iDSC 2021, Vienna, Austria

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Toward Applying the IEC 62443 in the UAS for Secure Civil Applications

Abdelkader Shaaban, Oliver Jung, and Miguel Angel Fas Millan

AIT Austrian Institute of Technology
Center for Digital Safety & Security (DSS)
Vienna - Austria

Labyrinth
Ensuring drone traffic control and safety

RESEARCH CARRIED OUT IN A NUTSHELL

- **Develope** the first steps toward **implementing IEC 62443 security standard** in Unmanned Aircraft Systems (**UAS**).

- We employ the **ThreatGet** tool to **automatically identify** and **determine** relevant threats and estimate risk severities associated with a **UAS case study.**

- ThreatGet‘s outcomes are used to **outline** a mapping **procedure** between **threats** and **security requirements.**

- This strategy aims to identify a set of **security requirements** to address **potential** threats and protect critical **assets** in UAS.

AGENDA

- Introduction
- Motivational Background
- Contribution
- Applying IEC 62443 Security Standard in UAS
    - **Action1:** Asset Identification
    - **Action2:** Identify Security Zones
    - **Action3:** Risk analysis
    - **Action4:** Risk Evaluation
    - **Action5:** Security Target Estimation
    - **Action6:** Apply Security Requirements
    - **Action7:** Map FRs with STRIDE
- Conclusion and Future Work

INTRODUCTION

- The growing demand for **drones** in **civil applications** is usually satisfied with commercial **off-the-shelf devices.**

- These can always be **adapted** to meet the final user's needs, but they **could not satisfy** critical aspects such as **performance**, **efficiency**, or **security**.

- **Cybersecurity** is one of the critical **issues** in Unmanned Aircraft Systems (**UAS**), where cyberattacks on this system could lead to **multiple negative consequences.**

- **Cybersecurity protects** data and **critical units** responsible for **controlling** the UAV's functional safety from various **attack scenarios.**

MOTIVATIONAL BACKGROUND

- **A safety-security** relationship is considered **directly** proportional, which any malicious cyber activity against the UAS network could lead to **safety** hazards **against civilians, infrastructure,** and **other targets.**

- **Attackers** could **compromise** transmitted **commands,** and the UAV might then **receive falsified commands.**

- This attack could **jeopardize** the **safety** of UAV's **operations,** or also other scenarios could be expected, such as **camera hijacking** when critical cybersecurity **properties** are exploited.

- Furthermore, a **UAV** under cyberattack is considered a **weapon** by **injuring** people or damaging **infrastructure.**

MOTIVATIONAL BACKGROUND

- It is necessary to define applicable security requirements for each system's **node** (e.g., **UAVs**, **roadside base stations**, **central base station**, etc.) to protect the whole system against cyberattacks and address existing security vulnerabilities.

- **Integrating requirements** into system **design** are considered a **challenging** process since these requirements could be **redundant** or **unsuitable** for addressing identified security issues.

- There are many existing security standards from **related** domains that can build **secure UAS applications**, such as the **ISO27000** family, **Common Criteria,** and the **IEC 62443** family.

- "ISO/IEC 27000 – key international standard for information security revised," https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2018/03/Ref2266.html, (accessed on: October 20, 2021).
- "ISO 15408, information technology - security techniques – evaluation criteria for IT security (Common Criteria)," 2009.
- ISA, "The 62443 series of standards: Industrial automation and control systems security," no. 1-4, 2018

CONTRIBUTION

- This work Introduces the first steps into adopting **IEC 62443** security standard in the UAS.

- We define security **zones** and **conduits** in the system design and specify the security requirements according to the **Foundational Requirements (FRs)** defined in IEC **62433.**

- Each security zone and conduit has **particular Security Targets (ST)** that need to be achieved.

- Therefore, we use the **ThreatGet** threat modelling approach to assist in this process.

- **ThreatGet** is a **plugin** for the **Enterprise Architect UML** modelling tool developed jointly by **AIT - Austrian Institute of Technology and LieberLieber Software GmbH.**

https://www.ait.ac.at/en/ https://www.threatget.com/ https://www.lieberlieber.com/en/home-en/

- IEC, "Security for industrial automation and control systems - part 4-2: Technical security requirements for IACS components," International Standard, Tech. Rep., Feb. 2019.
- https://sparxsystems.com/products/ea/

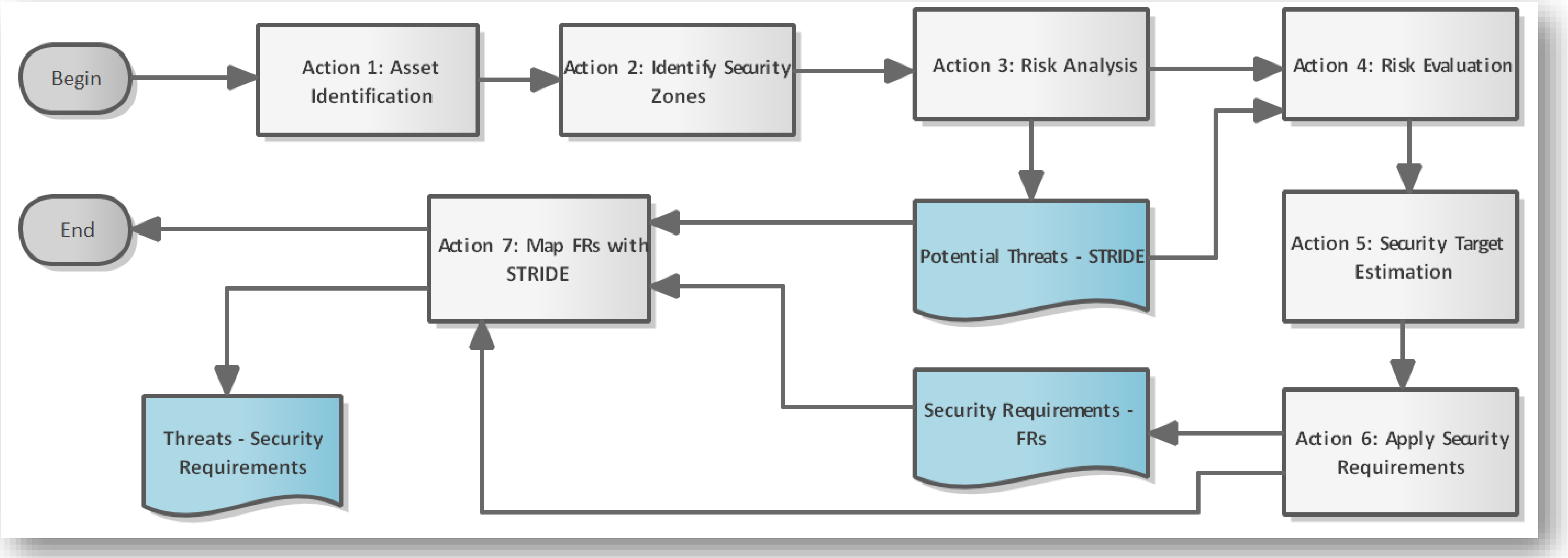
CONTRIBUTION

- The tool **analyses** the security-related **vulnerabilities** in a system model and estimates the risk **severity** for each **identified threats.**

- ThreatGet **helps** in :
  - **Estimating** the security **target for each zone/conduit** according to the risk degree of the identified threats.
  - Defining the security property **violations.**
  - **Identifying** all potential threats that could impact a given UAS model.
  - Classifying threats according to the **STRIDE** model.
  - **Evaluating** risk severity for each **threat**.
  - **The outcomes** used **to define a** mapping between **FRs** (security requirements) and **STRIDE** classification (threats).

APPLYING IEC 62443 SECURITY STANDARD IN UAS

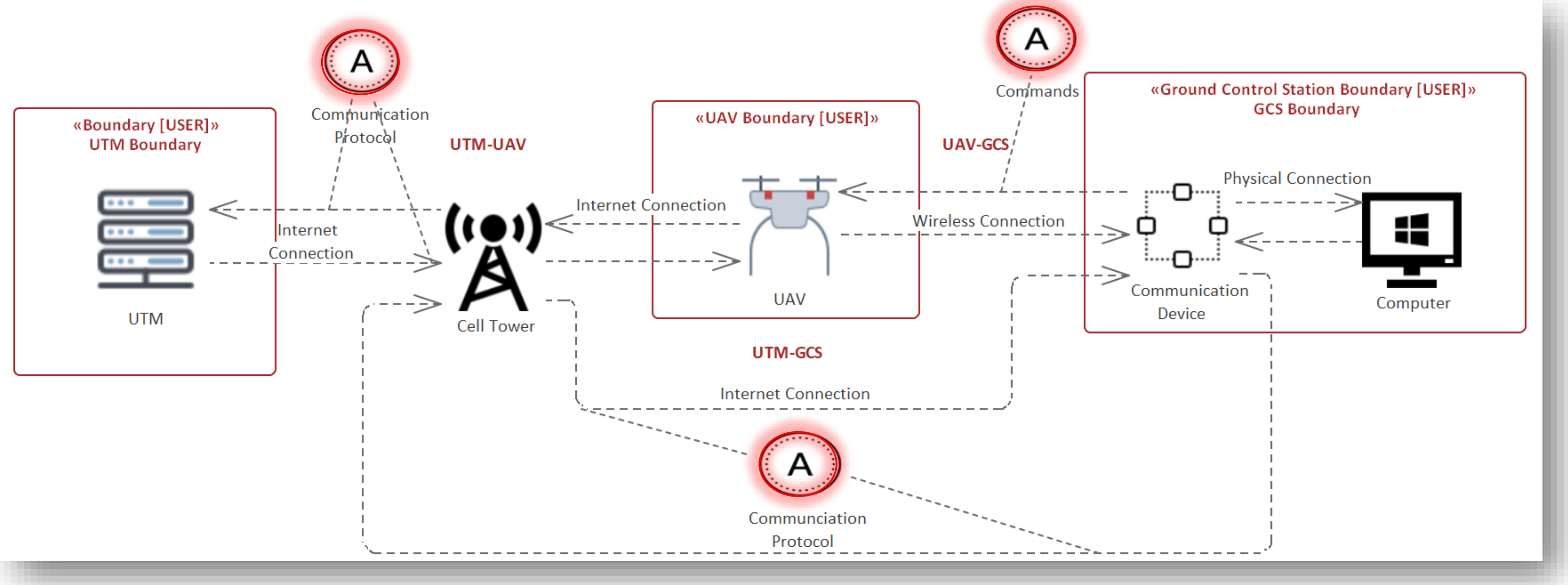
The proposed **steps** in the form of actions for adopting IEC 62443 and selecting the appropriate **requirements** for the **UAS domain** are defined as follows:


Begin
Action 1: Asset Identification
Action 2: Identify Security Zones
Action 3: Risk Analysis
Action 4: Risk Evaluation
Potential Threats - STRIDE
Action 5: Security Target Estimation
End
Action 7: Map FRs with STRIDE
Security Requirements - FRs
Action 6: Apply Security Requirements
Threats - Security Requirements

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION1: ASSET IDENTIFICATION

- We investigate the most **common components** (i.e., **elements, connectors,** and critical **assets**) in UAS.
  - An **asset** means **something** valuable for the **stakeholder,** which **needs** more security concerns.
  - Also, an asset is a **worthwhile target** for attackers (i.e., **information, signal, configurations,** collected **images,** etc.).



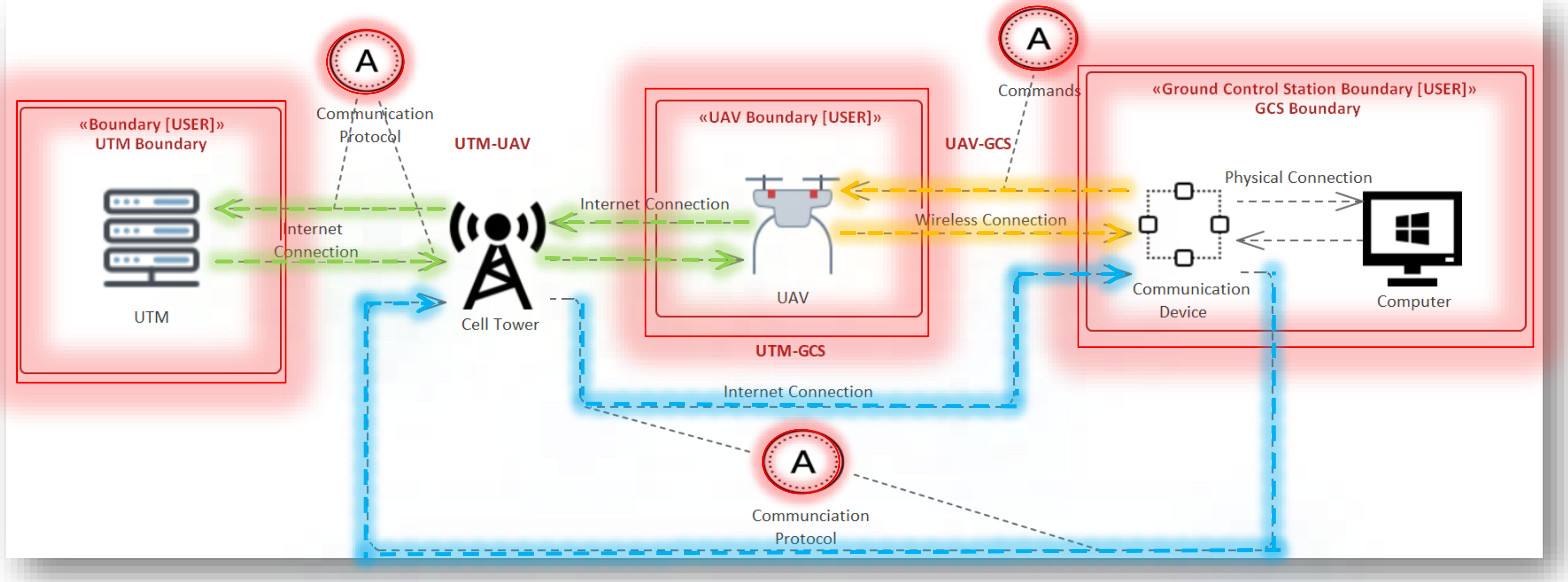
- Therefore, a complete component catalogue for ThreatGet is created.

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION2: IDENTIFY SECURITY ZONES

- Identifying security **zones** is essential in defining physical/logical parts of the system design.
- These **zones** consist of a set of system assets that share the corresponding **security requirements.**
- According to **IEC 62443-4-2, seven FR classes described** the security requirements.
- The **FR5 - Restricted Data Flow (RDF)** describes constraints of **unnecessary** data flows to limit the spread of any cyberattacks in the form of a set of zones.

Zones



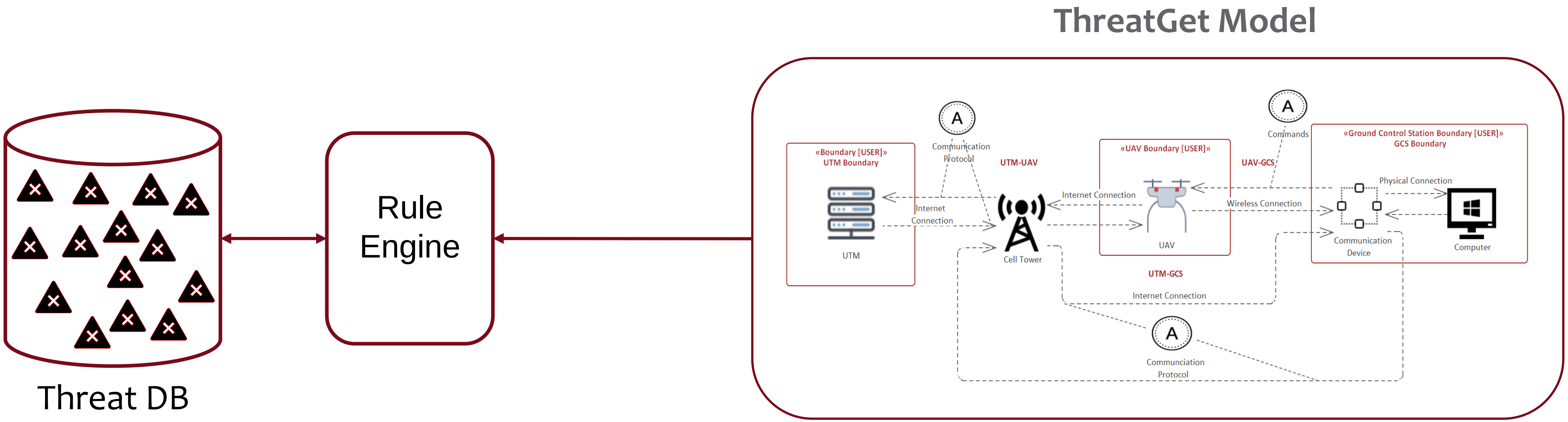
Conduits

ISA, "The 62443 series of standards: Industrial automation and control systems security," no. 1-4, 2018.

IEC, "Security for industrial automation and control systems - part 4-2: Technical security requirements for IACS components," International Standard, Tech. Rep., Feb. 2019.

APPLYING IEC 62443 SECURITY STANDARD IN UAS

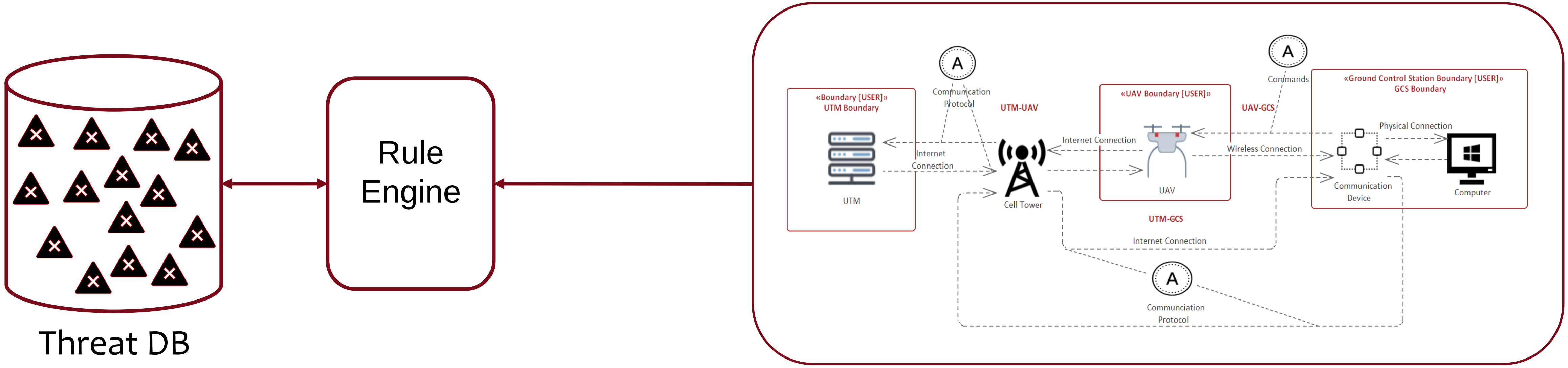
ACTION3: RISK ANALYSIS



APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS

ThreatGet Model



Rule Engine

Threat DB

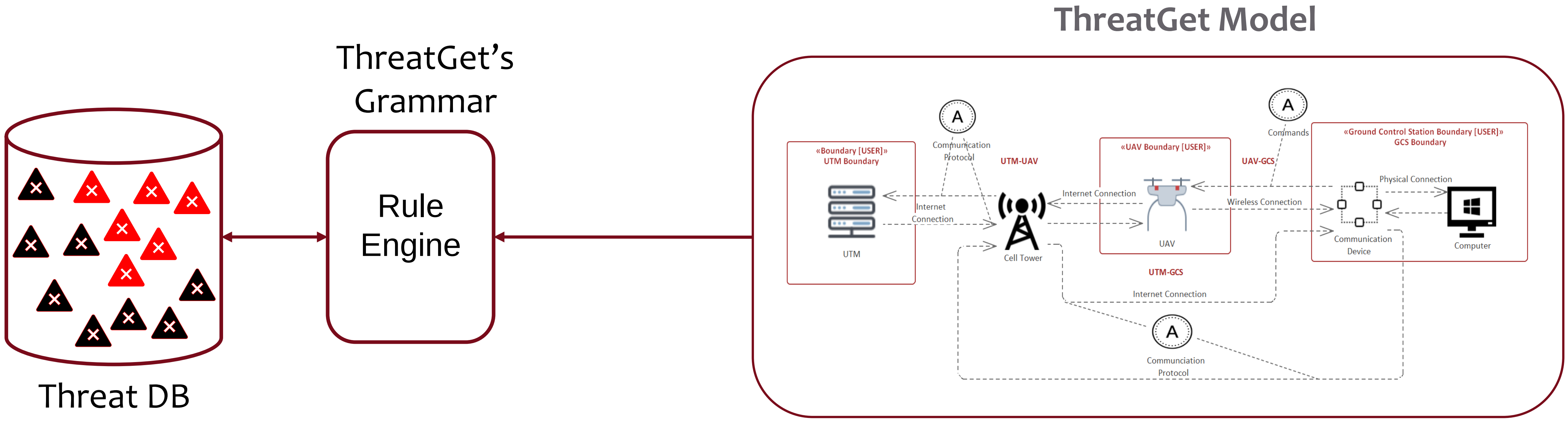
Threats based on SOTA

SOTA

1. A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” in 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE, 2012, pp. 585–590.
2. G. L. Lattimore, “Unmanned aerial system cybersecurity risk management decision matrix for tactical operators,” NAVAL POSTGRADUATE SCHOOL MONTEREY CA MONTEREY United States, Tech. Rep., 2019.
3. M. R. Manesh and N. Kaabouch, “Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions,” Computers & Security, vol. 85, pp. 386–401, 2019.
4. E. K. et al., “D2.3 Architecture Requirements and Definition (v2),” afarcloud deliverable, Tech. Rep., February 2020. [Online]. Available: http://www.afarcloud.eu/wp-content/uploads/2020/04/D2.3-ArchitectureRequirements-and-Definition-2.0VFINAL.pdf
5. Sander Walters, “How to set up a drone vulnerability testing lab,”https://medium.com/@swalters/how-to-set-up-a-drone-vulnerabilitytesting-lab-db8f7c762663, 2016, (Accessed on: May 12, 2021).
6. T. Macaulay, “The 7 deadly threats to 4g: 4g lte security roadmap and reference design,” Accessed: Jul, vol. 25, p. 2017, 2013.
7. U. N. E. C. f. E. UNECE, “CSOTA ad hoc ”threats 2”,”https://wiki.unece.org/download/attachments/45383725/TFCS-ahT2-06%20%28Chair%29%20Table%20on%20CS%20threats%20-%20changes%20agreed%20by%20ahT2%20-%20noncleaned%20up.xlsx?api=v2, 2017, (Accessed on: May 12, 2021).
8. K. Kotapati, P. Liu, Y. Sun, and T. F. LaPorta, “A taxonomy of cyber attacks on 3g networks,” in International Conference on Intelligence and Security Informatics. Springer, 2005, pp. 631–633.

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS



ThreatGet Model

ThreatGet’s Grammar

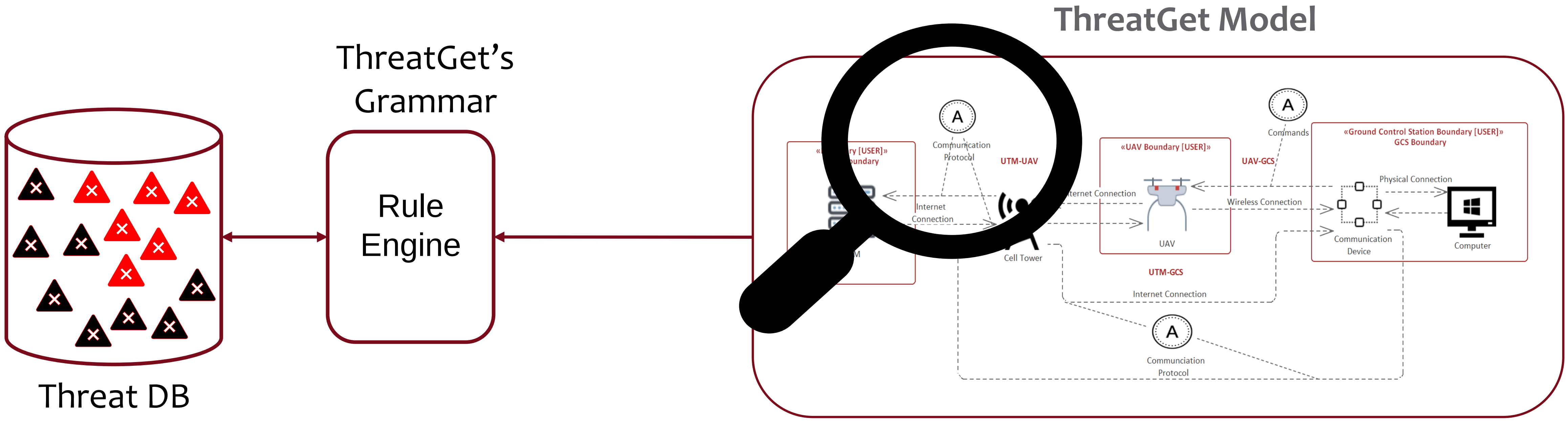
Rule Engine

Threat DB

Threats based on SOTA

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS



ThreatGet Model

ThreatGet's Grammar

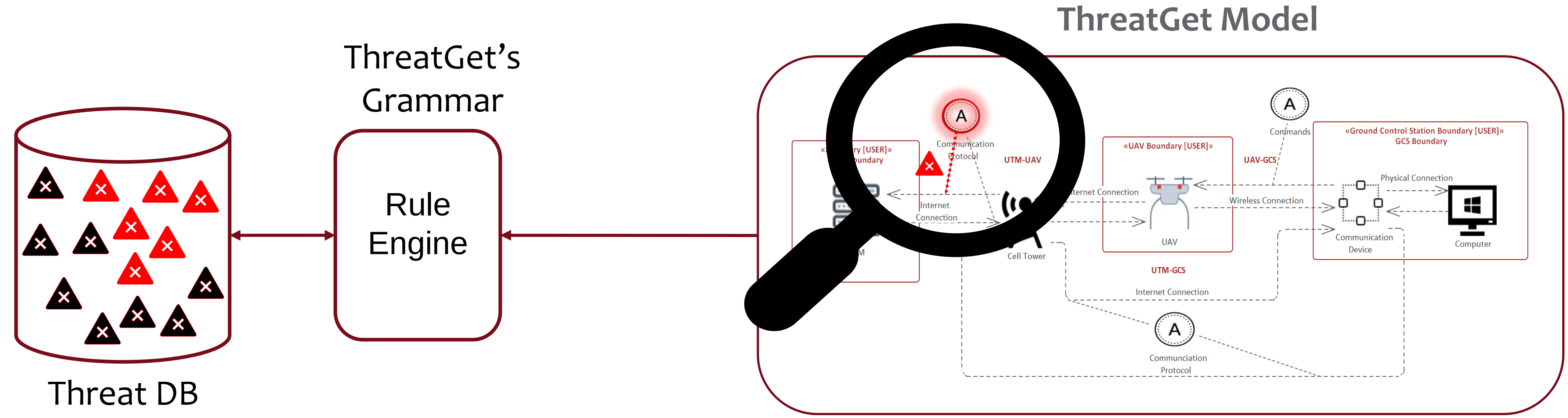
Rule Engine

Threat DB

Threats based on SOTA

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS



ThreatGet Model

ThreatGet's Grammar

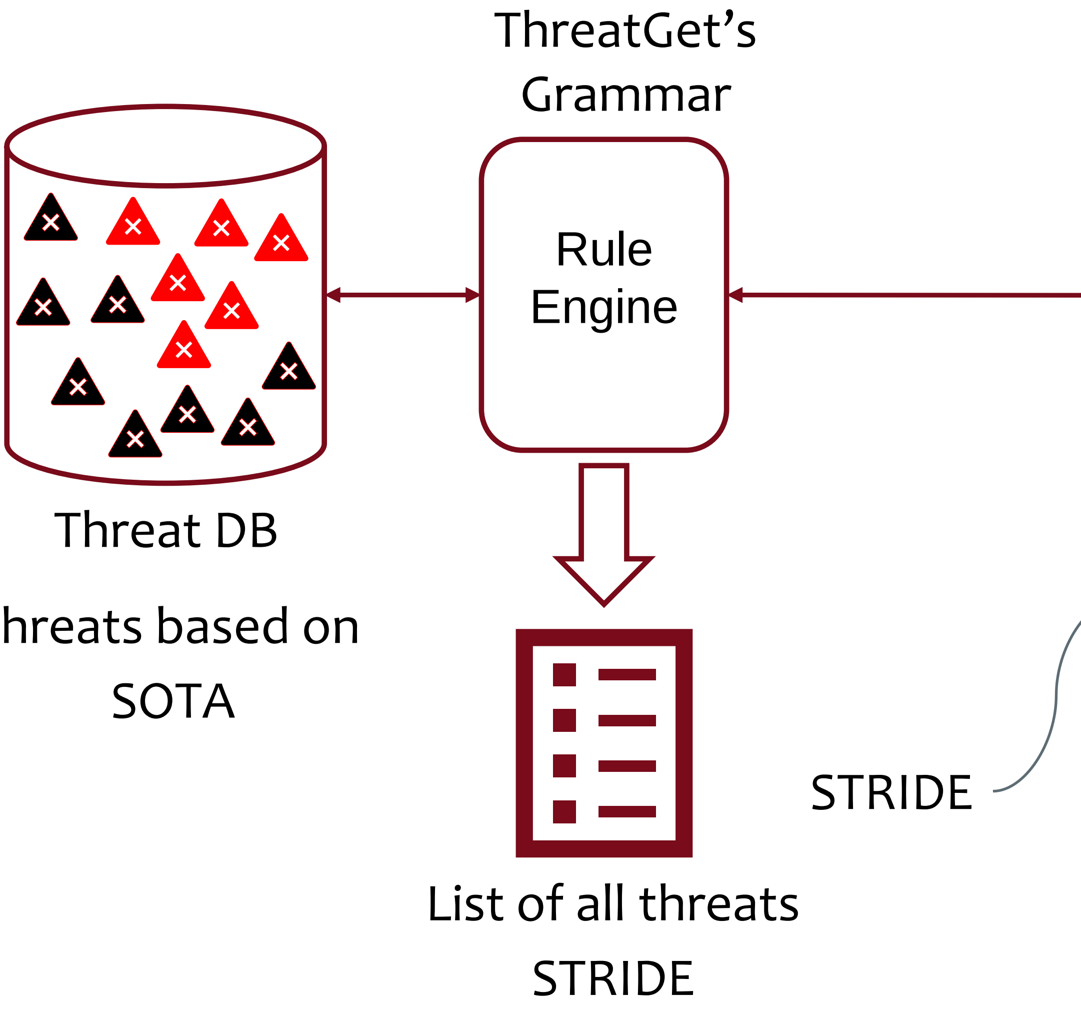
Rule Engine

Threat DB

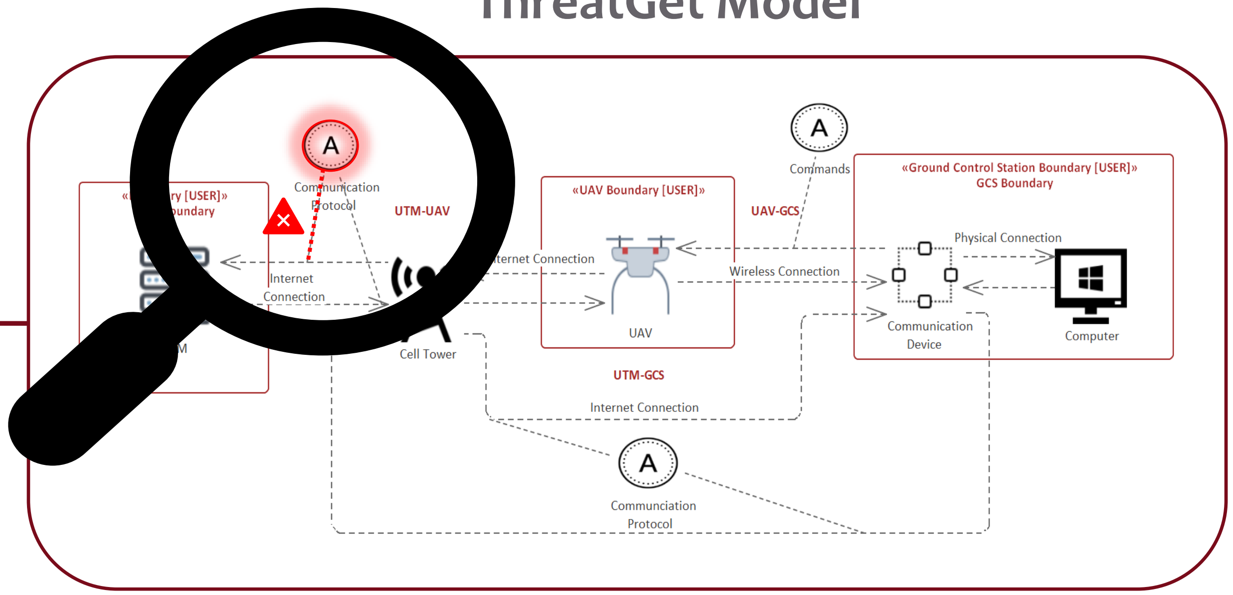
Threats based on SOTA

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS



ThreatGet Model



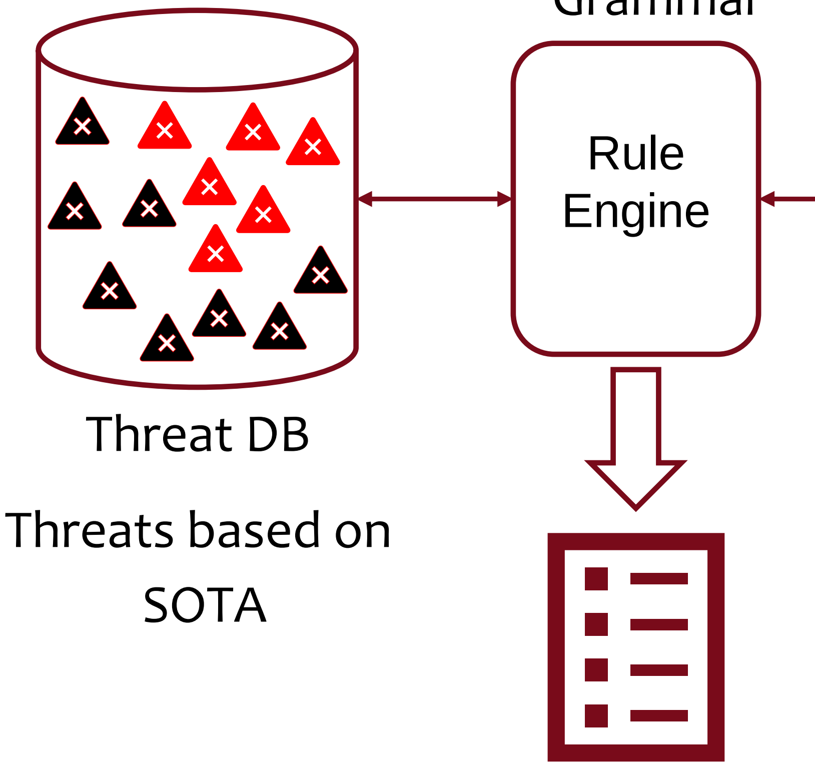
- Spoofing violates **authentication.**

- A. Shostack, Threat modeling: designing for security. Wiley, 2014, OCLC: ocn855043351

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS

ThreatGet's Grammar

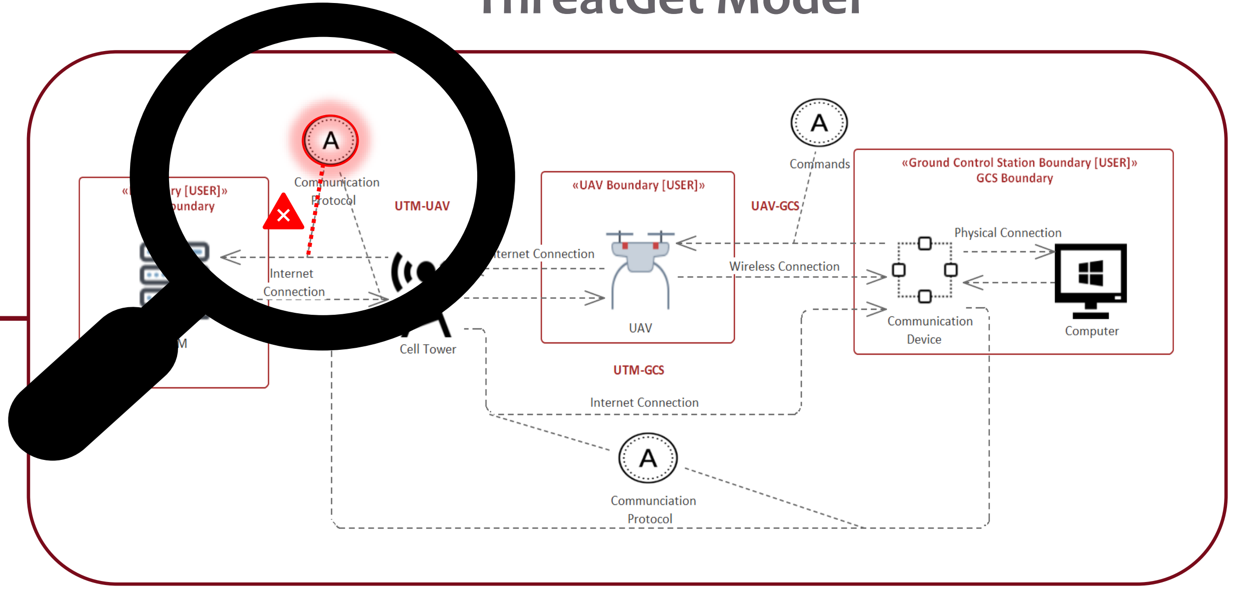


Threat DB

Threats based on SOTA

List of all threats STRIDE

ThreatGet Model



STRIDE

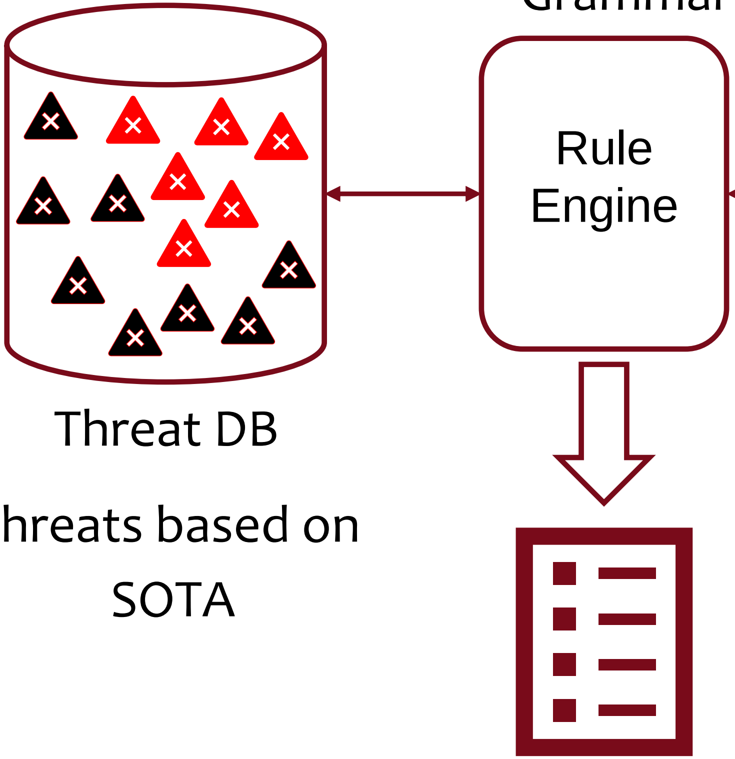
- Spoofing violates **authentication.**
- **Tampering** violates **integrity**.

- A. Shostack, Threat modeling: designing for security. Wiley, 2014, OCLC: ocn855043351

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS

ThreatGet's Grammar

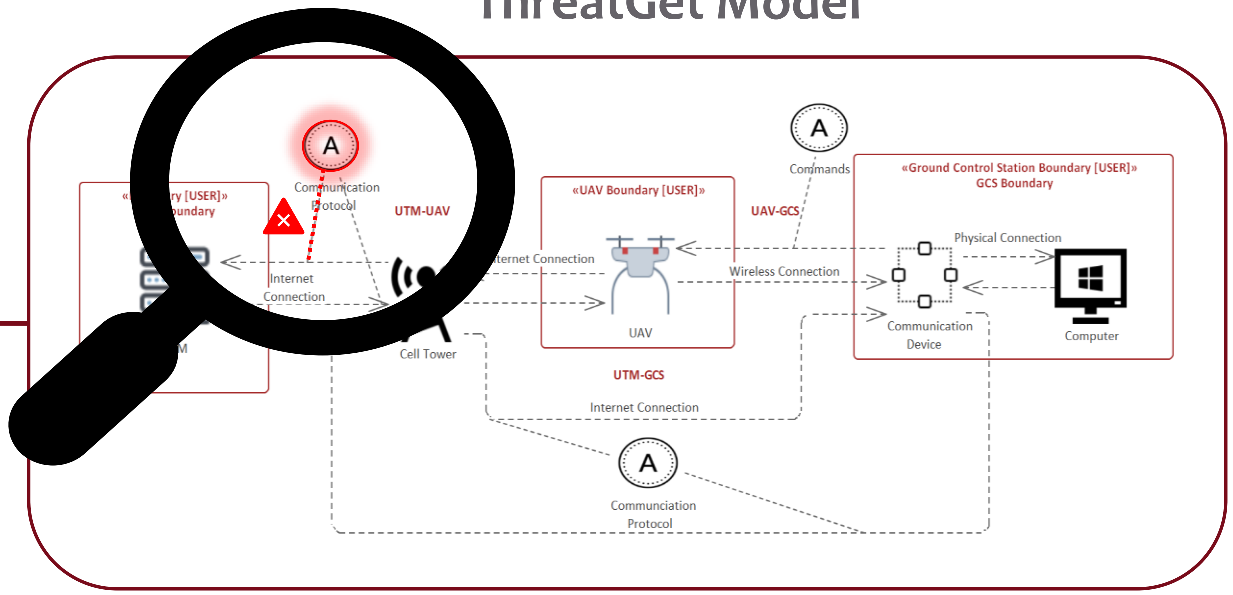


Threat DB

Threats based on SOTA

List of all threats STRIDE

ThreatGet Model



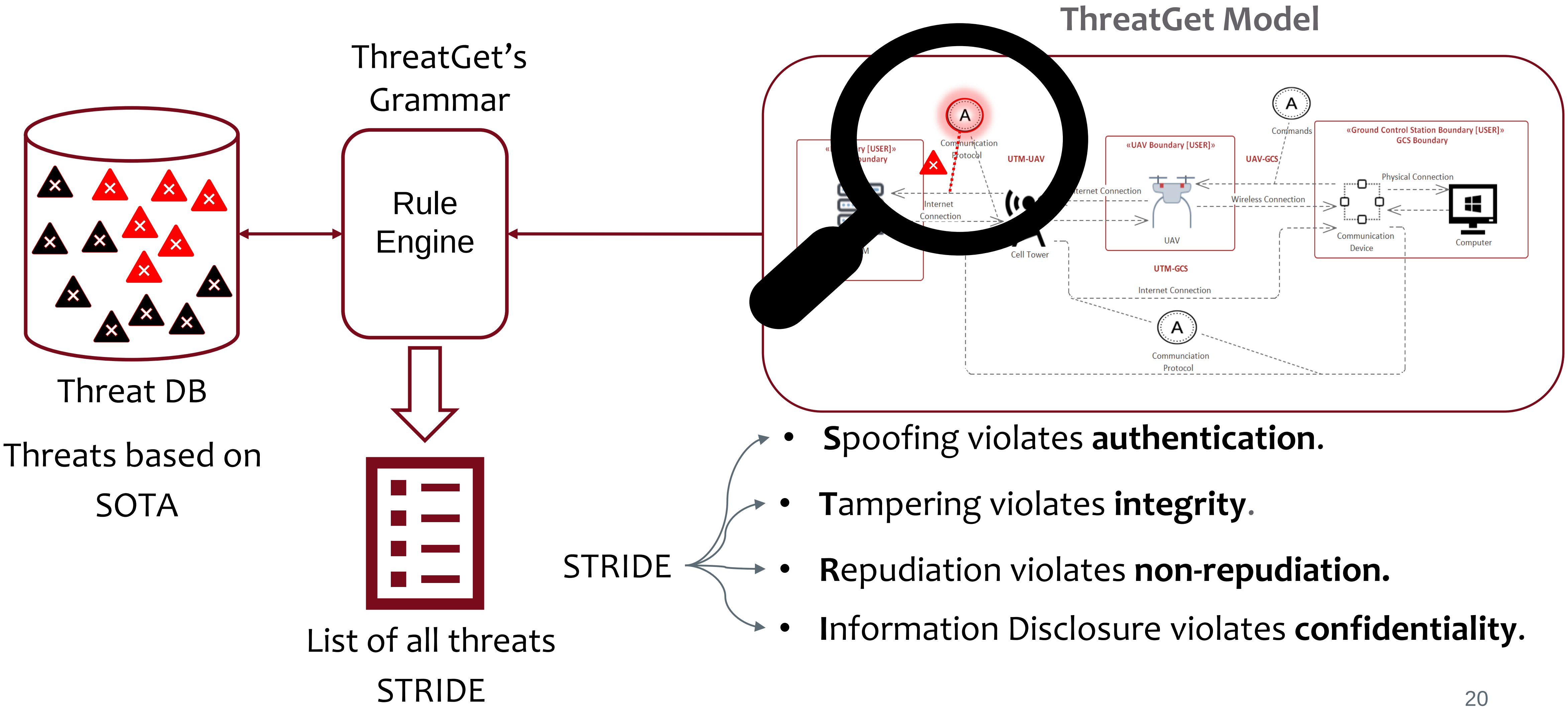
STRIDE

- Spoofing violates **authentication.**
- Tampering violates **integrity**.
- Repudiation violates **non-repudiation.**

- A. Shostack, Threat modeling: designing for security. Wiley, 2014, OCLC: ocn855043351

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS



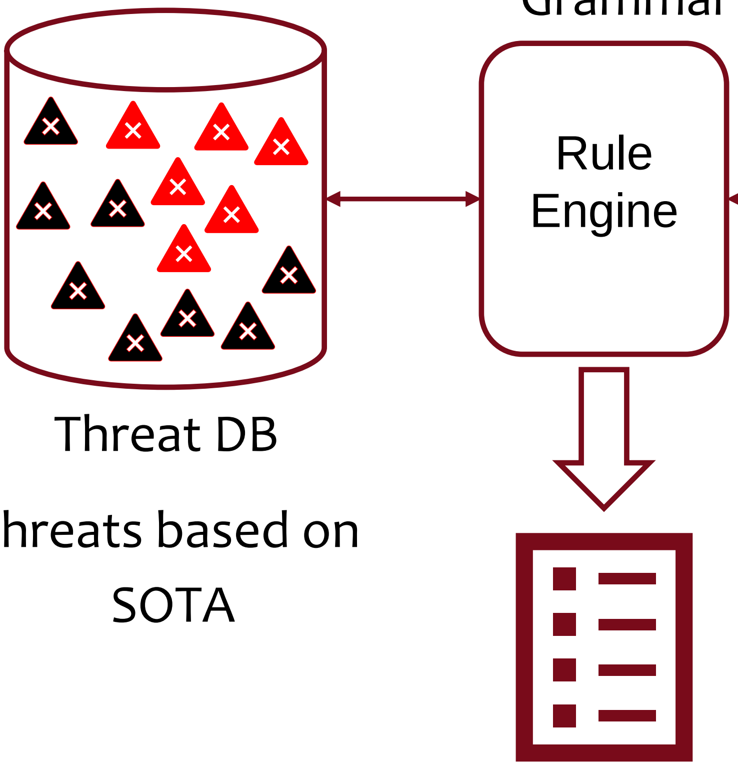
- Spoofing violates **authentication.**
- Tampering violates **integrity**.
- Repudiation violates **non-repudiation.**
- Information Disclosure violates **confidentiality.**

- A. Shostack, Threat modeling: designing for security. Wiley, 2014, OCLC: ocn855043351

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS

ThreatGet's Grammar



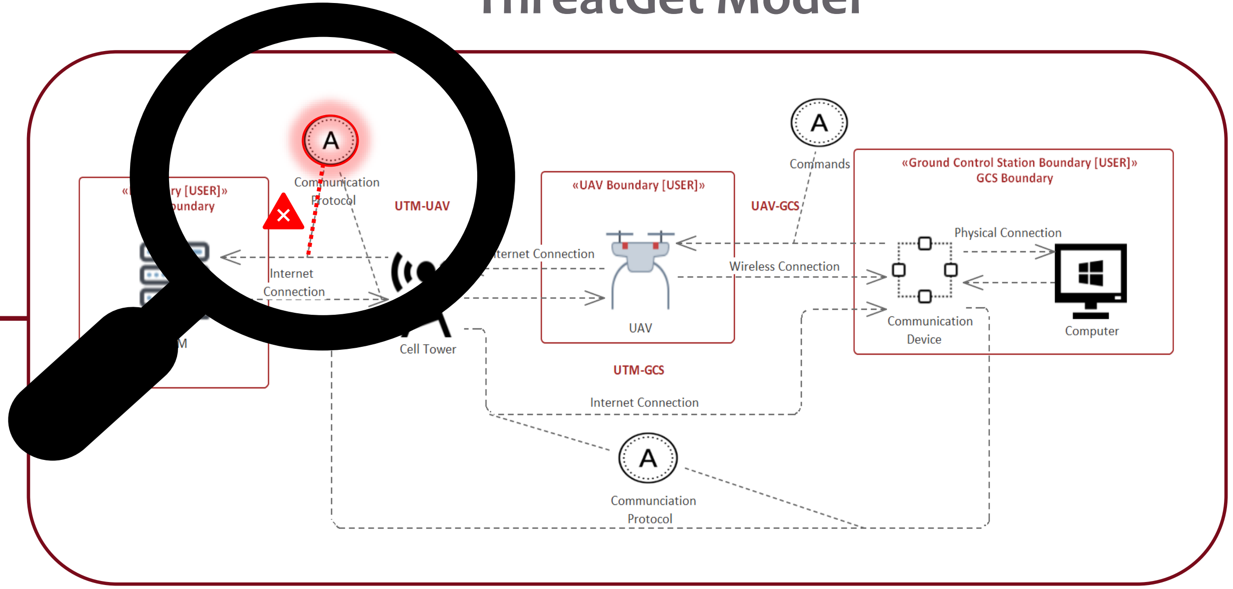
Threat DB

Rule Engine

Threats based on SOTA

List of all threats STRIDE

ThreatGet Model



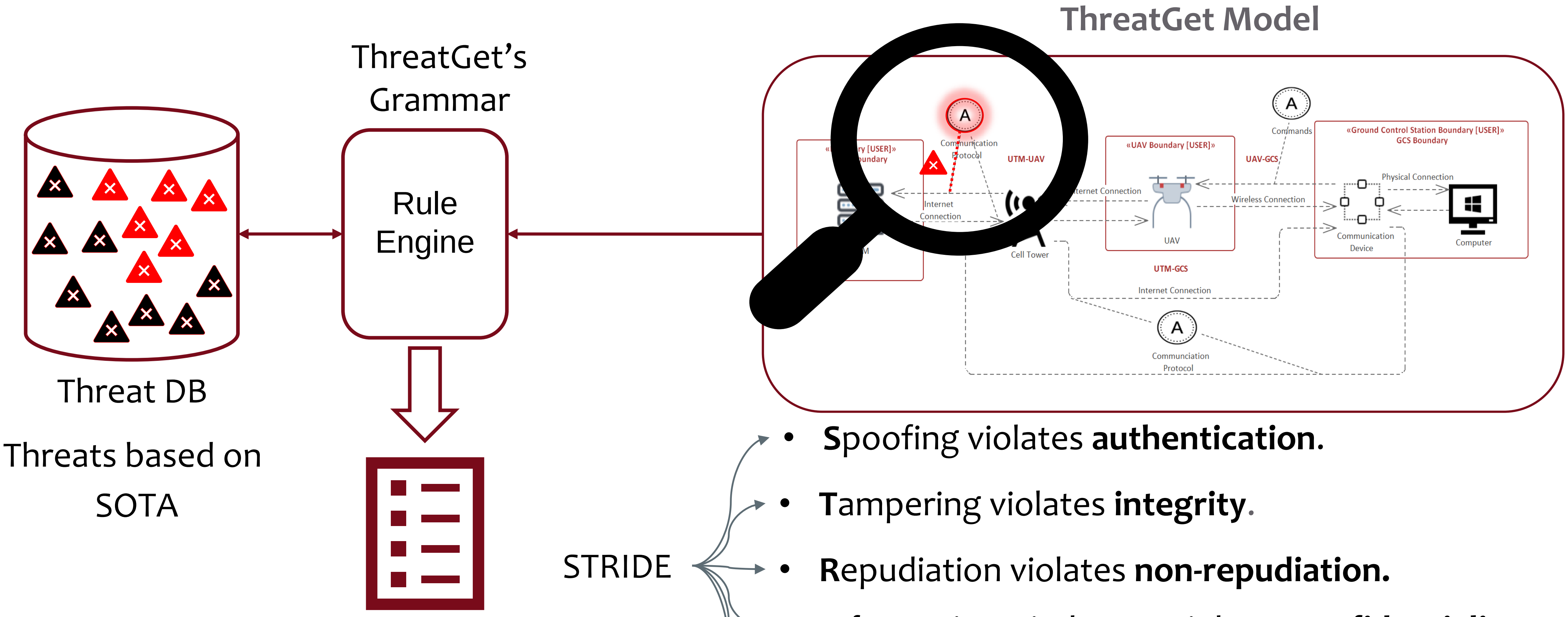
STRIDE

- Spoofing violates **authentication.**
- Tampering violates **integrity**.
- Repudiation violates **non-repudiation.**
- Information Disclosure violates **confidentiality.**
- Denial of Service violates **availability.**

- A. Shostack, Threat modeling: designing for security. Wiley, 2014, OCLC: ocn855043351

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS



Threats based on SOTA

List of all threats STRIDE

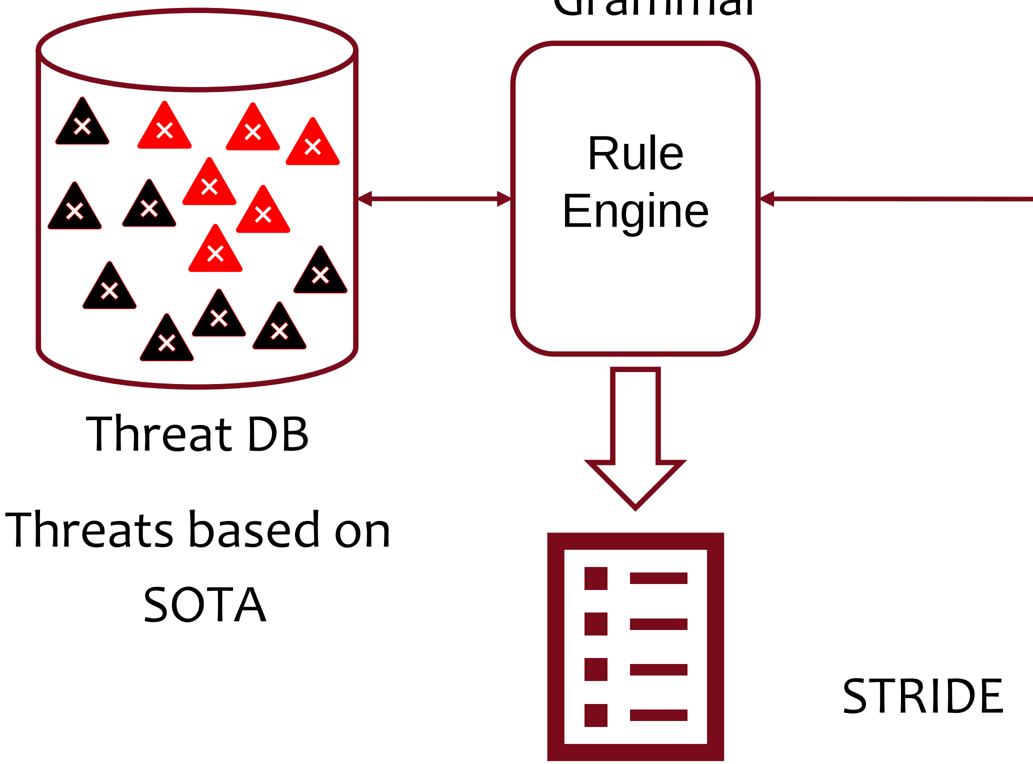
STRIDE

- Spoofing violates **authentication.**
- Tampering violates **integrity**.
- Repudiation violates **non-repudiation.**
- Information Disclosure violates **confidentiality.**
- Denial of Service violates **availability.**
- Elevation of Privilege violates **authorization.**

- A. Shostack, Threat modeling: designing for security. Wiley, 2014, OCLC: ocn855043351

APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION3: RISK ANALYSIS



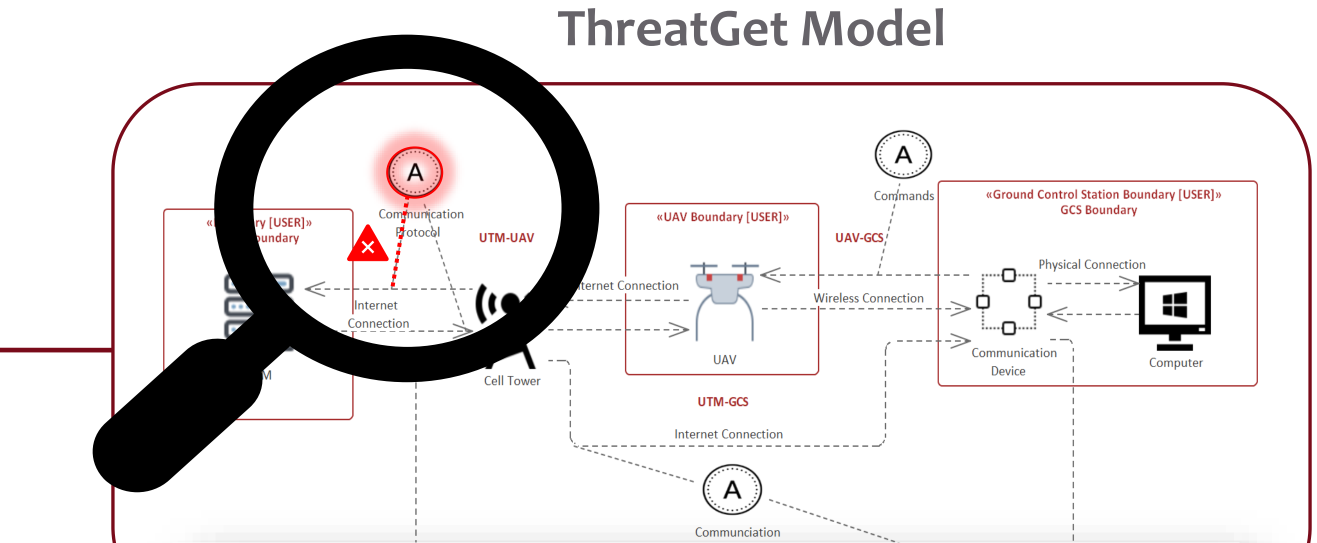
Threat DB

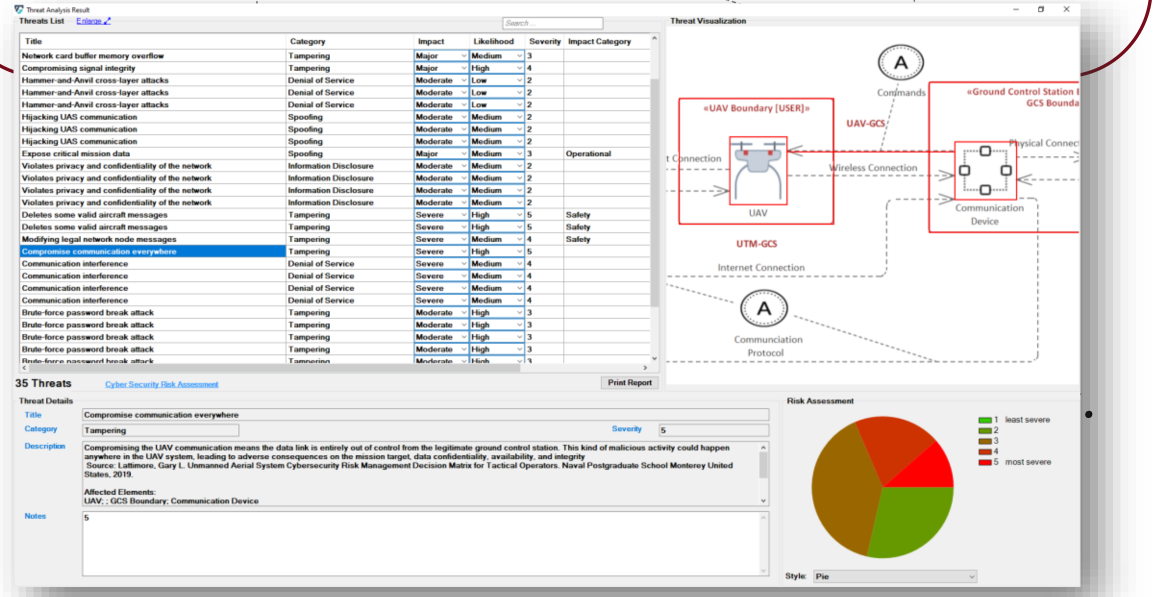
Threats based on SOTA

List of all threats STRIDE

STRIDE

ThreatGet Model





Title	Category	Impact	Likelihood	Severity	Impact Category
Network card buffer memory overflow	Tampering	Major	Medium	3	
Compromising signal integrity	Tampering	Major	High	4	
Hammer-and-Anvil cross-layer attacks	Denial of Service	Moderate	Low	2	
Hammer-and-Anvil cross-layer attacks	Denial of Service	Moderate	Low	2	
Hammer-and-Anvil cross-layer attacks	Denial of Service	Moderate	Low	2	
Hijacking UAS communication	Spoofing	Moderate	Medium	2	
Hijacking UAS communication	Spoofing	Moderate	Medium	2	
Hijacking UAS communication	Spoofing	Moderate	Medium	2	
Expose critical mission data	Spoofing	Major	Medium	3	Operational
Violates privacy and confidentiality of the network	Information Disclosure	Moderate	Medium	2	
Violates privacy and confidentiality of the network	Information Disclosure	Moderate	Medium	2	
Violates privacy and confidentiality of the network	Information Disclosure	Moderate	Medium	2	
Violates privacy and confidentiality of the network	Information Disclosure	Moderate	Medium	2	
Deletes some valid aircraft messages	Tampering	Severe	High	5	Safety
Deletes some valid aircraft messages	Tampering	Severe	High	5	Safety
Modifying legal network node messages	Tampering	Severe	Medium	4	Safety
Compromise communication everywhere	Tampering	Severe	High	5	
Communication interference	Denial of Service	Severe	Medium	4	
Communication interference	Denial of Service	Severe	Medium	4	
Communication interference	Denial of Service	Severe	Medium	4	
Communication interference	Denial of Service	Severe	Medium	4	
Brute-force password break attack	Tampering	Moderate	High	3	
Brute-force password break attack	Tampering	Moderate	High	3	
Brute-force password break attack	Tampering	Moderate	High	3	
Brute-force password break attack	Tampering	Moderate	High	3	
Brute-force password break attack	Tampering	Moderate	High	3	

35 Threats Cyber Security Risk Assessment

Threat Details

Title: Compromise communication everywhere

Category: Tampering

Severity: 5

Description: Compromising the UAV communication means the data link is entirely out of control from the legitimate ground control station. This kind of malicious activity could happen anywhere in the UAV system, leading to adverse consequences on the mission target, data confidentiality, availability, and integrity
Source: Lattimore, Gary L. Unmanned Aerial System Cybersecurity Risk Management Decision Matrix for Tactical Operators. Naval Postgraduate School Monterey United States, 2019.

Affected Elements:
UAV; ; GCS Boundary; Communication Device

Notes: 5

Risk Assessment

- 🟩 1 least severe
- 🟩 2
- 🟫 3
- 🟧 4
- 🟥 5 most severe

Style: Pie

- A. Shostack, Threat modeling: designing for security. Wiley, 2014, OCLC: ocn855043351

APPLYING IEC 62443 SECURITY STANDARD IN UAS

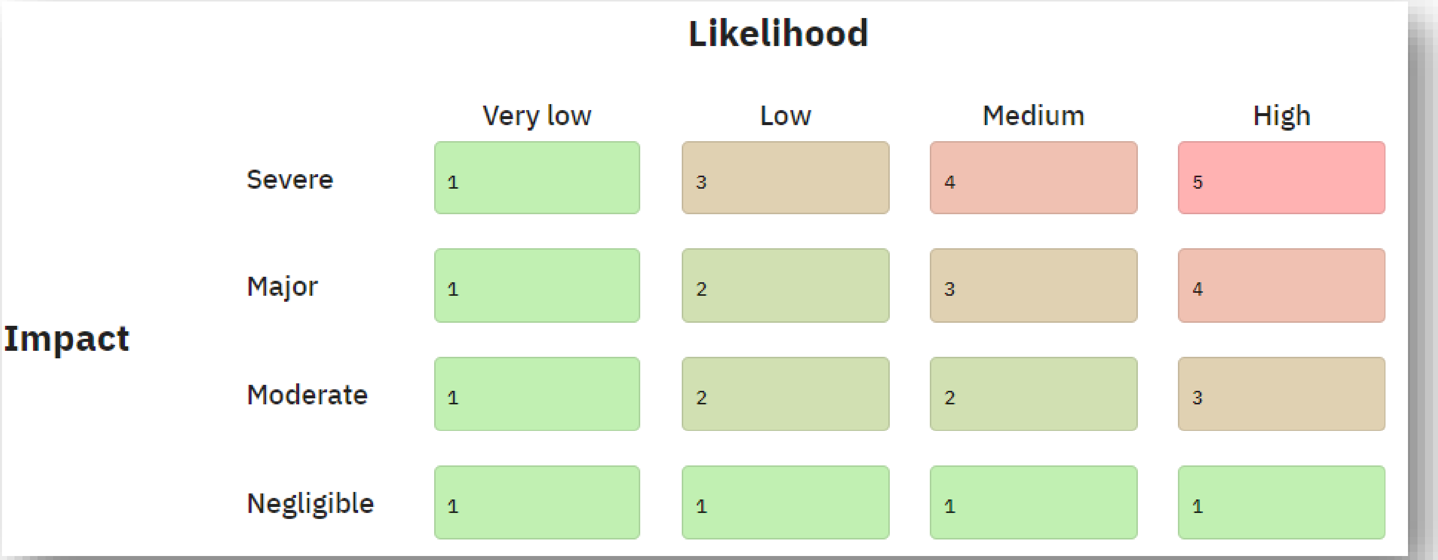
ACTION4 AND 5: RISK EVALUATION AND SECURITY TARGET ESTIMATION

- ThreatGet **calculates** the overall risk of the whole UAS model by estimating the **risk severity** of each identified threat.

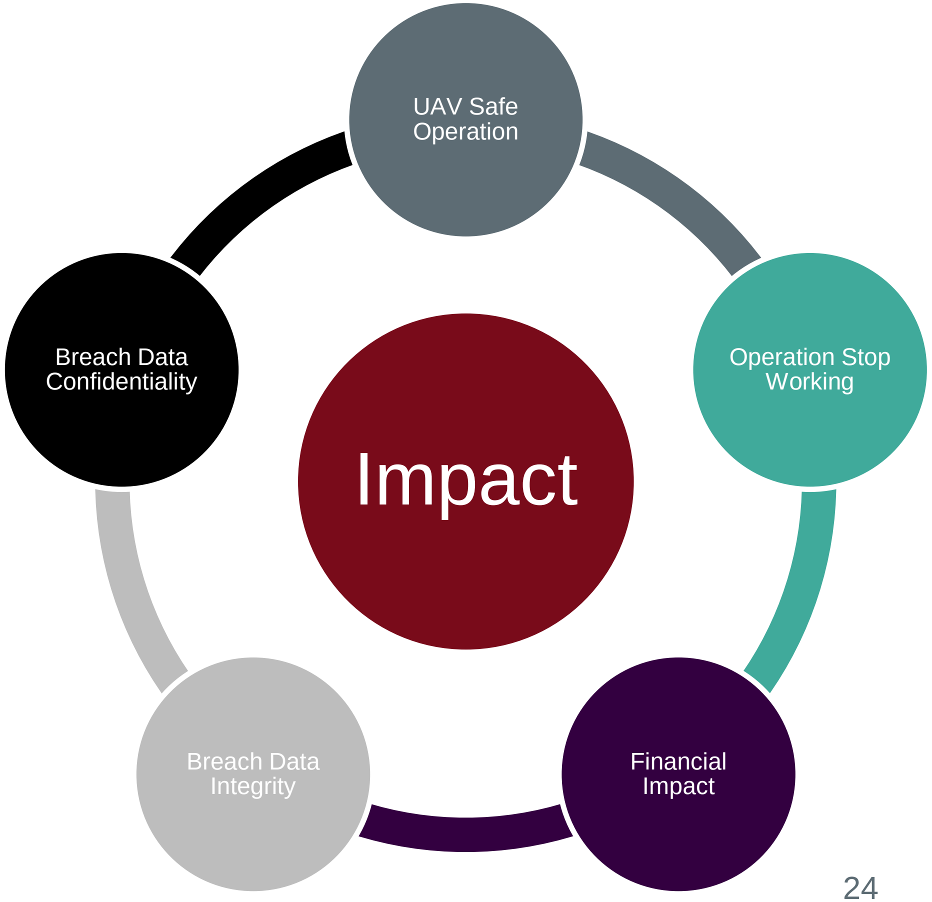
- Estimate the **ST** for **each zone** and **conduit** according to the risk **severity of threats.**

- Select the most **applicable** security requirements that **address** existing security issues.

ThreatGet Risk Matrix



		Likelihood			
		Very low	Low	Medium	High
Impact	Severe	1	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

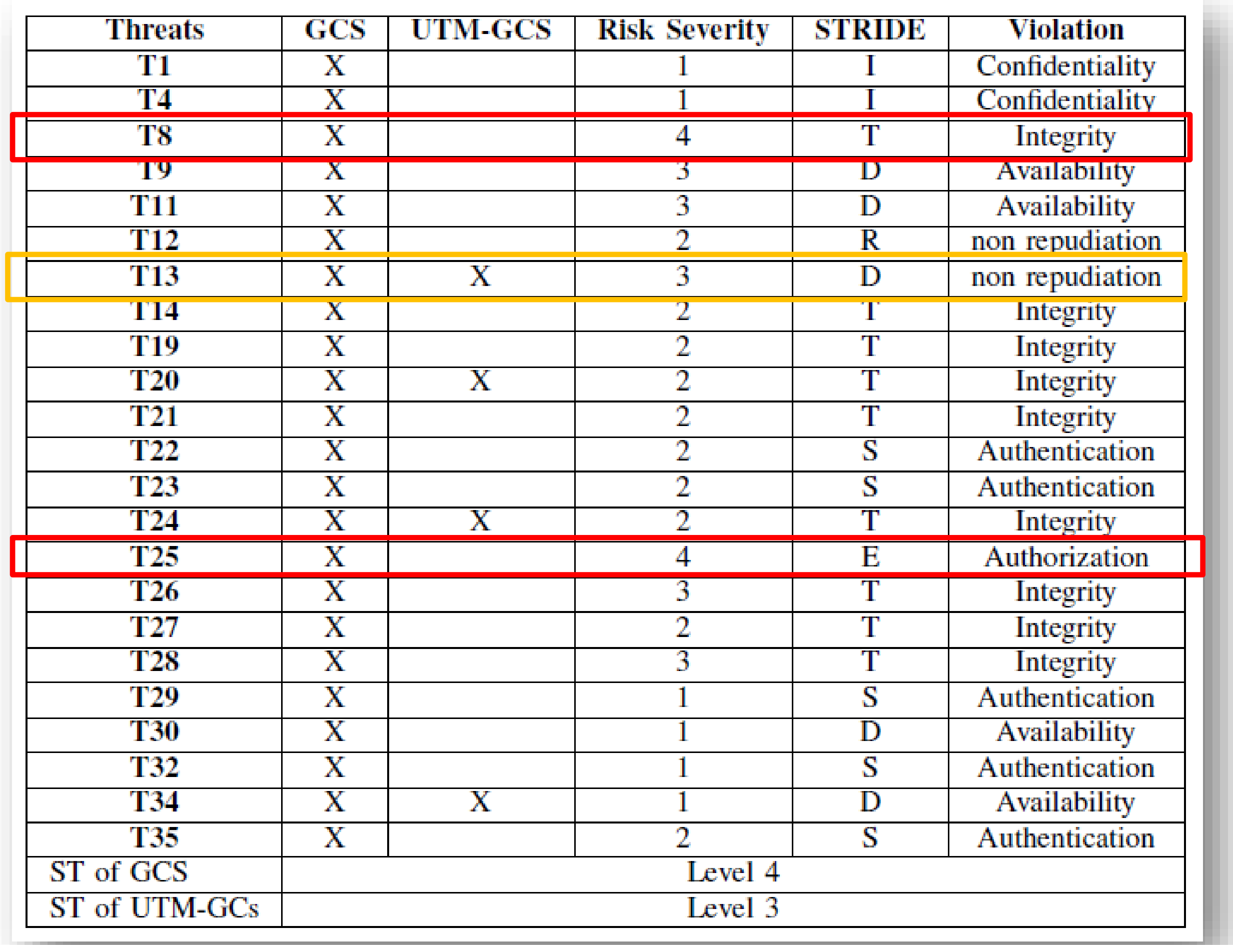


APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION4 AND 5: RISK EVALUATION AND SECURITY TARGET ESTIMATION

- Security target analysis of **GCS** security zone and **UTM-GCS** conduit based on ThreatGet's findings

23 threats



Threats	GCS	UTM-GCS	Risk Severity	STRIDE	Violation
T1	X		1	I	Confidentiality
T4	X		1	I	Confidentiality
T8	X		4	T	Integrity
T9	X		3	D	Availability
T11	X		3	D	Availability
T12	X		2	R	non repudiation
T13	X	X	3	D	non repudiation
T14	X		2	T	Integrity
T19	X		2	T	Integrity
T20	X	X	2	T	Integrity
T21	X		2	T	Integrity
T22	X		2	S	Authentication
T23	X		2	S	Authentication
T24	X	X	2	T	Integrity
T25	X		4	E	Authorization
T26	X		3	T	Integrity
T27	X		2	T	Integrity
T28	X		3	T	Integrity
T29	X		1	S	Authentication
T30	X		1	D	Availability
T32	X		1	S	Authentication
T34	X	X	1	D	Availability
T35	X		2	S	Authentication
ST of GCS	Level 4				
ST of UTM-GCs	Level 3				

GCS: highest risk severity = 4

UTM-GCS: highest risk severity = 3

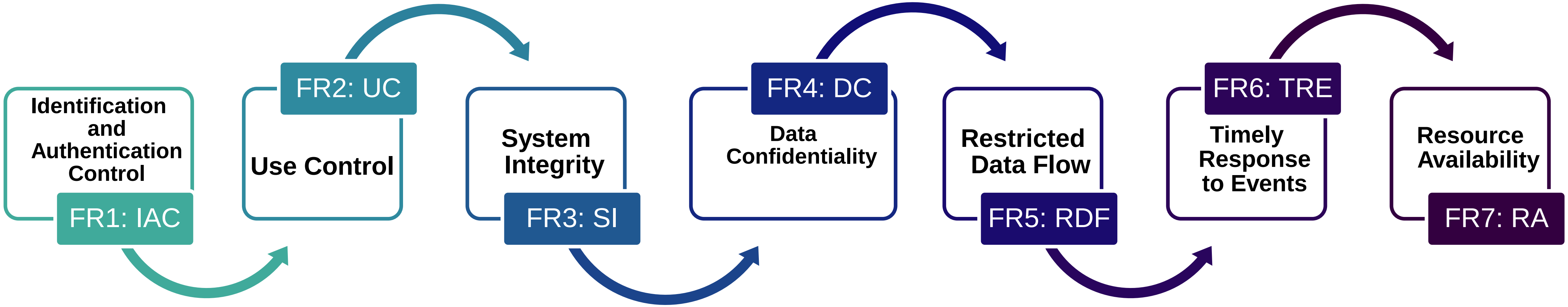
APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION6 AND 7: APPLY SECURITY REQUIREMENTS AND MAP FRS WITH STRIDE

- The IEC 62443 **provides** a complete cybersecurity framework for **addressing** existing cybersecurity issues.
- According to the IEC 62443 security standard, the associated four **Security-Level Capability** (SL-C).

SL1 SL2 SL3 SL4

- The standard describes security requirements into FRs:



FR1: IAC
Identification and Authentication Control

FR2: UC
Use Control

FR3: SI
System Integrity

FR4: DC
Data Confidentiality

FR5: RDF
Restricted Data Flow

FR6: TRE
Timely Response to Events

FR7: RA
Resource Availability

IEC, “Security for industrial automation and control systems - part 4-2: Technical security requirements for IACS components,” International Standard, Tech. Rep., Feb. 2019.

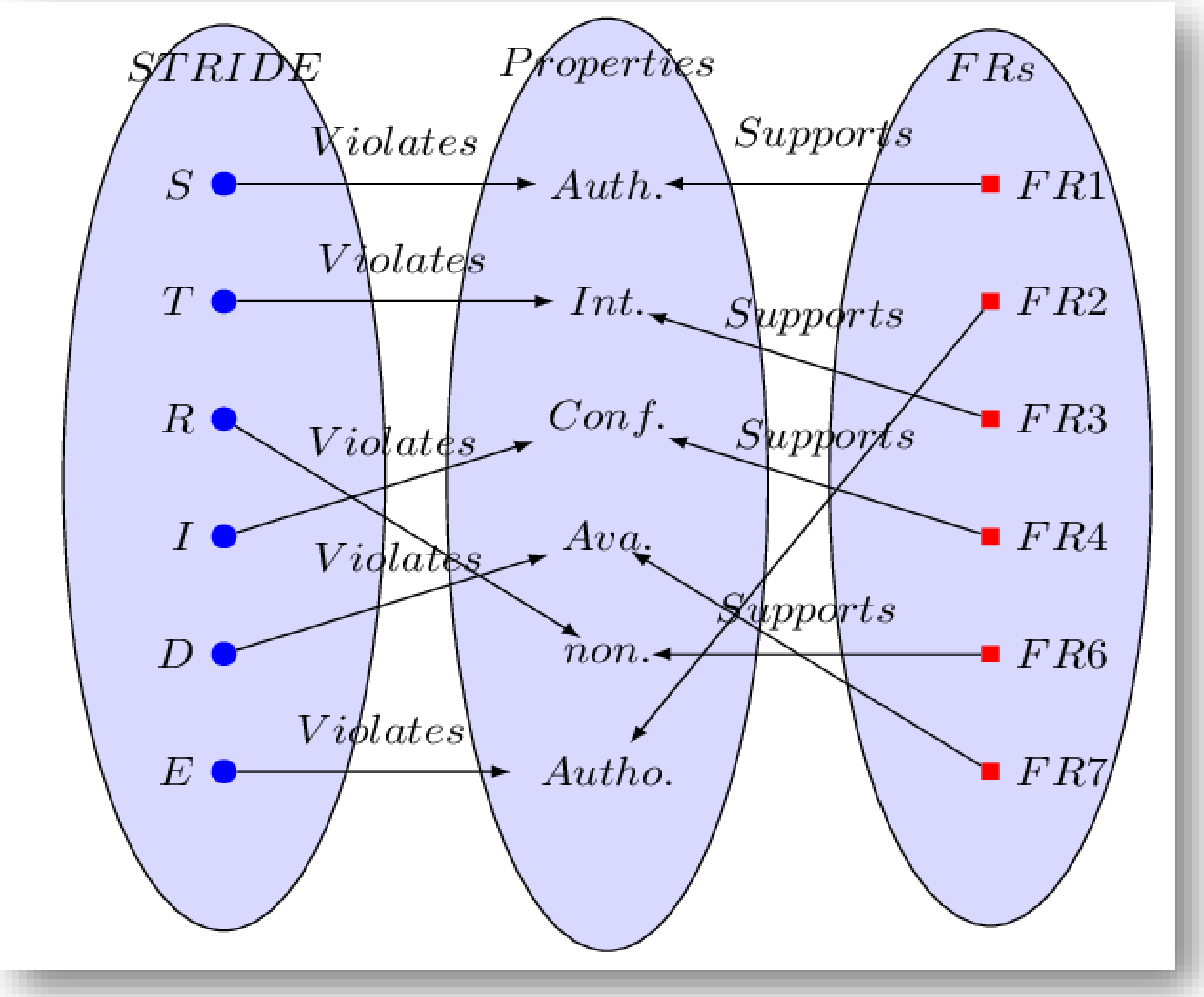
APPLYING IEC 62443 SECURITY STANDARD IN UAS

ACTION6 AND 7: APPLY SECURITY REQUIREMENTS AND MAP FRS WITH STRIDE

- This procedure enables a mapping between **security requirements** (defined in terms of FRs) and **threats** (defined in terms of STRIDE)

- Violation of security properties, relevant **security requirements** shall be selected to address existing security issues

- SL-C of **security requirements** should equal each threat's risk severity to achieve the main **ST** for each **security zone** and **conduit**.



IEC, "Security for industrial automation and control systems - part 4-2: Technical security requirements for IACS components," International Standard, Tech. Rep., Feb. 2019.

CONCLUSION AND FUTURE WORK

- We proposed a standard-based procedure based on **IEC 62443** to be integrated into the UAS-domain for addressing potential threats.
- We employ **ThreatGet** as a threat modelling tool to assist in this process:
  - We define **security zones/conduits** and define the main system's assets.
  - Then, we perform the **risk analysis** using ThreatGet for **analyzing**, **detecting**, and **prioritizing** security issues of a system design.
  - Afterwards, the tool estimates the **severity level** for each threat based on **impacts** and **likelihoods.**
- The proposed **mapping** strategy is based on selecting a set of security requirements according to their capabilities (i.e., **SL-C**) to fulfill the main security goal.

- A mathematical model is proposed as the next step to estimate the **security achieved** (SL-A) after **applying** security requirements.
- That helps to guarantee the **achieved level** is equal to the **security target level** and ensure the **correctness** of the applied security requirements.

ACKNOWLEDGMENT

This work is done in the **LABYRINTH project,** which has received funding from the **European Union's Horizon 2020** research and innovation program under grant agreement No **861696.**

Labyrinth
Ensuring drone traffic control and safety

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU

Any Questions?