UNIFLY
enabling autonomous aviation

Nexova

NAVISP EL3-023 "SecureUTM"

Final Presentation

NAVISP3-RPT-UF-023-FP-v1.0

25/09/2024

Agenda

- **Project team**
- Context and rationale for the development of the project
- Outcome of the project
- Demo Video
- Key Milestones
- Contribution of the project to national strategy
- Approach to sustain the activity
- Benefits of working with ESA
- AOB and Open Discussion

Project team

Prime

UNIFLY
enabling autonomous aviation

- The leading provider of UAS Traffic Management (UTM) technology
- Experience in deploying national systems in partnership with national ANSPs
- Based in Antwerp, Belgium

Subco

Nexova

- Specialised in advanced cybersecurity solutions.
- Offers a range of services including cybersecurity training, managed services, cyber-range and emulation services, tailored engineering solutions, and consulting.
- Operates from its Cybersecurity Centre of Excellence in Transinne, Belgium which hosts a security operations centre (SOC), cybersecurity classroom, and advanced facilities for cyber-range and emulation services based on proprietary technology (CITEF).

Agenda

- Project team
- **Context and rationale for the development of the project**
- Outcome of the project
- Demo Video
- Key Milestones
- Contribution of the project to national strategy
- Approach to sustain the activity
- Benefits of working with ESA
- AOB and Open Discussion

Context and rationale for the development of the project

- **UAS (Unmanned Aircraft Systems**) are well on the way to becoming a **major player in the field aviation** and an important tool for beyond visual line of sight (BVLOS) missions
- To foster this new technology, the European Commission has adopted a **new set of drone regulations called** '**U-space**' aiming at the safe and secure integration of drones into the existing airspace
- **The integration and acceptance of UAS/drones** into the current commercial airspace operations poses **a risk to safety and security** in the event of successful cyberattacks targeting network links, cloud infrastructure or GNSS signals
- Unmanned Traffic Management (UTM) systems will eventually need to adhere to the **same level of safety and security and certification standards** as current Air Traffic Management (ATM) systems for manned aviation
- **The assured security** of navigation signals, UTM software and network infrastructure **against attacks**, the capability to measure and quantify that risk, and the effectiveness of the **countermeasures** developed to mitigate it, as well as certification of the overall system, will become a valuable and mandatory asset in the near future

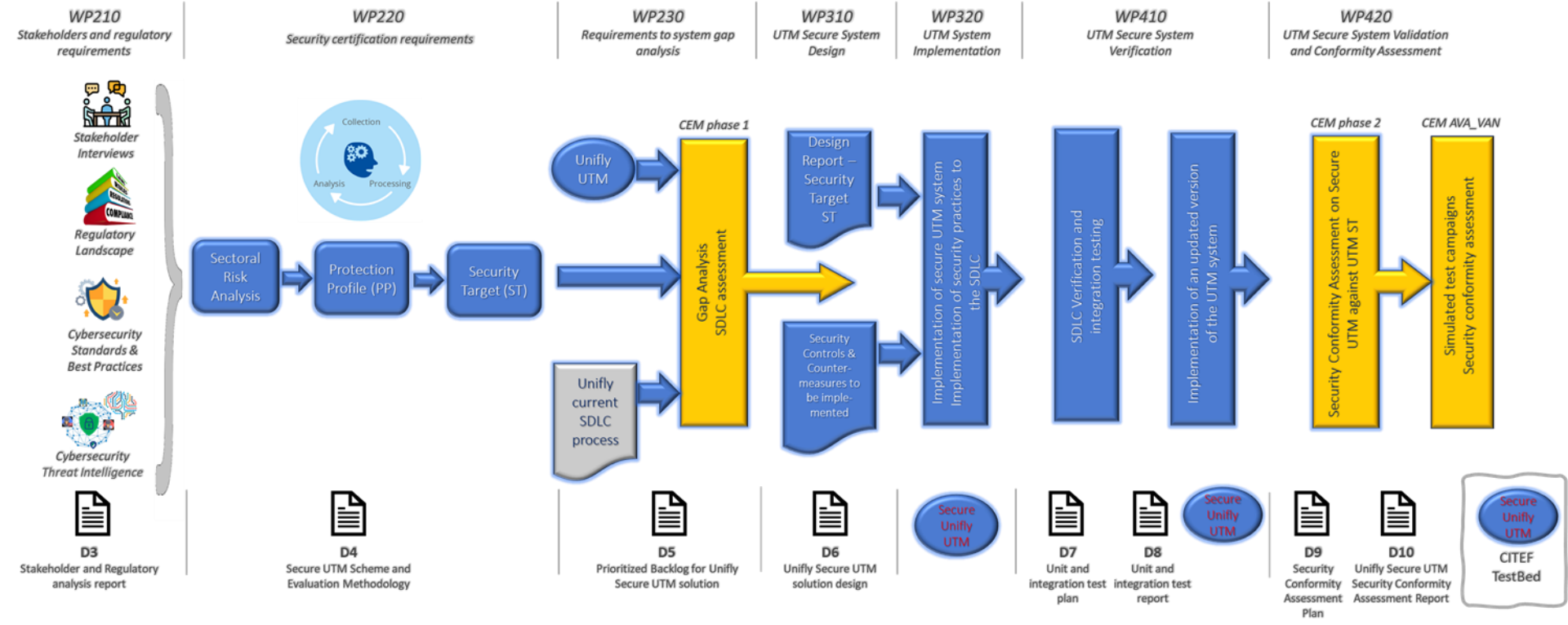
Agenda

- Project team
- Context and rationale for the development of the project
- **Outcome of the project**
- Demo Video
- Key Milestones
- Contribution of the project to national strategy
- Approach to sustain the activity
- Benefits of working with ESA
- AOB and Open Discussion

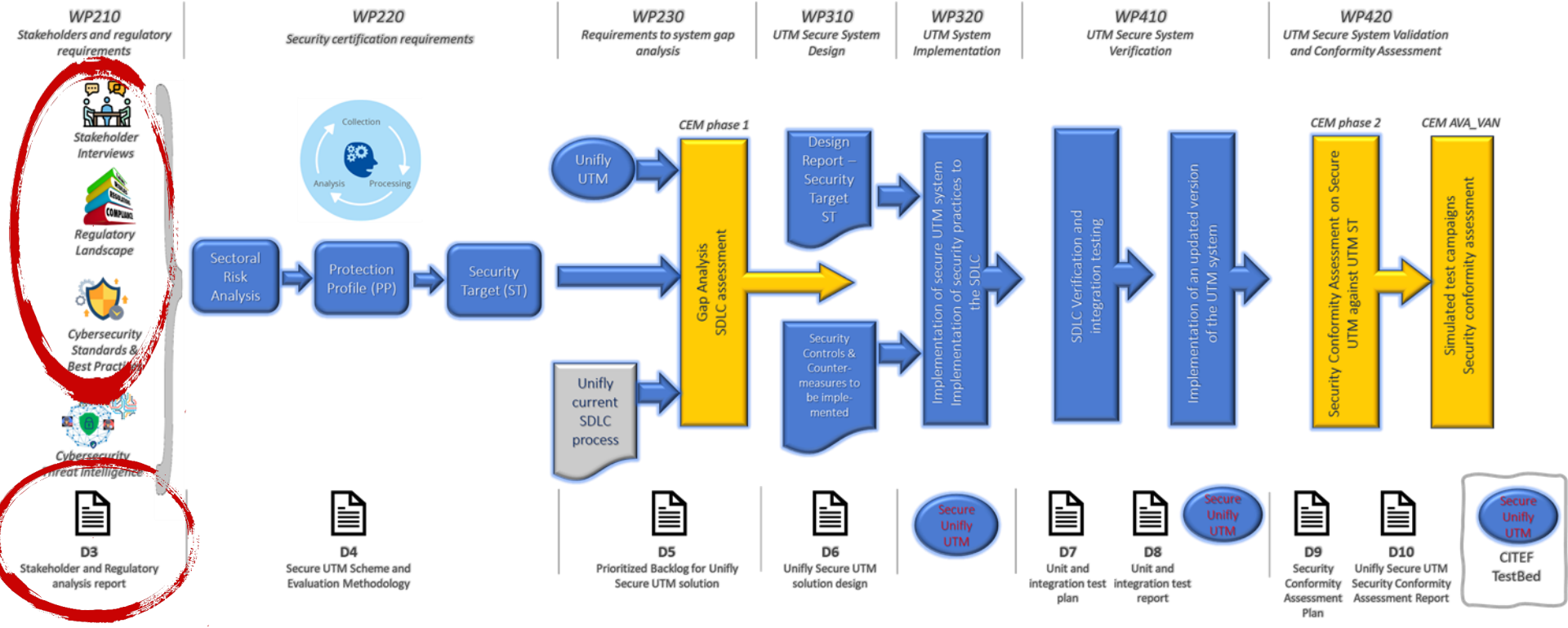
Outcome of the project

- The full **objective and scope** of this project consists of:
  - The definition of a potential cyber certification scheme for UTM in the EU, compliant with the EU Certification Framework with the applicable EU regulations for UTM and drones.
  - Design and develop a compliant proof of concept (PoC) of a secure national UTM for the Belgian airspace, and successfully perform a conformity assessment in accordance with the elicited certification scheme.
  - “Securely” inject the PNT data of drone operations into the traffic management system
- **following main project activities**
  - Comprehensive Stakeholder Analyses and Regulatory Compliance
  - Recommendations for a potential Certification Scheme
  - Execution of a gap analyses
  - Creation of a Prioritized backlog for development
  - Development of a Secure UTM System
  - Verification of a Secure UTM system
  - Rigorous Validation

Outcome of the project



Comprehensive Stakeholder Analyses and Regulatory Compliance



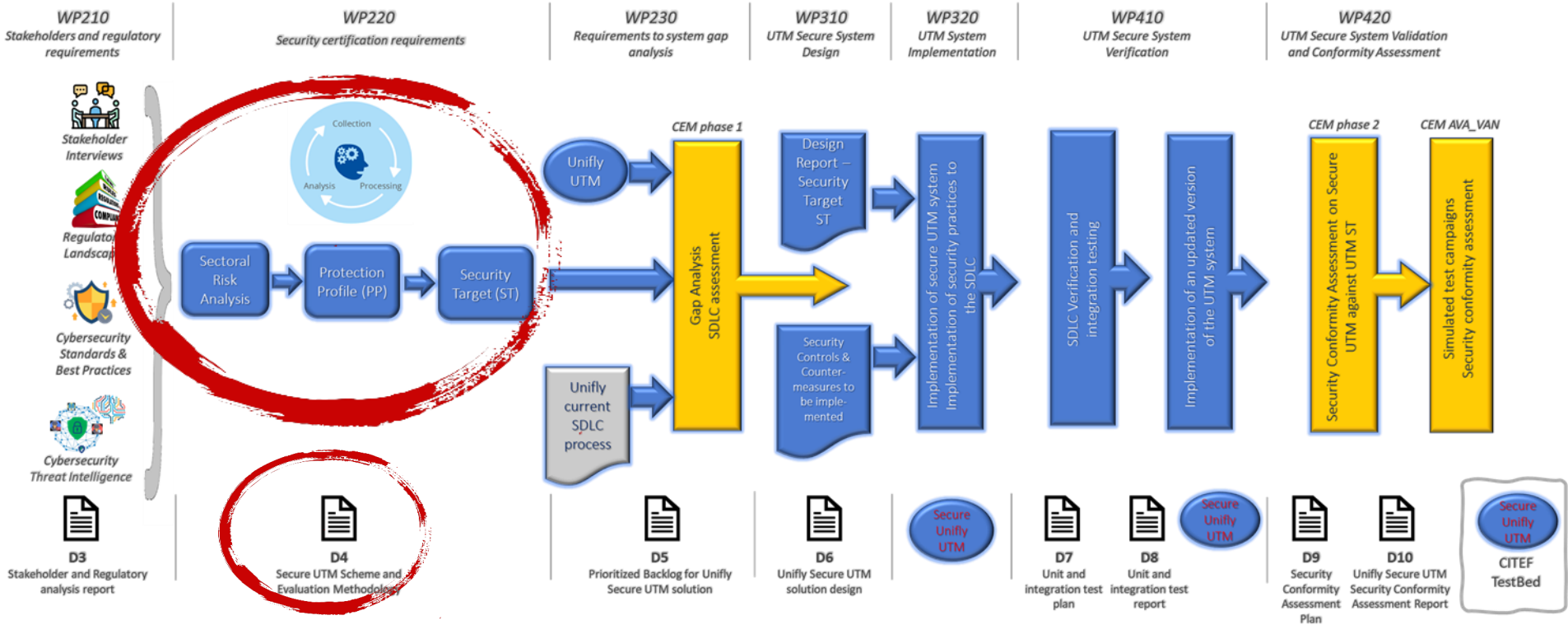
Comprehensive Stakeholder Analyses and Regulatory Compliance

- Engaged with major stakeholders from the UTM ecosystem to present the UTM cybersecurity model and asked for their **input** via specific questions to learn about current **security requirement, feared events and cyber threats**
  - **Bulatsa** - Air Navigation Service Provider of Bulgaria
  - **EU DG Move** - Directorate General Mobility and Transport
  - **DFS** - Air Navigation Service Provider of Germany
  - **EASA** – European Union Aviation Safety Agency
  - **Skeyes** - Air Navigation Service Provider of Belgium

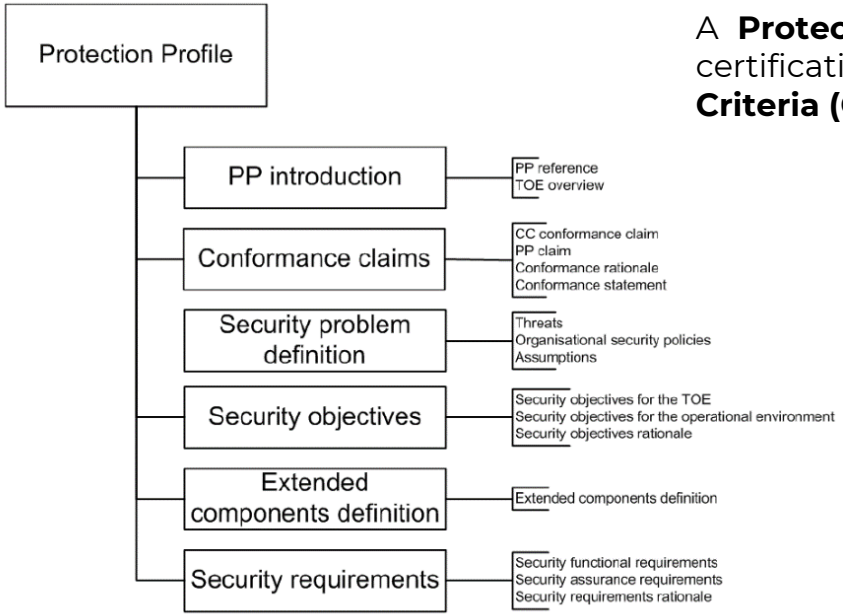
- Execution of an **analyses on current and future regulations on drones and UAS** on European level.

- Combination resulted in a **list of relevant frameworks and standards** to be used further in the project

Recommendations for a potential Certification Scheme



Recommendations for a potential Certification Scheme

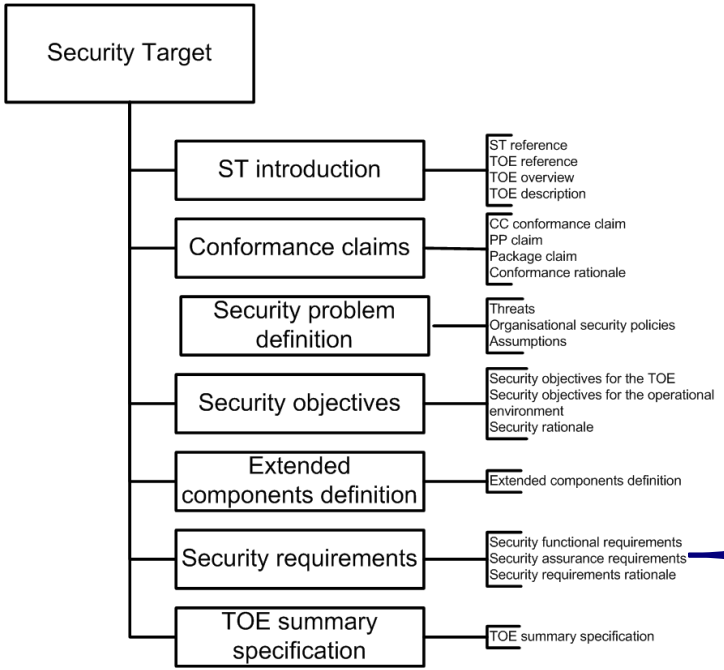


A **Protection Profile (PP)** is a document used as part of the certification process according to ISO/IEC 15408, **Common Criteria (CC)** and **EU-CC**

- PP is an "implementation independent" set of security requirements for a category of ICT product that meets specific consumer needs.
- PPs are widely used by consumer groups and communities of interest, may become standards and be referenced into EU regulation
- **Technical Requirements and Standards are sued to build a PP for a specific TOE***

*A TOE is defined in CC Part 1 as "*a set of software, firmware and/or hardware possibly accompanied by documentation. While there are cases where a TOE consists of an IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these*".

Recommendations for a potential Certification Scheme



Common Criteria defines the **Security Target (ST)** as an "implementation-dependent statement of security needs for a specific identified **Target of Evaluation (TOE)**". In other words, the ST defines boundary and specifies the details of the TOE.

In a product evaluation process according to the CC the ST document is provided by the vendor of the product.

- **Security Functional Requirements** - the SFRs form a clear, unambiguous and well-defined description of the expected security behaviour of the **TOE**.

- **Security Assurance Requirements** - the SARs form a clear, unambiguous and established description of the expected activities that will be undertaken to gain assurance in the **TOE**.

- **Security Requirements Rationale** – the justification for a security objective for the TOE demonstrates that the SFRs are sufficient and necessary.

Recommendations for a Certification Scheme

Benefits of EU Cybersecurity Certification (EU CC) 1/2

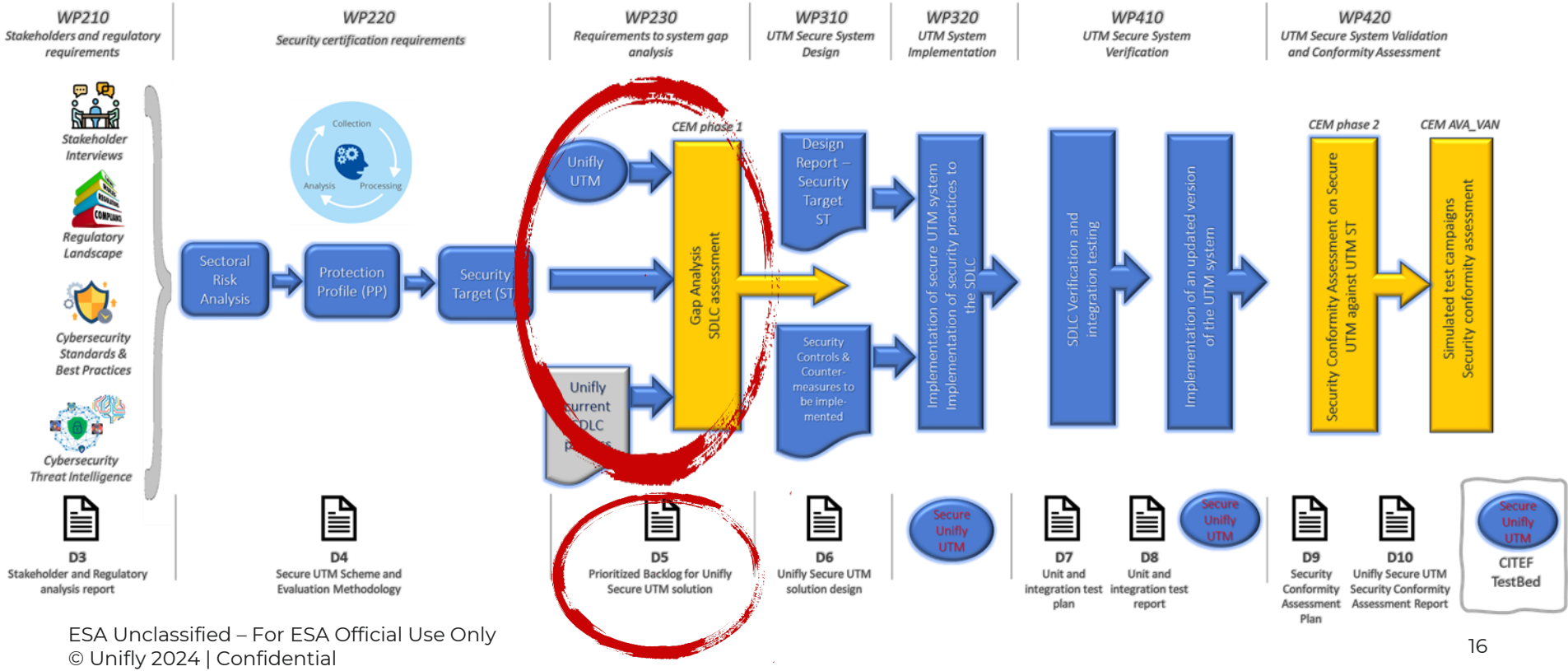
- **Establishes a Baseline for Comparison**
  - Protection Profiles (PPs) provide clear criteria, allowing customers to compare products on the market based on standardized security requirements.
- **Improved Trust and Transparency**
  - Certified products are subjected to independent evaluations, giving users confidence in the security claims made by vendors and enhancing trust in the product's reliability.
- **Consistency Across the Market**
  - Provides a common framework for evaluating the security of products, creating consistency in how cybersecurity features are assessed across the EU, regardless of the vendor.
- **Global Recognition**
  - Certifications issued under the EU CC can be recognized internationally, simplifying the process for vendors to enter global markets, particularly in countries that also adopt Common Criteria.
- **Supports Innovation and Security-by-Design**
  - Encourages product developers to incorporate security into the design phase, aligning with the EU's focus on secure-by-design principles and fostering innovation in secure product development.

Recommendations for a Certification Scheme

Benefits of EU Cybersecurity Certification (EU CC) 2/2

- **Reduces Costs and Risks for Organizations**
  - Helps businesses lower risks associated with deploying unverified or insecure products, reducing potential costs related to breaches, incidents, or regulatory fines.
- **Enhanced Security Assurance for Critical Infrastructure**
  - Ensures that products and services used in critical infrastructure meet high security standards, safeguarding essential services like energy, healthcare, and communications.
- **Supports Procurement Processes**
  - Certified products facilitate easier procurement processes for organizations, particularly in government and critical sectors, as it ensures compliance with established security standards.
- **Encourages Compliance and Reference Framework for Developers**
  - Offers developers a concrete reference framework (Protection Profiles) that guides them to build products that comply with known security requirements, reducing ambiguity and accelerating development cycles.
- **Mitigates Legal and Compliance Risks**
  - Provides organizations and vendors with a legally recognized certification, mitigating risks of non-compliance with national and EU-level cybersecurity regulations.

Gap analyses and creation of prioritized backlog



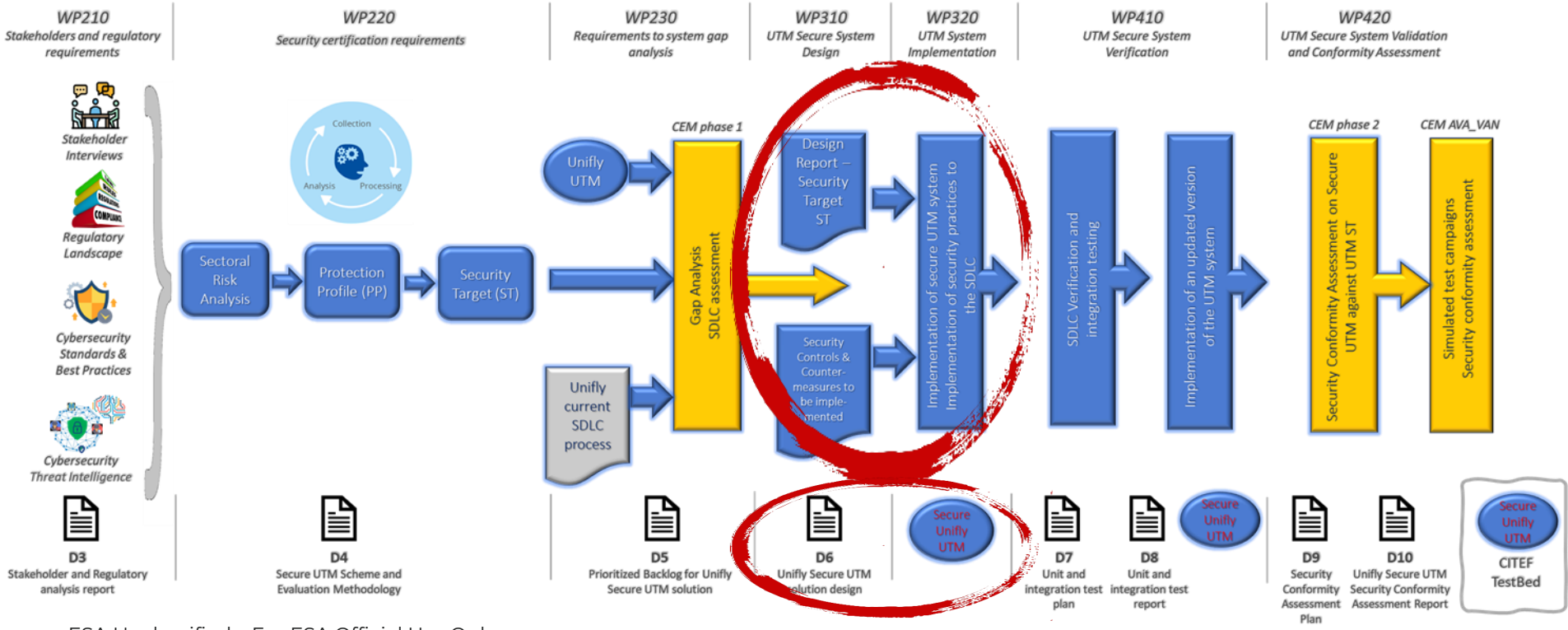
Gap analyses and creation of prioritized backlog

- **“As-is” UTM system** underwent gap analyses to check compliance with **“to-be” system design requirements, security controls and counter measures** defined in cybersecurity model refinement
- **Result is list of all nonconformities/gaps** for which implementation plan and corresponding tasks were created
- Based on classification criteria, a set of non-conformities was **prioritized to serve as gaps to be be closed**. This resulted on a prioritized backlog for the Unifly Secure solution

UID	Security domain	CONTROL OBJECTIVE	SECURITY CONTROL	SECURITY CONTROL Implementation according to a certain strength	PASS/FAIL	Notes
T1.1	1. Access control	Information Flow control Function	Simple security attributes	1.1 The TSF shall explicitly deny an information flow based on rules or security attributes, that explicitly deny information flows. The perimeter of TSF is limited by ToE (Target of Evaluation) which is Unifly UTM system.	PASS	Policy based access control is implemented
T1.2	1. Access control	Authentication Failures	Authentication failure handling	1.2 The TSF shall detect when an administrator configurable number of unsuccessful authentication attempts occurs	PASS	Resolved by ticket UP-6656. The number of unsuccessful authentication attempts can be configured by each customer
T1.9	1. Access control	TOE access history	TOE access history	1.9 Upon successful session establishment, the TSF shall display the date, time and IP address of the last successful session establishment to the user.	Partially	It is tracked but not displayed yet. The corresponding ticket is created in Jira, its priority is low.

Implementation ID	UP-6659
Security Domain	1. Access control
Security Control	1.9 Upon successful session establishment, the TSF shall display the date, time and IP address of the last successful session establishment to the user.

Secure UTM System Design and Implementation

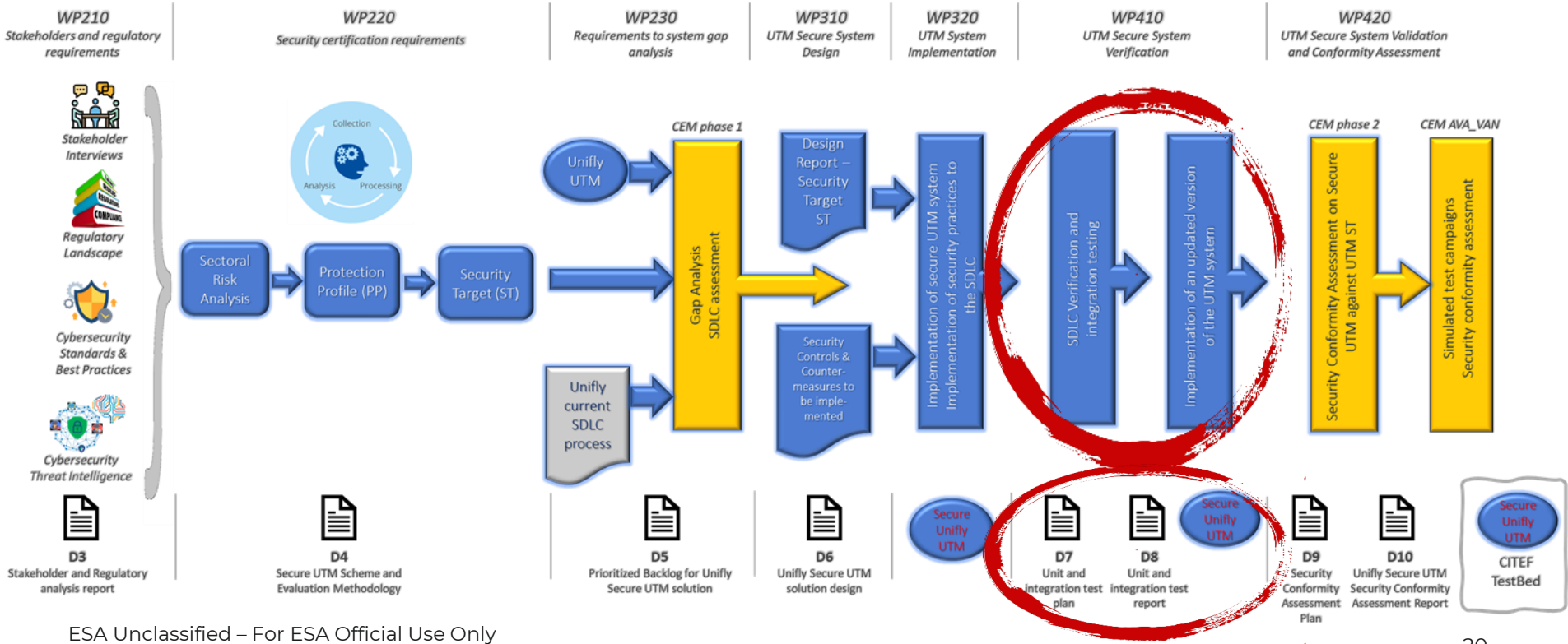


Secure UTM System Design and Implementation

- **Design specification of the Secure UTM system** to implement the counter measures for the identified gaps
- Creation of **security requirements** and assess impact of the implementation on the Unifly UTM **architecture**
- **Update the Unifly UTM** by implementing the identified gaps, covering both development (ex. technical code base implementation) and non-development tasks (ex. Implementations on policy level)

ID	Description	Developer Remarks	Agg ID	Architecture Impact	Comments
SR-OwP-SEC-0010	When a user performs a login to the operator portal, an advisory message MUST be shown to the operator user	UI/UX decision needs to be taken on 1) where this message will be shown and 2) what the exact message is that will be shown.	n.a.	No The implementation of the above described requirement will have **no Impact** on the Unifly Architecture	implemented in JIRA task UP-6658
SR-HL-SEC-0050	Data integrity MUST be verified	Integrity control mechanisms are provided by database infrastructure. Also, O.DATA_INTEGRITY security objective exists. Preservation of integrity of flight, positioning information is achieved through correct settings of "security by design" and "default", and with specific integrity checks. In the	n.a.	Yes The implementation of the above described requirement will have **Impact** on the Unifly Architecture.	Implemented in JIRA task UP-6673

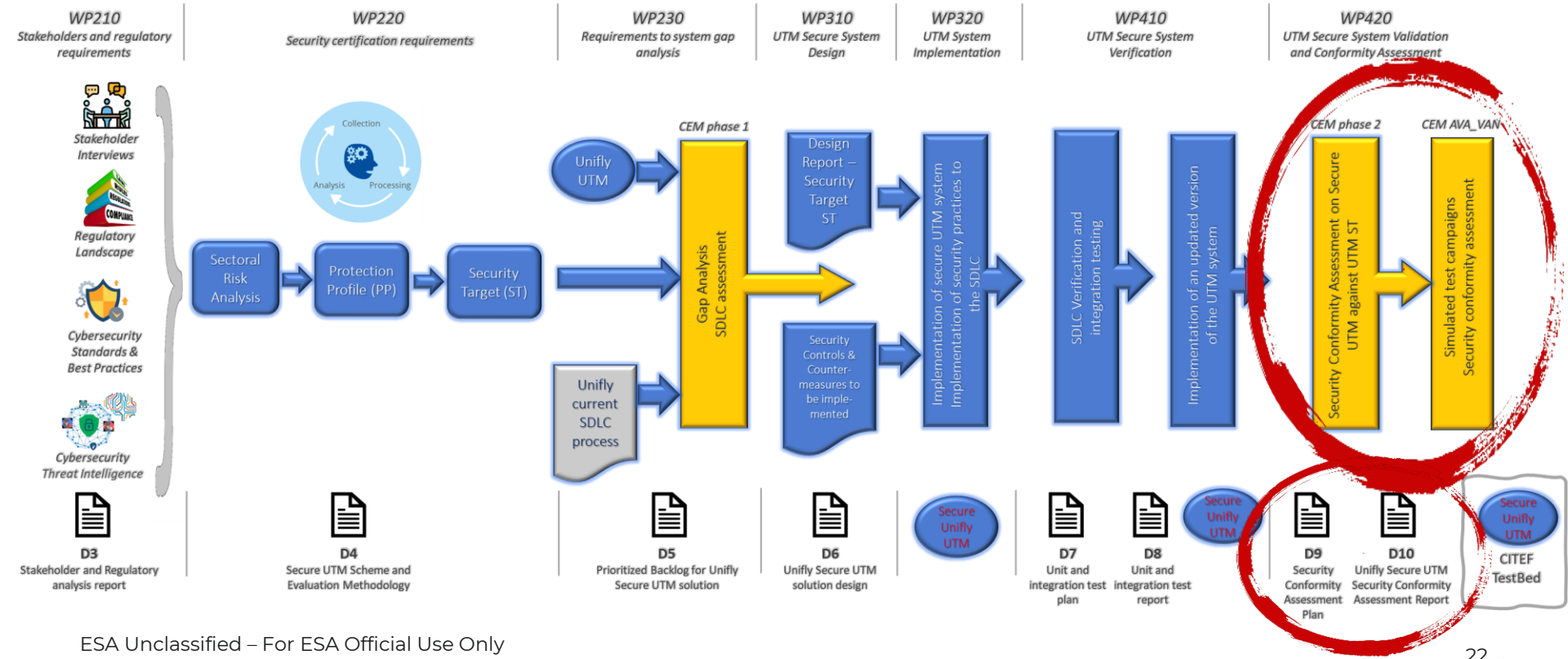
UTM Secure System Verification



UTM Secure System Verification

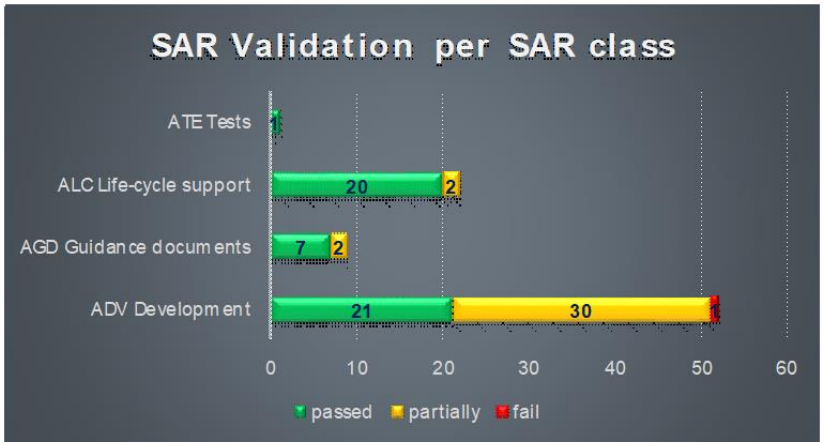
- Prepare the **verification and integration test strategy, plan and procedures**
  - Based on acceptance criteria defined during refinement of the development
  - Use of appropriate tooling (Jira, TestRail) to manage development and testing
- **Conduct verification and integration testing** of the Unifly Secure UTM release
  - (Non) functional testing in sprint and per release
- **Report the results of the verification activities**, including the results of the application of Secure Software Development procedures and tools (quality metrics, security metrics)
- **Update the Unifly Secure UTM Solution** with respect to the performed tests to make it ready for validation

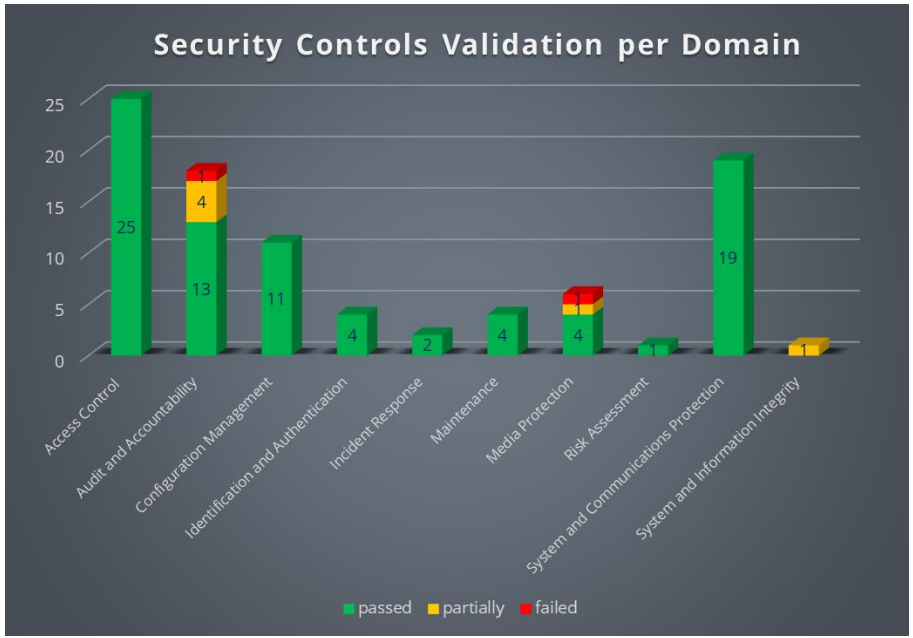
Rigorous Validation



Rigorous Validation

- **CEM* phase 2**: Audit assessment of the Security Assurance Requirements and Security Functional Requirements defined in the Unifly UTM Security Target v1.0



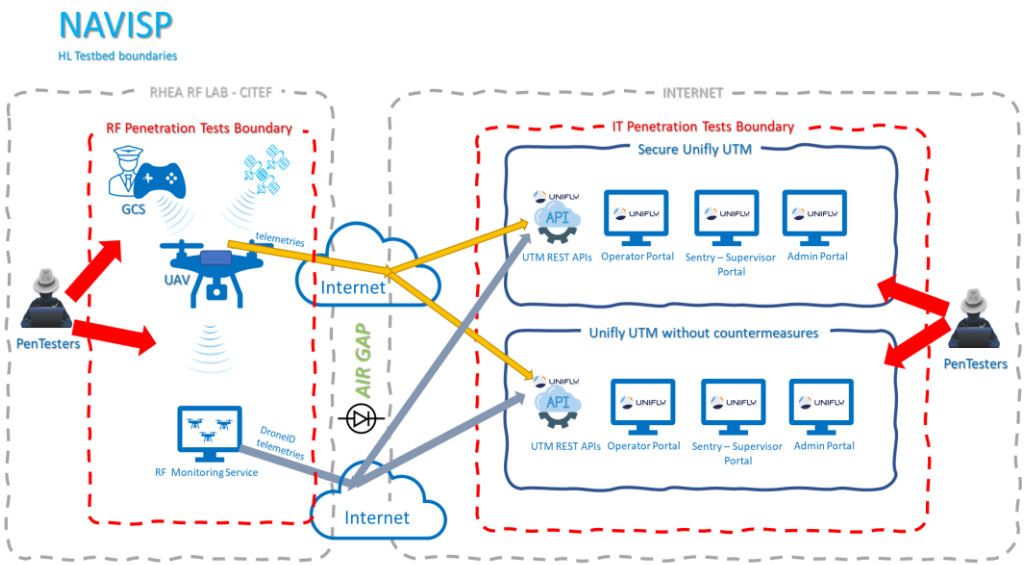


CEM Common Methodology for Information Technology Security Evaluation

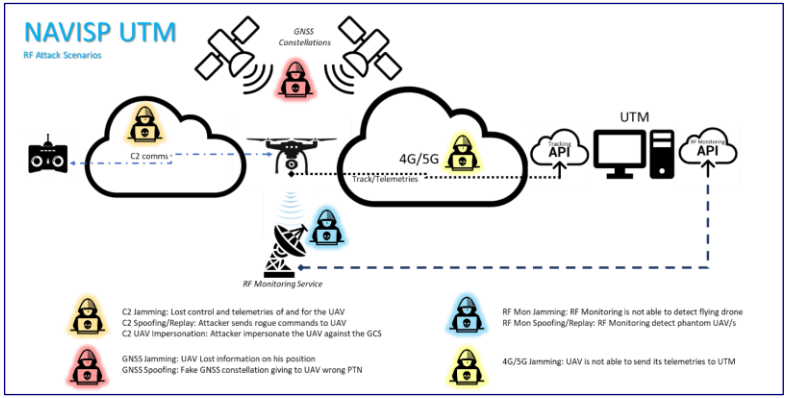
Rigorous Validation

- **CEM Phase 2 Final Report:**
  - The majority of the Security Assurance Requirements (SARs) and nearly all the Security Controls (SCs) are compliant, achieving near-complete adherence.
  - Some SARs were rated as partially compliant, as the analysed documentation, although well-structured and demonstrating a quite robust security-by-design approach, requires further detail and enhancement.
  - Just few SCs initially evaluated as passed in the GAP Analysis were moved to Partially and Fail status after the thorough audit activity

Rigorous Validation



CEM AVA_VAN: AVA_VAN** assurance tests (Penetration Tests) through simulated cybersecurity attacks conducted by penetration testers toward the UTM platform in operation integrated into the Demonstration testbed environment following the elicited RF and Cyber Attack Scenarios



***AVA: "Assurance - Vulnerability Assessment." - VAN: "Vulnerability Analysis."*

Rigorous Validation

In planning RF penetration testing strategy for the UTM system, focus was spent on selecting meaningful RF attack scenarios that would provide useful insights into the system's capabilities and weaknesses.

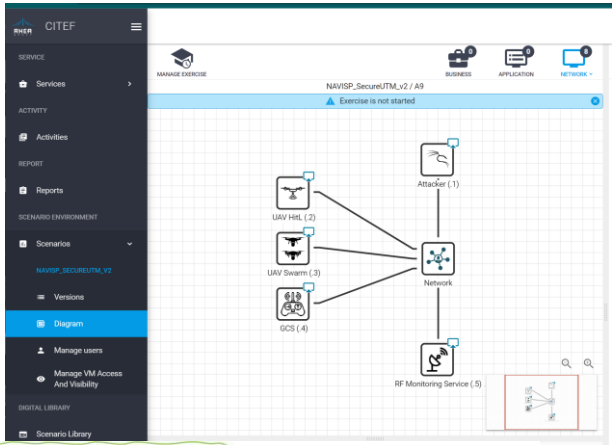
The rationale for this selective approach is twofold:

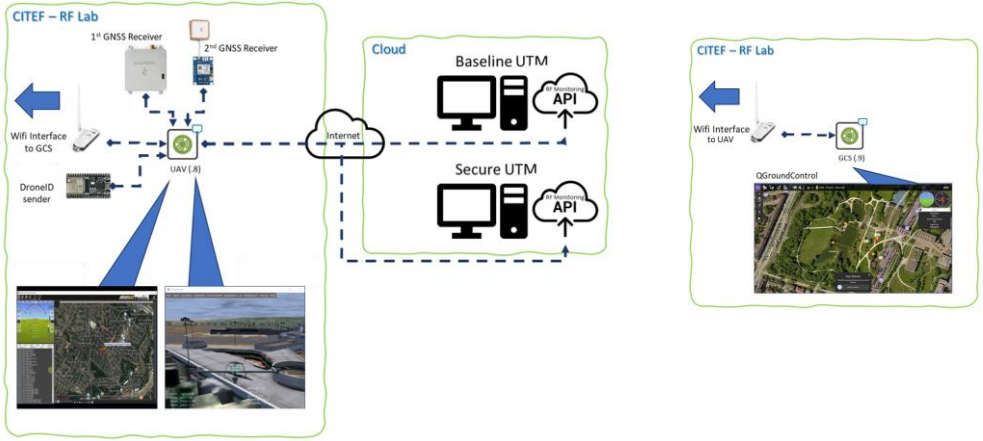
- **Validation and Management of PNT Data**: One of the primary objectives is to assess how Positioning, Navigation, and Timing (PNT) data are validated and managed by the UTM system. Understanding the system's response to these scenarios helps in evaluating the robustness of the PNT data handling processes which are crucial for the operational integrity of the UTM.

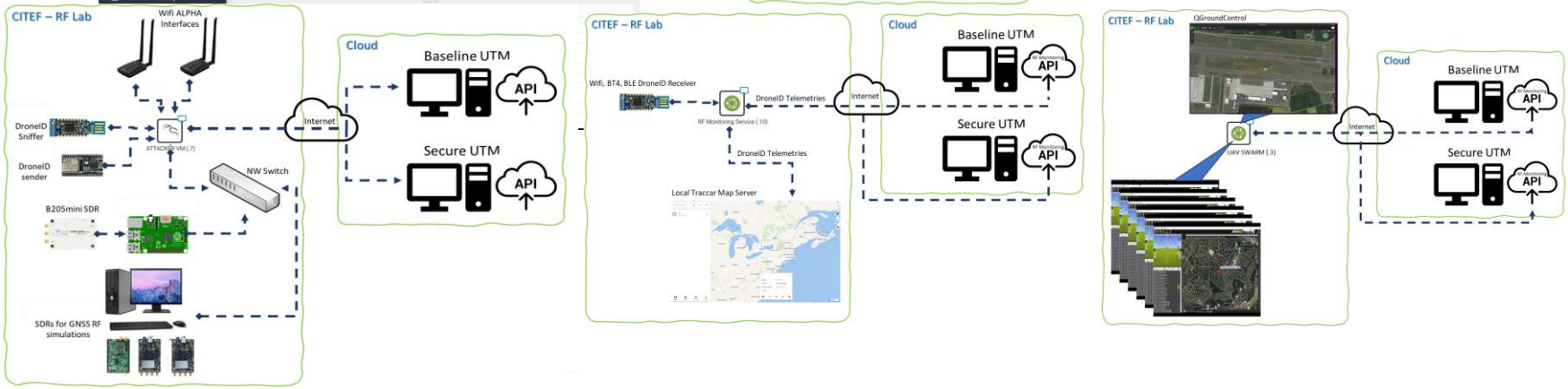
- **Avoidance of Redundant Testing**: The scenarios that were not included in testing plan were excluded because they tend to produce similar ripple effects on the UTM as those already selected for testing. This strategic choice ensures that penetration testing is time-efficient and focused on uncovering unique vulnerabilities without unnecessary repetition.

RF attack	RF Target	RF technology	Attack Scenario
Jamming	GNSS	GNSS: GPS, Galileo	GNSS Jamming scenario: A semi-autonomous UAV is flying following a predefined authorized flight plan using GNSS. The attacker starts the jamming attack and the UAV receiver is not able anymore to calculate its current position. The attacker goal is to trigger the automated safety measure of the UAV which starts a safe landing procedure.
Replay	RF Monitoring Service	BT4 BLE5	Monitoring Service DroneId Replay scenario: The attacker is able to record the DroneID RF Telemetries sent by real flying drone and it replies back to the RF Monitoring service which accepts them as good telemetries and it sends them to the UTM. The attacker goal is to disrupt the traffic management.
Spoofing	RF Monitoring Service	BT4 BLE5	Monitoring Service DroneId Spoofing scenario: An Attacker starts to send bogus DroneID telemetries toward the RF Monitoring Service. The RF Monitoring Service receives these telemetries and sends them to the UTM. The attacker objective is to flood the UTM map of fake drones to cover rogue one or to create disruptions in the traffic management.
	GNSS	GNSS: GPS, Galileo	GNSS Spoofing scenario: UAV is flying following an authorized flight path. The attacker starts to send toward the UAV GNSS receiver bogus PNT data with a correct timing but a very different position. The UAV'GNSS receiver start to consider the new fake constellation and sends the new coordinates to the UTM Tracking API. The attacker goal is to redirect the UAV in a different direction then the initially planned.

Rigorous Validation - Testbed



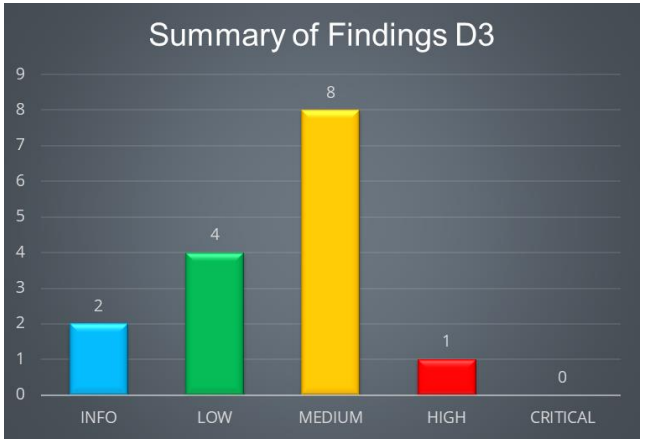




Rigorous Validation

CEM AVA_VAN Final Report:

- the **completeness** and **depth** of the tests carried out **reflects** the level of **EAL required** for the Attack Potential (AP) defined for the version of the ToE with the respect of its defined Security Target (ST) which is **AP 3**
- Some findings have been reported, the majority with a **Medium** to **Low** impact and just one with **High** level of impact. The **High impact finding** showed a risk of a temporary Denial of Service in case of successful attack
- The overall UTM platform responded well to the attacks in terms of cybersecurity robustness, no way to bypass authentication or authorizations has been found. The mechanism to define and check user permissions assigned to the different roles has been found robust and reliable
- The penetration testing activities **revealed novel** weaknesses on UTM outside the initial GAP analysis.
- Regarding the RF ASs, **creating a secure closed lab environment, was crucial for conducting realistic penetration tests** on the UTM platform. This approach ensures thorough and safe testing, which would not be possible in an open-air setting
- **No vulnerability** has been **discovered to gain access to the backend services and components** of the UTM (Services, docker, databases, etc.), neither during the black box attacks nor in the gray box having valid credentials to access the UTM application portals



Agenda

- Project team
- Context and rationale for the development of the project
- Outcome of the project
- **Demo Video**
- Key Milestones
- Contribution of the project to national strategy
- Approach to sustain the activity
- Benefits of working with ESA
- AOB and Open Discussion

Demo Video

Agenda

- Project team
- Context and rationale for the development of the project
- Outcome of the project
- Demo Video
- **Key Milestones**
- Contribution of the project to national strategy
- Approach to sustain the activity
- Benefits of working with ESA
- AOB and Open Discussion

Key Milestones

- The project team conducted a **comprehensive analysis of stakeholders and regulatory requirements**, ensuring alignment with EU regulations for UTM and drones.
- A **robust methodology was developed for evaluating the UTM system's security**, incorporating best practices and standards from the cybersecurity domain.
- The project team created a **prioritized backlog** that guided the development and implementation of the UTM solution, ensuring that critical features were addressed first.
- The project team **designed a secure UTM system that integrated advanced cybersecurity measures** to protect against potential threats and attacks.
- **Extensive testing was conducted to validate the UTM system's functionalities and security**, ensuring that all specified requirements and standards are met.

Agenda

- Project team
- Context and rationale for the development of the project
- Outcome of the project
- Demo Video
- Key Milestones
- **Contribution of the project to national strategy**
- Approach to sustain the activity
- Benefits of working with ESA
- AOB and Open Discussion

Contribution of the project to national strategy

- **Skeyes** (ANSP of Belgium) is one of the stakeholders interviewed during the stakeholder analyses
- **Belgium is actively involved in developing and regulating PNT technologies**, vital to its infrastructure, economy, and security. Belgium works with the EU and international partners to strengthen PNT resilience against threats like interference, spoofing, and GPS disruptions.
- Belgium's PNT strategies strengthen infrastructure resilience and national security.
- **Belgium's regulatory and strategic framework** concerning Positioning, Navigation, and Timing is largely **aligned with broader European Union directives and international standards**.
  - The Cybersecurity Strategy Belgium 2.0
  - Defence, Industry and Research strategy
  - EU legal frameworks

Contribution of the project to national strategy

- **Secure UTM plays a critical role in Belgium’s defense and security strategies**, particularly as it relates to the Defence, Industry, and Research Strategy (DIRS) and Cybersecurity Strategy Belgium 2.0.
- **Secure UTM ensures the safe and efficient management of drone traffic**, particularly in urban or sensitive airspaces. Its implementation is crucial to integrating drones into Belgium's airspace while mitigating risks related to unauthorized use, cyber threats, or potential conflicts with other air traffic.
- **The integration of Secure UTM aligns with the objectives of DIRS by supporting Belgium’s strategic technological autonomy in critical fields such as air traffic management and defense**. DIRS emphasizes the need to strengthen Belgium's defense technological base, where UTM systems contribute to enhancing national security and defense capabilities through advanced monitoring, traffic management, and protection of airspaces.

Agenda

- Project team
- Context and rationale for the development of the project
- Outcome of the project
- Demo Video
- Key Milestones
- Contribution of the project to national strategy
- **Approach to sustain the activity**
- Benefits of working with ESA
- AOB and Open Discussion

Approach to sustain the activity

- The NAVISP EL3-23 “Secure UTM” project has **successfully achieved its objectives**, demonstrating significant progress in the development and deployment of a secure UTM system. The project's comprehensive approach, from stakeholder engagement and regulatory compliance to rigorous testing and effective communication, has laid a **solid foundation for the secure integration of drones into the airspace.** The project's outcomes and methodologies can serve as a model for future initiatives in the field of UTM and cybersecurity
- To sustain the activity, there are further objectives to be identified in a potential future work
  - **Further exploitation** of the SecureUTM project’s results
  - **Further security enhancement** based on the work and outcomes of the SecureUTM project
  - **Operational deployment** in order to run more complex validation trials

Agenda

- Project team
- Context and rationale for the development of the project
- Outcome of the project
- Demo Video
- Key Milestones
- Contribution of the project to national strategy
- Approach to sustain the activity
- **Benefits of working with ESA**
- AOB and Open Discussion

Benefits of working with ESA

- **Innovation Support:** Their focus on innovation accelerates the development of groundbreaking technologies in navigation and communication.
- **Collaborative Environment**: The culture of knowledge sharing at ESA fosters collaborative problem-solving and continuous learning.
- **Enhanced Reputation**: Association with ESA adds significant credibility to our company, enhancing stakeholder trust and industry recognition.
- **Standardization and Compliance:** ESA's involvement ensures adherence to international standards, facilitating wider acceptance and integration.
- **Industry Connections:** ESA's extensive network connects us with key players in the aerospace and navigation sectors.
- **Collaborative Projects:** Opportunities to engage in future projects and partnerships are amplified through ESA's platforms.
- **Project Management Excellence:** ESA's project management frameworks ensure timely progress, efficient resource utilization, project follow up and timely feedback
- **Security Enhancement**: Developing secure UTM solutions aligns with European priorities on safety and security in airspace management

Agenda

- Project team
- Context and rationale for the development of the project
- Outcome of the project
- Demo Video
- Key Milestones
- Contribution of the project to national strategy
- Approach to sustain the activity
- Benefits of working with ESA
- **AOB and Open Discussion**

AOB and Open Discussion