SESAR Engage KTN – catalyst fund project final technical report

Project title:	Collaborative cyber security management framework
Coordinator:	Winsland Ltd
Consortium partners:	Movable Type, MSDK, BULATSA
Thematic challenge:	TC1 Vulnerabilities and global security of the CNS/ATM system
Edition date:	30 June 2021
Edition:	1.0
Dissemination level:	Public
Authors:	Martin Hawley / Winsland Ltd
	Karol Gotz / Winsland Ltd
	Denis Kolev / MSDK
	Chris Veness / Movable Type

The opinions expressed herein reflect the authors' views only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.

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.

1. Abstract and executive summary

1.1 Abstract

To support the safety of the ATM system, the future ATM architecture needs to deliver an exceptionally high level of cyber security. The objective of this project was therefore to advance cyber security management in several directions: (a) to develop a more collaborative approach to cyber security management; (b) to prototype these collaborative approaches; and (c) to adapt SESAR's existing risk assessment methodology, 'SecRAM', to more quantitative methods, from which Bayesian Network analysis could be applied. The outputs of the project were a concept of operations for collaborative security management, a basic prototype for collaborative security management, and an approach for the application of Bayesian Networks. The prototype was developed to support a risk assessment that could be done in collaboration between several partners, such as by the members of a SESAR Solution Project. The outcome of the project is a step forward in information sharing, productivity and methods of knowledge exchange in cyber security.

1.2 Executive summary

While the ATM industry has been addressing cyber security since the mid-2000s [1], progress has been faster in the more operational and tactical side of security than the more strategic, management side. Within the safety domain, safety management systems have been continuously researched and developed[2], through practical experience and extensive collaboration. The practice of security derives from a 'need to know' approach, where information sharing is done sparingly, and collaboration is light. A recent World Economic Forum WEF study[3] comments on the limited participation to the Aviation ISAC, where the need is for a collaborative approach from all actors in the aviation value chain, building on the strong history of safety management. The WEF study also emphasises the need for systemic risk assessment. This sets the context for this project, which addresses several themes in security management, centred around collaboration and risk.

The project has addressed a new concept of 'collaborative cyber security management' and to do this connects several different strands of work: risk, architecture and collaboration. Two initiatives in particular have provided inspiration for this project:

- **ED-201**: EUROCAE's ED-201 'Aeronautical Information System Security (AISS) Framework Guidance' [4]. This provides guidance for different aviation organisations to cooperate on aeronautical information systems security (AISS).
- **STORM**: EASA's Shared Trans-Organisational Risk Management (STORM). This is a framework under development by EASA and EUROCONTROL, to support sharing of information as foreseen in ED-201. It requires methods to harmonise risk-assessment and share appropriate outputs, which map to organisations' functions and the interfaces between them.

The project addressed the following research questions:

1. How could ATM stakeholders collaborate better through productivity tools?
2. How can we evolve risk methods in ATM from purely qualitative to quantitative methods that support better use of information?
3. How can we connect risk management to architecture in a simpler, less resource intensive way?

The research was organised into two main work packages:

- WP1 CONOPS Development: covering the main elements of the project: collaboration, risk and architecture integration.
- WP2 Prototype Development: using an agile approach with regular iterations between the developing CONOPS and findings from the prototyping.

The project consulted ATM industry experts, particularly those knowledgeable with EASA's STORM concept and ED-201 guidance on Aeronautical Information Systems Security (AISS).

The risk aspects of the project focused firstly on quantification and secondly on exploiting quantified methods. This enabled the project to introduce a probabilistic graphical model (PGM) representation, using Bayesian Networks.

Prototyping was a key component of the project as it supported development of the CONOPS, which allowed the team to assess how productivity tools can support greater collaboration and improve the effectiveness and efficiency of security management. The prototyping was then done in three parts:

1. A prototype for risk management within an organisation or trusted community of practice, such as a SESAR, extended to quantitative risk assessment.
2. A prototype information broker to exchange information between risk assessments.
3. Bayesian network modelling: proof of concept modelling for future adaptation to STORM 1.

Functional architecture for the prototyping was developed in MS PowerPoint and LucidChart. The main prototyping was developed on a Node.JS platform programmed in the JavaScript language, based on a MySQL database.

The results of the project were assessed within the project team, with BULATSA providing an internal review as security practitioners. Overall, the project provided insight and emerging methods and tools that should improve cyber security management in ATM. Specifically, the project has:

a) **Identified how ATM stakeholders could enhance their collaboration on cyber security through productivity tools**. The concept of operation has considered the factors that can encourage or discourage exchange of information and proposes a way of collaborative working, which also requires productivity tools to support information exchange and increase efficiency.

b) **Evolved risk methods in ATM from purely qualitative to quantitative methods**. The project has also provided insight into the use of quantitative methods in risk assessment and adapted the SecRAM methodology to this. We also conclude that quantification does not add significant overhead to risk assessment, and there is an opportunity for partners to share, for example, impact assessments of the loss of CIA to primary assets. 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. This said, harmonisation of methodology, such as through ISO 27005 or SecRAM, is likely to have a bigger impact on sharing risk management information.

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. Although the prototyping was fairly simple, the visualisation provides user benefits in terms of appreciating the overall system. This light approach means that risk assessment and enterprise architecture could be done more in parallel in the SESAR processes without a need for resource intensive architecting to proceed first. This makes the process easier to do for early stage development of SESAR Solutions at V1 and V2 validation stages where Solution architecture may be incomplete.

2. Overview of catalyst project

2.1 Operational/technical context

The ATM industry has been addressing cyber security since the mid-2000s [5]. By necessity, progress has been faster in the more operational and tactical side of security than the more strategic, management side. This has resulted in mostly reactive cyber security through a patch-work of efforts, mostly done in siloes with limited collaboration. However, ATM is fundamentally a network industry, requiring consistent levels of performance, including security, across the network.

The current levels of collaboration are typical for matters of security, which can be seen through the lens of the largely ingrained principal of 'need to know'. As discussed in Reference 6, 'need to know' is effective in organisations where the primary mission is security, but less so in organisations where security has become a twenty first century addition. Such organisations are on a constant learning curve, trying to keep up with understanding cyber security and mitigating the risk of attack. These are the organisations that we focus this project on, where collaboration can lead to learning from shared knowledge and yield productivity gains. The latter point on productivity may seem mundane but is rather crucial, as the level of cyber expertise is generally insufficient. The 'firehose' of information facing security operations means that there is always a need to triage threats and prioritise vulnerabilities. This leaves security managers continuously exposed to making the 'wrong' decisions. It also puts the focus on reacting to threats and vulnerabilities rather than being more pro-active.

By requiring 'design-in' security into SESAR, there is the potential to gradually improve the future security of the ATM industry, and avoid common errors in system and software design and development. This project considers security in the context of SESAR projects, with the potential to extend the ideas of collaboration through to operations.

A particular analogy for security management is safety management, where safety is 'designed-in' and then continuously managed in operation. A key vehicle for through life management of safety is the safety case, which is developed to support approvals to operate and then kept up-to-date through safety management systems. Within the safety domain, safety management systems are continuously researched and developed[7], and there is extensive collaboration; with EUROCONTROL initiatives such as 'generic safety cases', routine sharing of information, such as voluntary and mandatory occurrence reporting and incident analyses, and safety communities of practice throughout the industry.

While safety experts seek continuous improvement in safety management, it appears that security management has been neglected. Recent industry comments illustrate this point. In 2020, the World Economic Forum (WEF) commented on the aviation industry that: *"it is crucial that all stakeholders along the supply chain embrace a collaborative and risk-informed cybersecurity approach to adapt and ensure resilient aviation ecosystems"* [8]. More recently, a WEF / Deloitte study [9] identified numerous issues, including the following:

- *"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".*
- *"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".*
- *"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."*
- *"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.*
- *"Collaboration must go beyond subscription to information feeds and include active participation in industry action groups, which should strive to coordinate actions against cybercriminal groups and nation-state actors, thus having a more strategic impact on adversaries by sharing contextual and actionable insights".*

The implications of these and other WEF findings are:

- Cyber security needs collaboration beyond organisational boundaries.
- This collaboration needs to extend to the widest set of organisations possible.
- The high level of resources needed for risk management means that it is rarely done sufficiently or effectively.
- Security management can learn from safety management.
- True collaboration can be a force multiplier against cyber crime.

The challenge for the industry, and which this work begins to address, is to leverage existing resources and increase impact through collaboration. Concepts around collaboration have already been developed, notably by the triumvirate of EASA, EUROCONTROL and SESAR, who have collectively been promoting frameworks and methodologies to improve cyber security at both strategic and operational levels. Arising from these organisations' work, two initiatives in particular provide inspiration for this project:

- **ED-201**: EUROCAE's ED-201 'Aeronautical Information System Security (AISS) Framework Guidance' [10]. This provides guidance for different aviation organisations to cooperate on aeronautical information systems security (AISS). The aim is to reduce risks to the safety of flight and significant disruptions to operations. A fundamental principal is that organisations share information about security wherever there is shared responsibility for systems and operations. ED-201 assumes that the organisations involved have formal security management systems and risk assessment methods, although these may not follow the same standard. The guidance proposes a comparison of organisations' risk management methods against the ISO27005 framework. Once comparability of risk assessment is established, organisations are able to identify risks that may be shared by virtue of the interfaces with partner organisations.

- **STORM**: EASA's Shared Trans-Organisational Risk Management (STORM). This is a framework under development by EASA and EUROCONTROL, to support sharing of information as foreseen in ED-201. It requires methods to harmonise risk-assessment and share appropriate outputs, which map to organisations' functions and the interfaces between them. Across these interfaces are flows of information, and there exist 'interface risks' according to the security controls applied by individual organisations. Sharing information about these risks enables the different organisational partners to ensure that appropriate controls are in place.

In the preceding paragraphs, we see that collaboration is strongly linked to risk management, which is also a key theme of the project and the WEF study also emphasises the need for systemic risk assessment. The project also responds to industry needs set out by the Industry Consultation Body[11] (ICB). This includes the need to improve links between cyber-security and architecture, legacy system integration, the perils of selective risk assessments, safety-security, coordinating software changes etc.

We see the issues identified by WEF, the ICB and commentators as fundamentally about cyber security management and specifically a concept of 'collaborative cyber security management'[12], which we address by connecting several strands of work: collaboration, risk and, to a smaller extent, architecture.

2.2 Project scope and objectives

Scope

The scope for this work is within ATM digital productivity tools for cyber security, in the context of a more collaborative working between actors in the sector. The project scope is further defined by our ambition to develop the work to TRL 3/4, developing some key functions with some basic validation. As such the expectation was to gain clarity in a concept of operations for collaborative cyber security management and demonstrate some of the resulting ideas through prototyping. The scope included several related ideas: collaboration, quantified risk and architecture and we aimed to achieve the following outcomes:

- Ensure ATM security keeps pace with the development of SESAR Solutions through enhanced methodologies and future productivity tools to leverage scarce cyber resources.
- Managing the complexity of ATM security within the aviation ecosystem by linking security into architecture.
- Spearheading a model for collaborative and risk informed decision making within aviation by:
    - enhanced information sharing support through anonymous and open data sharing repositories; and
    - opening a pathway to quantitative risk and Bayesian network analysis.

Research questions

The project addressed the following research questions:

4. How could ATM stakeholders collaborate better through productivity tools?
5. How can we evolve risk methods in ATM from purely qualitative to quantitative methods that support better use of information?
6. How can we connect risk management to architecture in a simpler, less resource intensive way?

The research questions were addressed in the project through the development of a concept of operations for collaborative cyber security management and some early prototyping. The intention is that this work will advance the state of the art and lead to a system that could be adopted by ANSPs in Europe and more widely. More specifically, we defined the following objectives:

1. To develop a CONOPS for a framework for collaborative cyber security management.
2. To create a prototype for collaborative exchange of cyber security design, including architecture.
3. To evolve risk assessment approaches, including quantified risk.

Our assessment is that current work is at TRL 2/3 and we aim to mature this to TRL 3/4. Rapid development thereafter is then possible, to feed into SESAR 3.

2.3 Research carried out

2.3.1 Introduction

The research was organised into two main work packages:

WP1 CONOPS Development: covering the main elements of the project: collaboration, risk and architecture integration.

WP2 Prototype Development: using an agile approach with regular iterations between the developing CONOPS and findings from the prototyping.

WP1 covers the first objective of the research, to develop a CONOPS for a framework for collaborative cyber security management. WP2 covers the second objective, to create a prototype for collaborative exchange of cyber security design, including architecture. The third objective, to evolve risk assessment approaches is covered in both WP1 and WP2.

2.3.2 Collaborative cyber security management operational concept

2.3.2.1 Overview

The R&D has defined a concept of operations through which to address the research question 'how could ATM stakeholders collaborate better through productivity tools?'

The CONOPS were developed from extensive desk research, covering the following main areas:

- the basis for organisations to collaborate and the factors that influence the success of the collaboration;
- the use of quantitative risk assessment and Bayesian Networks in cyber security.

The desk research was used to establish an initial set of requirements for the operational concept, from which a CONOPS was iteratively developed. The CONOPS addressed:

- **Collaboration**. The project focuses on information sharing, noting that 'Information Sharing and Analysis Centres' (ISACs) have emerged as the predominant cooperative vehicle for organisations to share information and analyses on threats, incidents and other topics. The project treats Information as data that has been analysed and/or contextualised[13]. Security information comprises a variety of abstract and tangible items in the context of securing an enterprise within an ecosystem, e.g. Primary Assets, Supporting Assets, Risk, Likelihood, security observations.
- **Risk**. An underlying issue for the future ATM architecture is the ability to identify, explore, prioritise and make decisions on cyber security risk. For example, a recent unexpected use of

FlightRadar24 was its use by air traffic controllers following a brief but total outage. This wide-area loss of integrity or availability of surveillance and communications is an important systemic risk scenario to address. With respect to the current SESAR risk assessment methodology, SecRAM [14], the project explored how greater insight could be gained by more mathematical approaches:

- Quantified risk assessment to support refined decision making. Quantified impact is already mature in cost benefit analysis. Likelihood may be estimated from incident reports and shared strategic and tactical threat intelligence (indicators of compromise). Semi-quantified methods may be an intermediate step.
- Applying Bayesian probability to ATM cyber security, for which there is precedent in other contexts[15], and potential linking to architecture and creating dynamic risk models, already being examined for safety[16]. Bayes is chosen for a number of reasons. It provides a set of standard methodologies for decision making and state estimation under uncertainty and noisy data, using probabilistic notation[17].

- **Architecture**. We observe that architecture alone is not sufficient to address the variety of security questions that SESAR is uncovering, but is an important baseline as it provides inputs and coherence to risk management, and risk management informs architecture.

The CONOPS and prototyping have been iterated, so ideas developed in the CONOPS are prototyped and trialled by the team, leading to updates in the CONOPS. The team members drew on their extensive practical experience in conducting risk assessments in SESAR to validate the CONOPS internally.

The project also consulted ATM industry experts, particularly those knowledgeable with EASA's STORM concept and ED-201 guidance on Aeronautical Information Systems Security (AISS).

2.3.2.2 Bayesian network modelling

To evolve risk methods we first considered risk quantification to make a step change in the accuracy of risk assessments. Further to this, we sought to evolve the risk methodology towards more analytical approaches. The project considered the use of probabilistic graphical models (PGMs).

A probabilistic graphical model (PGM) is a probabilistic model for which a graph defines the conditional dependence structure between random variables. PGMs use a graph representation as a descriptor in order to encode a joint probability distribution over a multi-dimensional space, where the graph nodes define the random variables, and the graph arcs define the dependencies between subsets of variables. Two different types of graphical models are commonly used: Bayesian networks and Markov random fields. Both families encompass the graphical representation of interdependencies, but they differ in terms of the way they define the corresponding probability distribution. Given the graph $G = (N, A)$, the corresponding rules for the definition of the probability distribution include the following:

- Bayesian networks are defined by a directed and acyclic graph, where the directed edges illustrate causal relationships between variables in the network. The probability for a set of variables (or nodes) follows the following factorisation rule:

$$P(x_1, \dots, x_k) = \prod p(x_i \mid Pa(x_i))$$

  where the operator $Pa(x_i)$ defines the set of direct "parents" of the node x_i (i.e., the nodes that have edges ending in x_i). From the definition, it is obvious that the graph structure that encodes the PGM should not have any loops, as it may prevent the proper definition of the factorisation rule and introduce a logical error, where the variable will be causing its own value.

- Markov random fields are defined by an arbitrary graph, and the interdependency is defined in such a way that, for a set of variables (or nodes) $\{x_1, \dots, x_k\}$, the following holds:

$$p(x_i \,|x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_k) \;=\; p\big(x_i \,\big|\, x_j, j \,:\, (i,j) \in \; A \; or \; (j,i) \in \; A\big)$$

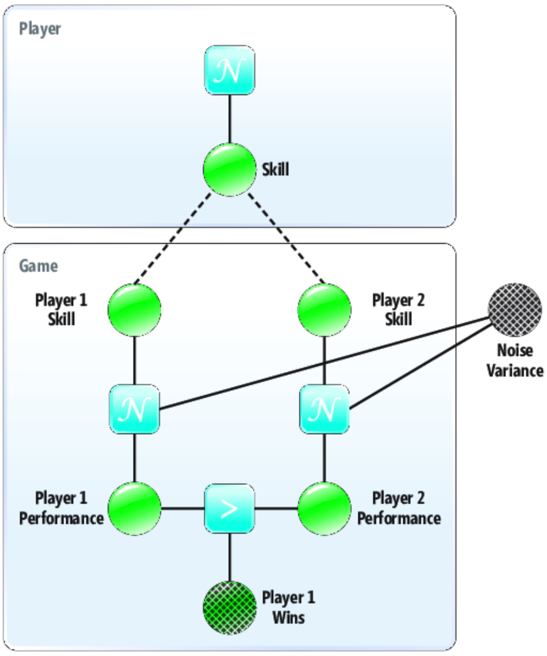
  Each variable is conditionally independent of the non-adjusted nodes, given the adjusted nodes. No explicit causal relation is given.

Probabilistic methods nowadays are applied in a wide range of domains. They are used for smugglers interdiction, fare evasion minimisation systems, cyber-attack detections, and recommendation systems. The latest stays as an important example for the scope of the project, as it allows to join the formal structures of the security risk assessment and the features of the statistical learning.

Example PGM

One of the most prosperous examples of the applications of PGMs (Bayesian networks) is TrueSkill. The model was applied for the assessment and quantification of the “levels” of online game players. The system observed a sequence of game results (win/loss) for all players and (based on that) was able to derive a quantitative “value” of the experience of the player and its own confidence in the assessment. Formally, the experience of each player was encoded by a Gaussian variable with an unknown mean and variance. The game is a two-player game (“first” and “second” without loss of generality) with a simple outcome for each player: win or loss. The outcome of a game between two players was encoded using a Boolean variable (victory of the “first” player) with a probability of being “true” equal to a probability that the experience of the first player is higher than the probability of the second one, plus random noise. An example of the directed graph for this model is presented in the following figure.

Figure 1 TrueSkill Bayesian network graph



Initially, the skill of each player was assumed to have the same mean with a large variance (upper part of the figure). After that, the information about the game outcomes was supplied and a conditional (posterior) distribution for the skill of each player was computed. The exact form of the posterior distribution is too complex (a mix of truncated Gaussians). Therefore, it is approximated with a "standard" Gaussian distribution by using the Expectation Propagation technique. In the end, for each player, a skill distribution in a form of a Gaussian is available, i.e. the mean (average skill) and variance (confidence of the model and stability of the player).

As conclusion, PGMs allow both for "in-depth" analysis of the values and adjustment to the observed data given the relations between observed and unobserved variables; and for explicit definition of the causal/interdependency models.

Application of graphical models to security risk assessment

Within the scope of the project, the main functionalities and requirements of the PGM-based engine were defined. The engine was designed to support and integrate into the STORM system. It is based on SecRAM methodology, and it uses the same entities and terminology, and metrics.

Namely, the following requirements were identified:

1. The model should be able to take results of the SecRAM as an input, i.e.
   - list of PAs and SAs, links between them,
   - CIA-based impact assessments for each PA,
   - list of threats and their connections to the SAs, list of likelihoods for each threat,
   - list of security controls
   - list of deployed security controls
   - list of mitigated impacts and likelihoods.
2. The model shall be able to suggest which SAs are (typically) connected to which PAs, identify possibly missing or redundant connections.
3. Same as point 2 for connections between threats and SAs.
4. Automatic impact computation/suggestion.
5. Automatic suggestion of possible threats.
6. Automatic suggestion of mitigated impacts given PAs, SAs, and selected security controls.
7. Automatic suggestion of the most efficient security controls to be used.

2.3.2 Prototyping

2.3.2.1 Overview

Prototyping was done in three parts:

1. STORM 1: A prototype for risk management within an organisation or trusted community of practice, such as a SESAR, extended to quantitative risk assessment.
2. STORM 2: A prototype information broker to exchange information between STORM 1 users.
3. Bayesian network modelling: proof of concept modelling for future adaptation to STORM 1.

Functional architecture for the prototyping was developed in MS PowerPoint and LucidChart. The main prototyping was developed on a Node.JS platform programmed in the JavaScript language, based on a MySQL database.

2.3.2.2 STORM 1

The STORM 1 prototype was initially developed from a set of use cases and user stories, derived from the CONOPS. For example, reflecting the SecRAM, we have the following user stories:

Table 1: Example user stories for STORM 1

No.	User Story
2.	As a user, I want to be able to input or select my airport's assets (primary and secondary or subject to risk methodology), so that I can correctly model my organisation's information flows and risk.
3.	As a user, I want to be able to adjust/edit/update the asset information (primary and secondary including information), so that any changes to the systems or user errors can be corrected/updated.
5.	As a user, I want to be able to link multiple supporting assets to a single primary asset, so that I know which supporting assets support the primary asset.

An initial user interface was designed and prototyped. Following the main development of the CONOPS, this prototype was then re-developed to accommodate an architectural approach to entering data and quantified risk assessment. Not all of the elements were fully integrated but were sufficient to validate the ideas with our operational partner, BULATSA.

2.3.2.3 STORM 2

This module followed the same development as STORM 1 and example user stories are shown below. A particular focus in the development was on topologies for connecting STORM 1. A REST API[1] approach was taken to connect STORM1 and 2.

Table 2: Example user stories for STORM 2

No.	User Story
1.	As a User, I want to be able to exchange information across organisational boundaries and networks, so that information can be shared across trust zones, networks, and organisational boundaries.
2.	As a User, I want all communication encrypted, so that any traffic is safe from prying eyes.

2.3.2.3 Bayesian network modelling

Modelling methodology

In this sub-section, we define the main parts of the probabilistic graphical model (PGM), responsible for the implementation of requirements 1-7 described earlier. First, we introduce the main variables and distributions of the PGM.

The list of variables is presented as follows:

1. Supporting assets – input to the system. No associated distribution.
2. Primary assets – input to the system. No associated distributions.
3. Links between SAs and PAs. Defined using a latent-links variable that defines which links are more probable to be presented together. Namely, 2 variables are defined:
   a. Latent-link variable $\boldsymbol{l} \sim \mathcal{N}(\boldsymbol{m}, \Sigma)$ – multidimensional Gaussian distribution for each link. The dimensionality is equal to the number of possible links between SAs and PAs, encoded by n.
   b. Link-presence Boolean vector, $\boldsymbol{L} = [\boldsymbol{l} + \boldsymbol{\xi} > 0], \boldsymbol{\xi} \sim \mathcal{N}(\boldsymbol{0}, \alpha I)$ – random noise, operator $[]$ returns 1 if inner condition is true, 0 otherwise. The vector $\boldsymbol{L}$ encodes the presence of each link.

[1] Representational state transfer Application Programming Interface.

Latent-link variables encode inner relations between the presence of the links. This way, if $\sigma_{ij} > 0$, it is more probable for the links L_i, L_j (corresponding components of i, j from vector $\boldsymbol{L}$) to be present together. For example, the model may take into account that the link (computer -> video surveillance) is usually present if a link (camera -> video surveillance) is present. The component m_j is higher if the corresponding link is used more frequently.

4. Impacts for each PA. Impacts for each PA are to be modelled using multidimensional Gaussian $i_p \sim \mathcal{N}(\boldsymbol{m}_p + A\boldsymbol{w}, \Sigma_\mathrm{p})$, where $\boldsymbol{m}_p$ defines the standard CIA impacts for each PA, $A\boldsymbol{w}$ stays for a "linear-regression" term used to incorporate the presence of each SA, A is a connectivity matrix, indicating the presence of each link between SA and PA (basically, reshaped vector $\boldsymbol{L}$), Σ_p is the covariance matrix. The prior distribution over $\boldsymbol{w}$ may be defined by a product of normal distributions, which is equivalent to a regularization technique.
5. A structure similar to $\boldsymbol{l}, \boldsymbol{L}$ connectivity-distribution may be used to encode the links between the threats and SAs.
6. For each security control, an "effectiveness" variable is defined. This variable is used to quantify the mitigation level for each threat for each PA. An explicit definition of the effectiveness level is a subject of experiments, but in the experimental section the effectiveness of a controls c, e_c, is stated as a Gaussian variable with the following "mitigation" mechanism:

   $$i_{mp} = \sigma\left(\sigma^{-1}(i_p) * e_c\right)$$

   Where σ, σ^{-1} are sigma-function and an inversed sigma-function correspondingly, i_{mp} stays for the mitigated impact.

The definition of the variables above allows the implementation of the requirements 2-7 (requirement 1 is fully technical).

Requirement 2 (3 and 5 too) may be satisfied by inferring the most probable links given the SAs, PAs of the system, and existing links. This may be done by computing the conditional distribution of the components of $\boldsymbol{L}$.

Requirement 4 is achieved by direct sampling from the $\mathcal{N}(\boldsymbol{m}_p + A\boldsymbol{w}, \Sigma_\mathrm{p})$

Requirements 6 and 7 are achieved by inferring the conditional distributions over i_{mp} given SA/PA structure, set of threats, and deployed security controls. Security controls suggestion may be done with an aim to minimise the expected mitigated impact.

Test application

A proof of concept was developed in order to demonstrate the implementation of a subset of the requirements to the model defined before (requirements 6 and 7). In addition, a selection of development tools was conducted allowing faster future development.

Two main frameworks were selected and tested: Bayes server and Infer.NET. This selection of frameworks was done according to the best experience of the team in programming languages/frameworks. The comparison table is presented below.

Table 3: Comparison of frameworks for Bayesian Network modelling

Feature	**Bayes Server**	**Infer.NET**
Supported languages	Has open API for Python, C#, Java, JavaScript, Matlab, Excel integration, etc.	Only part of .NET and NET.Core languages
Subscription	Paid, works via server connection	Free
Visualisation	Allows straight-forward visualisation and modelling	Visualisation should be programmed
Modelling flexibility	Restricts certain connections between nodes (for example, continuous to discrete variable connection)	Has restriction in the inference engine for certain connections, but much more flexible.
Available distributions	Only discrete and Gaussian	Wide range of distributions
Approximate inference availability	No, only exact inference using expectation-maximisation algorithm	Wide range of exact and direct inference algorithms

Given the table above and a proposal for the modelling defined in the previous section, Infer.NET was selected as a development framework. It has its own limitations in terms of integration/visualisation/complexity, but it provides a set of flexible means for PGM definition.

Apart from the listed frameworks, there exist a set of python libraries for Python and R. The R-language is out of scope, as it is not designed for production services, which we intend in future. Python library (bayespy) is of interest, but it is still a pre-release version.

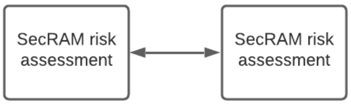
2.4 Results

2.4.1 CONOPS

In this section we present selected findings that support a CONOPS for collaboration between ATM stakeholders.

The high level concept of operation is a simple exchange of information between risk assessments. The factors that support such an exchange of information are discussed in the following paragraphs.

Figure 2: High level sharing concept



2.4.1.1 Success factors in collaboration

Collaboration is different to cooperation, which may be more transactional, for example, when two or more parties enter into an agreement on the exchange of information. The ATM sector has good experience with collaboration, through 'Collaborative Decision Making' or 'CDM'. Within CDM, partners share information and then collaborate on subsequent actions. In ATM, CDM concepts are most developed a the Airport level, through Airport-CDM or A-CDM. CDM is also developing along other lines, particularly in SESAR and Network Manager concepts.

Collaboration in the aviation context is common with other sectors and has several key requirements to be effective [18, 6]:

The need to collaborate for a common purpose, which must be strong, as at times individual actors will lose out, but overall will benefit greatly. A-CDM exemplifies the practical issues; the concept has been developed since the early 2000s, and is still being deployed at major airports. The key factors for successful, and rapid, implementation appear to be:

1. To make a business case at the holistic and individual partner levels.
2. To share accurate and up-to-date information.
3. To integrate processes horizontally, across organisations. In airport CDM, there are common milestones for airport turn-around times standardised terms and definitions. In theory, one flight's 'target off block-time' means the same to everyone, and this data can be used as a reliable planning input [14]; in horizontal process integration, organisations must put the quality of output first – and not be compromised by organisational boundaries.
4. Individuals adapt to truly collaborative behaviour. Managers need to learn to act collegiately, to construct relationships based on an agreed mutual interest, and aim for mutual confidence through reliability.

The above factors reflect the characteristics of what is now commonly known as ‘leading without authority’ or 'Collaborative Leadership'. This is markedly different to conventional, authority-based leadership techniques, which, if applied in a collaborative context, will not only tend to be ineffective, but run a high risk of actually making matters worse.

The above factors also indicate that a high level of trust is needed, or alternatively that a ‘trust-less’ form of collaboration can be achieved through, e.g. Blockchain [19].

2.4.1.2 Information sharing

Information-sharing is not a new challenge in the information security space, but it is one that has remained relevant and pertinent in the complex ATM environment. Information [20] is data that has been analysed and or contextualised [21]. Security information comprises a variety of abstract and tangible items in the context of securing an enterprise within an ecosystem, e.g. Primary Assets, Supporting Assets, Risk, Likelihood, security observations.

Information sharing is a common communicative activity and exceeds the propensity of people to share goods [20]. It is mostly observed through direct interaction between people but increasingly online. Conceptually, there is also an expectation that information sharing is free. Information can be considered as a ‘public good’, and is copied rather than transferred, so the consumption by one user does not deprive another. The online context of information sharing is one that is decentralised [22], as opposed to libraries which are centralised.

The main focus on information sharing in cyber security to date has been threat related (a specific type of attack method/vector) or vulnerability (a specific vulnerability, e.g. that may require a software patch). Threat sharing has been formalised in many contexts, such as via Information

Sharing and Analysis Centres (ISACs) and an industry standard information exchange model, STIX, has been created. The focus on threat and vulnerability has, however, led to less consideration of the benefits of sharing other security information.

In the STORM concept, information sharing is focused on so-called ‘functional chains’, where information flows across organisational boundaries are limited to cases where there is a ‘functional dependency’ across the boundary [23]. The current project considers that there are wider opportunities for information sharing of cyber security information. This however, requires addressing some key information sharing behaviours [20,24] as follows:

- Sharing is based on self-interest and reciprocity, but may also be seen as supporting a public good.
- Experts may be more willing to share in return for gratitude. People who are more knowledgeable see the knowledge as more owned by them personally, which makes it easier for them to share.
- The need to avoid ‘under-contribution’ of information by ‘free riders’.

There is an existing tradition of sharing (e.g. collaborative software development) and the above behaviours suggest that there is no inherent block to increased sharing in cyber security. These behaviours do, however, point to the need for reciprocity and the advantage of sharing via communities of practice, such as ATM, where the common good is self-evident. Privacy may also be factor for encouraging information sharing, so the project also considered the means to share information anonymously [25].

Cloud platforms and trust

The Ponemon Institute “2018 Global Cloud Data Security Study” reports different levels of caution in sharing information stored in the cloud with third parties [26]. There were significant differences to the likelihood of organisations to secure information in the cloud based on state: UK (35%), Brazil (34%) and Japan (31%), Germany (61%). This willingness to share, store and communicate with cloud-based platforms is one that is considered in the design of the project.

2.4.1.3 Quantified risk assessment

A key consideration in the project has been how to transition the existing SESAR SecRAM 2.0 to a quantified approach to risk management. To develop this the project developed a road transport risk case study of a vehicle’s Remote Keyless System (RKS), which is present in the majority of modern cars.

The functions of an RKS include: unlocking a car’s doors from a distance (remote keyless entry) and starting the engine without inserting the car key (remote keyless ignition). This system is also known as a ‘Passive Keyless System’ or PKES. The authors have no specialist knowledge of the area and the example was developed purely to illustrate the process. We initially took a qualitative approach to risk evaluation and later add the quantitative approach. The use case considered the risk from two different perspectives, that of a car owner and that of a manufacturer. The following paragraphs explore the manufacture’s perspective pf risk.

Risk is assessed as per the SESAR SecRAM, with Risk defined as Impact x Likelihood, and three primary assets are defined:

1. Service to unlock the car
2. Service to start the car

3. Key information

The impact on the loss of CIA to these services is assessed as follows:

Table 4: Impact of loss of CIA on Primary Assets

	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).

The impact on loss of CIA to these primary assets is inherited by the supporting assets. In the remainder of this description we focus on the 'key fob', which comprises the electronics for transmission of key information between the driver and the car. This leads to the following threat scenarios:

Table 5: Threat scenarios

Supporting asset	Key fob
Threat Scenario 1	**Theft of key fob** A thief obtains the key fob, makes a copy of the data and replaces it back into the driver's possession. If the data is not stored in an encrypted format, this leads to the negation of the RKS key data and theft of the car at a later time.
Threat Scenario 2	**Interception of wireless signal from key fob** A thief intercepts and copies the wireless transmission between the key fob and the car unit. The attacker then replays this transmission to the car unit when the key fob is no longer nearby, resulting in theft of the car.
Threat Scenario 3	**Relay of wireless transmission from key fob** A thief relays the key transmission from the car unit to the key fob, using a high gain antenna, gaining sufficient access to open and start the car.

Likelihood

The likelihood of each of the threat scenarios is assessed as follows:

Table 6: Comparison of qualitative and quantitative likelihood

Threat scenario	**Qualitative**	**Quantitative (Expectation Value)**
1. Theft of key fob	Likely	53% (5)
2. Interception of wireless signal	Very likely	53% (5)
3. Relay of wireless transmission	Very likely	49% (203)

Risk

The risk is evaluated from a qualitative risk matrix and using the quantitative expression of risk = impact x likelihood as below.

Probabilistic expressions using the binomial theorem have been used to calculate likelihood, so values below are based on expectation values of the number of car thefts. Hence there is a 53% likelihood of losing 5 cars to theft in threat scenarios 1 and 2, and a 49% chance of losing 203 cars in scenario 3. The impact of each scenario is different because the low number of car thefts is not considered sufficient to trigger an impact on branding, which is substantial.

Table 7: Comparison of qualitative and quantitative 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

2.4.2 Prototyping

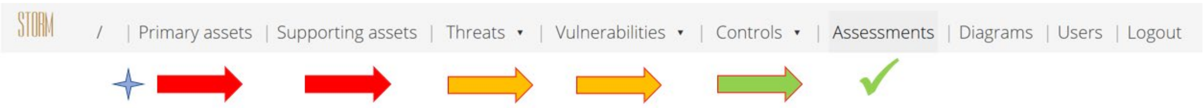
2.4.2.1 Introduction

In this section we describe the prototyping undertaken. Prototyping was a key component of the project as it supported development of the CONOPS, which allowed the team to assess how productivity tools can support greater collaboration and improve the effectiveness and efficiency of security management.

2.4.2.2 STORM 1 prototype

The STORM 1 prototyping was initially done within the ISO 27005 framework, but following a discussion with EUROCONTROL, the prototype was adapted to fit the SecRAM methodology. Because SecRAM was previously defined within ISO27005 so the differences were not substantial. The user interface was not highly developed, but user experience was considered in terms of work flow and data presentation. The high level menu structure was developed in the form of a risk assessment work flow:

Figure 3: Prototype work flow follows SecRAM



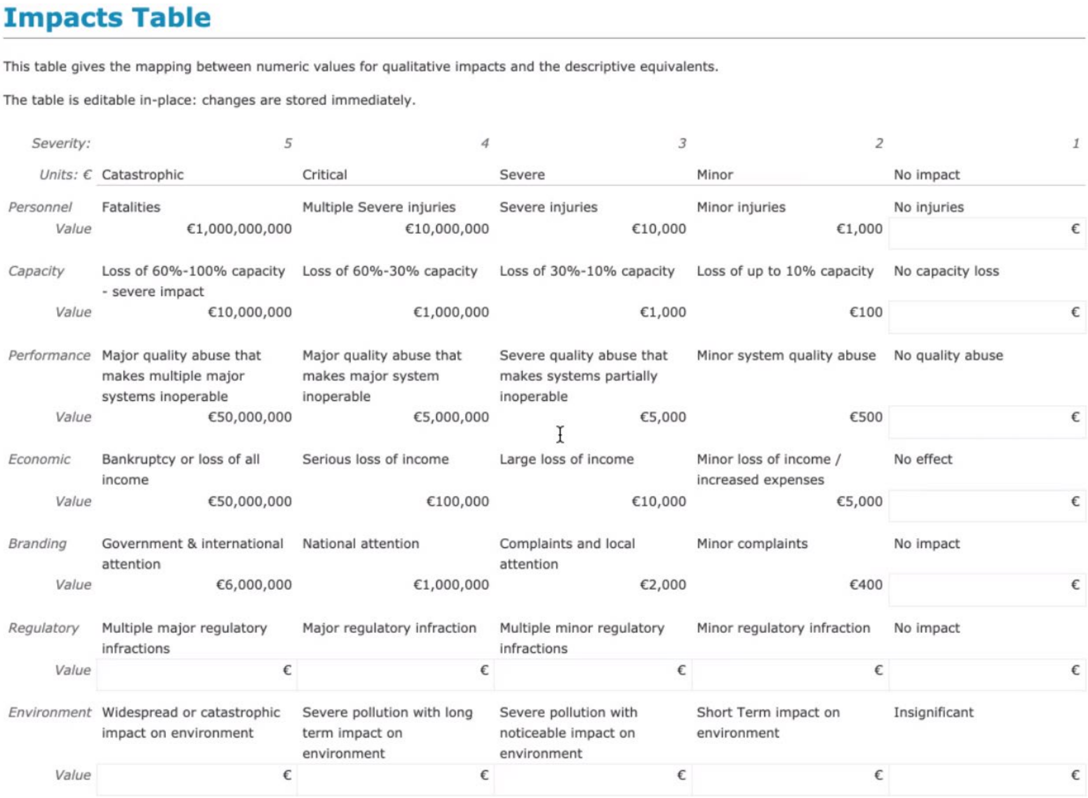
Additions to the SecRAM methodology include a diagramming function, which enables primary and supporting assets to be entered, and the approach to quantified risk.

The user journey for risk quantification was considered in three phases, firstly as the qualitative approach in SecRAM, secondly as a semi-quantitative approach, shown below, and thirdly as a purely quantitative approach as described in section 2.4.1.3.

The semi-quantitative approach considers that the severity of impacts in qualitative terms can be translated into ranges of quantitative impacts. The scale in the figure below is illustrative, showing, for example, a critical loss of capacity as costing up to €1M and catastrophic as costing €1-10M. In our testing, this approach was found to simplify the step between qualitative and quantitative statements. The impact table is defined per risk assessment or may be common to a group of risk assessments. This means a SESAR solution risk assessment for an airport can be defined with the same concept of severity (catastrophic, critical etc.), but scalable to different contexts, such as ACC or TWR control, several TWRs, several ACCs etc. This improves the capability to look across multiple risk assessments and make comparisons.

The next step in quantification is to develop specific estimates of impact as done in section 2.4.1.3, with values entered manually from separate spreadsheet models.

Figure 4: Implementation of semi-quantitative risk scale (impacts table)



Impacts Table

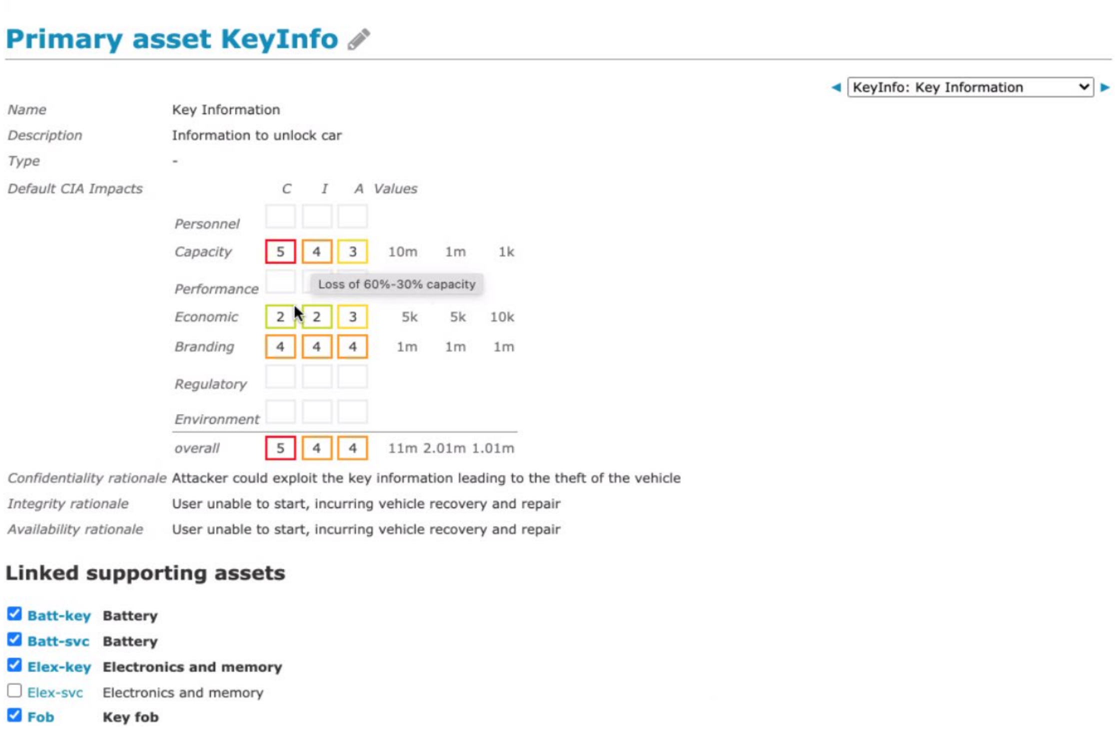
This table gives the mapping between numeric values for qualitative impacts and the descriptive equivalents.

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	€
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	€
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	€
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	€
Branding	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
Value	€6,000,000	€1,000,000	€2,000	€400	€
Regulatory	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
Value	€	€	€	€	€
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	€	€	€	€	€

Following the SecRAM methodology, impact is a property of Primary Assets which is inherited by Supporting Assets, as seen below:

Figure 5: Primary assets and linked supporting assets



Primary asset KeyInfo

Name	Key Information
Description	Information to unlock car
Type	-
Default CIA Impacts	

	C	*I*	*A*	*Values*		
Personnel						
Capacity	5	4	3	10m	1m	1k
Performance						
Economic	2	2	3	5k	5k	10k
Branding	4	4	4	1m	1m	1m
Regulatory						
Environment						
overall	5	4	4	11m	2.01m	1.01m

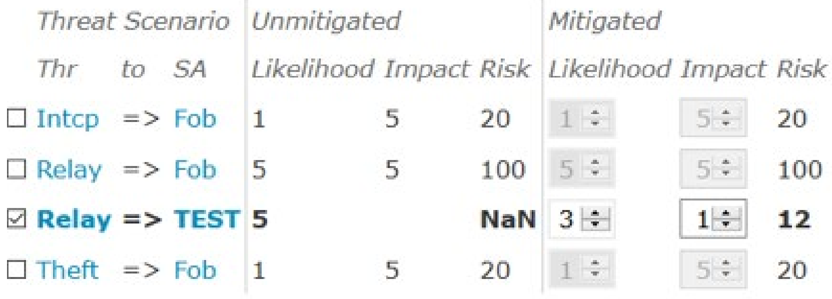
Confidentiality rationale	Attacker could exploit the key information leading to the theft of the vehicle
Integrity rationale	User unable to start, incurring vehicle recovery and repair
Availability rationale	User unable to start, incurring vehicle recovery and repair

Linked supporting assets

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

The CONOPS and prototyping of the quantitative approach shows that calculation of risk can be simplified to Impact x Likelihood. This creates a finer distinction between individual risks. When a qualitative approach is used, the protype calculates the risk as 1..5 impact x 1..5 likelihood and then categorises the result as low, medium high. The qualitative calculation from the SESAR risk matrix is shown below. The quantitative results are as in Table 7 shown earlier.

Figure 6: Qualitative calculation of risk (using risk matrix)



Threat Scenario			*Unmitigated*			*Mitigated*		
Thr	*to*	*SA*	*Likelihood*	*Impact*	*Risk*	*Likelihood*	*Impact*	*Risk*
☐ Intcp	=>	Fob	1	5	20	1	5	20
☐ Relay	=>	Fob	5	5	100	5	5	100
☑ **Relay**	**=>**	**TEST**	**5**		**NaN**	3	1	**12**
☐ Theft	=>	Fob	1	5	20	1	5	20

Another objective of the work was to explore a ‘light’ architecture approach. The prototyping therefore included a diagramming function, which was used to capture primary and supporting assets in diagram form and link them to the other functions. This is shown in Figure 7. This approach was found to benefit the initial construction of risk assessments, as it helped users visualise the scope of the risk assessment and relationships between assets.

Figure 7: Light architecting for primary and supporting assets

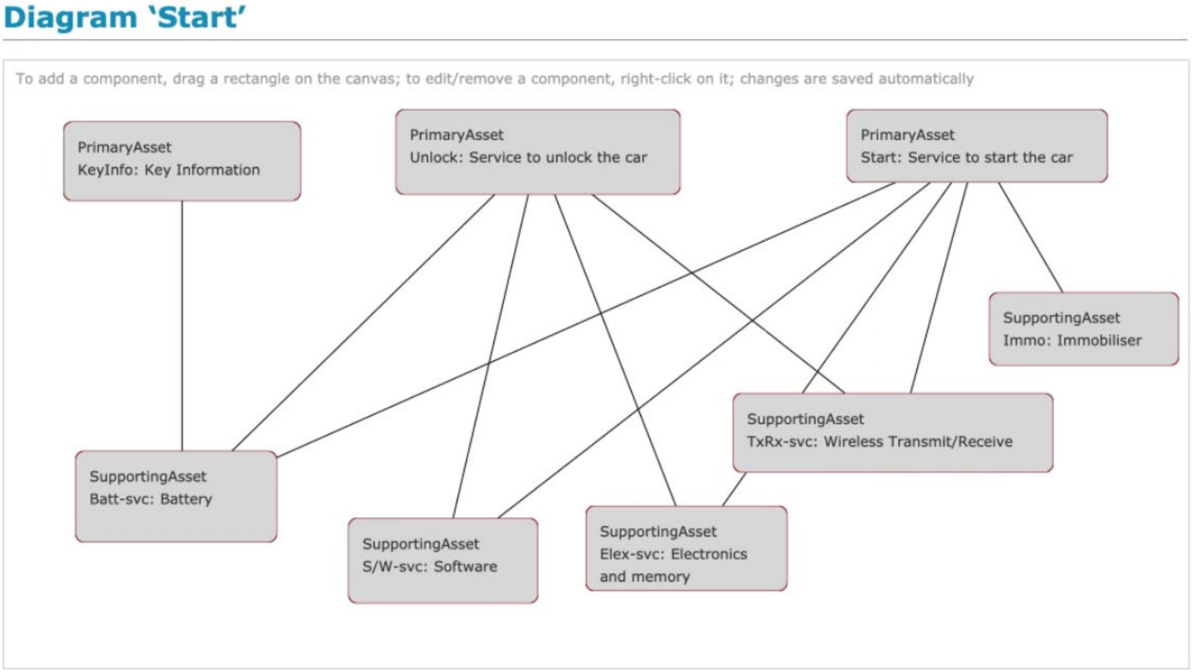


Diagram 'Start'

To add a component, drag a rectangle on the canvas; to edit/remove a component, right-click on it; changes are saved automatically

PrimaryAsset KeyInfo: Key Information
PrimaryAsset Unlock: Service to unlock the car
PrimaryAsset Start: Service to start the car
SupportingAsset Immo: Immobiliser
SupportingAsset TxRx-svc: Wireless Transmit/Receive
SupportingAsset Batt-svc: Battery
SupportingAsset S/W-svc: Software
SupportingAsset Elex-svc: Electronics and memory

2.4.2.3 STORM 2 prototype

The STORM 2 prototyping was limited in comparison to STORM 1 and focused on how to share different levels of information based on the level of trust between the sharing parties. At the highest level of trust, STORM 2 is not required as information sharing can be directly through STORM 1. For example, a shared cyber security risk assessment of radar network could be established by ANSPs in a FAB, or sharing of security information between ANSPs in an ATM Systems technology collaboration. Such information sharing would be underpinned by ED-201 type agreements. For less close partnerships, the role of STORM 2 is to share less specific information. The project focused on the utility of this, with a simple use case being the sharing of a template risk assessment among ATM service providers; the benefit being the creation of a common approach and understanding of interfaces, if not the exact details.

2.4.2.4 Bayesian network modelling

A proof of concept was developed to show the feasibility of some of the functions. The simulations were performed for a simplified system consisting of a single supporting asset, a single threat type, and 2 different security controls: SC1 and SC2. The model observes different incidents (or risk assessments performed by different specialists) that are fitted into our inference engine. Each incident/assessment description consists of the following information:

1. Mitigated impact - the impact that was assessed/registered for this incident by the experts.

2. Presence of SC1 and SC2 for the case, when the impact was registered

In total, 10 incidents were recorded.

The following assumptions for the model were made:

1. In the case where there are no security controls, the impact is (or is assessed by experts as) a random variable with mean 4.4.

2. When security controls are deployed, the impact is reduced according to some ‘efficiency’ parameter of the corresponding security control. This reduction also has a random nature and can be described by some probability distribution. The mean efficiency for SC1 is 0 (which means that it is useless within the scope of the model), mean efficiency for SC2 is -3 (quite efficient).

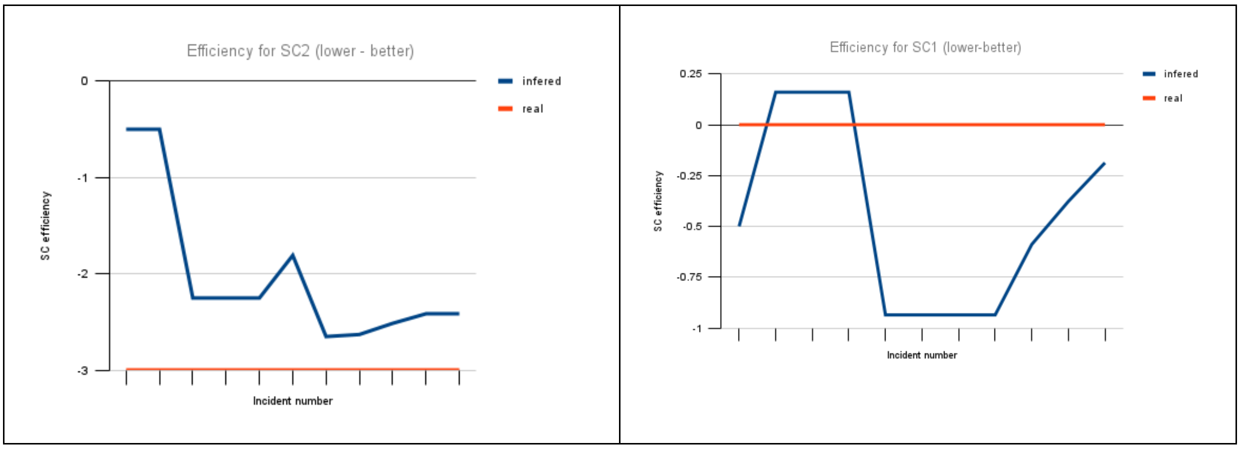
Initially, the "no-security-control" impact and efficiencies for each security control are unknown. We start with the assumption that the impact with no security controls is 3.3, efficiency parameter for each SC is -0.5. After that, the model observes the data entries one by one in the order they are presented (simulating an online inference). For each new incident, the model updates the understanding about:

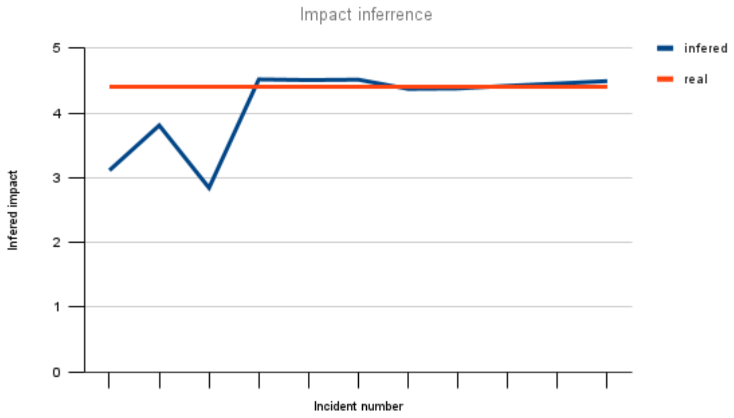
1. "No-security-control" impact mean and variance.

2. SC1 efficiency mean and variance.

3. SC2 efficiency mean and variance.

The results of the modelling are presented in the following figures. It can be seen that the correct value of the “non-mitigated” impact is available just after 4 observed incidents. The efficiency of each security control is assessed less precisely, but after just 3-4 observations it is clear that SC1 is not effective and SC2 is.





3. Conclusions, next steps and lessons learned

3.1 Conclusions

Overall, the project has provided insight and emerging methods and tools that should improve cyber security management in ATM. Specifically, the project has:

a) **Identified how ATM stakeholders could enhance their collaboration on cyber security through productivity tools**. The concept of operation has considered the factors that can encourage or discourage exchange of information and proposes a way of collaborative working, which also requires productivity tools to support information exchange and increase efficiency.

b) **Evolved risk methods in ATM from purely qualitative to quantitative methods**. The project has also provided insight into the use of quantitative methods in risk assessment and shown how to adapt the SecRAM methodology to this. We conclude that quantification does not add significant overhead to risk assessment, and there is an opportunity for partners to share, for example, impact assessments of the loss of CIA to primary assets. 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. This said, harmonisation of methodology, such as through ISO 27005 or SecRAM, is likely to have a bigger impact on sharing risk management information.

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. Although the prototyping was fairly simple, the visualisation provides user benefits in terms of appreciating the overall system. This light approach means that risk assessment and enterprise architecture could be done more in parallel in the SESAR processes without a need for resource intensive architecting to proceed first. This makes the process easier to do for early stage development of SESAR Solutions at V1 and V2 validation stages where Solution architecture may be incomplete.

The outputs from the project have moved the work from TRL2 maturity (outline concept) to a more mature concept, a demonstratable prototype and software test pieces, which we estimate at TRL3-4.

3.2 Next steps

This has been a fairly broad project, looking at several lines of innovation and there is significant potential to develop the work through development of an end-to-end prototype. In the near term, the team plans to conduct further validation and demonstrations. Following from this and subject to stakeholder feedback, the team envisages the following next R&D steps, potentially funded through future SESAR calls:

- Co-creation of the user experience with end users. The user interface developed in this project was fairly sparse and we developed numerous ideas to present risk data differently, with the aim of increasing the effectiveness of the prototypes as productivity tools.
- 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 to explore how to connect the cyber security of different domains in aviation.

3.3 Lessons learned

The catalyst funding was invaluable for this type of low TRL project and a good size. It allowed the project team to explore a variety of ideas and determine future direction for development. The freedom to make multiple minor 'pivots' in the project were very welcome and the project outputs are now of sufficient maturity to specify a much larger project that could be accelerated through the innovation pipeline.

From a management perspective, the project would have benefited from bringing our operational partner into the project earlier. The reason for not doing this was because it was felt that the ideas needed to be demonstrated to be understood. This point is still valid, but the team could have spent some early prototyping time using 'Wizard of Oz'[2] prototyping. The pandemic caused some disruption and a series of face-to-face consultations would have benefited the project.

A final remark is that the catalyst funding supported what is a very under-researched area, cyber security *management*, particularly at systems level, compared with safety management. As is often noted, safety is not assured if cyber security is not managed, and there is scope for continued development of cyber security management throughout the SESAR programme and more widely in aviation.

4. Dissemination

The quantitative risk case study has fed into a forthcoming book on cyber security in transport systems, to be published by the IET in late 2021. There has been no further dissemination of the work during the project. The authors plan to submit a paper to a future SESAR Innovation Days event.

[2] In the field of human–computer interaction, a Wizard of Oz experiment is a research experiment in which subjects interact with a computer system that subjects believe to be autonomous, but which is actually being operated or partially operated by an unseen human being. Source: https://en.wikipedia.org/wiki/Wizard_of_Oz_experiment.

5. References

5.1 Project outputs

[1] Operational concept for 'Collaborative Cyber Security Management'.

[2] Prototype tool for quantitative risk assessment.

[3] A case study comparing quantitative and qualitative approaches to risk management.

5.2 Other – external references

1. Koelle, Rainer. 2007. Aviation / ATM Security: An Introduction to Resilience. In Proceedings International Summer School of Aviation Psychologist (ISAP) 2007.
2. Fowler D, Mana P, Tiemeyer B. Safety management on a European scale. In The First Institution of Engineering and Technology International Conference on System Safety, 2006. 2006 Jun 6 (pp. 10-pp). IET.
3. World Economic Forum and Deloitte. Pathways Towards a Cyber Resilient Aviation Industry. April 2021.
4. Sträter O, Dolezal R, Arenius M, Athanassiou G. Status and needs on human reliability assessment of complex systems. SRESA Journal of Life Cycle Reliability and Safety Engineering. 2012;1(1):22-43.
5. Koelle, Rainer. 2007. Aviation / ATM Security: An Introduction to Resilience. In Proceedings International Summer School of Aviation Psychologist (ISAP) 2007.
6. M Hawley, P Thomas, R Koelle, P Saxton, 'Collaborative Security Management', International Conference on Availability, Reliability and Security (ARES), September 2013.
7. Fowler D, Mana P, Tiemeyer B. Safety management on a European scale. In The First Institution of Engineering and Technology International Conference on System Safety, 2006. 2006 Jun 6 (pp. 10-pp). IET.
8. Kuri Tiscareno K et al, What can Darwin teach the aviation industry about cybersecurity? https://www.weforum.org/agenda/2019/08/aviation-industry-cybersecurity/. Accessed 2 April 2020.
9. World Economic Forum and Deloitte. Pathways Towards a Cyber Resilient Aviation Industry. April 2021.
10. EUROCAE Document ED-201 - Aeronautical Information System Security (AISS) Framework Guidance. 2015.
11. Industry Consultation Body. ATM Cyber Security Position Paper. 8 February 2018.
12. M Hawley, P Thomas, R Koelle, P Saxton, 'Collaborative Security Management', International Conference on Availability, Reliability and Security (ARES), September 2013.
13. Ahituv, N. and Neumann, S. (1986) Principles of Information Systems for Management, Dubuque, Wm, C. Brown Publishers.
14. Security Risk Assessment methodology for SESAR 2020. Version 02.00.00 17 September 2021.
15. Chockalingam S et al. Bayesian network models in cyber security: a systematic review. In Nordic Conference on Secure IT Systems 2017 Nov 8. Springer.
16. Fota N et al, Using Dynamic Risk Modelling in Single European Sky Air Traffic Management Research (SESAR). In European Safety and Reliability Conference ESREL, Wroclaw, Poland 2014.
17. Chivers H, Clark JA, Nobles P, Shaikh SA, Chen H. Knowing who to watch: Identifying attackers whose actions are hidden within false alarms and background noise. Information Systems Frontiers. 2013 Mar 1;15(1):17-34.

18. Saxton P. The impact of consensus on performance in monopolistic supply situations in the air transport industry. DBA Thesis. 2004.
19. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 2017 Jul 24;5:14757-67.
20. S Rafweli and D Raban, 'Information sharing online - a research challenge', 2005.
21. Ahituv, N. and Neumann, S. (1986) Principles of Information Systems for Management, Dubuque, Wm, C. Brown Publishers.
22. Raymond, E.S. (2001) The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary, Cambridge, MA: O'Reilly.
23. Garrido-Pelaz, R., González-Manzano, L. and Pastrana, S., 2016, October. Shall we collaborate? A model to analyse the benefits of information sharing. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 15-24).
24. Connolly, T. and Thorn, B.K. (1990) 'Discretionary databases: theory, data, and implications', in J. Fulk and C.W. Steinfield (Eds.) Organizations and Communication Technology, Newbury Park: Sage Publications, Inc., pp.219–233.
25. C Perentis et a. Anonymous or not? Understanding the Factors Affecting Personal Mobile Data Disclosure.
26. Cybersecurity Insurance | CISA - CISA.govwww.cisa.gov › cybersecurity-insurance.
27. For context: https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/gemalto-and-ponemon-institute-study-big-gaps-emerge-between-countries-on-attitudes-towards-data-protection-in-the-cloud.

Annex I: Acronyms

Term	Definition
ACC	Air Traffic Control Centre
AISS	Aeronautical Information Systems Security
BULATSA	Bulgarian Air Traffic Services Authority
CDM	Collaborative Decision Making
FAB	Functional Airspace Block
ICB	Industry Consultation Body
ISAC	Information Sharing and Analysis Centre
PA	Primary Asset
PGM	Probabilistic Graphical Model
PKES	‘Passive Keyless System’ or
RKS	Remote Keyless System
SA	Supporting Asset
SC	Security Control
SecRAM	(SESAR) Security Risk Assessment Methodology
STORM	Shared Trans-Organisational Risk Management
TWR	Tower air traffic control
WEF	World Economic Forum