Broad Agency Announcement
Call #003

Final Report

Contract Number 697DCK-22-C-00258
UAS Integration Office
Program & Data Management Branch
(AUS-410)

Project Title: Unified UTM Cybersecurity Model
Company Name: Unifly
Submitted By: Wim Vanderheyden (Unifly)
Report Date: 09/04/2023
Contract Period of Performance: 09/05/2022 – 09/04/2023

[INTENTIONALLY LEFT BLANK]

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The Cybersecurity Model developed during the project is based on sectoral risk analysis, gap analysis of Security Target, development and implementation of gaps, verification and validation of the results, field testing in operational conditions and under cybersecurity attacks.

The importance of this work is confirmed by the results of Cybersecurity Model refinement and implementation. Thus, being compliant with the existing regulations (for example, ISO 27001) does not lead to compliance with the UTM specific security controls and requirements which was shown at the verification and validation phase. So, the existing info- and cybersecurity standards from NIST, ISO, ISA and other organizations do not cover the UTM ecosystem in full, but only partially.

The major risks before the model implementation were:

- No defined UTM Security Objectives, Assurance Requirements and Controls so it was difficult to understand for a vendor/developer what security features a UTM product should have, and for the clients/evaluators no objective way to clearly understand if a UTM product was developed in a “secure-by-design” approach.
- No single standard/framework could cover all necessary SARs and security controls for UTM.

The Application of the developed Cybersecurity Model (it means the possibility to implement a Security Target because of the previous activity of defining a general UTM Protection Profile and use it as a reference for the gap analysis before and for the validation after), allows to have the following quantitative data as a result:

- 26 findings (8 security controls not implemented at all and 18 implemented partially) at the gap analysis stage (before the model application) compared to 11 (1 security control not implemented at all and 10 implemented partially) findings after the implementation. Their impact, priorities and resources required were analyzed and corresponding Jira tickets created.
- 18 total vulnerabilities before the model implementation compared to 16 vulnerabilities after the model implementation. Criticality level of the findings before and after the model implementation are:
    - *Before*: 4 Info, 2 Low, 9 Medium, 3 High
    - *After*: 4 Info, 3 Low, 7 Medium, 2 High

The residual risks after the model implementation are:

- For the UTM PP there are still evolving rules, regulations, threat landscapes around the UTM ecosystem. Regular re-assessment will mitigate this risk.
- Not all SARs and security controls are implemented by Unifly yet, but this is an ongoing process. At first, all high-risk items were closed in scope of the project. For all other items, the corresponding tickets and tasks are created and taken to work.
- There are findings from the penetration test which shall be remediated.

Possible ways of further development:

- Convert the Cybersecurity Model to the public framework by removing the results of and references to Unifly UTM assessment. Release of this public framework under the FAA authority.

- Convert the Cybersecurity Framework to the UTM Cybersecurity Standard and release it under FAA, NIST, ISA, ISO or CC authority.
- Push the certification schema to accreditation authorities to give a possibility to UTM vendors to certify their products and solutions.

The project was successfully executed within the expected project timeline. During this execution, 2 deviations to the master schedule were introduced towards and agreed upon with the FAA. However, the project was executed and concluded within the identified period of performance of 1 year (09/05/2022 – 09/04/2023).

Next to the timely execution of the project, all identified objectives of the project were achieved. A UTM cybersecurity model was refined by means of requirements and certification schema definition.

2. INTRODUCTION

Background

The notional unmanned aircraft systems traffic management (UTM) architecture described by the FAA in UTM Concept of Operations (CONOPS) v2.0 consists of a complex 'ecosystem of systems, interconnected and operated by a set of different stakeholders. The key characteristics of UTM systems – software, highly automated, and relatively recent – make it by nature a very attractive target for cyberattacks that exploit vulnerabilities to threaten aviation safety, the privacy of airspace users, and business operations.

Although cybersecurity is unanimously recognized as a critical safety concern, to this date UTM cybersecurity has been only partially explored, either by considering a limited subset of security attributes (e.g., authentication) or by applying generic cybersecurity frameworks (e.g., NIST) that do not provide sufficient cyber resilience for the complex ecosystem that is UTM. As a result, no comprehensive approach to system requirements, and much less a unified certification scheme, has been developed to assess and validate cybersecurity for UTM systems.

This leads to the definition of this project – Unified UTM Cybersecurity Model as part of the Broad Agency Announcement call 003. The project was awarded on 08/26/2022 and the period of performance runs from 09/05/2022 until 09/04/2023

The consortium of the project consists of

- Unifly: UTM system provider serving as prime contractor.
- RHEA Group: Cybersecurity experts serving as subcontractor.
- NUAIR: New York Test Site Operations Manager serving as subcontractor.

Project objectives and scope

In partnership with the NY Test site and Rhea, the objective and purpose of the project was to demonstrate, in an operational environment, a unified cybersecurity model for UTM systems that follows the principle of 'security by design'.

The scope of this project encompasses the model refinement to factor in operational conditions, the UTM cybersecurity model demonstration and cybersecurity certification scheme validation. The updated prototype model is demonstrated by conducting actual flights for system testing and data gathering in an operational environment.; three scenarios shall be considered during the scheme validation: (1) operations under ideal conditions, (2) operations under attack, and (3) operations while employing attack countermeasures.

In general, the project objective is twofold:

- Refine a UTM cybersecurity model (requirements and certification).
- Validate this refined UTM cybersecurity model in operational conditions.

3. APPROACH

Project phases

The followed approach was to define the entire project into 5 phases:

- Phase 1: Project Initiation
- Phase 2: Model Refinement
- Phase 3: Secure UTM System Deployment
- Phase 4: Testing & Validation
- Phase 5: Project Closing

These 5 phases were addressed in the following tasks and subtasks:

- Task 1 – Project Initiation
  - 1.1 Kick-off Meeting Presentation
  - 1.2 Integrated Master Schedule (IMS) creation
- Task 2 – Cybersecurity model refinement
  - 2.1 Stakeholder interviews
  - 2.2 Cybersecurity model refinement
  - 2.3 Design report
  - 2.4 - Initial Test and Evaluation Master Plan (TEMP) creation
- Task 3 – Secure UTM system deployment
  - 3.1 Software Development Life Cycle (SDLC) conductment
  - 3.2 System Gap Analysis conductment
  - 3.3 Identified gaps implementation
  - 3.4 Secure UTM system deployment and validation
  - 3.5 Final Test and Evaluation Master Plan (TEMP) creation
  - 3.6 Cyberattack Scenarios documentation
  - 3.7 Test Flight Plan creation
- Task 4 – Testing and validation in operational conditions
  - 4.0 Preparation
  - 4.1 Demonstration 1: UTM operations under ideal conditions
  - 4.2 Demonstration 2: UTM operations under attack
  - 4.3 Demonstration 3: UTM operations under attack while employing attack Countermeasures
  - 4.4 Test Report – Prepare the Test Report on demonstrations 1-3
- Task 5 – Project closing and reporting
  - 5.1 Final Technical Report
  - 5.2 Final Project Presentation
  - 5.3 Monthly Project Progress Reports
  - 5.4 Quarterly Project Management Review (PMR) Briefings

Project initiation

The initiation of the project was covered by means of the following 2 activities:

- An official **kick off meeting** took place between the FAA and the prime contractor Unifly. Within this meeting the participants received information about the project (the scope, milestones and deliverable) and the steps were outlined for the upcoming tasks in the project.

Next to this, some administrative aspects like invoicing was explained and how the lines of communication between the project participants are managed.

- Next to the official kick off meeting, a task was identified to create an **Integrated Master Schedule (IMS)**. This IMS described the project overview (Partners roles & responsibilities), the scope of each (sub)task and the linked deliverables together with a detailed project timeline. Next to this, if applicable for a (sub)task, the related personnel, equipment and facilities were described. This IMS was delivered in the format of a word/PDF document together with an Excel annex.

During the course of the project, 2 revisions to the IMS were introduced by the prime contractor. The first revision introduced an extension of task and milestone 2 - Cybersecurity model refinement. The second revision introduced an extension of task and milestone 3 -Secure UTM system deployment. Both revisions were needed to make sure that the tasks identified in these milestones could be executed and would adhere to the quality expectation needed. Both suggested planning updates were discussed and agreed with the FAA in a dedicated meeting.

Despite these modifications to the planning, a mitigation was found and put in place within the milestone 4 - Testing and validation in operational conditions in which the original timespan of 5 weeks to perform the flights for the 3 demonstrations was reduced to 2 weeks. By means of this mitigation, it was possible to complete the project within the projected time of 1 year.

Cybersecurity model refinement

During the second phase of the project, the **cybersecurity model refinement**, the approach was used to consult with several representatives from the UTM ecosystem stakeholders in which we presented the unified UTM cybersecurity model and asked for their input via specific questions.

Unifly engaged with major **stakeholders** in the field of aviation to learn about current security requirements required to exchange with current ATM systems and which could be applicable to future UTM systems. The world of aviation in general and Air Traffic Management in particular, is very well regulated and has very high standards and requirements when it comes to safety and security both on the hardware, environments, systems and platforms that are being used. As a consequence, ATM systems need to adhere to very high security standards and are often operated on proprietary platforms. UTMs, which are a fully digital system have several points of exchange with existing ATM systems to exchange information (e.g., on airspace) and data (such as traffic data of manned and unmanned aircraft) and thus one will need to ensure that this integration and/or exchange of data between the two systems can be performed in a secured way.

Unifly has conducted 5 interviews with following stakeholders:

- DroneUp – Drone industry enabler
- NASA – National Aeronautics and Space Administration
- CNA - The National Security Analysis
- FAA ATO – Federal Aviation Administration – Air Traffic organization
- Nav Canada - The Air Navigation Service Provider of Canada

All interviews lasted between 1 and 2 hours and were conducted with the same structure to maintain uniformity between the different stakeholder interviews. The following questions were asked during the interviews:

- Cybersecurity frameworks - The following questions were asked related to cybersecurity frameworks to obtain feedback
  - Is there a need for a UTM specific cybersecurity framework?
  - Are there cybersecurity frameworks that should be part-of or used as a baseline? (ISO27001, NIST 800-53, ….)
  - Are there other sector specific (related to Traffic Control) frameworks that should be part-of or used as a baseline? (ICAO, …).
  - What should be excluded / avoided in a UTM cybersecurity framework?
  - Insights in do's and don'ts / Lessons learned?
- Feared events and cyber threats - The following questions were asked related to feared events and cyber threats to obtain feedback
  - Who are the potential Threat Actors against a UTM platform? (Same as ATM? ….)
  - Which are the feared events/threats that must be considered
  - Which are the feared events/threats that must be excluded
- Question and feedback - Opportunity for the participants to ask questions or provide feedback.

During the interview, the feedback from the participants was gathered on the slide deck. In parallel, more detailed notes were kept a well. After every interview, the interview notes were shared with the participants together with slide deck containing the feedback.

Together with this input, the project team refined both the system requirements and the security controls to be used in the model for design freeze. This resulted in the **design report**, which documented the refined cybersecurity model consisting of 3 components:

- UTM Certification Scheme: A description of key elements of the certifications, customized where necessary for the aviation sector in which the UTM system operates. Also, the protection profile for the UTM system, based on the context assessment, sectoral risk assessment, threat intelligence, security problem definition and selection of security objectives and controls was described
- System Design requirements: An outline of the requirements of the UTM specific technological solution (The UTM security target) that needs to be implemented in order to comply with the identified protection profile
- Security Controls and Countermeasures: A description of a set of security controls and countermeasures selected from the security domain to fulfill the security objectives, based on controls from ISO 27001 and mapped towards the NIST controls.

Next to the cybersecurity model refinement and the creation of the design report, the **Initial Test and Evaluation Master plan (TEMP)** was created to outline the suggested methodologies, based on international standards and best practices to;

- Implement a secure Software Development Life Cycle (SDLC) methodology
- Conduct the System Gap Analyses methodology
- Approach a UTM Cybersecurity Certification

The test and evaluation methodology which was followed to assess/validate and report:

- The maturity level of Unifly in applying a Secure Software Development Lifecycle (SSDLC) approach.
- The GAPs between the current Unifly UTM solution against the System and Security requirements (controls and countermeasures) identified during the Cybersecurity model refinement.
- The Unifly UTM after the implementation of the needed system and security requirements in an operational environment and also through realistic cyber-attack scenarios (Penetration Tests).

Secure UTM system deployment

The third phase of the project, the **secure UTM system deployment**, started with the conductment of the **Software Development Life Cycle (SDLC)** of the Target of Evaluation (TOE): The Unifly System. The SDLC was performed by the independent cybersecurity experts of Rhea. During the SDLC conductment, a thorough analysis has been conducted on the Unifly policies, processes, procedures, and tools against the Security Assurance Requirements (SARs) and the Security Controls (SCs) strictly related to the SDLC process defined in the Unifly UTM Security Target.

In parallel, the "as-is" UTM system would undergo a **System Gap Analysis** to check the compliance with the "to-be" system design requirements, security controls and counter measures defined in the cybersecurity model refinement. The gap-analyses also contained scores by security domains and a classification of the nonconformities/gaps was documented based on different criteria (risk level, dev or non-dev work, resources needed, testable in attack scenarios, within or beyond FAA scope and overall priorities. This resulted in a list of all nonconformities/gaps identified for which the implementation plan and corresponding tasks were created. Based on the classification criteria mentioned, a set of non-conformities was prioritized to serve as gaps that would be closed in the scope and timespan of this project.

After the conclusion of the gap analyses, the task to **implement the identified gaps** was started. This implementation consisted of both development tasks (technical tasks directly performed in the UTM system) and non-development tasks (For instance implementations on policy level). After the implementation, the secure Unifly UTM was securely deployed in the operational environment.

The security experts of the subcontracting partner Rhea had to validate this production environment against the system design requirements. This resulted in **UTM validation report** with 3 sections:

- SAR Prerequisites Validation Report: List of all the Security Assurance Requirements
- SAR Primary Validation Report: List of all the Primary Security Assurance Requirements
- Security Controls Validation Report: List of all the Security Controls defined in the "UTM

In each section a description of the check result (pass/partially/fail) together with notes and evidence was presented in table form.

Next to this implementation steps, the **final Test and Evaluation Master Plan (TEMP)** was created. On top of the content of the initial TEMP described above, the final TEMP contains the test and evaluation methodology that was followed to assess, validate and report:

- The maturity level of Unifly in applying a Secure Software Development Lifecycle (SSDLC) approach.

- The GAPs between the current Unifly UTM solution against the System and Security requirements (controls and countermeasures) identified during the Cybersecurity model refinement.
- The Unifly UTM after the implementation of the needed system and security requirements in operational environment.

The final TEMP also used the input from other tasks in this milestone in order to describe SDLC Analyses Report, Gap Analyses report, UTM Validation report. In order to prepare the testing and evaluation in operational conditions, a task was identified to create cyberattack scenarios for the identified system requirements and security controls to be conducted during the testing and evaluation of the system in operational conditions. The list of these attack scenarios were also documented in the final TEMP.

The last task of the Secure UTM deployment phase covered the description of the flight test plan that will be executed during the demonstration phases. A test flight plan is a generic flight plan that was used to cover all needed flights. It describes the different actors (the Unifly UTM platform, The Unifly tracking device (BLIP), the UAS, the pilot and mission commander and the flight details). Next to this, the prerequisites, actions on take-off, actions during flight and actions at the end of the flight were described as flights together with an overview of the demonstration environment for the penetration test. To conclude, a list of rules of engagement were outlined containing some assumptions and mitigation actions to ensure safe flights.

Testing and evaluation in operational conditions

The fourth phase of the project, the **testing and evaluation in operational conditions,** started with some **practical flight preparation** time between Nuair and Unifly to make sure that everything was in place and tested to conduct the flights. The main activity performed was the test that an operational area could be created in the UTM system and that tracking positions of the drone were received in the UTM by means of the BLIP tracking device mounted on the drone.

After the preparations, the flight demonstrations were executed. The project plan defined the following 3 phases:

- **Demonstration 1**: UTM operations under ideal conditions, with 20 live flights of at least 15 minutes each, following the Test Flight Plan. The UTM system used was the non-secured UTM system.
- **Demonstration 2**: UTM operations under attack, with 20 live flights of at least 15 minutes each, following the Test Flight Plan and the Cyberattack Scenarios. The system used was the non-secured UTM system.
- **Demonstration 3**: UTM operations under attack while employing attack countermeasures, with 20 live flights of at least 15 minutes each, following the Test Flight Plan and the Cyberattack Scenarios. The system used was the secured UTM system, which contains the implementation of the selected gaps.

For the execution of the flights, the project team concluded together with the FAA to step away from the timing of the flights and how it was defined in the project schedule. Instead of using, for every demonstration phase, a dedicated week and a reserve week in between the demonstrations for reporting, the decision was made to **combine all demonstration flights** in a timespan of 2 weeks (1 week where members of all project partners were present at the test site, and 1 week of “remote” flights to conduct the remainder of the flights). This was introduced as a mitigation measure to make

sure the project stayed on track regarding timing so the project can be closed within the 1-year timeframe. This even had the result we landed before the initial project schedule after the flights of demonstration 3, leaving enough time for reporting. Next to this, organizing all flights like this was more efficient with respect to travel arrangements and equipment reservation.

The consolidation of the flights into 1 flight campaign also had the result that all flight data was captured in 1 flight data report instead of 3. Next to this flight data report, a dedicated test report on the demonstrations was created to describe the result of the penetration test activities executed by means of the attack scenarios against the non-secured versus the secured UTM target.

Project closing

The fifth and final phase in the project is the **project closing** task.

As a first task, a **final report** was created outlining the activities performed during the project. Focus is mainly put on the approach that was used in the project, the general results and achievements, and the data analyses. Also, lessons learned were documented together with some recommendations for future potential projects.

Next to this, a **final project presentation** was organized in which the project partners prepared a final project briefing slide deck which was presented toward the FAA in a zoom meeting.

4. OBSERVATIONS / RESULTS

Main project results

The UTM Cybersecurity Model developed in this project, consists of the three main components:

- UTM Certification Scheme:
  - Certification Key elements
  - UTM Protection Profile
- System Design Requirements:
  - UTM Security Target
- Security Controls and Countermeasures:
  - Customization of security controls and countermeasures

The certification scheme is compliant with the U.S. and European regulations and takes inspiration from existing recognized certification frameworks.

The Key elements are related to the procedural part of the certification and have been suggested by sector experts by maintaining the general alignment of settings from the certification framework. This information will be used in the future lifecycle of the certification achievement and maintenance.

The Protection Profile has been developed taking into consideration the needs and obligations of a general UTM provider so that it can be considered in the future, within the context of the USA and EU, as a security baseline for security and assurance requirements to be considered for certification purposes of a UTM System.

Based on the UTM Protection Profile, the UTM Security Target reflects the proposed solution of UTM implemented by the specific developer represented by Unifly. The UTM Security Target inherits and extends the Protection Profile, according to specific implementation decisions and needs of the UTM Unifly solution. A typical Security Target (ST) fulfils two roles:

- Before and during the evaluation, the ST specifies “what is to be evaluated”. In this role, the ST serves as a basis for agreement between the developer and the evaluator on the exact security properties of the Target of Evaluation (TOE) and the exact scope of the evaluation. Technical correctness and completeness are major issues for this role.
- After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST describes the exact security properties of the TOE in an abstract manner, and the potential consumers can rely on this description because the TOE has been evaluated to meet the ST. Ease of use and understandability are major issues for this role.

The UTM System is evaluated against the UTM ST. All work produced can be seen as a Cybersecurity Model Refinement, that with the complete gap analysis with respect to the SDLC completes the refinement of the existing UTM System.

Nevertheless, the UTM ST has been drafted, taking into consideration all of the security and architectural features that exist at the moment for the production of this deliverable.

The results of the gap analysis with respect to the SDLC, security and assurance requirements serve to improve the UTM System version. The applied enhancements are tested: it is part of the assurance activities. Both the results of documental checks and penetration tests are the assurance evaluations that are reported in a document called Evaluation Technical Report and the final version of the TEMP deliverable.

The results of this project clearly show that the developed model goes far beyond NIST CSF, ISA 62443, ISO 15408, ISO 27001 and other existing standards.

The selected security controls represent a finely granulated extract of existing controls in other standards but covering all aspects of the UTM where the triad CIA (Confidentiality, Integrity and Availability) is replaced with AIC (Availability, Integrity and Confidentiality) and the safety is more important than information security.

Security in UTM systems is primarily concerned with maintaining the availability of all system components. Integrity is second in importance. Confidentiality is of lesser importance, because often the data is raw in form and must be analyzed within context to have any value. Depending on the circumstances, the integrity of the system could also have the highest priority. Certain operational requirements will cause individual components or the systems to have different priorities for the objectives (i.e., integrity or availability concerns may outweigh confidentiality, or vice versa). This may in turn lead an organization to deploy different countermeasures to achieve these security objectives. Based on this, the following security objectives were defined with their corresponding priority in security control implementation:

- High priority:
    - Data availability
    - Data integrity
    - Event logging & log management
    - Business continuity
- Medium priority:
    - Data confidentiality
    - Access control
    - SSDLC
    - Security by design & default

Assessment of the achievements in light of the objectives

The achievements in the creation of a Protection Profile for a UTM (Unmanned Traffic Management) platform inside a structured Certification Scheme can be detailed as follows:

- Holistic Approach: considering the vast amount of documentation, regulations, outcomes of stakeholder interviews, and cybersecurity frameworks, the project's team has managed to develop a comprehensive Protection Profile for UTM within a predefined time frame proving strong project management, research, and organizational skills.

- Defining Boundaries: Successfully defining the boundaries of the Target of Evaluation is crucial in any security domain, and it becomes even more challenging when dealing with emerging technology areas like a UTM. The ability to discern what falls within the scope of UTM and what's considered external is an achievement that helps establish clarity and sets a foundation for further security evaluations.

- Adapting to Lack of Historical Data: Given that the UTM ecosystem is relatively new and lacks substantial historical or statistical data as a foundation on cybersecurity attacks, the team's ability to define potential threat actors and evaluate their Attack Potentials brought to light through the project's innovative approach and flexibility.

- Creating a Comprehensive Security Baseline: The resultant UTM Protection Profile, designed considering the general needs and obligations of a UTM provider, has the potential to serve as a foundational security baseline for the US and EU. This ensures that future UTM systems can be certified with robust, well-understood, and agreed-upon security and assurance requirements.

- Facilitating Future Innovations: Given that the UTM space is rapidly evolving, the creation of such a Protection Profile aids paving the way for further innovations in the UTM space. With a defined security baseline, new entrants and existing stakeholders can build upon a standardized security framework, reducing ambiguities and accelerating development.

Furthermore, drafting a Protection Profile for a software product like the UTM platform brings numerous benefits. These benefits not only reinforce the significance of the above-mentioned achievements but also provide a rationale for creating a specific protection profile. Below are some of the most important achieved benefits:

- Standardized Security Requirements: A PP provides a set of standardized security requirements for products within a particular domain. This ensures that all products evaluated against this profile adhere to the same baseline, fostering interoperability and consistency.

- Facilitates Mutual Recognition: Products evaluated against a PP can benefit from mutual recognition agreements, meaning that a certification in one country can be recognized in other participating countries. This can lead to increased market access and reduces the need for multiple, redundant certifications.

- Boosts Stakeholder Confidence: Having a PP demonstrates to stakeholders, including customers, regulators, and partners, that the product has undergone rigorous security evaluation. This can improve trust and confidence in the product's security features.

- Resource Optimization: Adopting a PP provides a clear roadmap for security requirements, allowing developers to allocate resources more effectively. By adhering to an established framework, they can avoid unnecessary redundancies and ensure efforts are directed towards fulfilling well-defined security criteria.

- Competitive Advantage: In a market where security is becoming a primary concern, having a product evaluated against a recognized protection profile can offer a competitive edge, differentiating it from products without such validation. The UTM used in this Unified UTM Cybersecurity Model project poses strong foundations for a commonly adopted protection profile already proposing a well-defined framework that in the future could be proposed to be officially recognized (i.e. by Common Criteria, EU CC).

- Enhanced Product Development: The process of aligning a product with a protection profile often leads to the discovery of potential vulnerabilities or areas of improvement. This iterative process results in a more robust and secure final product.

- Flexible Risk Management: a PP defines high level potential threats associated with security domains. With the guidance of a security domain, any security catalogue can be applied to counteract the threat.

- Continuous Evolution: A protection profile isn't static. As new threats emerge and technologies evolve, the profile can be updated, ensuring that products evaluated against it are always aligned with current best practices and threat landscapes.

- Legal and Regulatory Compliance: Especially in sectors where regulatory scrutiny is high, a PP ensures that a product adheres to industry standards and regulations. This can reduce legal risks and streamline compliance processes.

- Promotes Security Culture: The process of drafting and adhering to a PP nurtures a security-focused culture within an organization. It fosters awareness and emphasizes the importance of security throughout product development and lifecycle.

In conclusion, the achievements in crafting the Protection Profile for the UTM platform, given the challenges faced, are multifaceted. They encompass rigorous research, adaptive thinking, strong organizational skills, and a forward-looking approach that serves both the current and future needs of the UTM ecosystem establishing a strong security baseline. This also offers multiple strategic, operational, and business benefits.

As a part of the Cybersecurity model refinement task and deliverable of this project, there was the drafting a specific Security Target (ST) for the Unifly UTM platform product. Below are the achievements of the implementation of the UTM ST, especially considering its use for Gap Analysis and subsequent validation of the Unifly Secure UTM version:

- Detailed Baseline for Evaluation: The ST provides a detailed and specific set of security requirements tailored for the Unifly UTM platform. This specificity means that any evaluation based on the ST is highly relevant to the product and is not merely a generic assessment.

- Structured Gap Analysis: By comparing the Unifly UTM platform's previous version with the ST, the project was able to systematically identify areas of improvement. This structured approach allows for a more targeted enhancement of the platform's security features.

- Guided Development of the Secure UTM Version: The ST served as a guiding document during the development of the Unifly Secure UTM version. It ensures that the new platform version integrates the desired security features and measures outlined in the ST.

- Informed Risk Management: A ST defines potential threats and associated countermeasures. With this knowledge, developers can make informed decisions about where to allocate resources and which security measures to prioritize.

- Efficient Resource Allocation in Time-Constraint: Given the project's tight timeline, having the ST helped focus the development and review processes. While some gaps identified were too extensive to address within the available time, the ST still highlighted critical areas, allowing for prioritization.

- Identification of Compliance Levels: Not all security assurance requirements and controls were fully compliant after the table-top validation. However, this non-compliance provides valuable insights into where the platform stands concerning desired security levels and identifies potential areas for future development.

- Insights into SDLC Enhancement Needs: The challenges experienced concerning the need for a more robust Software Development Life Cycle (SDLC) approach were highlighted through the ST. This emphasis on detailed documentation and procedures showcases areas where the product development process can be further strengthened.

- Continuous Improvement and Evolution: The ST serves as a touchstone for ongoing platform development. Future versions of the Unifly UTM platform can be continually assessed against the ST, fostering a cycle of improvement and refinement.

- Building Stakeholder Confidence: Knowing that the platform was developed and assessed against a formalized ST can increase trust and confidence among stakeholders. This is critical for products operating in sectors with high security and safety implications.

- Facilitating Future Evaluations: With the ST in place, future evaluations, certifications, and assessments become more streamlined. The groundwork has already been laid, and subsequent efforts can build upon the existing framework.

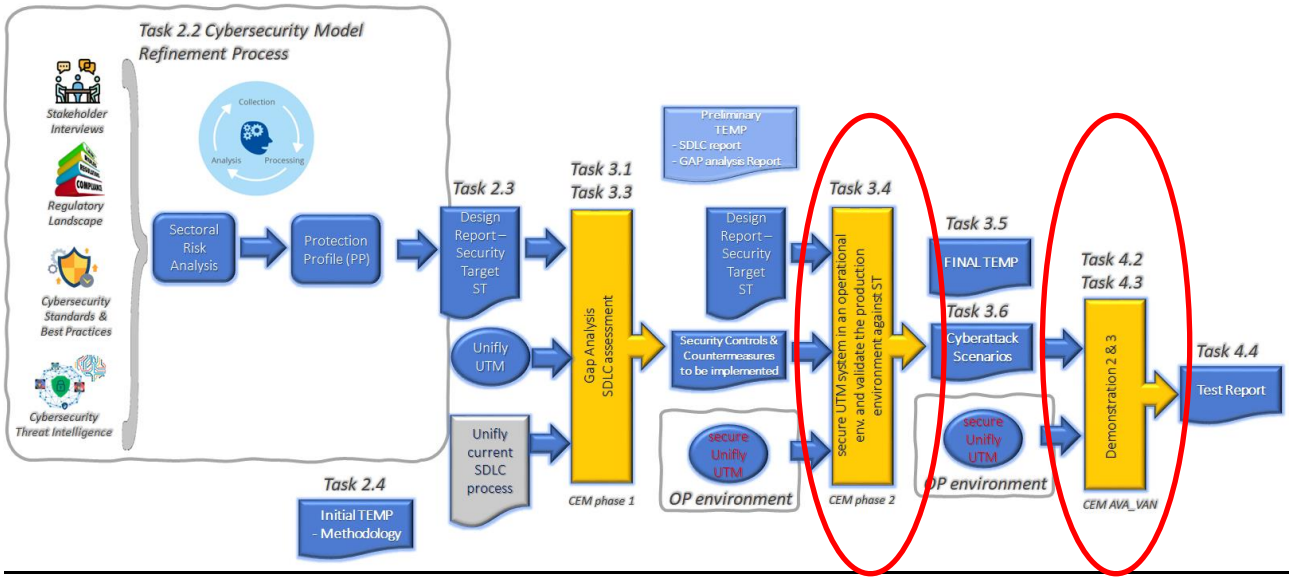
- Preparation for Future Compliance: As the UTM ecosystem evolves, there may be more stringent regulatory requirements in the future. Having a ST positions the Unifly UTM platform advantageously for meeting such emerging standards.

In summary, the drafting and implementation of a specific Security Target for the Unifly UTM platform provides a structured framework for demonstrating and enhancing product security. Despite the project's time constraints and challenges, the ST offers numerous benefits, from guided platform development to insights into potential areas of improvement.

Validating the secured 'Unifly Secure' UTM platform in an operational environment and then breaking it down into specific phases with unique objectives presents a series of intricate achievements.

In the following scheme extracted from the "1046 FINAL Test and Evaluation Master Plan (TEMP)" Section "Test & Evaluation methodology" deliverable highlighted the two final validation steps :

- Task 3.4 CEM Phase 2
- Task 4.2 and 4.3 CEM AVA_VAN



Below is a comprehensive outline of these achievements based on the described validation process:

CEM Phase 2: Secured UTM validation in an operational environment via a Table-Top Assessment Using UTM ST

- Structured Methodology Foundation: The entire validation process for CEM Phase 2 (UTM Validation in Operational Environment) was conducted using a well-structured approach based on the Common Methodology for Information Technology Security Evaluation (CEM) by Common Criteria, as outlined in the TEMP deliverable. This rigorous methodology ensured the validity and comprehensiveness of the evaluation.

- SARs Validation for a selected Attack Potential (AP): Adhering to the CEM framework, the assessment ensured that all applicable Security Assurance Requirements (SARs) were thoroughly analyzed with the respect of the Unifly Secure UTM platform in the operational environment.

- Operational Readiness of Controls & Countermeasures: With the guidance of CEM, the validation confirmed the deployment and effectiveness of security controls and countermeasures in the actual operational setting.

CEM AVA_VAN: Real Penetration Test (AVA_VAN) in Operational Environment in Demonstration exercises

- **Demonstration 1**: Unifly UTM with Flying Drones (No Cyber Attacks):
  - Operational Integrity: Before introducing complexities, this phase confirmed that the Unifly UTM functioned seamlessly in real operational environments with flying drones. It assured stakeholders of the platform's basic performance and reliability.
  - Baseline Functionality: Before introducing attacks, ensuring the platform's core functionality establishes a baseline for subsequent evaluations. If any changes are noticed in later phases, they can be attributed to introduced variables (like cyber-attacks).

- **Demonstration 2**: Unifly UTM with Flying Drones under attack through Attack Scenarios:
  - CEM-Guided Stress Testing: Exposing the UTM to penetration tests and attack scenarios from the TEMP deliverable was guided by the structured approach of CEM, ensuring that the evaluation was comprehensive and methodical.
  - Real-world Vulnerability Identification: The rigorous CEM framework facilitated a meticulous identification of vulnerabilities, some of which represented a high level of risk.
  - Quantifiable Assessment Using CEM: Aligning with the CEM approach, a precise and quantifiable assessment of the platform's vulnerabilities was achieved.
  - Risk Classification: The identification and classification of risks were systematized and made more robust by adhering to the CEM framework.

- **Demonstration 3**: Unifly Secure UTM with Flying Drones under attack through Attack Scenarios with Implemented Security Countermeasures in Operation:
  - Effective Implementation of Countermeasures: The CEM-guided approach provided a structured pathway to evaluate how security countermeasures, developed from previous insights, were integrated and operationalized.
  - Mitigation Validation Using CEM: The demonstration validated the mitigation of previously identified vulnerabilities, further emphasizing the efficacy of the countermeasures and the reliability of the CEM methodology.
  - Resilience Post-Countermeasures: Validating the platform's resilience, especially under simulated cyber-attacks, was made more effective by using the structured CEM approach.
  - Validation of Evolutionary Improvement: The improvements in the platform's security posture, illuminated during this phase, were evaluated in line with the rigorous standards of the CEM methodology.

Incorporating the use of the Common Methodology for Information Technology Security Evaluation (CEM) throughout both phases emphasizes the structured, systematic, and comprehensive nature of the validation process. By adhering to this established methodology, the project ensured a high level of rigor and standardization in its security evaluation efforts. Moreover, it underscores the platform's foundational security features, exposes it to real-world vulnerabilities, and then validates

the implemented solutions, ensuring that the platform isn't just secure in theory but in practice as well.

5. DATA ANALYSIS

Findings from the validation results

This section summarizes the outcome of the validation process of the Unifly UTM in the operational environment done in the Task 3.4 of this project.
The validation process was structured in three phases:

- SAR Prerequisites Validation
- SAR Primary Validation
- Security Controls Validation

The validation results show that 11 requirements and 1 control are not implemented. Their impact, priorities and resources required were analyzed and corresponding Jira tickets were created to be picked up according to the UTM development pipeline.

Findings from Test report (Demonstrations 1- 3)

As shown in the following table, for each Demonstration phase, the minimum number of flights have been executed and the minimum number of expected flights and minimum flight duration x flight:

Demonstration phase	Minimum # of flight per phase	# Flights executed in the phase	Minimum flight duration (mins)	Min flight duration of the shortest flight
1	20	20	>=15	15m03s (FL1-06)
2	20	26	>=15	15m59s (FL2-02)
3	20	20	>=15	16m55s (FL3-17)

In the following table we reported the number of flights and tracking data recorded by the UTM (NON Secure and Secure releases). All executed fights have been recorded by the UTM instances:

TOE	Demonstration 1 # flight executed vs recorded	Demonstration 2 # flight executed vs recorded	Demonstration 3 # flight executed vs recorded
NON-Secured UTM	20 on 20	26 on 26	n.a.
Secured UTM	20 on 20	n.a.	20 on 20

In the following table we reported considerations about the data collected in the NON-Secured UTM and Secure UTM per Demonstration phase:

Demonstration phase	NON-Secured UTM notes:	Secured UTM notes:

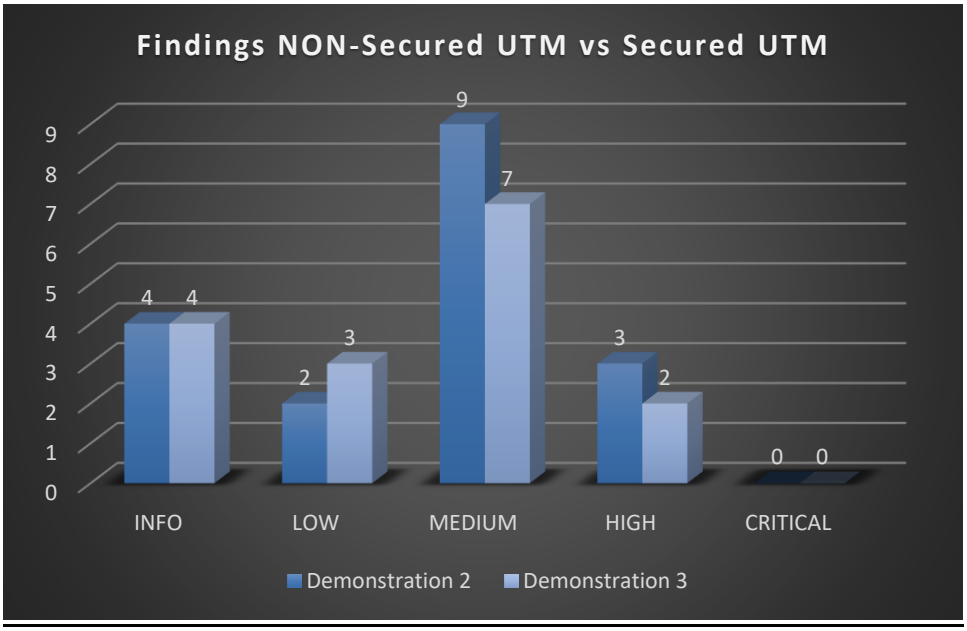
1	Some deviations in timing between these flights and the flights recorded on Secured UTM, as there is a manual action needed to register the landing of the UAS in the UTM system	Some deviations in timing between these flights and the flights recorded on NON-Secured UTM, as there is a manual action needed to register the landing of the UAS in the UTM system
2	During some flights, the flight track showed some deviations. This is because of loss in LTE connections during the flight because of the Airport area. At that moment, the UTM will link the last known tracking points	n.a.
3	n.a.	During some flights, the flight track showed some deviations. This is because of loss in LTE connections during the flight because of the Airport area. At that moment, the UTM will link the last known tracking points

In the following section we reported and summarized the analysis of the Penetration Tests (AVA_VAN) data collected during the Demonstration phases 2 and 3 (in phase 1, no attacks were expected to be executed) in this project that are extensively reported in the following deliverable which covers the test report on demonstrations 1-3 (1051).

Analyzing the data and comparing them between the two demonstration exercises, it is clear that the Secured UTM does not show new visible vulnerabilities, so no security regression has been recorded. Furthermore, the Secured UTM has demonstrated to have less vulnerabilities than the NON-Secured UTM:

- N. 2 Medium level Vulnerabilities completely fixed
- N. 1 High level Vulnerability mitigated to Low

As you will see in the following diagram where we reported the total number of Findings per Demonstration exercise aggregated per criticality following the CVSS scoring methodology:



Other than the above-mentioned findings, the overall UTM platform responded well to the attacks in terms of cybersecurity robustness. The Authentication and Authorization mechanisms worked flawlessly under the attacks, no way to bypass authentication or authorizations has been found

Analyzing the discovered vulnerabilities and the possible mitigations proposed for each in the 1051 - Test report on demonstrations 1-3 deliverable (under the “Recommendations” section), it can be said that they are not substantial in terms of a lack of “secure-by-design” approach, despite the High vulnerabilities discovered. Also, with some non-structural fixes and configuration setup to the UTM platform together with some enhancements in the security gates during the software security and quality assurance validation, can fix all vulnerabilities and reduce the risk of future similar findings.

To conclude and confirm, as no direct connection was established between UAVs and the UTM other than the unidirectional telemetries sent by the tracking device installed on board the UAVs and recorded in the UTM, no ripple effect due to the cyberattacks against the UTM was possible hence no safety related issues were reported.

6. LESSONS LEARNED

Every project comes with a number of challenges. These lead to a number of lessons learned from the project team experienced during the execution of the project:

- When looking back at the timeline on different tasks that were executed, we saw that the design and model refinement phase took longer than anticipated. This led to an extension of the milestone 2 and 3 timeline. Therefore, it is a good lesson to anticipate that in general design and model refinement work, that these are not tasks to be underestimated.

- In the stakeholder interview phase of this project, outputs were gathered based on interviews with relevant stakeholders in the UTM ecosystem. When planning these interviews, it became clear that there can be a long duration between the initial contact with the stakeholder and the effective interview taking place. This had an effect on the lead time of the cybersecurity model refinement in general. Therefore, we take this as a lesson that if stakeholder interviews need to be conducted in a project, these are identified very early to achieve scheduling as soon as possible.

- We had learned that the whole UTM service is composed of many different actors and separated systems and services that have to be properly interconnected. The UTM platform is the central system. Even if this platform is secure, the security must be guaranteed on all other systems as well. For example, if a tracking device is used, and an attacker gets access to the credentials of the device, it is possible to inject bogus data and/or create disruption in the UTM platform.

- The majority of regulations, technical documents, frameworks, etc. reviewed during the Model refinement phase (taking into consideration the ones suggested from the stakeholders interviews) were related to ATM are not directly applicable to UTM environment. A lesson learned is although there is a lot of information available, and it takes time to process it and extract the applicable areas, information for ATM cannot always directly be applied or considered as relevant for UTM.

- Part of the UTM protection profile definition, we the project team needed to make sure that the boundaries of the TOE are properly defined. Especially because there are more UTM services in the future that can change these boundaries. A lesson learned is that there is some degree of flexibility needed, as future services can change the boundaries of the TOE and the linked protection profile.
- During the process of evaluating and balancing the risk level, the lesson learned was that threat actors in the risk analysis of the UTM considering it is a very new sector still in the development phase and without background history.

- During the flight executions at the NUAIR Test site, the project team was faced with operational challenges. These included intermittent rainstorms and unexpected smoke-induced visibility challenges related to the Canada wildfires, which impacted visibility throughout much of the continental U.S. during the days prior to testing and during the flight testing weeks. NUAIR pilots started early and ended late during the testing weeks to provide the needed flights in support of the UTM/cyber test activities. Therefore, it is a lesson that

doing projects in operational environments can have these challenges. Proper mitigation plans are therefore needed to cope with them as much as possible. This to make sure that the testing in operational environments can be executed, as these generate the highest project value.

7. RECOMMENDATIONS

The project team shares the following recommendations for future work.

- In light of the validation of the Security Controls, we could add more value by adopting both the “tabletop” assessment and the Penetration Test in an operational environment. This would lead to having more confidence in the Security Controls to fully cover the known identified threats.

- As also described in the lessons learned, the UTM platform is a part of interconnected systems/services and can be deployed in many different ways (on premise, in cloud as IaaS, PaaS…. Even if the UTM product per se is validated as secure, all the other systems/services must follow the same cybersecurity approach to mitigate as much as possible (the threats). Examples of other systems/services are UAS, Weather Services, RF Monitoring, the environment where the UTM is deployed, Potential tracking devices sending positions to the UTM etc.

- Due to the limited time frame on which the cyber-attacks were conducted, there hasn’t been the opportunity to attempt any Advanced Persistent Threat (APT) attacks as well as possible attack vectors using phishing campaigns, social engineering or supply chain. Either to enlarge the scope of the Attack Scenarios to other external systems and services using edge CEMA (Cyber Electro Magnetic Attacks) methodologies. Some have been listed below but is not exhaustive.
    - CEMA (Cyber Electro Magnetic Attacks) attacks to
        - GNSS: Spoofing, Jamming;
        - UAS C2 communications: Jamming, Spoofing/Replay;
        - UAS to UTM communication (4g/5g/VHF): Jamming, Spoofing/Replay;
        - RF Monitoring service: Jamming, Spoofing
- Having the chance to validate the UTM with a longer test window would be useful to prepare the cyber-attack artifacts for more complex ASs to be executed against the UTM. This could provide the opportunity to collect more data to be analyzed and used as positive feedback to further enhance the UTM Protection Profile, UTM Security Target and in general the robustness of the cybersecurity framework for the UTM ecosystem.
- As the topic of the project is currently very fluid within an evolving environment related to the UTM service (evolution and refinement of the laws and regulations, technical solutions and constrains, cybersecurity and socio economical aspects, etc.) a future reassessment and update on the UTM PP is strongly suggested. During this potential future assessment, a proper amount of time and resources need to be allocated Review UTM PP with respect to UTM services evolution.

- Specifically, from the stakeholder interviews, it became clear that it is needed to raise awareness about why a cybersecurity framework for UTM is important. The protection profiles and the security targets are an objective way to evaluate the maturity of the security level of the UTM project. The project team recommends to execute a dissemination effort after the project closing on the results of this project to all relevant stakeholders, certainly on the main advantages of having a certification scheme in place.