

SESAR



Engage

Collaborative cyber security management framework

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287

Project objectives

- Develop a CONOPS for collaborative cyber security management
- Create a prototype for collaborative exchange of cyber security design
- Evolve risk assessment approaches, including quantified risk

- The development of security management needs as much emphasis as safety management
- We need to ‘zoom out’
 - top-down architecture driven
 - system of systems
 - same, similar and shared assets
 - audit friendly
- Cyber security is instinctively done in siloes – we need to share by default
- We need productivity tools to make the best use of all experts (not only cyber)
- Risk needs to be articulated more

Pathways to cyber resilience in aviation



Ensuring systemic risk assessment and prioritization. Knowing what needs to be protected is the first step to advancing systemic cyber resilience. ✓

A collaborative approach from all actors in the aviation value chain should be leveraged, building on a strong history of safety management systems and cross-sector safety collaboration. ✓

Existing practices of information security management systems and corporate governance are inherently limited to individual organizations. This means that governing and managing cybersecurity and its related risks are often not performed beyond the perimeter of the organization. ✓

Current risk-assurance practices rely on resource-intensive and laborious mechanisms that are unable to keep up with the scale and pace of change in supply chains. This leaves organizations with increasing unknown residual risks and blind spots that further exacerbate exposure to cyberattacks. ✓

Aviation ISAC also plays an important role in facilitating collaboration across the industry by sharing threat-intelligence analysis, and through action-oriented working groups. However, these communities are often membership based, regional, limited to specific aviation stakeholders, and cover only certain use cases.

Collaboration must go beyond subscription to information feeds and include active participation in industry action groups. ✓

- SESAR 1 experience
- ED-201
- EASA Shared Trans-Organisational Risk Management (**STORM**)
- Safety management
- End user conversations
 - ANSPs, airports

Architecture

- Security needs to be in parallel to enterprise architecting

The new context for collaboration

- Information sharing is essential

- Prevalent on-line and in some industry contexts (A-CDM)

- Anonymisation facilitates sharing

Risk

- Semi-quantitative and quantitative approaches create a better framework for decision making

 - Prioritisation

 - Opportunity for Bayesian network analysis

(a) Identified how ATM stakeholders could enhance their collaboration on cyber security through productivity tools

(b) Evolved risk methods in ATM from purely qualitative to quantitative methods

- Adapted the SecRAM methodology to this

- Conclude that quantification does not add significant overhead to risk assessment

- Quantifying the results of risk assessment may also benefit information sharing, as the outputs of different partners are comparable, even if the underlying risk assessment methodology is different

(c) Identified how to connect risk management to architecture in a simpler, less resource intensive way

- The creation of a 'light' architecting approach has shown the benefits of visualising primary and supporting assets as functional diagrams

Three main components:

STORM1

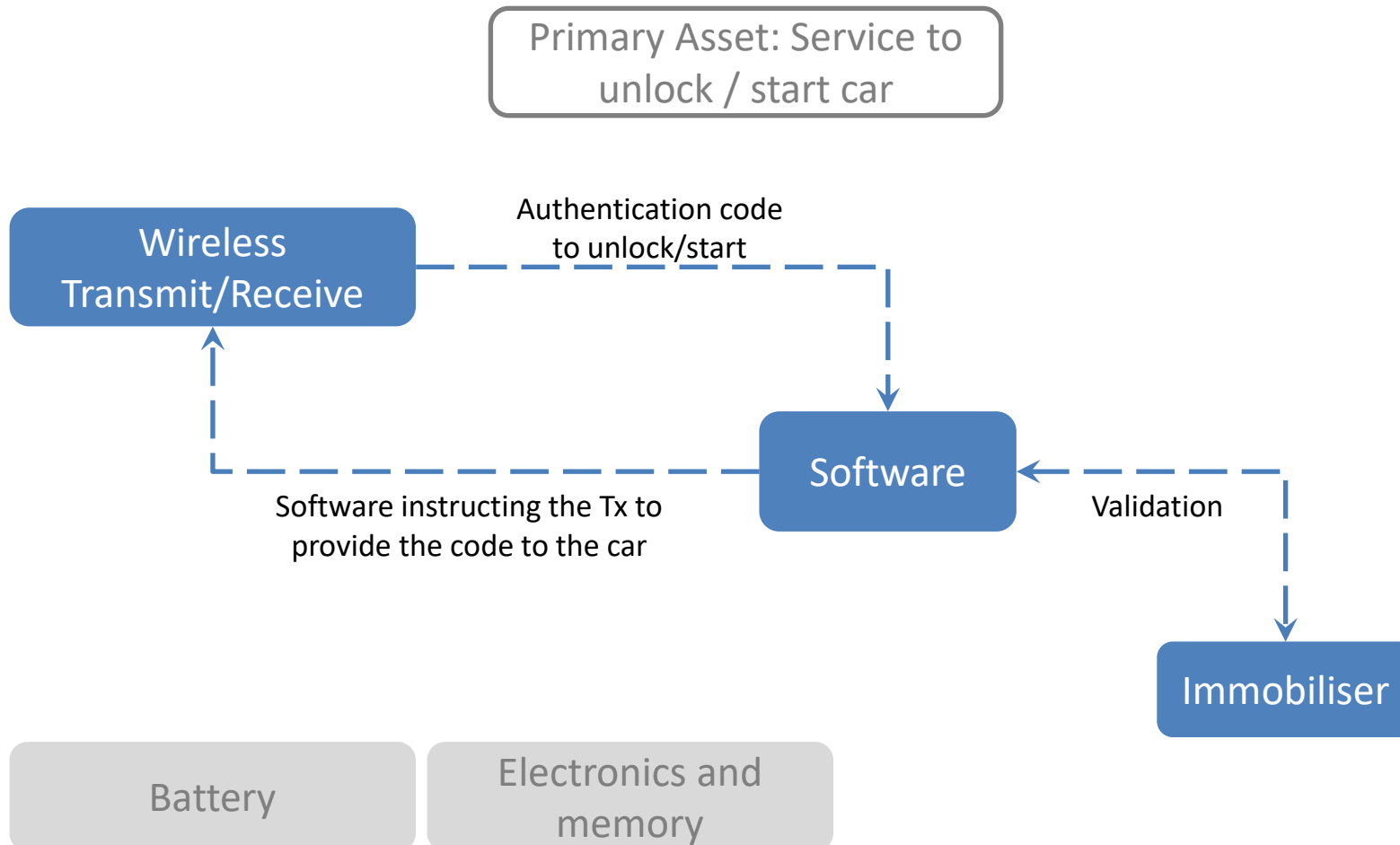
- A platform for sharing information and CONOPS experimentation:
- Developed to SESAR SecRAM 2.0 requirements
- Collaborative – multiple users can work on the same risk assessment
- Mixed Qualitative and Quantitative approaches
- Diagramming

STORM2

- APIs developed to exchange information between STORM 1 instances
- Bayesian network modelling

Example risk assessment

Chosen to be familiar for demonstrations



Quantified approach - impacts

Impact with loss of CIA for the case of many cars

Primary asset	Confidentiality	Availability	Integrity
Service to unlock the car	Inability to unlock known to others with no impact. Effects the brand image of the manufacturer, potentially leading to 5% fewer sales over 1 year while the problem is solved plus recall and repair costs).	The user will be unable to enter the vehicle. This incurs a vehicle recovery and repair and more significant brand damage as for confidentiality impact.	Any modification or deletion of data within the primary asset could lead to the user being unable to enter the vehicle, incurring a recovery and repair cost. Additional impact of car thefts may lead to increased brand damage (8% of sales lost) and insurance costs for owners.
Impact level (value)	4 (€28M: 100,000 cars recalled at a cost of 200 per fix (20M) plus profit reduction by 8M, assuming 20k revenue per car, 8% net profit margin and 5% reduction in sales).	As for confidentiality.	4 (€31M: 100,000 cars recalled at a cost of 200 per fix (20M) plus profit reduction by 11M, assuming 20k revenue per car, 8% net profit margin and 7% reduction in sales).
Service to start the car	Inability to unlock known to others with no impact.	User unable to start, incurring vehicle recovery and repair.	As for availability.
Impact level (value)	4 (€28M as above)	As for confidentiality.	As for confidentiality.
Key information	Attacker could exploit the key information leading to the theft of the vehicle.	User unable to start, incurring vehicle recovery and repair.	As for 'Service to unlock the car'.
Impact level (value)	4 (€28M as above)	As for confidentiality.	4 (€31M as above).

Quantified approach - risk

Scenario	Approach	Impact	Likelihood	Risk
1. Theft of key fob	Qualitative	Major	Likely	High
	Quantitative (Expectation Value)	€5k	53% (5)	€2.5k
2. Interception of wireless signal	Qualitative	Major	Very likely	High
	Quantitative (Expectation Value)	€5k	53% (5)	€2.5k
3. Relay of wireless transmission	Qualitative	Major	Very likely	High
	Quantitative (Expectation Value)	€31M	49% (203)	€15.2M

Prototyping quantified approach

Primary asset KeyInfo

Name	Key Information					
Description	Information to unlock car					
Type	-					
Default CIA Impacts	C	I	A	Values		
Personnel	<input type="text"/>	<input type="text"/>	<input type="text"/>			
Capacity	5	4	3	10m	1m	1k
Performance	<input type="text"/>	Loss of 60%-30% capacity				
Economic	2	2	3	5k	5k	10k
Branding	4	4	4	1m	1m	1m
Regulatory	<input type="text"/>	<input type="text"/>	<input type="text"/>			
Environment	<input type="text"/>	<input type="text"/>	<input type="text"/>			
overall	5	4	4	11m	2.01m	1.01m

Confidentiality rationale Attacker could exploit the key information leading to the theft of the vehicle

Integrity rationale User unable to start, incurring vehicle recovery and repair

Availability rationale User unable to start, incurring vehicle recovery and repair

Linked supporting assets

- ☒ **Batt-key** Battery
- ☒ **Batt-svc** Battery
- ☒ **Elex-key** Electronics and memory
- ☐ **Elex-svc** Electronics and memory
- ☒ **Fob** Key fob

◀ KeyInfo: Key Information ▶

Semi-quantitative impacts

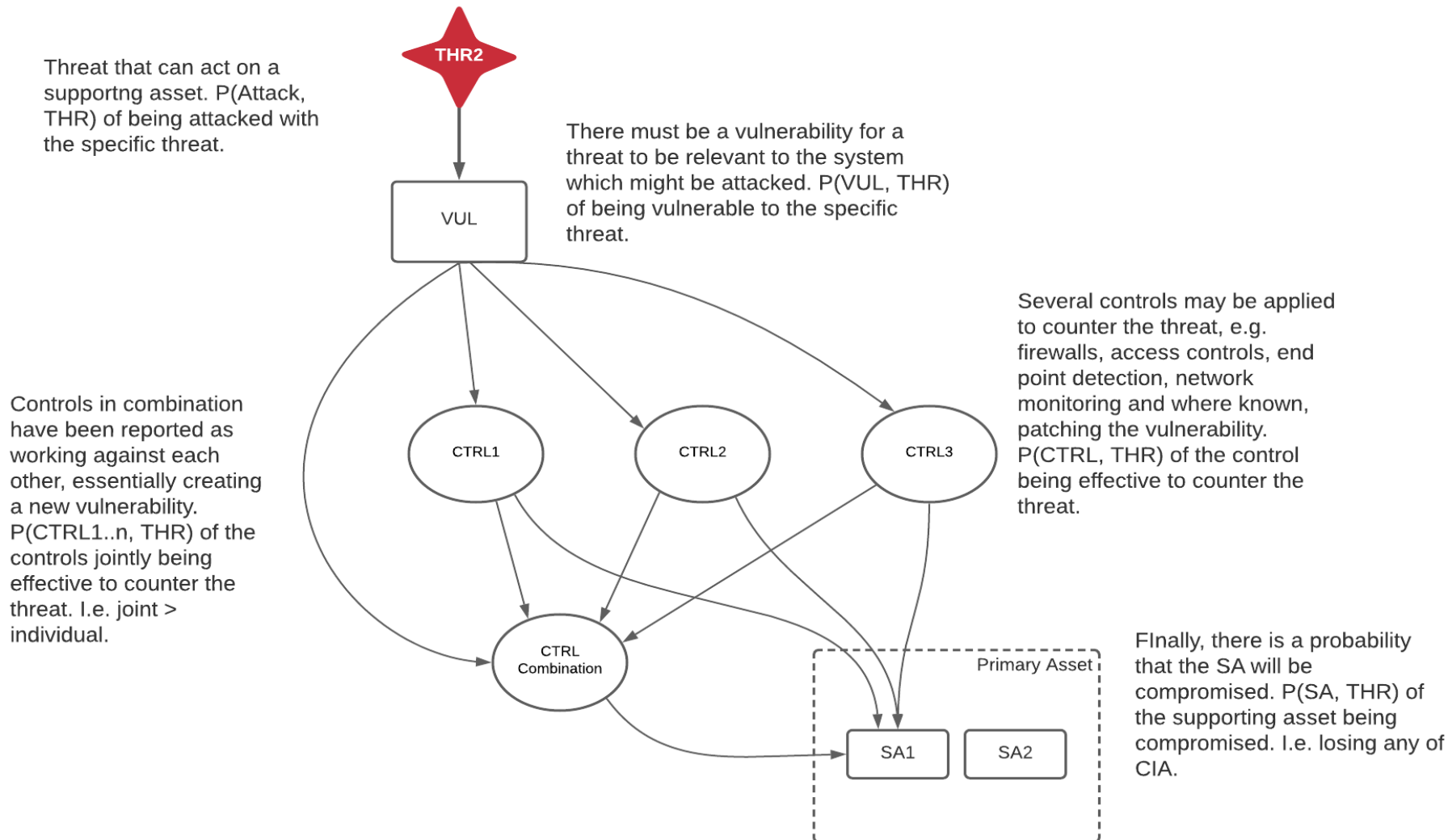
Impacts Table

This table gives the mapping between numeric values for qualitative impacts and the descriptive equivalents.

The table is editable in-place: changes are stored immediately.

Severity:	5	4	3	2	1
Units: €	Catastrophic	Critical	Severe	Minor	No impact
Personnel	Fatalities	Multiple Severe injuries	Severe injuries	Minor injuries	No injuries
Value	€1,000,000,000	€10,000,000	€10,000	€1,000	<input type="text"/> €
Capacity	Loss of 60%-100% capacity - severe impact	Loss of 60%-30% capacity	Loss of 30%-10% capacity	Loss of up to 10% capacity	No capacity loss
Value	€10,000,000	€1,000,000	€1,000	€100	<input type="text"/> €
Performance	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
Value	€50,000,000	€5,000,000	€5,000	€500	<input type="text"/> €
Economic	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income / increased expenses	No effect
Value	€50,000,000	€100,000	€10,000	€5,000	<input type="text"/> €
Branding	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
Value	€6,000,000	€1,000,000	€2,000	€400	<input type="text"/> €
Regulatory	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
Value	<input type="text"/> €	<input type="text"/> €	<input type="text"/> €	<input type="text"/> €	<input type="text"/> €
Environment	Widespread or catastrophic impact on environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short Term impact on environment	Insignificant
Value	<input type="text"/> €	<input type="text"/> €	<input type="text"/> €	<input type="text"/> €	<input type="text"/> €

Risk – BN defence in depth



Next steps

- Co-creation of the user experience with end users
- A longer period of validation
- Integration of the Bayesian Network approaches explored in this project and expansion of the role of Bayesian Networks
- Additional security hardening, to support practical use across organisational boundaries
- Extension to other risk assessment methodologies
 - while focus on the SESAR programme creates a natural harmonisation of risk assessment methods through the SecRAM, there is scope to integrate other risk methods, particularly for different domains in aviation