threats sources

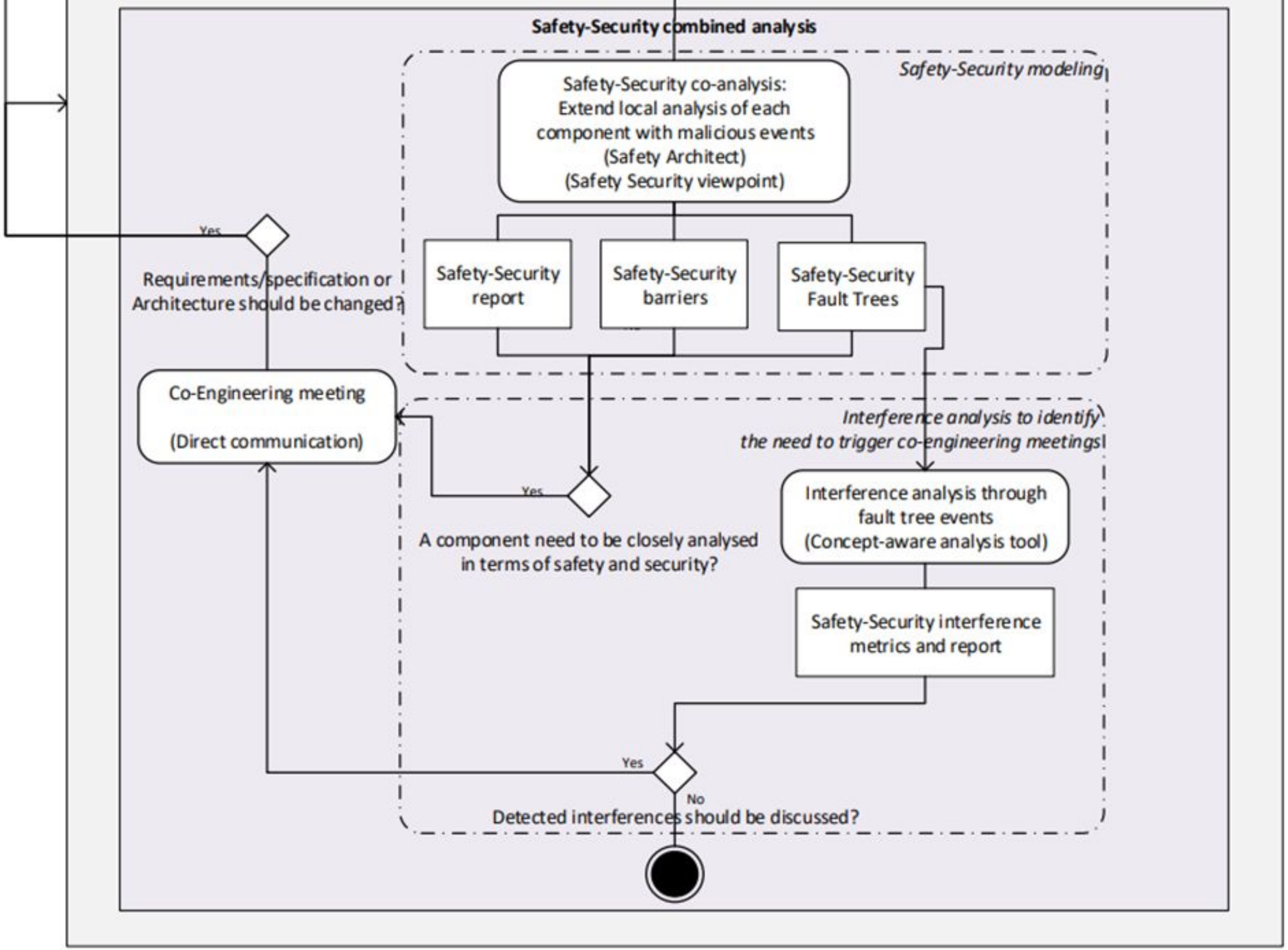
Base content

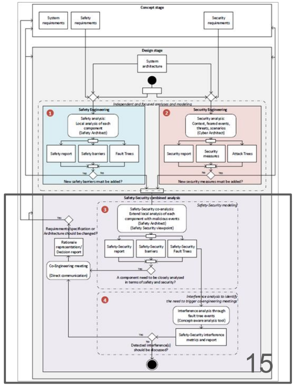
	☑ ✓/X	Name	Capacity	Source nature	Origin	Access type	Description
1	☑	People or groups of people who are malevolent	Weak Important Unlimited	Intentional	Humane	Internal External	People or groups of people who are malevolent, whether they are physical or legal, and who may be the origin of risks. They may be internal or external to the subject of the study. Their capabilities (intrinsic strength) depend mainly on their resources, their expertise and the time they have available. Their motivation may be playful or terrorist, due to cupidity, vengeance, ideology, ego, they seek a competitive advantage, wish to blackmail, etc.
2	☑	Malevolent member of staff with possibilities of action limited	Weak	Intentional	Humane	Internal	Malevolent member of staff with possibilities of action limited to the information system (someone at the end of their contract or wishing to get back at his/her employer or colleagues, etc.), someone on workplace training who is not very serious, customer wishing to gain some advantage, maintenance personnel.
3	☑	Malevolent member of staff with significant knowledge and possibilities for action	Important	Intentional	Humane	Internal	Malevolent member of staff with significant knowledge and possibilities for action directed at the information system (ambitious manager at the end of his/her contract, or wishing to get back at the employer or colleagues, developer acting by ego or playfully, fraudster, shareholders, etc.) sub-contractor or service provider, maintenance or remote help personnel.
4	☑	Malevolent member of staff with unlimited knowledge and possibilities for action	Unlimited	Intentional	Humane	Internal	Malevolent member of staff with unlimited knowledge and possibilities for action directed at the information system (system or network administrator acting by vengeance, director, etc.)
5	☑	Script-kiddies, vandal	Weak	Intentional	Humane	External	Script-kiddies, vandal.
6	☑	Militant	Important	Intentional	Humane	External	Militant acting ideologically or politically, enthusiastic hacker, burglar or fraudster, former employee wishing to avenge a sacking, competitor, professional group, lobbying organisation, union, journalist, NGO.
7	☑	Criminal organization	Unlimited	Intentional	Humane	External	Criminal organization, government agency or organization under the control of a foreign state, spies, terrorist organization.
			Weak				People or groups of people who are not malevolent, whether they are physical or legal, and who may be the origin of risks. This

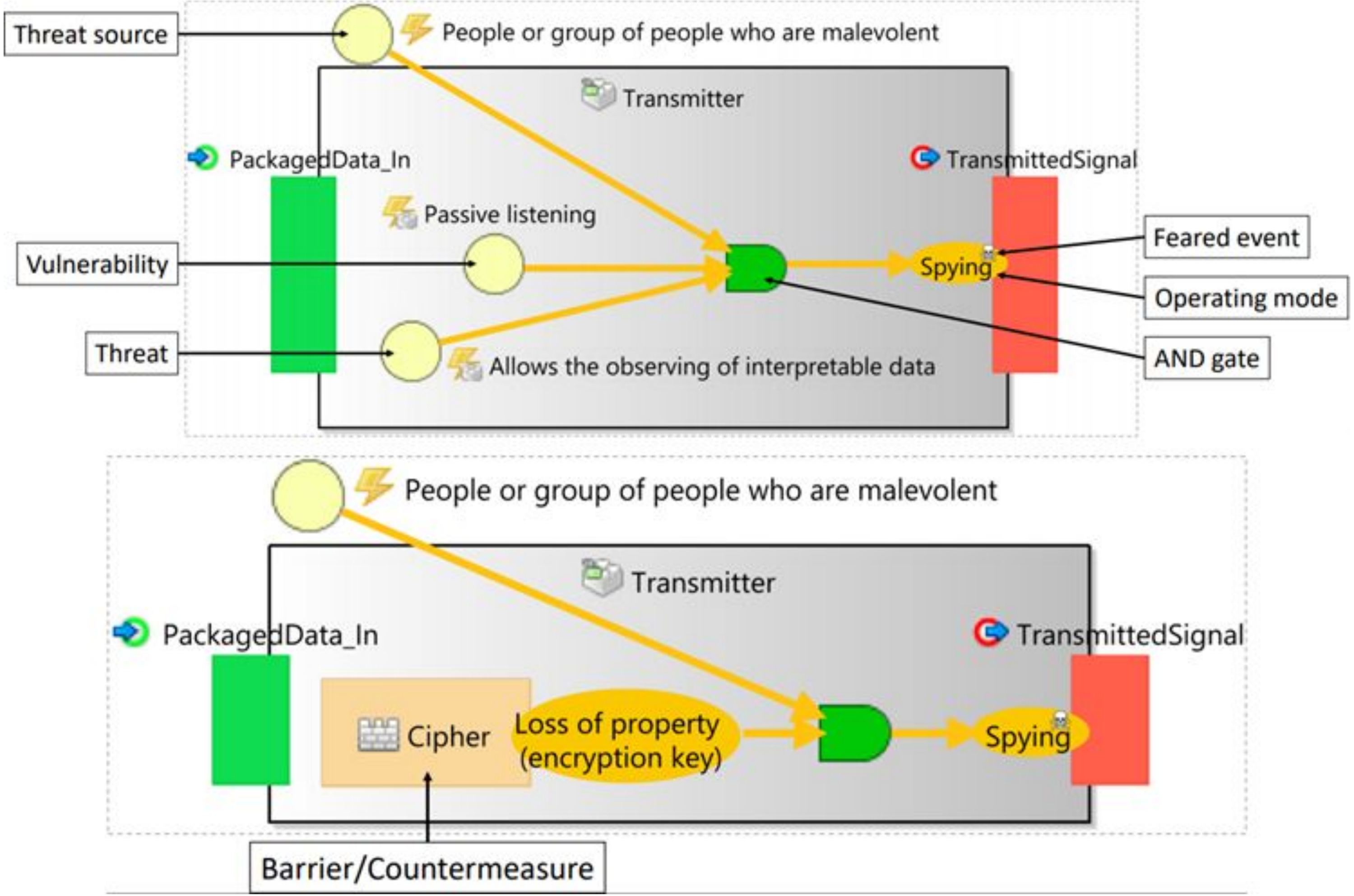
Risks evaluation table

Evolution between net risk evaluation (displayed in italic) and net residual evaluation (displayed in bold)

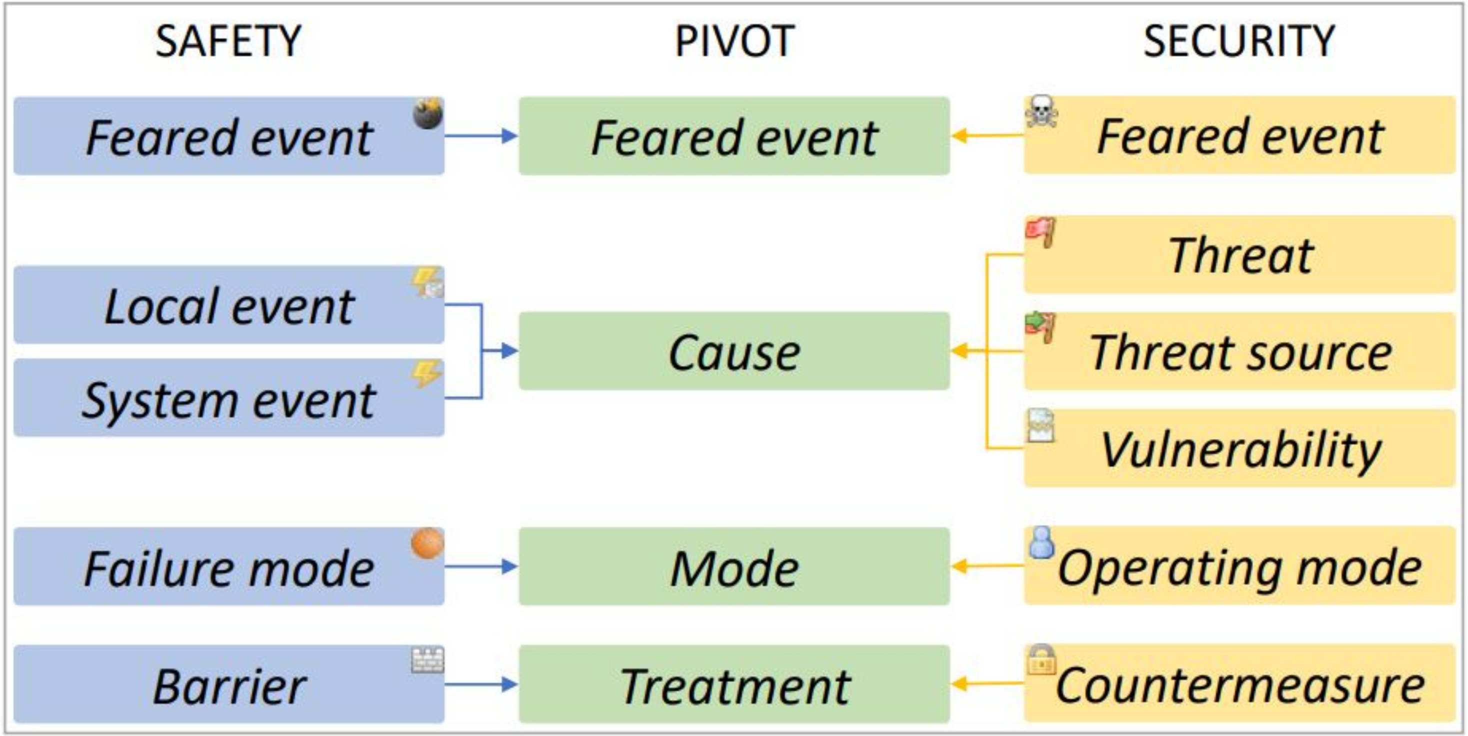
Likelihood \ Severity	1. Negligible	2. Limited	3. Important	4. Critical
1. Minimal	🟩	🟩	🟨	🟧 **Risk**
2. Significant	🟩	🟨	🟧	🟧
3. Strong	🟨	🟧	🟥	🟥 ~~*Risk*~~
4. Maximal	🟧	🟧	🟥	🟥


Safety-Security combined analysis
Safety-Security modeling
Safety-Security co-analysis:
Extend local analysis of each
component with malicious events
(Safety Architect)
(Safety Security viewpoint)
Safety-Security report
Safety-Security barriers
Safety-Security Fault Trees
Yes
Requirements/specification or
Architecture should be changed?
Co-Engineering meeting
(Direct communication)
Interference analysis to identify
the need to trigger co-engineering meetings
Yes
A component need to be closely analysed
in terms of safety and security?
Interference analysis through
fault tree events
(Concept-aware analysis tool)
Safety-Security interference
metrics and report
Yes
No
Detected interferences should be discussed?

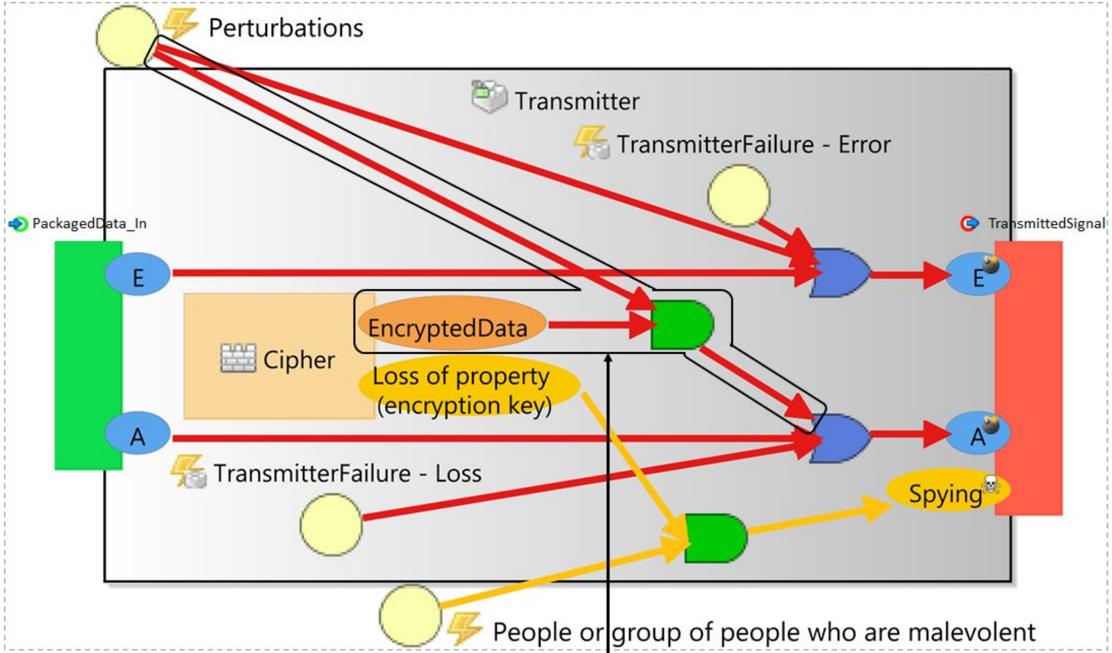



Threat source
People or group of people who are malevolent
Transmitter
PackagedData_In
TransmittedSignal
Passive listening
Vulnerability
Threat
Allows the observing of interpretable data
Spying
Feared event
Operating mode
AND gate
People or group of people who are malevolent
Transmitter
PackagedData_In
TransmittedSignal
Cipher
Loss of property (encryption key)
Spying
Barrier/Countermeasure

Safety-security co-analysis in the design stage with interference analysis

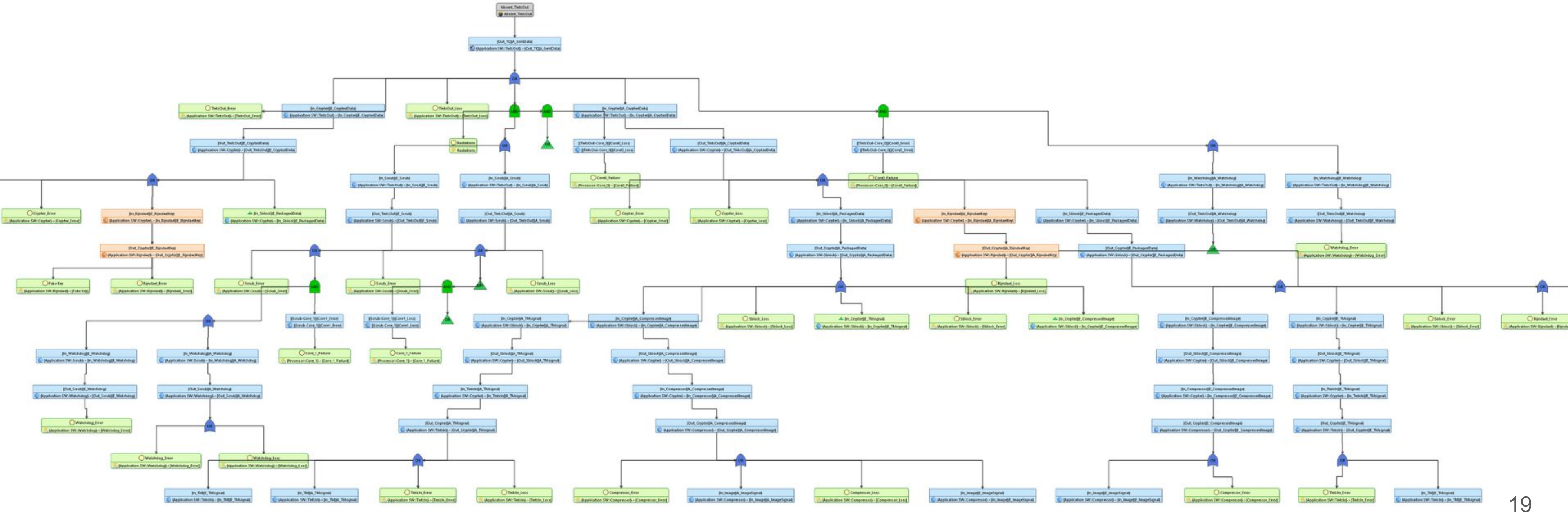


Safety-security co-analysis in the design stage with interference analysis



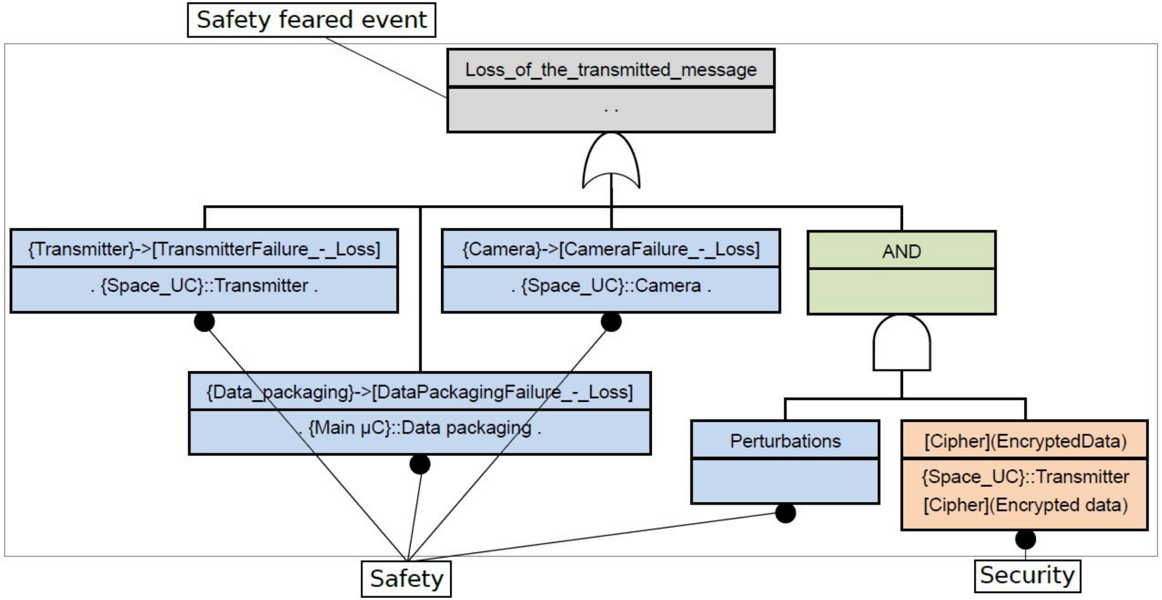
New safety propagation caused by the integration of the security countermeasure

Safety-security co-analysis in the design stage with interference analysis


Absent_TielcOut
[Out_TC][A_SentData]
[Application SW::TielcOut] - [Out_TC][A_SentData]
OR
AND
TielcOut_Error
[In_Crypter][E_CryptedData]
TielcOut_Loss
[In_Crypter][A_CryptedData]
[Out_TielcOut][E_CryptedData]
Radiations
[TielcOut-Core_0][Core0_Loss]
[Out_TielcOut][A_CryptedData]
[TielcOut-Core_0][Core0_Error]
[In_Scrub][E_Scrub]
[In_Scrub][A_Scrub]
Core0_Failure
[Processor::Core_0] - [Core0_Failure]
Crypter_Error
Crypter_Loss
[In_Rjndael][E_RjndaelKey]
[In_Rjndael][A_RjndaelKey]
[In_Sblock][A_PackagedData]
[In_Sblock][E_PackagedData]
[In_Watchdog][A_Watchdog]
[In_Watchdog][E_Watchdog]
[Out_TielcOut][A_Watchdog]
[Out_TielcOut][E_Watchdog]
Watchdog_Error
Watchdog_Loss
Fake Key
Rjndael_Error
Rjndael_Loss
Scrub_Error
Scrub_Loss
Core_1_Failure
Sblock_Loss
Sblock_Error
[In_Crypter][A_TMsignal]
[In_Crypter][A_CompressedImage]
[In_Crypter][E_CompressedImage]
[In_Crypter][E_TMsignal]
[In_Compressor][A_CompressedImage]
[In_Compressor][E_CompressedImage]
[In_TmtcIn][A_TMsignal]
[In_TmtcIn][E_TMsignal]
TmtcIn_Error
TmtcIn_Loss
Compressor_Error
Compressor_Loss
[In_Image][A_ImageSignal]
[In_Image][E_ImageSignal]
[In_TM][A_TMsignal]
[In_TM][E_TMsignal]

Safety-security co-analysis in the design stage with interference analysis

Illustrative excerpt

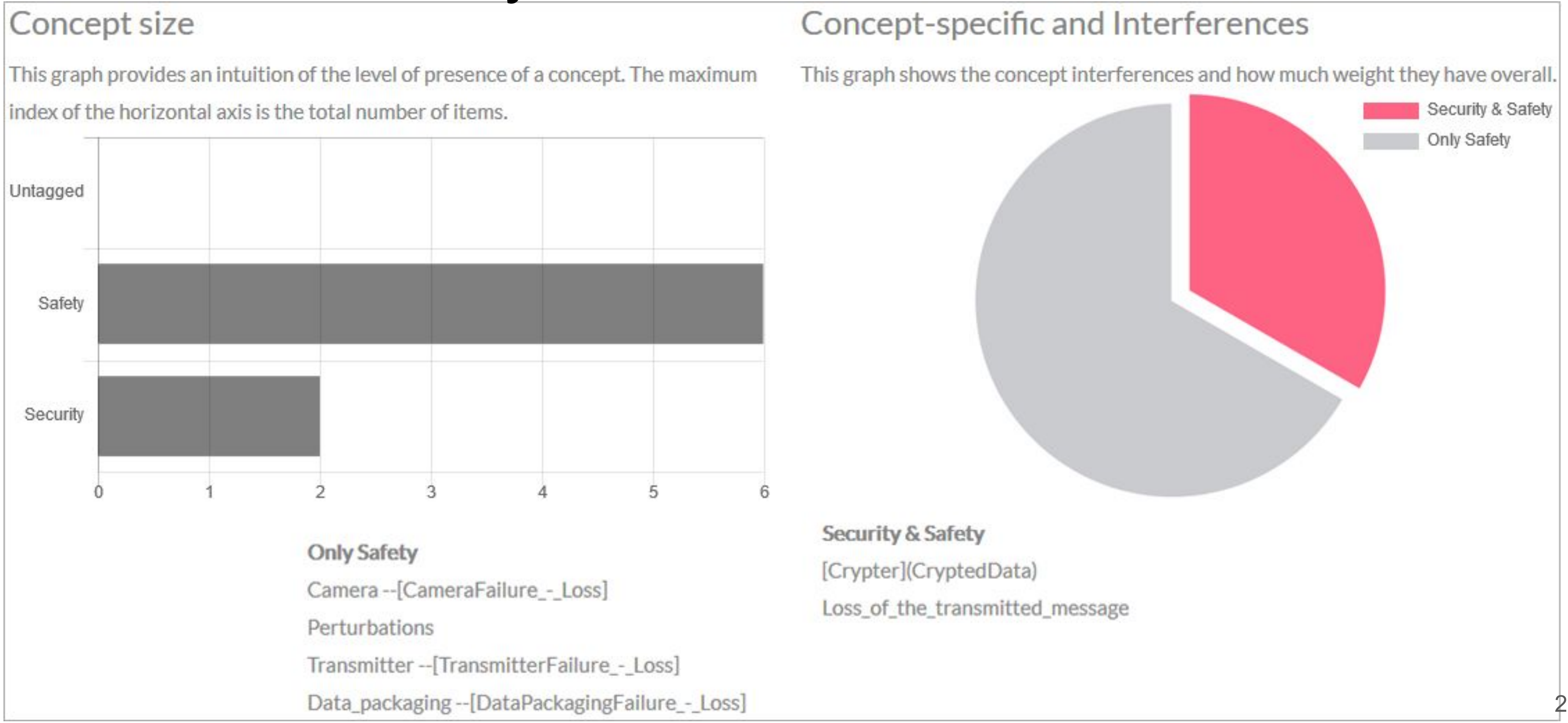

Safety feared event
Loss_of_the_transmitted_message
. .
{Transmitter}->[TransmitterFailure_-_Loss]
. {Space_UC}::Transmitter .
{Camera}->[CameraFailure_-_Loss]
. {Space_UC}::Camera .
AND
{Data_packaging}->[DataPackagingFailure_-_Loss]
. {Main µC}::Data packaging .
Perturbations
[Cipher](EncryptedData)
{Space_UC}::Transmitter
[Cipher](Encrypted data)
Safety
Security

Safety-security co-analysis in the design stage with interference analysis

Formal Concept Analysis

- To identify the number of fault tree events which are specific/exclusive to a quality attribute
- To identify the size of the intersections of the quality attributes

Safety-security co-analysis in the design stage with interference analysis



Concept size

This graph provides an intuition of the level of presence of a concept. The maximum index of the horizontal axis is the total number of items.

Only Safety

Camera --[CameraFailure_-_Loss]

Perturbations

Transmitter --[TransmitterFailure_-_Loss]

Data_packaging --[DataPackagingFailure_-_Loss]

Concept-specific and Interferences

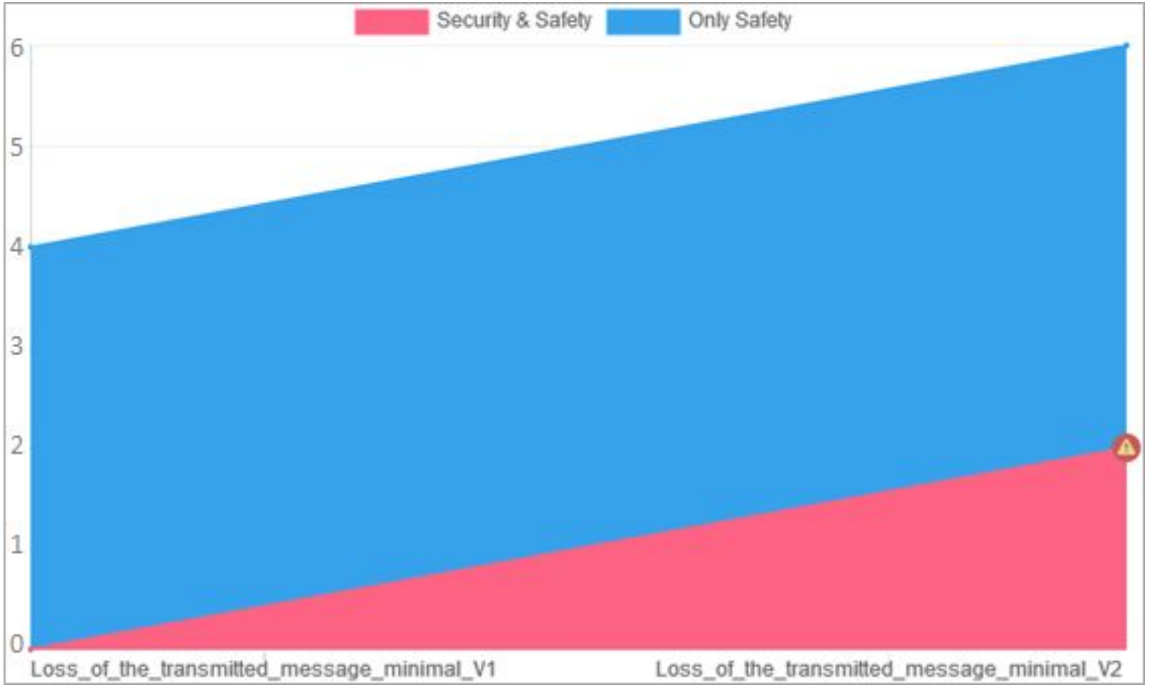
This graph shows the concept interferences and how much weight they have overall.

Security & Safety

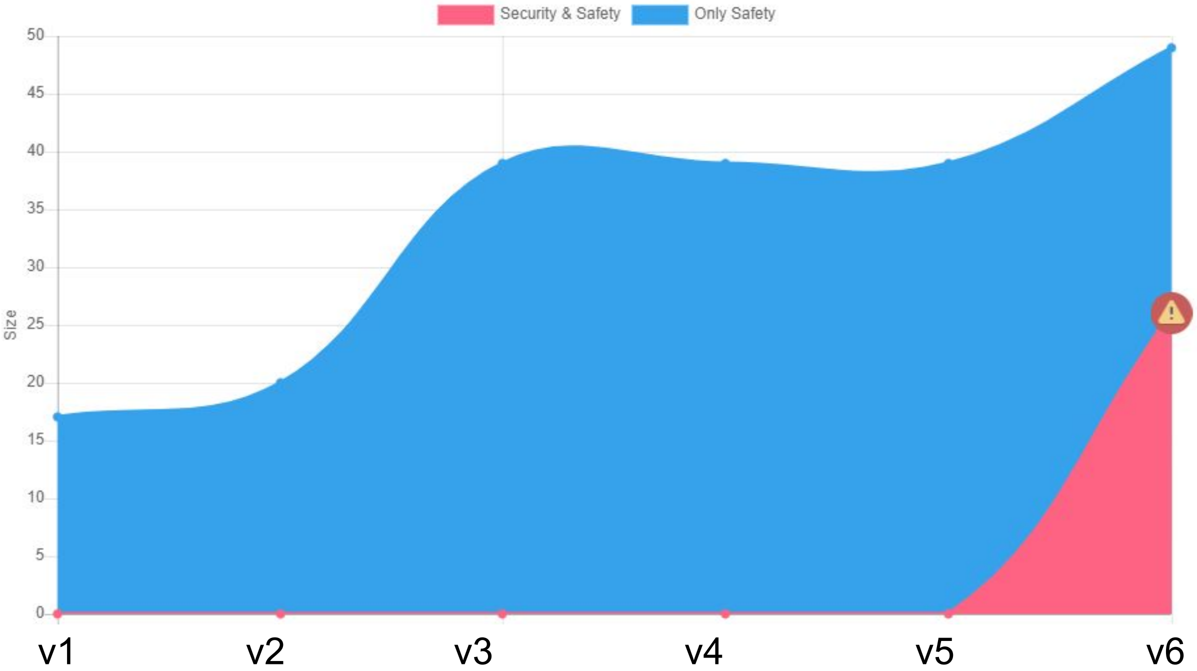
[Crypter](CryptedData)

Loss_of_the_transmitted_message

Safety-security co-analysis in the design stage with interference analysis



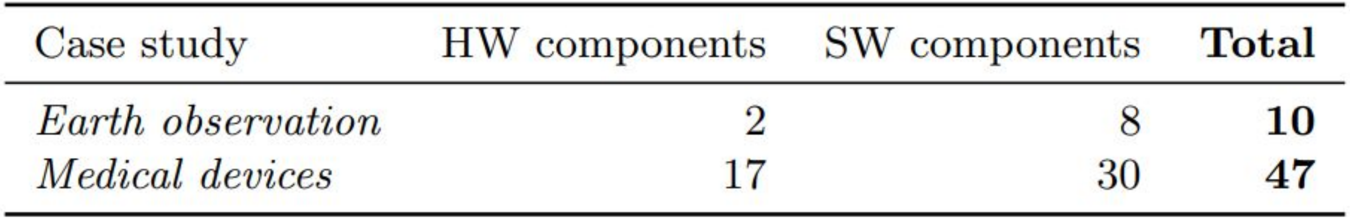
Safety-security co-analysis in the design stage with interference analysis



Discussion from the industrial partners

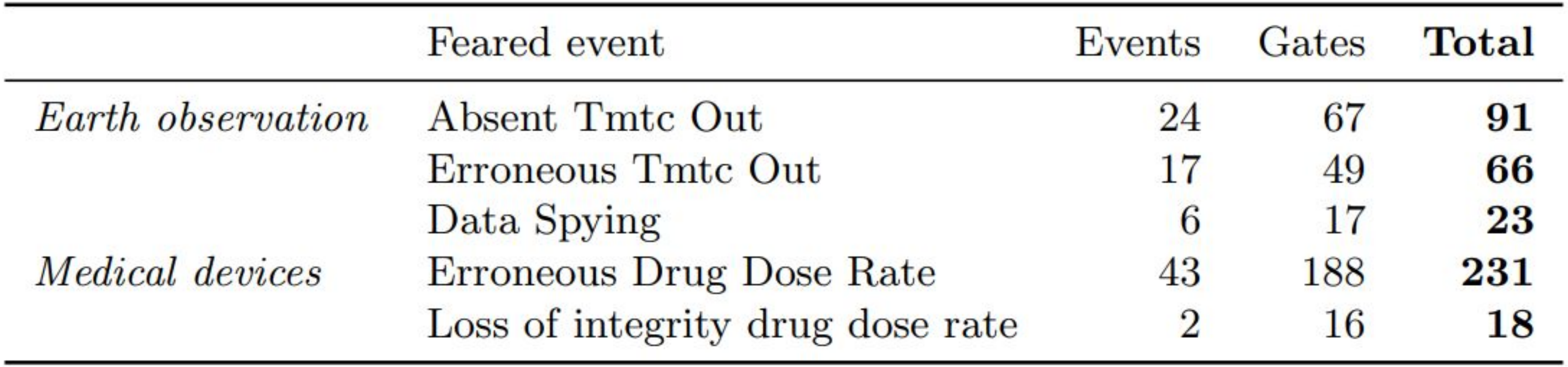
Size of the two industrial pilots

Number of components (HW: Hardware, SW: Software) for the two pilots



Case study	HW components	SW components	**Total**
Earth observation	2	8	**10**
Medical devices	17	30	**47**

Elements in the fault trees (Tmtc: Tele-Metrics to TeleCommunication)



	Feared event	Events	Gates	**Total**
Earth observation	Absent Tmtc Out	24	67	**91**
	Erroneous Tmtc Out	17	49	**66**
	Data Spying	6	17	**23**
Medical devices	Erroneous Drug Dose Rate	43	188	**231**
	Loss of integrity drug dose rate	2	16	**18**

Discussion from the industrial partners

Thales Alenia Space (Earth observation project)

- In the context of large projects, different teams lack of visibility of the fine-grained details.
- The high level report can help to make “trade-offs” decisions at the design stage.
- It should be analysed to check whether the elements in the interference requires a decision, an action, or introduces a trade-off.

Discussion from the industrial partners

RGB Medical Devices (Medical device project)

- The proposed co-engineering method is a structured method that can help refining the design.
- An approach to be sure that issues related to saf-sec interference were considered, and eventually, discussed and treated.
- It may led to improve significantly the detection of interferences between safety and security requirements at early stages of the design. Positive impact on the reduction of cost and time.
- Drawback: Possible significant learning curve.

Conclusions

Contribution:

A method for co-engineering in the design stage based on enriching components' local analyses and enabling interference analysis

Objective:

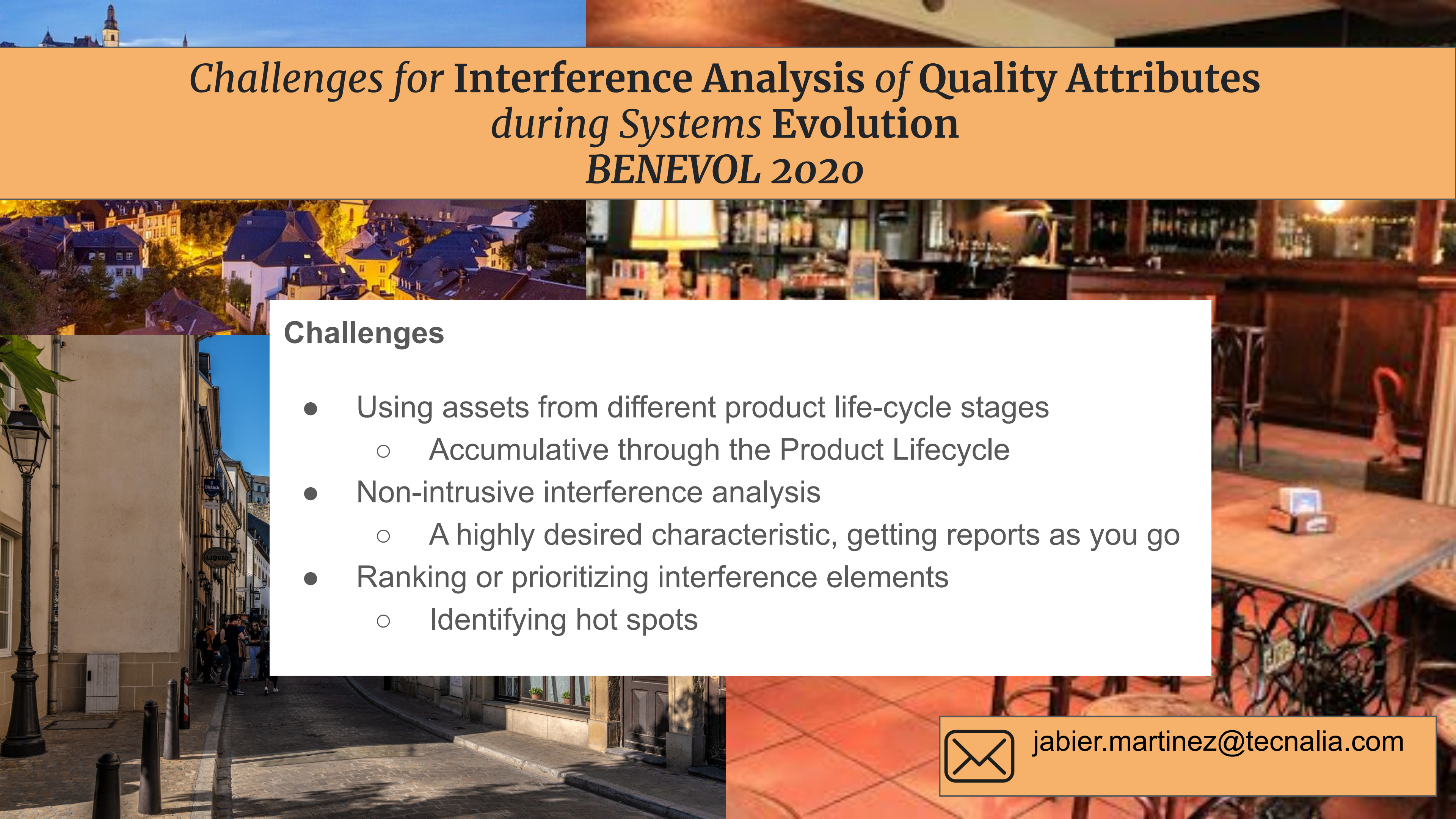
Avoid the late identification of issues and conflicts between safety and security aspects

Artefacts:

System-level reports on safety-security interference through generated fault tree models. They quantify the interference at a given point in time as well as from the historic of changes.

Challenges

- Using assets from different product life-cycle stages
  - Accumulative through the Product Lifecycle
- Non-intrusive interference analysis
  - A highly desired characteristic, getting reports as you go
- Ranking or prioritizing interference elements
  - Identifying hot spots



Challenges for **Interference Analysis** *of* **Quality Attributes** *during Systems* **Evolution** *BENEVOL 2020*

Challenges

- Using assets from different product life-cycle stages
  - Accumulative through the Product Lifecycle
- Non-intrusive interference analysis
  - A highly desired characteristic, getting reports as you go
- Ranking or prioritizing interference elements
  - Identifying hot spots

jabier.martinez@tecnalia.com