UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

itee PhD information technology electrical engineering

DIETI UNINA

Nicola d'Ambrosio

Boosting Cyber-Resilience in Networked Infrastructures via Risk Analysis and Active Deception Strategies

Tutor: Prof. Simon Pietro Romano

Cycle: XXXVII Year: 2022

itee PhD information technology electrical engineering

UNIONE EUROPEA FSE REACT-EU

MUR

PON RICERCA E INNOVAZIONE

Candidate’s information

- MSc degree: Computer Engineering
- DIETI Research group: ArcLab
- PhD start date - end date: 1/1/2022 – 31/12/2024
- Scholarship type: PON Dottorati di ricerca su tematiche dell'innovazione e green - Azione IV.4 (Innovazione)
- Period abroad: Accenture Cyber Fusion Center Prague (6 months)
- Internship: Accenture Italia (6 months)

Summary of study activities

- **9 courses:**
  - 6 PhD Courses
  - 1 MSc Course
  - 2 PhD Schools

- **20 Seminars**

- **5 Conferences:**
  - Black Hat Asia and Black Hat USA
  - International Conference on Electrical, Computer and Energy Technologies
  - IEEE Conference on Network Function Virtualization and Software Defined Networks
  - 1st Workshop on Network Digital Twin for Innovative Networks

Research areas

- Main research areas:

Combination of **safety models** (STPA) and **cybersecurity frameworks** (based on NIST 800-53 and MITRE ATT&CK) to evaluate the impact of cyberattacks on critical infrastructures

Integration of **Bayesian Attack Graphs** to analyze the impact and likelihood of insider threats on enterprise infrastructures, with the aim of estimating the costs and benefits of mitigation strategies

Design of **deception strategies** for **enterprise and industrial networks** aimed at mitigating internal and external threats to network infrastructures

- Other Projects:
  - Blockchain and security
    - e-voting with ring signatures, tamper-proof IoT communications
  - OSINT (Open Source Intelligence)
  - Digital Twins and Cyber Ranges

Research results

- Definition of a comprehensive methodology starting with risk assessment and followed by the implementation of innovative deception strategies capable to neutralize identified risks effectively
- Development of solutions for creating vulnerable cyber range environments and enabling semi-automated exploitation of the exposed vulnerabilities
- Design and implementation of a toolkit allowing individuals with no technical expertise to conduct Open-Source Intelligence

Research products

[P1]	Nicola d’Ambrosio, Gaetano Perrone, Simon Pietro Romano, Alberto Urraro *A Cyber-Resilient Open Architecture for Drone Control,* **Computer and Security,** vol. 150, pp. 104205, 2025
[P2]	Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano *Including insider threats into risk management through Bayesian threat graph networks,* **Computer and Security,** Volume 133, pp. 103410, 2023
[P3]	F. Caturano, N. d’Ambrosio, G. Perrone, L. Previdente, S. P. Romano *ExploitWP2Docker: a Platform for Automating the Generation of Vulnerable WordPress Environments for Cyber Ranges* **International Conference on Electrical, Computer and Energy Technologies,** Prague, Czech Republic, 2022, pp. 1-7, IEEE
[P4]	N. 'Ambrosio, E. Melluso, G. Perrone S. P. Romano *A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense* **IEEE Conference on Network Function Virtualization and Software Defined Networks,** Dresden, Germany, 2023, pp. 213-219, IEEE

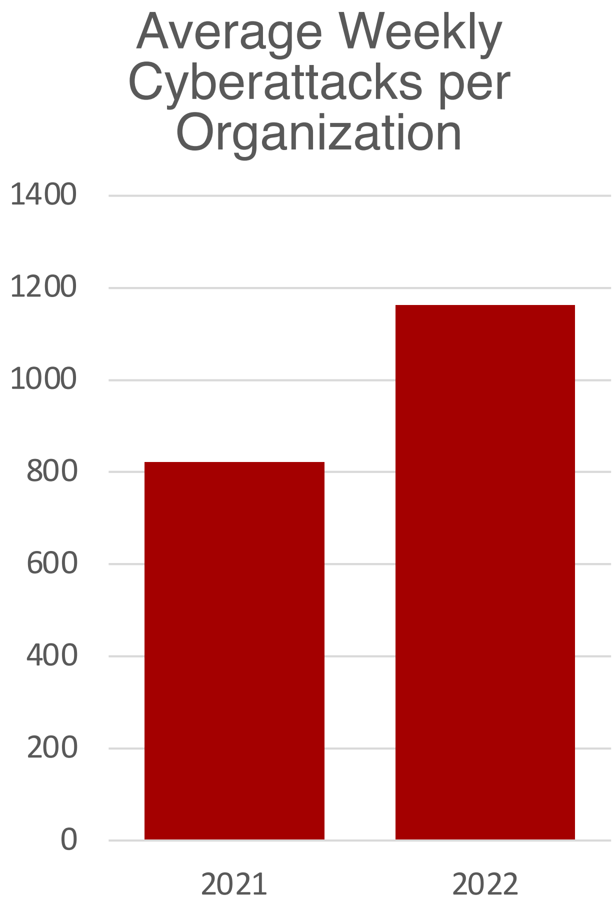
Research products

[P5]	Raffaele Cuorvo, Nicola d'Ambrosio, Domenico Iorio, Gaetano Perrone, Simon Pietro Romano *Securing Industrial Systems: A Testbed for Cyber-Defense Evaluation and Data Collection,* **1st Workshop on Network Digital Twin for Innovative Networks (NDT4IN),** Prague, Czech Republic, 2024, Yet to Appear, IEEE
[P6]	Giulio Capodagli, Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano *SCASS: breaking into SCADA Systems Security,* **Computer and Security** (under second review round)
[P7]	Nicola d'Ambrosio, Gaetano Perrone, Vittoria Pacchiano, Simon Pietro Romano ExploDox - Unleashing Exploit-DB Data for Automated Exploits Generation, **Journal of Systems & Software** (under review)
[P8]	Nicola d'Ambrosio, Claudio Lista, Gaetano Perrone, Simon Pietro Romano *SMASH: SDN-MTD Automated System with Honeypot Integration,* **Computer Networks** (under review)
[P9]	Antonio Avolio, Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano *LLM-assisted generation of vulnerable containers,* **Expert Systems with Applications** (under review)

PhD thesis overview

Problem - Rising cyber-attacks are targeting enterprise and industrial networks with increasing precision and complexity.

Objective - Leverage Risk Analysis to evaluate the potential impacts and consequences of cyber-attacks on critical systems and empower the design of tailored cyber-defense solution.



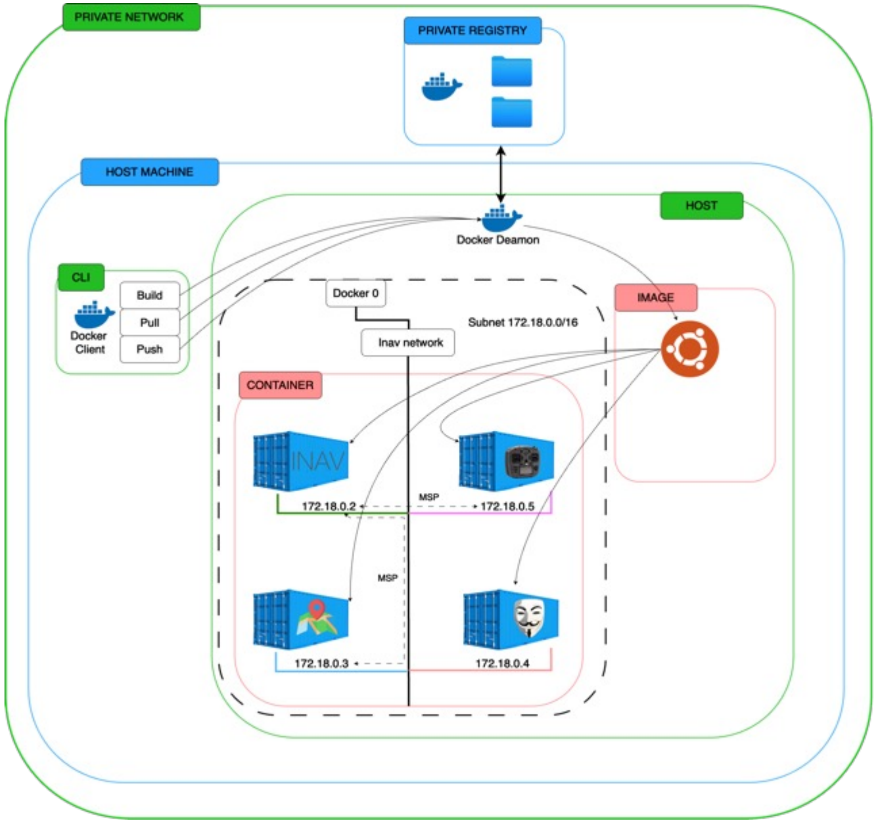
From Safety Analysis to Cyber Risk Analisys

Methodology – It relies on Safety Analysis to evaluate the impact of cyberattacks. It is structured into three main steps:

1. **Build the architecture under consideration.**
2. **Construct a Cyber-Resilience Model**
   - STAMP/STPA Model Construction
   - Attack Graph Generation
3. **Cyber-Resilience Model Validation**

A cyber-resilient open architecture for drone control - Experimental Setup

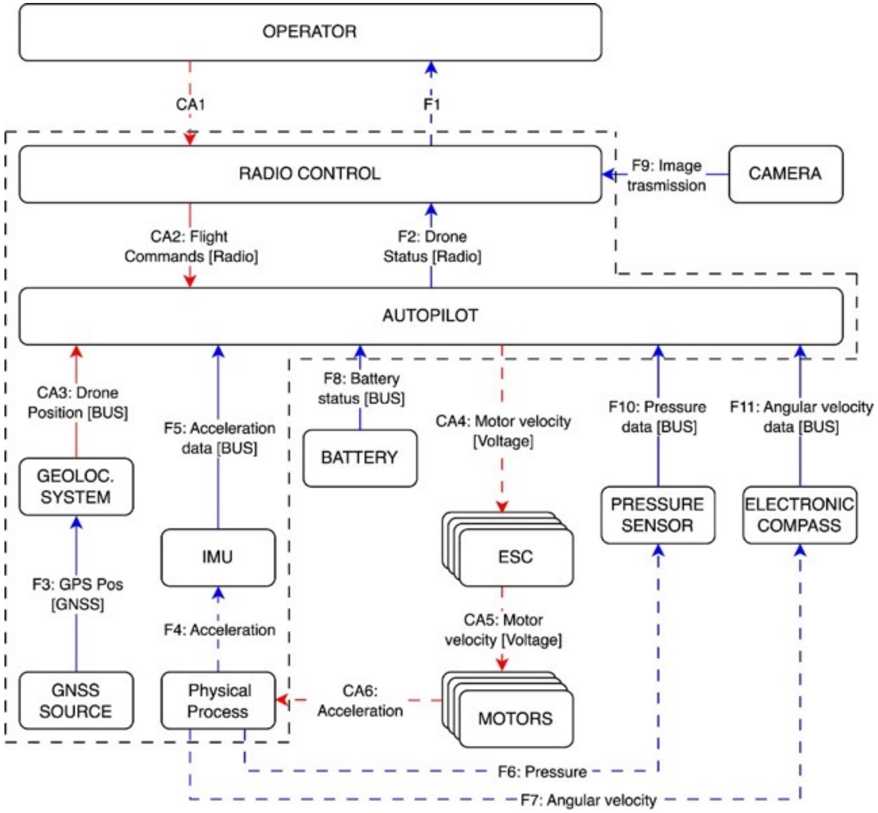
The main outcome of the **first stage** is to develop a flexible and modular architecture. This architecture, leveraging Open System Architecture (OSA) principles, serves as the foundation for analyses conducted in subsequent stages.



A cyber-resilient open architecture for drone control - STAMP/STPA Model

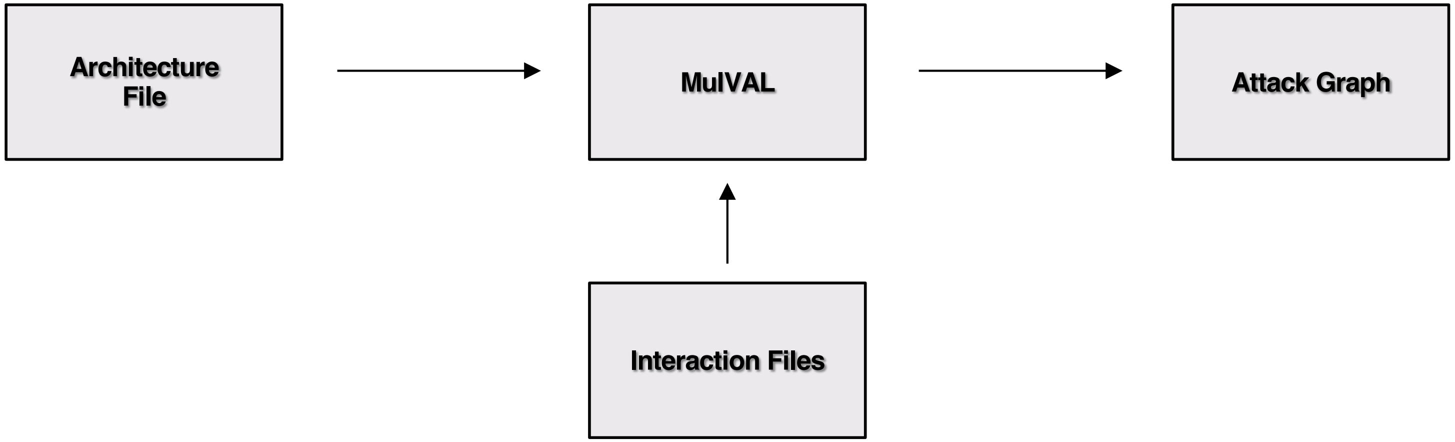
The **second step** of this process is composed of four different substages:

Deception strategy
Construction of the STAMP Model
Identification of Accidents *(A)*, Hazards *(H)*, and Losses *(L)*
Definition of the Safe Control Structure *(SCS)*
Identification of Hazardous Control Actions *(HCA)*



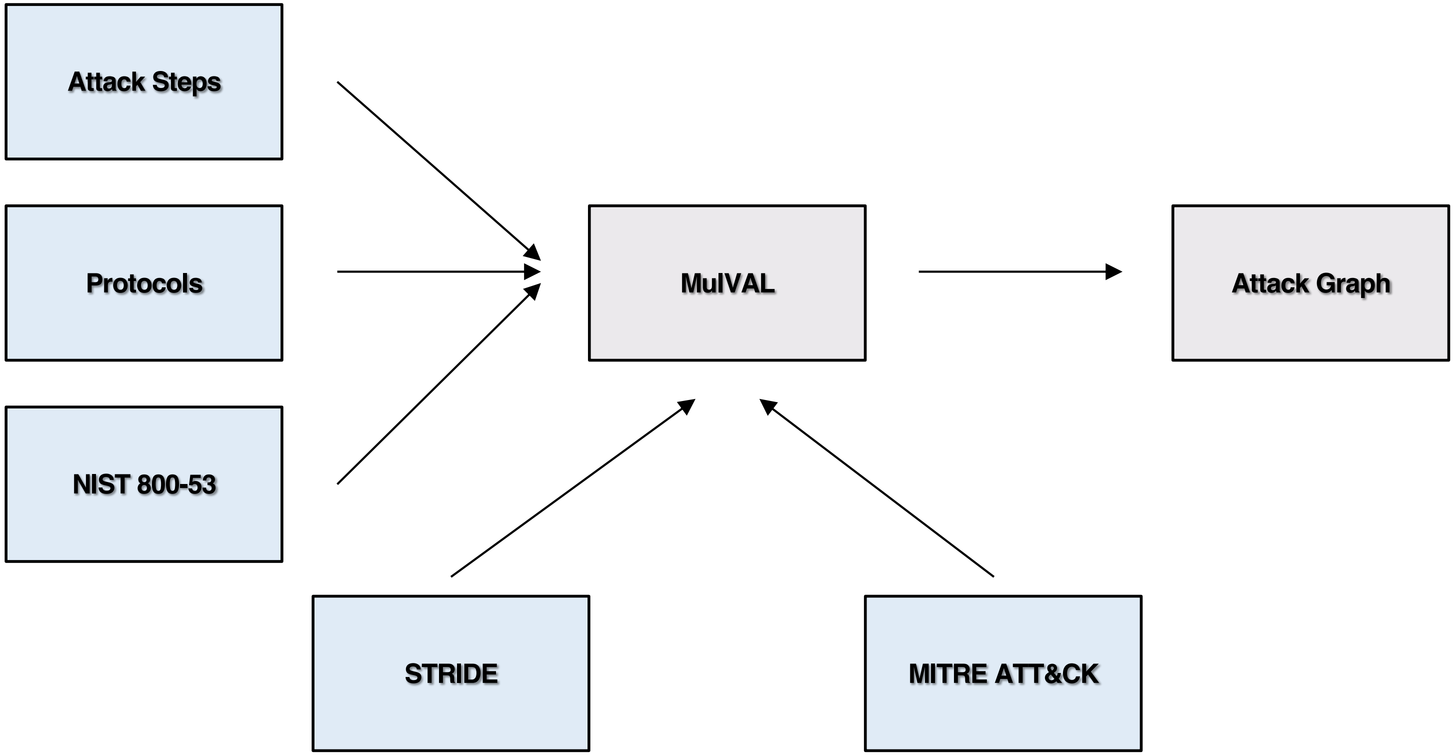
A cyber-resilient open architecture for drone control - Attack Graph

The **third step** in this process enables the generation of an attack graph, which illustrates how to trigger a specific hazardous condition.



A cyber-resilient open architecture for drone control - Attack Graph

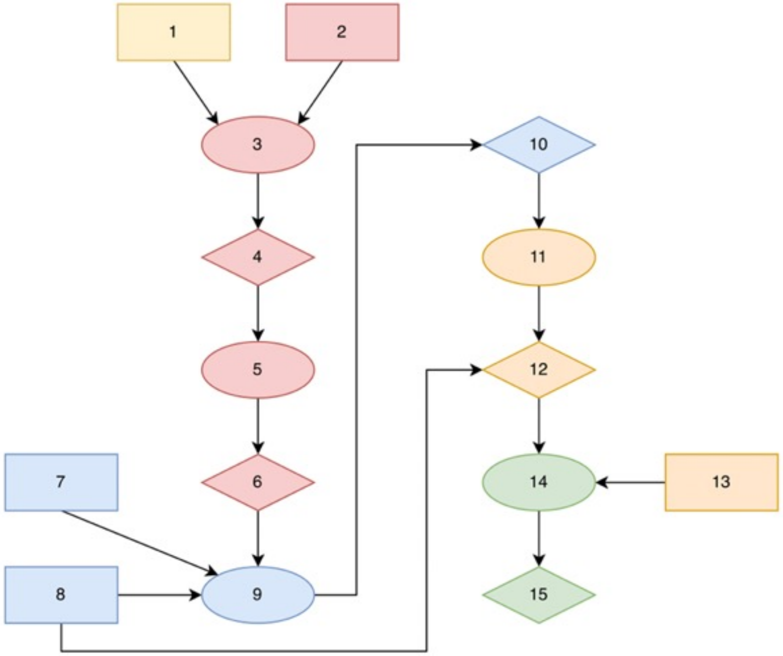
The **third step** in this process enables the generation of an attack graph, which illustrates how to trigger a specific hazardous condition.

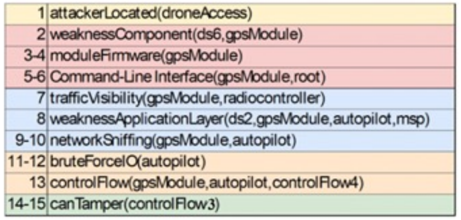


A cyber-resilient open architecture for drone control - Attack Emulation

The attack graph illustrates the sequence of actions an attacker must take to achieve their malicious objective.

The same methodology was applied to develop a hybrid MicroGrid digital twin, referred to as SCASS.



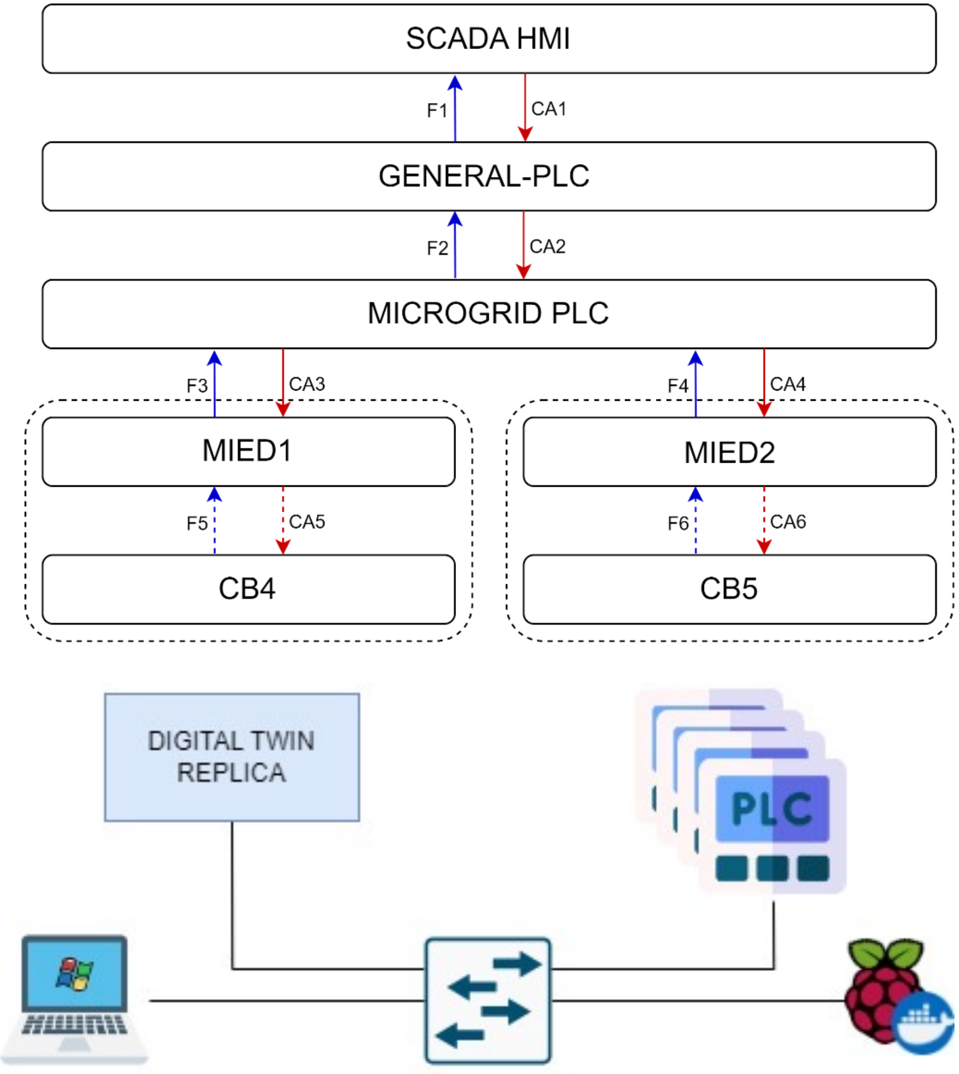


1	attackerLocated(droneAccess)
2	weaknessComponent(ds6,gpsModule)
3-4	moduleFirmware(gpsModule)
5-6	Command-Line Interface(gpsModule,root)
7	trafficVisibility(gpsModule,radiocontroller)
8	weaknessApplicationLayer(ds2,gpsModule,autopilot,msp)
9-10	networkSniffing(gpsModule,autopilot)
11-12	bruteForceIO(autopilot)
13	controlFlow(gpsModule,autopilot,controlFlow4)
14-15	canTamper(controlFlow3)

Integration of Safety Analysis and Active Deception for Mitigating Threats

We leveraged the insights gained from the STAMP/STPA analysis to effectively address and mitigate the threats identified in the previously mentioned assessment using Active Deception Techniques:

- The SCS is used to derive all legit interaction between components
- In case of malicious interaction, Moving Target Defense is applied to isolate the attacker and substitute the exploited component

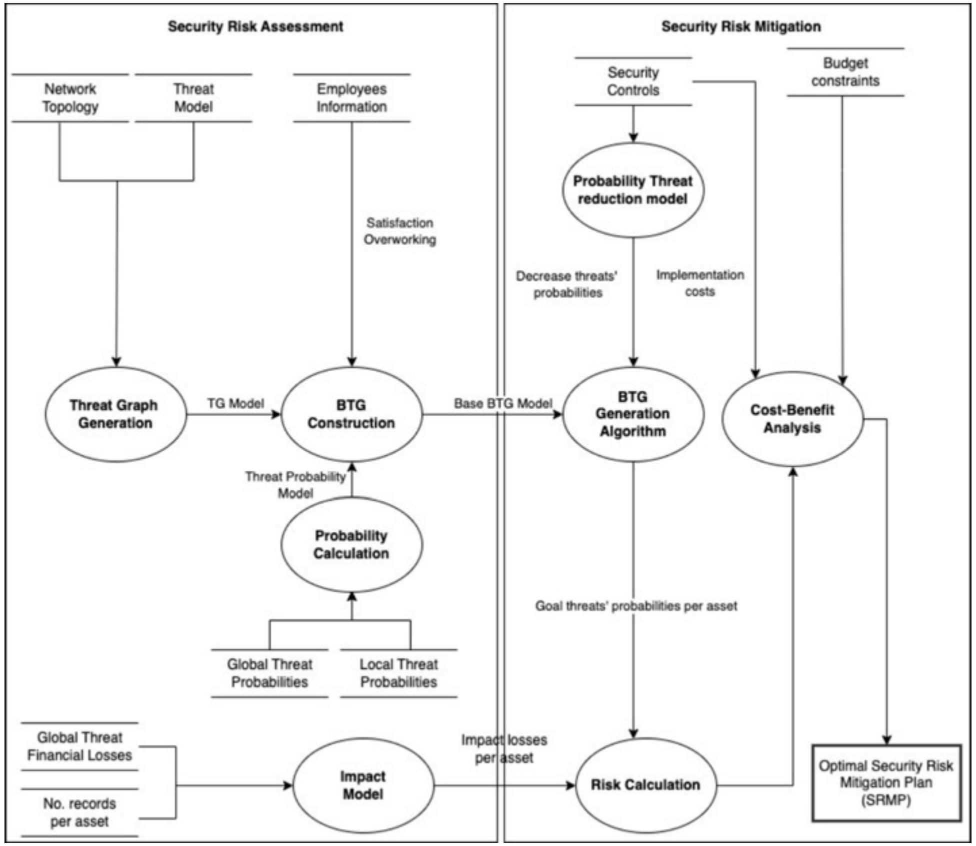


Including insider threats into risk management frameworks

Problem - The presented methodology cannot effectively evaluate the risks associated with insider threats or assess the resulting economic losses.

Objective - Minimize the negative impact of these risks on an organization and maximize the security of its information and systems.

Methodology - Risk management framework based on Bayesian Decision Networks that allows the selection of the best security controls' combination under budget constraints

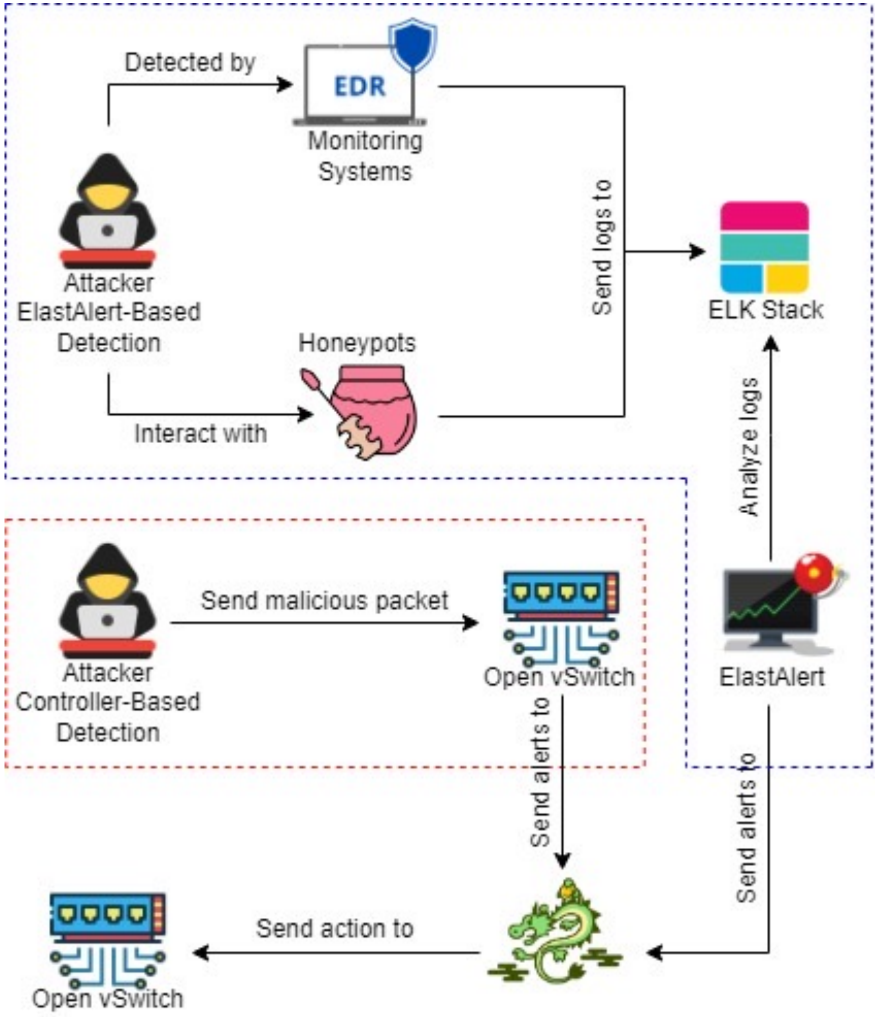


SDN-MTD Automated System with Honeypot Integration

Problem - Mitigating Insider (and also external) threats

Objective - Implementation, in a typical business network, of Defensive Deception Techniques, like Moving Target Defense (MTD) and Honeypots, as an added benefit to traditional ones, in order to overcome their shortcomings

Methodology - Design a solution leveraging Software Defined Network (SDN) principles and honeypot-as-a-service mechanism to increase the attack complexity and provide insights into attacker behaviors.



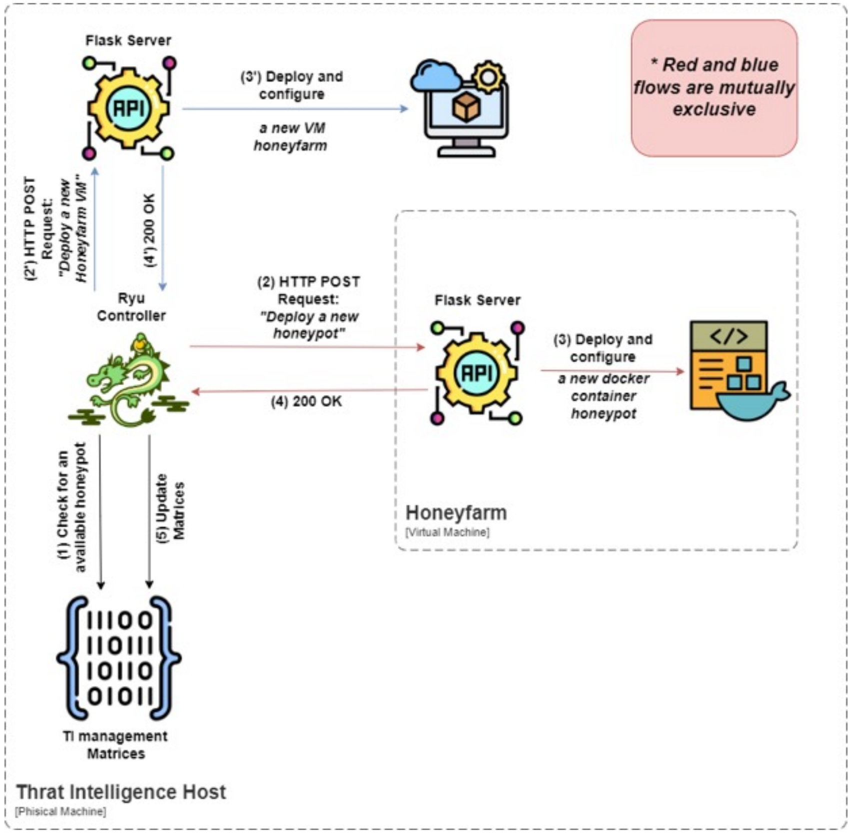
SDN-MTD Automated System with Honeypot Integration

Honeypot-as-a-Service (HaaS) simplifies honeypot deployment in network environments by provisioning both virtual machines and containers as required.

Dynamic Deployment: HaaS allows dynamic honeypot deployment enabling rapid setup in response to changes in the environment.

Scalability: HaaS enhances scalability by deploying and managing multiple honeypots across networks as needed.

Automation: HaaS automation streamlines honeypot setup, configuration, and monitoring, minimizing manual effort.


Flask Server
(3') Deploy and configure
a new VM honeyfarm
* Red and blue flows are mutually exclusive
(2') HTTP POST Request: "Deploy a new Honeyfarm VM"
(4') 200 OK
Ryu Controller
(2) HTTP POST Request: "Deploy a new honeypot"
(4) 200 OK
Flask Server
(3) Deploy and configure
a new docker container honeypot
Honeyfarm
[Virtual Machine]
(1) Check for an available honeypot
(5) Update Matrices
TI management Matrices
Thrat Intelligence Host
[Phisical Machine]

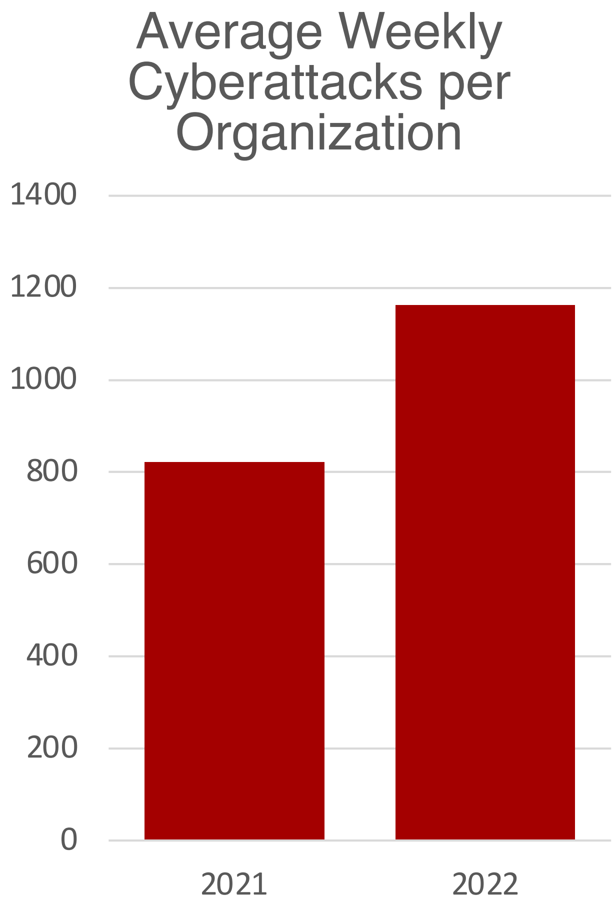
Thanks for your attention!

PhD thesis overview

Problem statement: Rising cyber-attacks are targeting enterprise and industrial networks with increasing precision and complexity. To stay ahead, **proactive defense strategies are mandatory.**

… BUT HOW?

Objective: Develop a methodology to **pinpoint high-impact cyber risks and integrate proactive defense strategies with traditional tools** like firewalls to effectively mitigate cyber attack consequences.

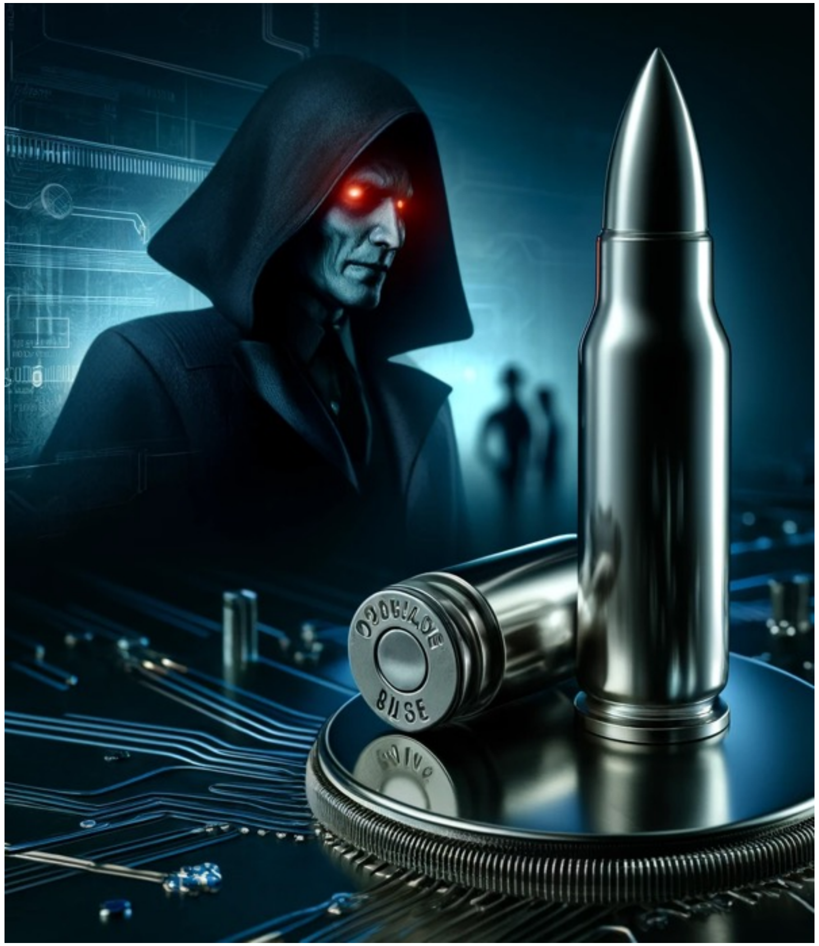


PhD thesis overview

Targeted Approach: Industrial and Enterprise networks demand **unique risk assessment strategies tailored to the consequences of cyberattacks.**

Cybersecurity has no "silver bullet"

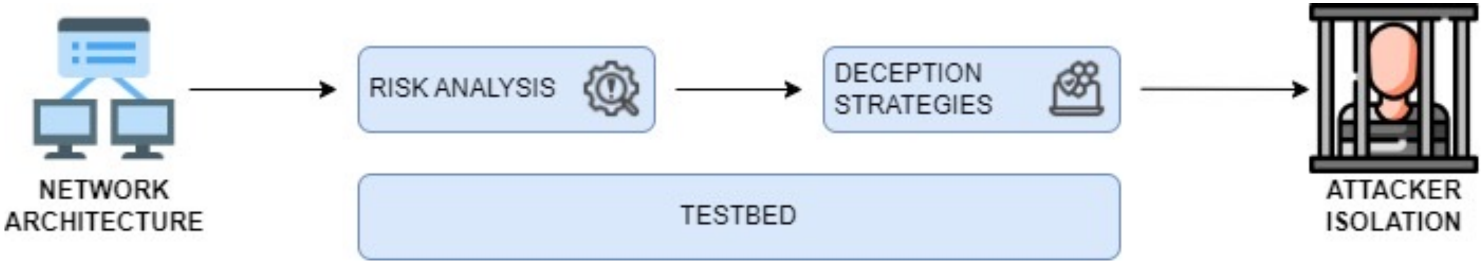
Unified Methodology: Different challenges require customized solutions, yet share a ***common framework*** for effective implementation.



PhD thesis overview

This methodology is based on three elements:

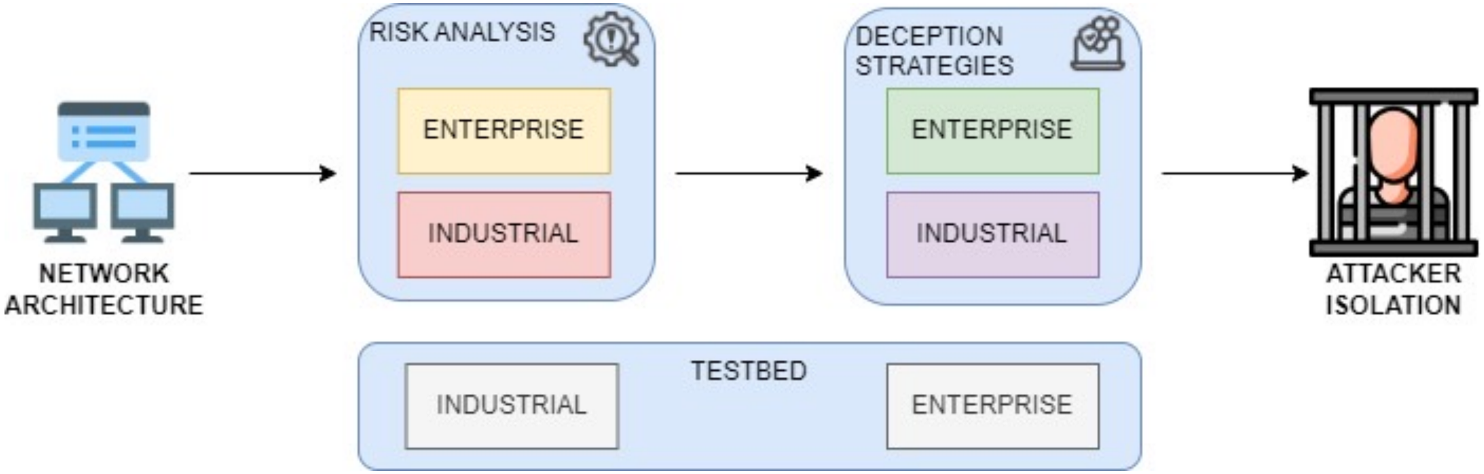
1. **Risk Assessment:** Identify and prioritize factors with the highest risk to your network infrastructure
2. **Deception Strategies:** Implement targeted strategies to address these critical risk factors
3. **Testbed Validation:** Use controlled test environments to evaluate the effectiveness of the proposed strategies



PhD thesis overview

This methodology is based on three elements:

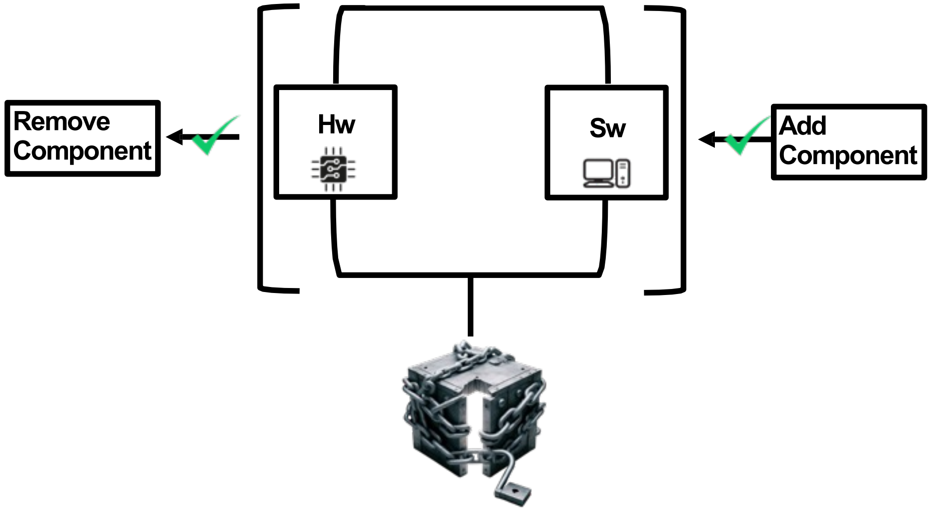
1. **Risk Assessment:** Identify and prioritize factors with the highest risk to your network infrastructure
2. **Deception Strategies:** Implement targeted strategies to address these critical risk factors
3. **Testbed Validation:** Use controlled test environments to evaluate the effectiveness of the proposed strategies



A cyber-resilient open architecture for drone control

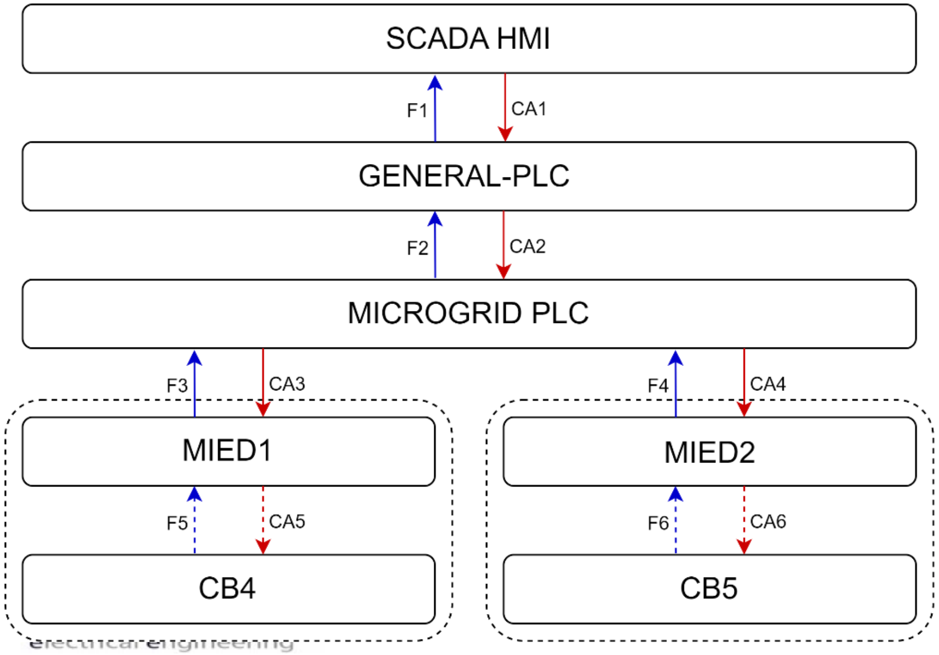
Problem - Drones, increasingly prevalent in both military and civilian domains, face limitations associated with current monolithic architectures.

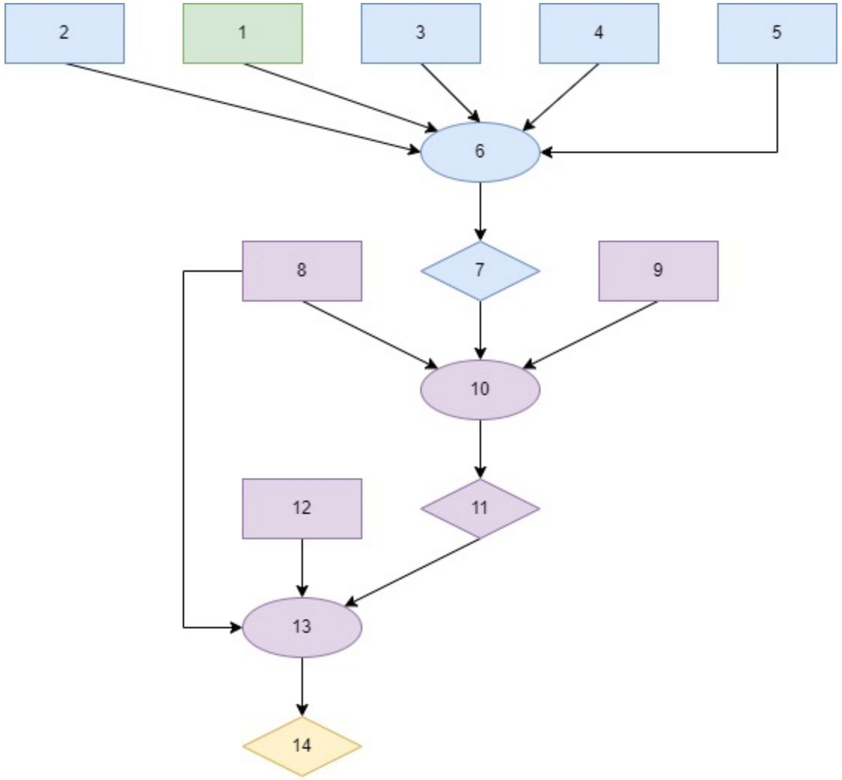
Objective - Implementation of a new drone architecture based on the Open paradigm with microservices in order to enhance flexibility, maintainability, scalability, and security



From Safety Analysis to Risk Analysis

We utilize the integration of the safety model with the deployed system's architecture to construct the attack graph (AG) that outlines the privileges an adversary must obtain to execute a specific threat scenario.





1	attackerLocated(microgrid)
2	inSubnet(microgridPLC,microgrid)
3	l2Discovery(microgridPLC,arp)
4	l2Discovery(mled2,arp)
5	inSubnet(mled2,microgrid)
6-7	arpPoisoning(mled2,microgridPLC)
8	feedbackFlow(mled2,microgridPLC,feedbackAction3)
9	protocol(feedbackAction3,plaintext)
10-11	canForgeSegment(feedbackAction3)
12	protocol(feedbackAction3,unauthenticated)
13-14	lossVisibility(feedbackAction3)