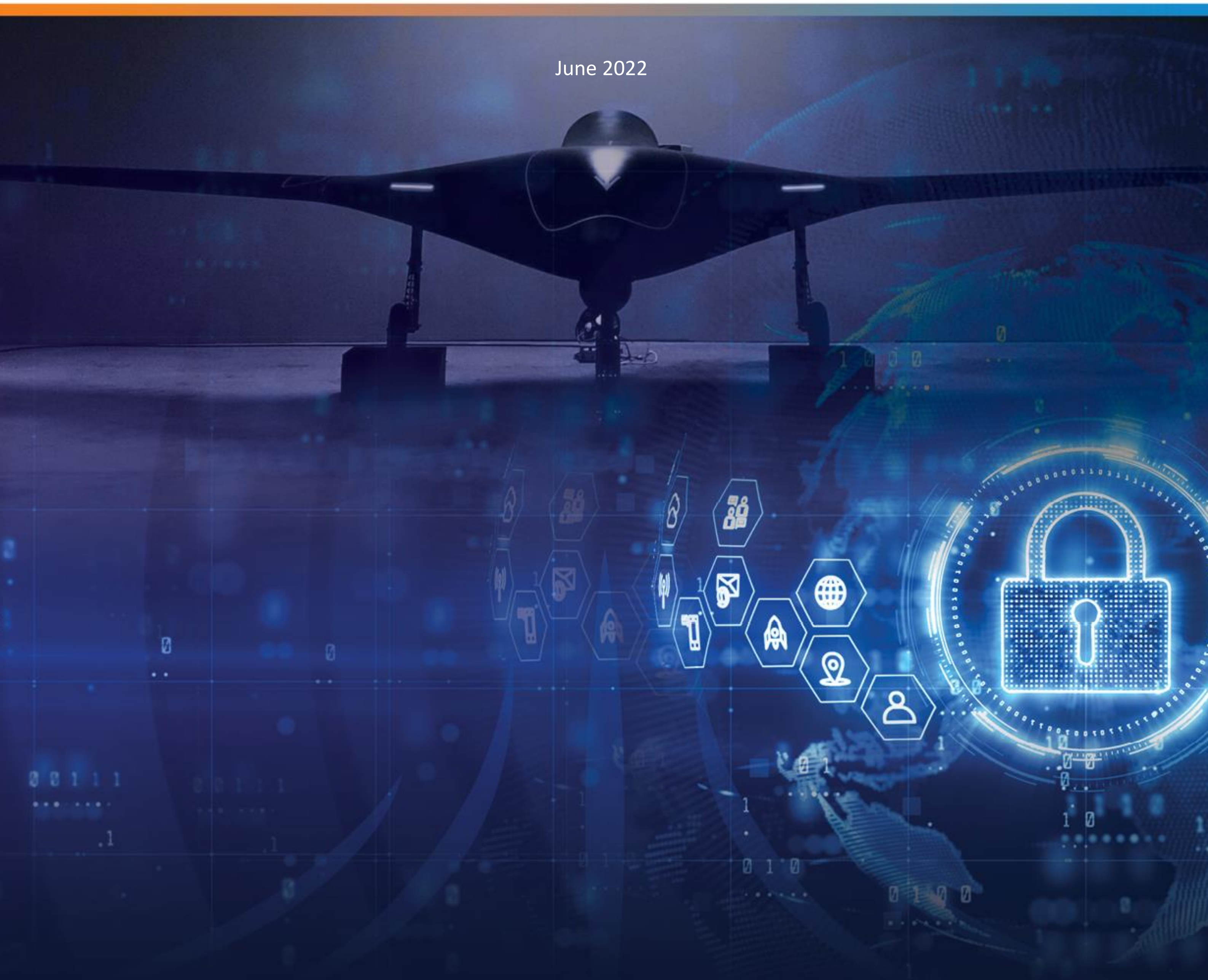
RHEA GROUP

LOTUS: Security Aware Concurrent Design for a Low Observable Tactical Unmanned Air System



June 2022

Overview

The Low Observable Tactical Unmanned Air System (LOTUS) project is a €9.7 million initiative to create a Europe-wide, cyber-resilient unmanned aircraft with a stealth design. Funded by the European Commission (EC) through the European Defence Industrial Development Programme (EDIDP), the aim is that it will contribute to the competitiveness and growth of the European Union’s defence capabilities. Uniquely, it is being designed in Europe and made with mainly European parts.

The 4-year project covers the design, production of prototypes and testing. RHEA System B.V., RHEA Group’s company in The Netherlands, is part of the LOTUS consortium that is developing this next generation of tactical remotely piloted aircraft systems (TRPAS). We were chosen to lead the cybersecurity work and provide concurrent design expertise. This dual role presented an opportunity to integrate both methodologies and develop a process that enabled a full-scale cybersecurity assessment early in the project.

Timescale

- LOTUS project start: December 2020
- Duration: 45 months
- Scheduled completion: 2024

Authors

Sam Gerené
Programme Manager National Accounts / Competence Area Lead Concurrent Design & MBSE
s.gerene@rheagroup.com

Gwendolyn Kolfschoten
Concurrent Design Expert
g.kolfschoten@rheagroup.com

Danilo Ingami
Senior Technical Project Manager
d.ingami@rheagroup.com

Felice Maccaro
Senior Technical Project Manager
f.maccaro@rheagroup.com

Ana-Maria Matejic
Senior Manager, Security Services
am.matejic@rheagroup.com

Matteo Merialdo
Director, Engineering – Security Services
m.merialdo@rheagroup.com

This project has received funding from the European Union’s European Defence Industrial Development Programme under Grant Agreement EDIDP-ISR-TRPAS-2019-030

About LOTUS

The LOTUS project aims to produce an all-European, low-observable, airworthy and interoperable TRPAS targeted at intelligence, surveillance and reconnaissance (ISR) missions with high survivability and advanced autonomy. It is unique in that it will be an all-European aircraft designed on European soil and made with mainly European parts.

The Hellenic (Greek) Ministry of Defence is the main stakeholder in this European Union project, supported by the Cypriot, Spanish and Dutch Ministries of Defence.

The RPAS platform is autonomous and consists of a mothership and several 'child' drones that serve as a swarm. The development will include:

- A mothership TRPAS equipped with ISR sensors, designed for low observability and high endurance, incorporating a self-protection system against enemy threats
- A system of tube-launched, foldable-wing drones, deployable from the mothership, which will remain at a safe distance
- On-board sensor data processing capabilities for target detection, recognition, identification and classification
- A ground station.

One requirement is that the aircraft should be able to take off from official airports. In addition, the aircraft(s) should be stealthy and cyber secure, be retrievable and be able to interoperate with several partner systems.

Context

Defence programme funding in Europe

The LOTUS project is being funded by the EC through the EDIDP, which is targeting the study, design and demonstration of cutting-edge technologies in the defence domain. The project will serve as a 'technology demonstrator' and was awarded following a highly competitive bidding process.

EDIDP was set up as a precursor to the European Defence Fund (EDF) and was adopted by the EC in June 2017.

The EDF is the EC's flagship programme for the support of defence capabilities in Europe through cross-border collaboration. It supports collaborative research and development and aims to foster an innovative and competitive defence industrial base, including participation by small and medium-sized enterprises. The EDF started functioning in 2021 with funding of €7.9 billion for 2021-2027.

Security by design

The return on investment of incorporating the analysis of security as early as possible in the development lifecycle of any system is well recognized. Estimates vary of the relative costs of fixing a flaw at different stages of the system development lifecycle (SDLC), but all show that it increases significantly as a programme moves further through the lifecycle. The National Institute of Standards and Technology, for example, estimated that fixing a flaw at the integration/component testing stage is 10 times more costly than at the requirements stage, and this increases to 15 times more at the system acceptance testing stage and 30 times more at the production and post-release stages. This includes making changes due to security requirements.

The LOTUS project aimed to apply the principle of 'security by design' and to incorporate a cyber-security strategy early in the project. For this purpose, several cyber risk analyses were incorporated in the project plan. However, to ensure security by design, the project went further, seeking an approach to incorporate the security assessment in the early design cycles.

Why concurrent design?

Concurrent design is a powerful methodology used to accelerate the early phases of complex, multidisciplinary engineering projects.

In a series of collaborative sessions, the client, experts from various domains and system engineers work together to develop an integrated, consistent design based on shared understanding and rigorous design decisions. The method improves the rigour and relevance of the study, accelerates the process, improves shared understanding and is focused on identifying key trade-offs and challenges early in the design process.

Concurrent design emphasizes a quantitative, fact-based approach to increase the quality of decision-making, despite the uncertainties and interdependencies characteristic for the early phases of design.

RHEA Group has applied concurrent design in a wide range of projects including defence systems, factory design and luxury yachts. Our experts have been closely involved in its application by the European Space Agency (ESA), which routinely uses it for space programmes.

Security aware concurrent design for the LOTUS project

(Cyber)security by design – the MEHARI approach

A security risk is a potential unwanted event that negatively affects an organization's security objective.

RHEA used the MEHARI methodology[1] as part of the security aware concurrent design approach adopted for LOTUS. MEHARI is a widely known European open source risk assessment methodology that is fully compatible with ISO 27001.

The actual risk analysis starts by defining risk scenarios, with each risk scenario defined as follows:

> If a certain ‘threat’ exploits a ‘vulnerability’ (exposed by one or more assets), then a negative ‘impact’ occurs to (part of) the organization.

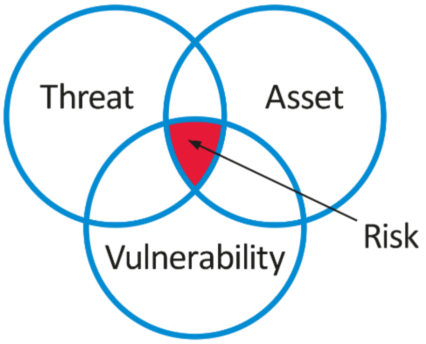


Figure 1: The three components of a security risk assessment

There are three main categories of vulnerabilities that should be considered as part of the MEHARI procedure:

- Organizational/procedural
- By design
- Technological/ implementation-related.

[1] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

In order to implement the MEHARI methodology for LOTUS, RHEA used the Secure Engineering Software Tool (SEST), a prototype software originally developed to support the system development challenges encountered by ESA in its space programmes, where cybersecurity has long been recognized as a concern.

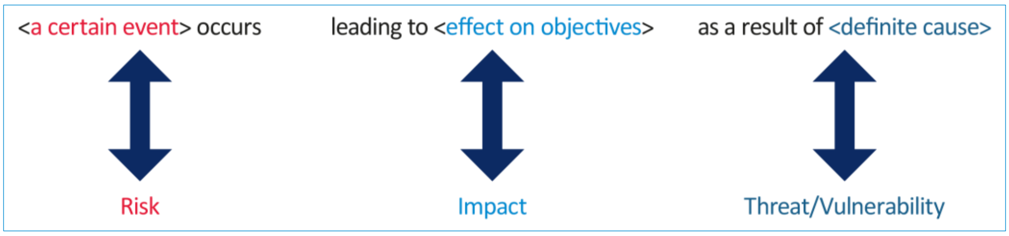

<a certain event> occurs
leading to <effect on objectives>
as a result of <definite cause>
Risk
Impact
Threat/Vulnerability

Figure 2: The correlation between threat/vulnerability and risk in determining the resulting impact

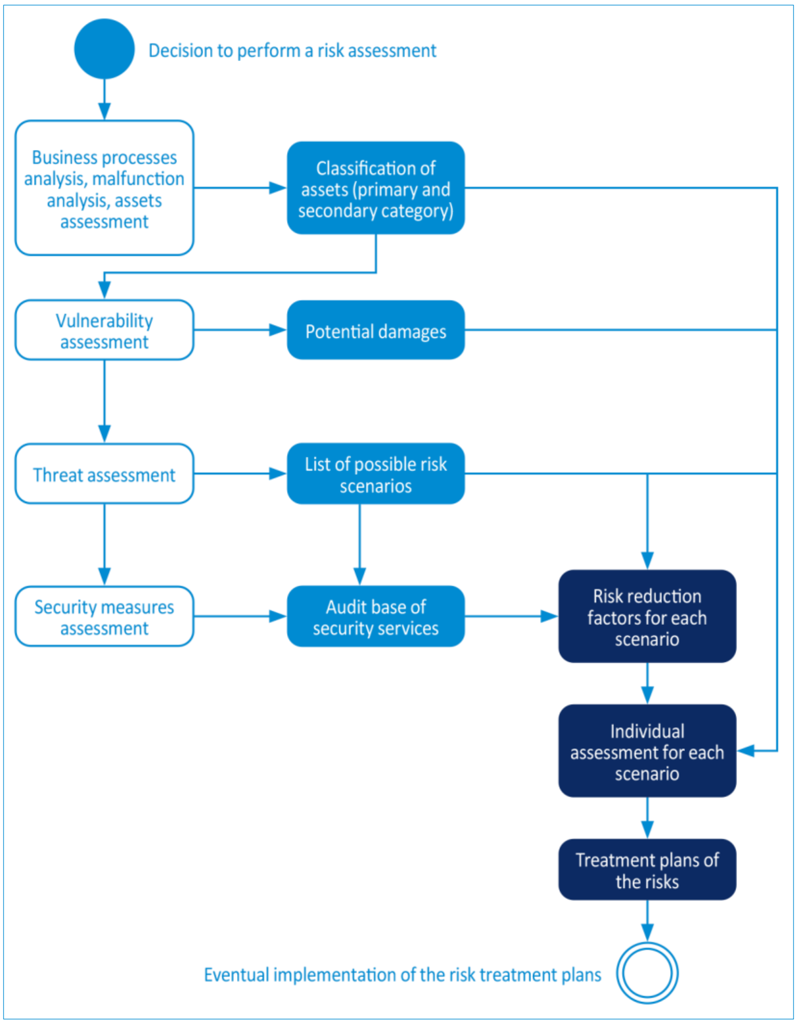

Decision to perform a risk assessment
Business processes analysis, malfunction analysis, assets assessment
Classification of assets (primary and secondary category)
Vulnerability assessment
Potential damages
Threat assessment
List of possible risk scenarios
Security measures assessment
Audit base of security services
Risk reduction factors for each scenario
Individual assessment for each scenario
Treatment plans of the risks
Eventual implementation of the risk treatment plans

Figure 3: The MEHARI risk assessment process

Integrating the methodologies

To enable security aware concurrent design, the MEHARI approach needed to be merged with RHEA's concurrent design methodology in a way that enabled security risks to be traced back to design elements and those to be traced back to design (and airworthiness) requirements. This integration was developed using the following steps.

Step 1

The first step was to import and analyze requirements. All requirements from the project as well as from airworthiness standards were incorporated in our COMET™ software for concurrent design. The requirements were analyzed and verified by the team to ensure they were unique and comprehensible.

Step 2

The system and its components were modelled in the COMET software. The components were identified and listed in several layers of abstraction to create a comprehensive system overview.

Step 3

As the project has many partners, it was important to ensure each component had an owner who was responsible for the design of the component. Using the branched system design, ownership was established for each element and domain experts were assigned.

Step 4

Similarly, requirements were analyzed again by all partners to identify who was responsible for which requirements and where partners shared responsibility.

Step 5

Linking elements to requirements, we were able to verify the completeness of the design as well as the completeness of the requirements. Some requirements were added to represent contributions of partners and, vice versa, elements were added to accommodate requirements or arguments were documented as to why a specific requirement was not relevant for the LOTUS project. This step helped the consortium to verify the completeness of the design.

In addition, important miscommunications were resolved in this phase; for instance, one partner assumed they had to purchase a device from the market whereas another partner had been contracted to design that part specifically for the project. Assigning ownership to the different components of the design ensured these misconceptions were resolved.

Step 6

Once the design was complete, all partners could start adding parameters such as mass, power consumption and other key aspects of the components to enable calculation of overall system performance, such as the mass and power budget.

Step 7

With this level of detail, the team was able to identify critical interfaces and the points where subsystems interfaced with each other. Critical interfaces were identified and partners aligned to solve integration issues. For instance, it was decided that the aircraft would have one central processor and partners were to specify performance requirements for the processor instead of adding their own hardware to the system.

In this phase, we also made everyone aware of the key design challenges; for example, the choice for the launching mechanism had a significant impact on many sub-systems. Such critical design choices were identified early and constraints from various partners were considered in the choice of a solution.

Step 8
With this initial complete design in place, the cybersecurity analysis could start.

First, the team identified key processes in the operation such as flight, maintenance, transport and storage. For each of these processes, key security risks were identified by surveying all the partners, asking them to assess the risks to determine if there was impact on integrity, availability and confidentiality.

Step 9
Once a first overview of risks was created, these were mapped on the overall system design, which meant all vulnerable elements in the design had to be identified. Using the COMET design decomposition, we were able to create a complete list of all components that were critical to aircraft control; for instance, the structure is not critical for aircraft control, but the navigation system is.

We called this step “asset classification”. During this step, we identified many elements that were critical to aircraft control beyond the obvious ones such as the CPU and communication devices.

Step 10
With the overview of assets and a first risk analysis, we could now create an overall threat analysis. For this purpose, we modelled the threats according to the MEHARI approach. However, we had to significantly extend the typology of assets to include different critical elements of the aircraft.

The model was created in our SACDP software to create a complete overview of cyber risks and to identify first critical security controls to harness and harden the aircraft.

Results

This approach rendered a first overview of security risks with a remarkably high level of detail.

The overview had several advantages compared with a regular cybersecurity assessment:

- **Completeness**: Due to the direct interface between the overall system model and the requirements, which were verified extensively by all partners in the project, we were able to generate a risk assessment with a high level of completeness.
- **Awareness and attention**: Using the collaborative concurrent design approach, the security assessment involved all key stakeholders; although some had more insights into the security risks of the overall system than others, the outcome was that all stakeholders were aware of both the key security risks and the overall impact of cybersecurity threats inherent in the system.
- **Full traceability**: The link between (airworthiness) requirements, design components and cybersecurity risks were systematically assessed. The assessment is fully traceable and the impact of design changes on the overall risk model can quickly be identified. Similarly, the impact of security controls on various system components can be analyzed with high levels of accuracy and completeness.

- **Identification of trade-offs**: As the impact of security controls and requirements are fully traceable, it will be possible to assess the impact of security measures; for instance, the use of better shielded cables will increase the weight of the harness and the overall costs of the aircraft. Such impacts can be calculated in much more detail at an early design phase.

Next steps

The LOTUS project is scheduled for completion in 2024. RHEA Group will be involved in two more tasks in the next phases of the project:

- Cybersecurity resilience testing of the ground station
- Cybersecurity resilience testing of the navigation system.

About RHEA Group

RHEA Group is a privately-owned professional engineering and solutions company, providing bespoke engineering solutions, system development and security services for space, military, government and other critical infrastructures. Since its creation in 1992, RHEA has built a reputation as a trusted partner, developing tailored solutions that help drive organizational and cultural initiatives, leading to sustainable added value for its customers.

Headquartered in Belgium, RHEA Group employs over 750 people and has offices in Belgium, UK, Czech Republic, Italy, France, Germany, Spain, Switzerland, the Netherlands, Luxembourg and Canada, and works at client premises throughout Europe and North America. RHEA is ISO 9001 and ISO 27001 certified.

RHEA Group Headquarters
Avenue Einstein 8, 1300 Wavre, Belgium
+32 (0)10 48 72 50
info@**rhea**group.com