DEFENDER

Defending the European Energy Infrastructures

4. fit4sec-Netzwerktreffen
Berlin, 03.04.2019

Nikolaus Wirtz

Institute for Automation of Complex Power Systems

RWTH Aachen

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 740898

H2020 DEFENDER

- Rahmendaten und Überblick
- DEFENDER Design-Ziele
- Bedrohungsanalyse und Szenarien
- DEFENDER Plattform

DEFENDER Rahmendaten

- **Start:** 01.05.2017
- **Dauer**: *36 Monate (Ende: 30.04.2020)*
- **Call**: *Secure Societies, Critical Infrastructure Protection*
- **Typ**: *Innovation Action (Ziel-TRL 7-8)*
- **EU-Beitrag**: 6.790.837,50 €
- **Partner**: **18** (aus **9** Ländern)
- **Länder**: *Italien, Griechenland, Frankreich, Rumänien, Deutschland, Slowenien, Portugal, UK, Israel*
- **Website:** *http://defender-project.eu/*

ICT Service & Technology providers

- ENGINEERING SingularLogic SIEMENS (*ICT*)
- THALES (*Security*)
- POWER Venaka Media UNINOVA (SME - *Solution Provider*)
- e-lex STUDIO LEGALE (Data Privacy/Protection Enforcement))

R&D/Academy

RWTH AACHEN UNIVERSITY, JSI, ICS

Stakeholders

- ASM (*Electricity Network Operator, DSO*)
- ENGIE (*Electricity Supplier, Bulk generation*)
- BFP (*Electricity Supplier, Wind farm)*
- ELES (*Electricity Network Operator, TSO*)
- (Law Enforcement Agency)

Projektziel

DEFENDER zielt auf die Sicherung

existierender und zukünftiger europäischer CEI

in Anbetracht von cyber-physischen-sozialen Bedrohungen,

durch die Entwicklung eines Ansatzes basierend auf

einem neuartigen Konzept der Lebenszyklusanalyse, Resilienz und Selbstheilung durch **Security-by-design**, und **fortgeschrittenen Systemen zur Erkennung und Eindämmung von Zwischenfällen.**

DEFENDER Übersicht

- Risikobewertung und -analyse
  - Basierend auf der ENISA-Taxonomie für Bedrohungen
  - Identifizierung relevanter Szenarien für DEFENDER
- Risiko „by design“ reduzieren
  - Abdeckung der 4 Design-Ziele
  - Hauptsächlich konzeptuelle und Laborarbeit
- Lageerkennung und Eindämmung
  - Entwicklung einer Plattform zur Erkennung und Eindämmung von Zwischenfällen
- Validierung an Versuchsstandorten

Kern-kraftwerk

Übertragungs-netz

Wind Farm

Verteilnetz und Prosumer

DEFENDER Versuchsstandorte

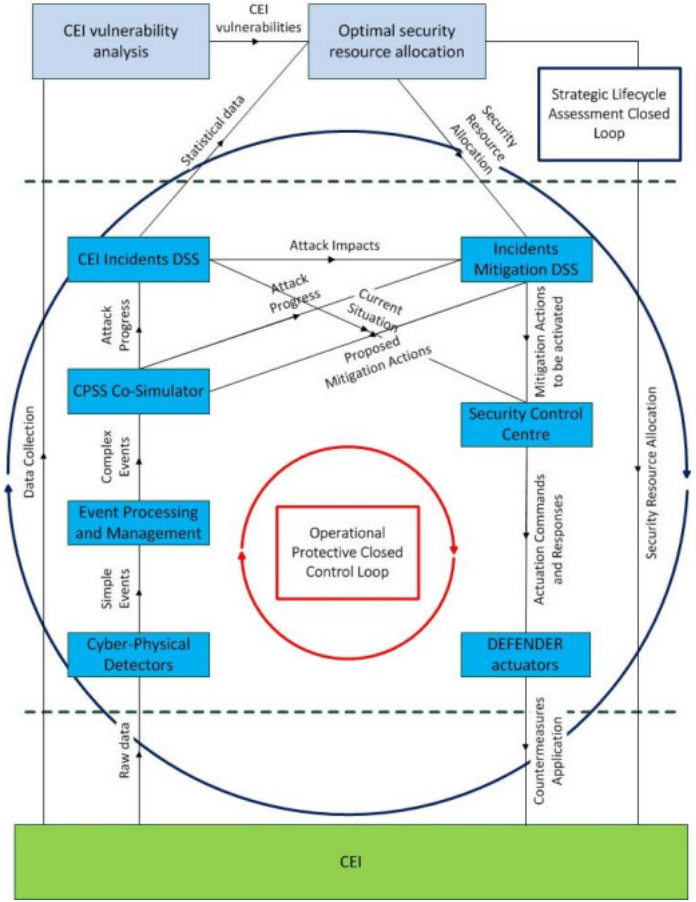
Physische Sicherheit
Cyber-Sicherheit
„Human in the Loop“

H2020 DEFENDER

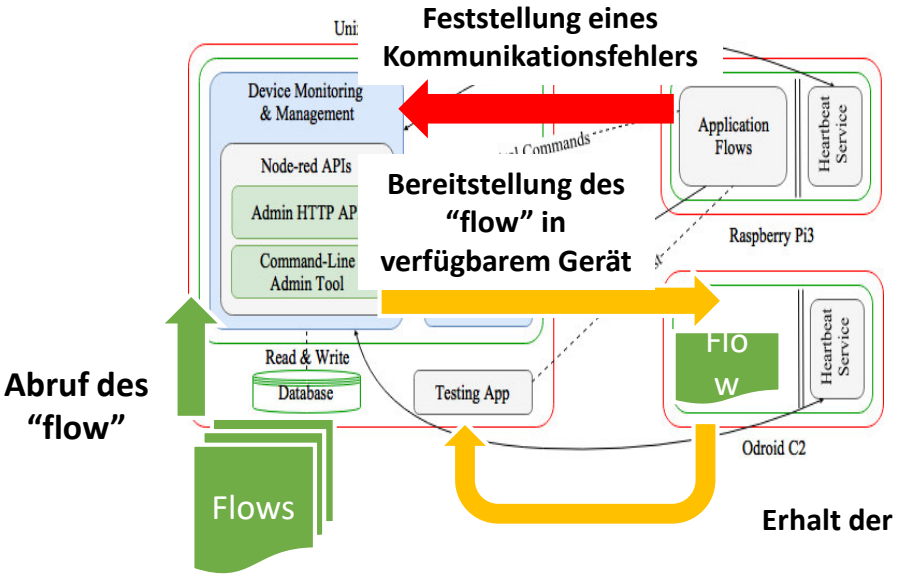
- Rahmendaten und Überblick
- DEFENDER Design-Ziele
- Bedrohungsanalyse und Szenarien
- DEFENDER Plattform

Lebenszyklusanalyse „by design”

- Zweischichtiger Ansatz zur Lebenszyklusanalyse
- Operative Schicht zur Aufrechterhaltung bzw. Wiederherstellung des anvisierten Servicelevels
  - Realisiert durch die DEFENDER Plattform und Schnittstellen zu bestehenden Systemen
- Strategische Schicht zur Langzeitüberwachung und zur effizienten Allokation knapper Sicherheitsressourcen
  - Monitoring der DEFENDER Plattform
    → Identifizierung relevanter Angriffe und wirksamer Gegenmaßnahmen
  - Schwachstellen-Analyse der Netzinfrastruktur
    → Identifizierung kritischer Komponenten



Resilienz „by design“



- „Double Virtualization” zur Virtualisierung von Funktionen und Datenbanken der Netzüberwachung und -steuerung
- Trennung der Funktionalität von einer spezifischen Hardware
- Migration der virtualisierten Komponenten
  - Optimierung der Ressourcenallokation
  - Gewährleistung der Funktionalität im Fall eines Angriffs oder Ausfalls

Selbstheilung „by design”

- Fehlerlokalisierung und –isolierung
  - Phasoren der Spannungen und Ströme aus 2 PMUs ausreichend zur Fehlerlokalisierung
  - Modellbasierter Algorithmus
  - Präzision der Lokalisierung abhängig von Kenntnis der Netzparameter und des Verbrauchs
- Netzrekonfiguration zur Wiederherstellung des anvisierten Servicelevels
  - Rekonfiguration nach Isolierung eines Fehlers
  - Optimale neue Netzkonfiguration, z.B. Maximierung der wieder versorgten Lasten
- Schwachstellen-Analyse der Netzinfrastruktur
  - Betrachtung der Strom- und Kommunikationsnetze
  - Einbeziehung von Interdependenzen

PMUs zur Fehlerlokalisierung

Datenschutz „by design”

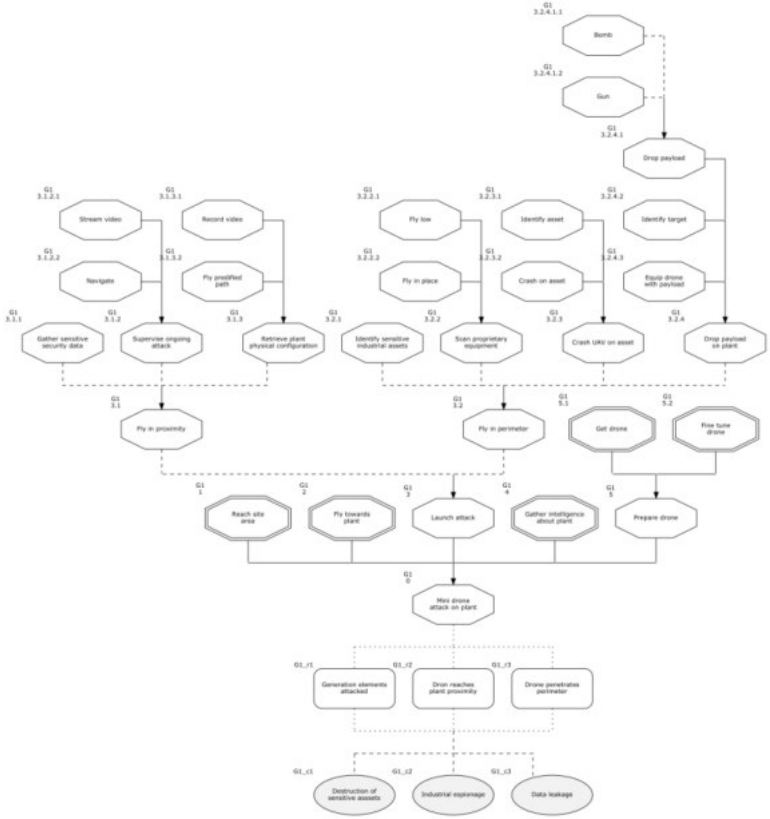
- Übersicht des **rechtlichen Rahmens in Bezug zu DEFENDER**
  - Schutz persönlicher Daten in der Durchführung des Projekts
  - Schutz persönlicher Daten im Hinblick auf die entworfenen und implementierten Systeme
- Richtlinien zur **Anwendung der GDPR-Prinzipien** im DEFENDER System-Design und der Implementierung wurden den Entwicklern bereitgestellt
- Sammlung von **Informationen über Projektdaten und die geplanten Versuche** zur Identifikation potentieller Datenschutz-Probleme
- Einführung von Richtlinien und Empfehlungen
  - Praktische Empfehlungen für den Umgang mit persönlichen Daten
  - Empfehlungen für den Umgang mit Datenschutzverletzungen

H2020 DEFENDER

- Rahmendaten und Überblick
- DEFENDER Design-Ziele
- Bedrohungsanalyse und Szenarien
- DEFENDER Plattform

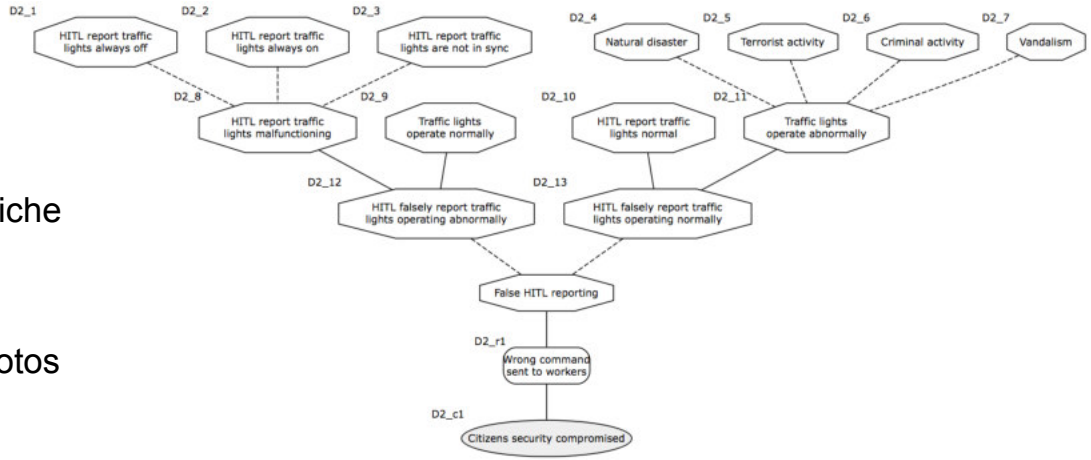
Bedrohungsszenarien

- Angriffsbäume zur Beschreibung der Bedrohungsszenarien
  - Pfade in den Bäumen zeigen mögliche Angriffssequenzen zur Durchführung eines erfolgreichen Angriffs
- Kombinierung von Schwachstellen von Systemen aus verschiedenen Domänen
  - Beinhaltet komplexe, Multi-Domänen-Angriffspfade
- Zeigt mögliche Resultate eines erfolgreichen Angriffs
  - Z.B. verletzte Personen, finanzieller oder Reputationsschaden
- Gegenmaßnahmen können als Mittel gegen bestimmte Angriffe integriert werden
  - Blocken entsprechender Pfade in den Angriffsbäumen



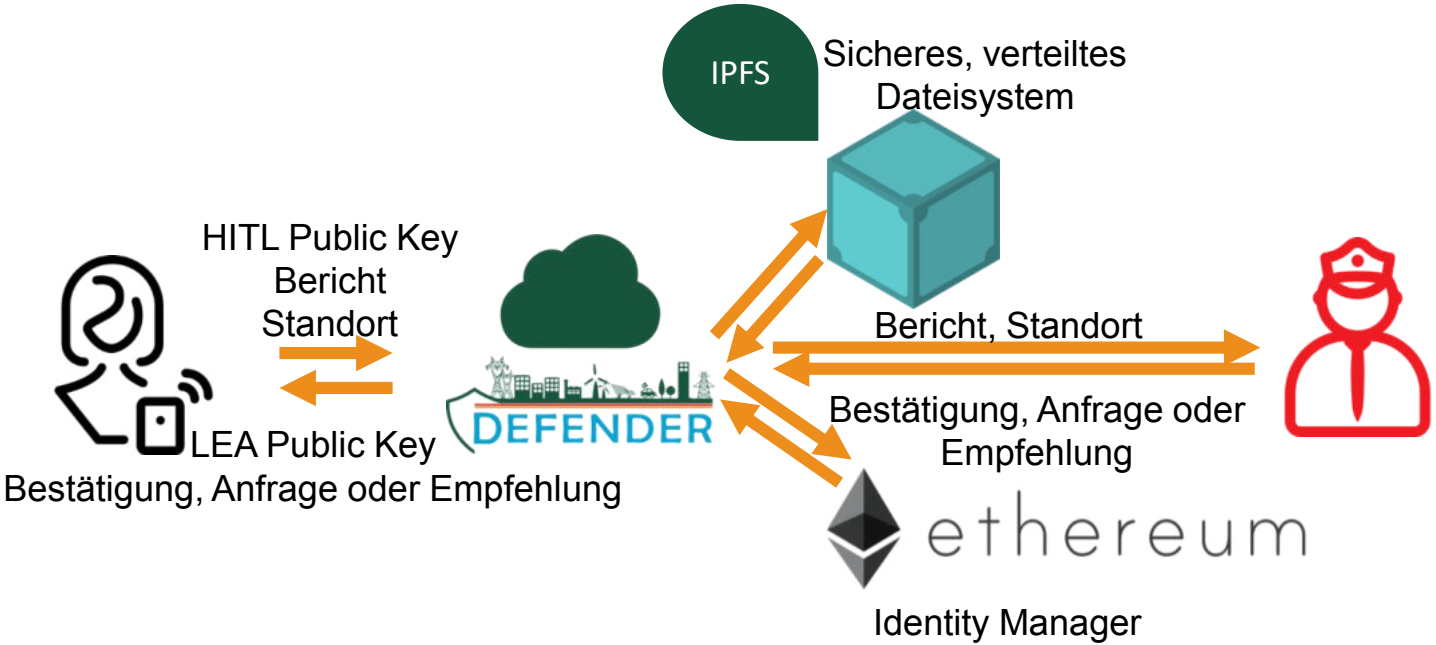
„Human in the Loop” Evaluierungsszenario

- Human in the Loop (HITL)
  - Vertrauenswürdige Freiwillige als “menschliche Sensoren”
  - Mobile App zum Teilen von Informationen
  - Verwendet strukturierten und freien Text, Fotos und Videos



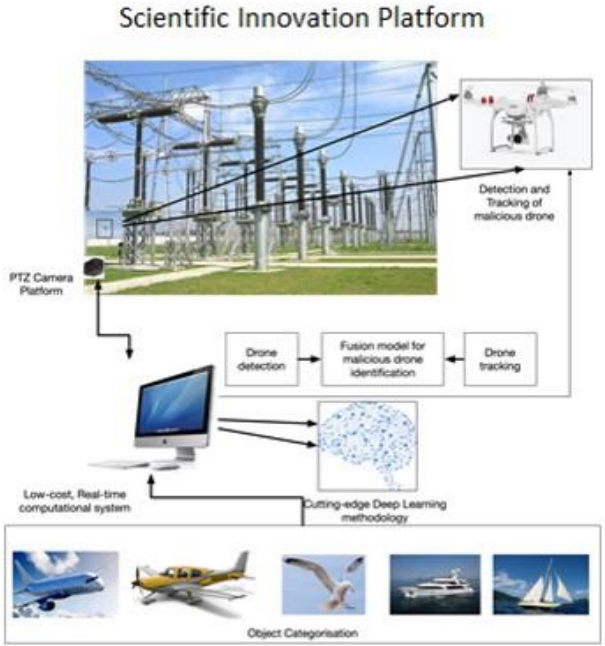
1. HITL-Nutzer A benachrichtigt den CEI-Betreiber, dass Ampeln nicht funktionieren
2. Der CEI-Betreiber prüft die Nachricht und fordert eine Bestätigung von allen Freiwilligen im entsprechenden Gebiet an
3. Ein bösartiger HITL-Nutzer B sendet eine Nachricht und behauptet dass alles Ampeln funktionieren
4. HITL-Nutzer A schickt ein Beweisfoto zum Status der Ampeln
5. Der CEI-Betreiber kann daraufhin Nutzer B von der Plattform bannen

„Human in the Loop”
Architektur und Informationsfluss



Drohnenbasierte Angriffsszenarien

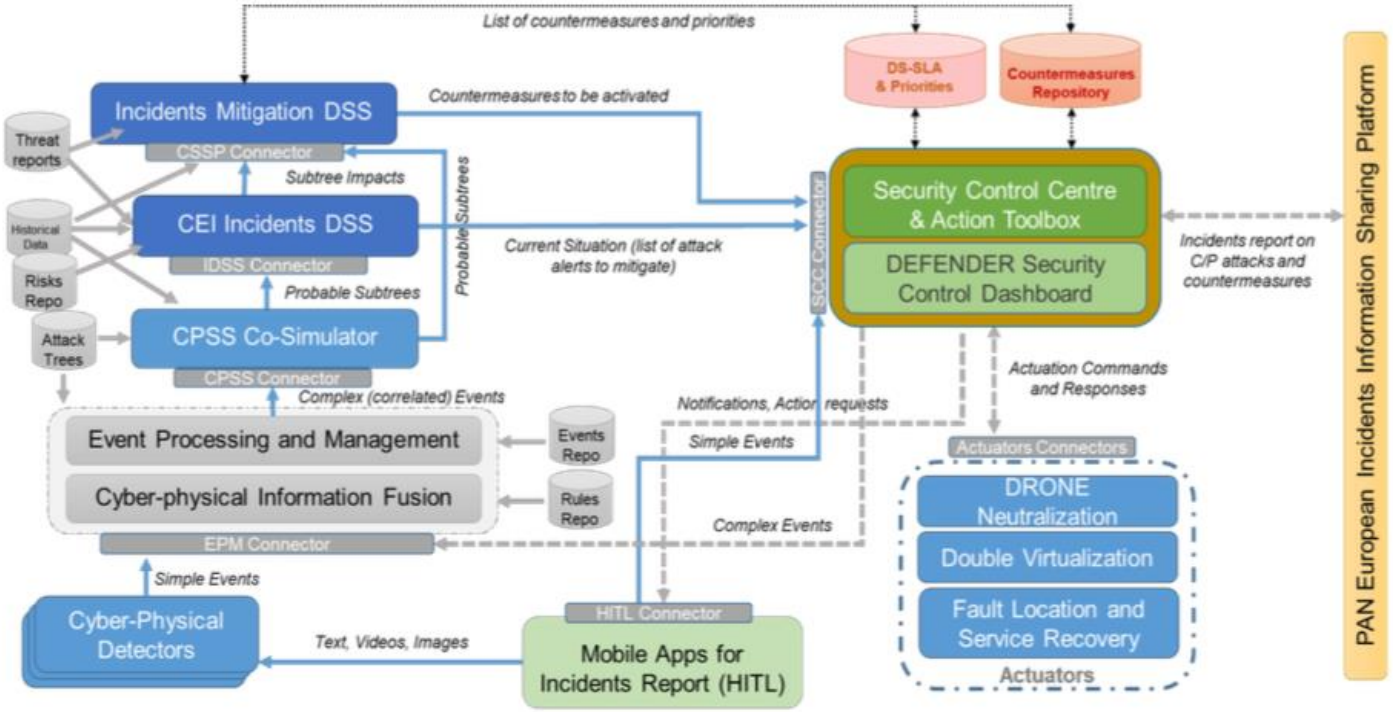
- Eindringen einer Drohne in den Bereich der kritischen Infrastruktur
- Überwachung des Luftraums mit Kameras, Drohne wird getrackt, sobald sie erkannt wurde
  - Kameras können schwenken, neigen und zoomen um die Drohne zu tracken
- Aus der Trajektorie der Drohne werden in Echtzeit Orientierung und Richtung des Angriffs bestimmt
- Die Ergebnisse werden zur DEFENDER Plattform exportiert und dort weiterverarbeitet



H2020 DEFENDER

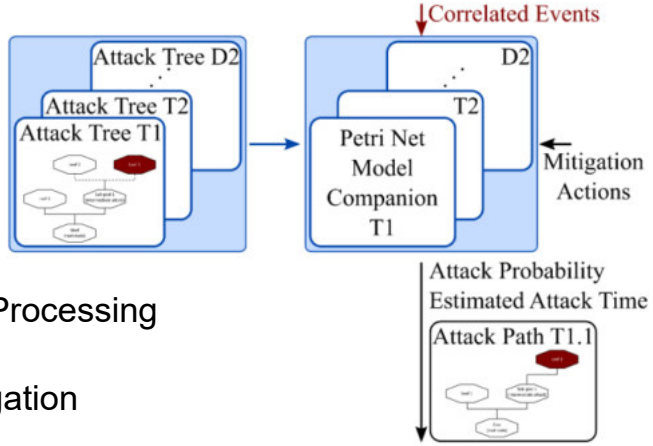
- Rahmendaten und Überblick
- DEFENDER Design-Ziele
- Bedrohungsanalyse und Szenarien
- DEFENDER Plattform

DEFENDER Architektur

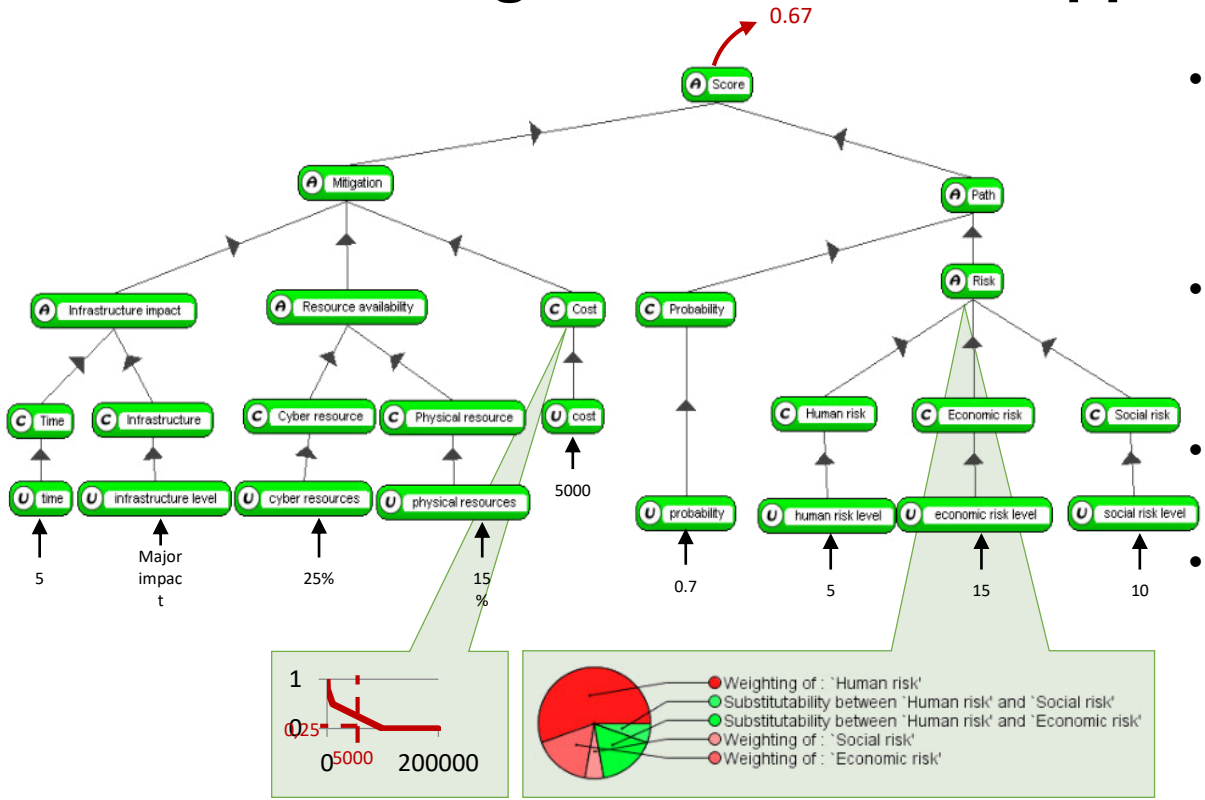


CEI Modellierung & CPSS Co-Simulator

- **CEI Modellierung**
  - Angriffsbäume der Bedrohungsszenarien
  - Petri-Netz Modelle, basierend auf den (erweiterten) Angriffsbäumen
- **Cyber-Physical-Social System (CPSS) Co-simulator**
  - **Input**
    - **Zustand der Umgebung**: korrelierte Ereignisse vom Modul “Event Processing and Management”
    - **Gegenmaßnahmen:** vorgeschlagen durch das Modul “Incident Mitigation Decision Support System”
  - **Simulation**: probalisitische Analyse des Angriffsfortschritts im Zeitbereich
  - **Output**:
    - **“Situation Perception”**: Knoten im Angriffsbaum mit assoziierten Wahrscheinlichkeiten und der geschätzten “time-to-attack”
    - **“Future Situation Projection”**: Vorhersage zur Effektivität ausgewählter Gegenmaßnahmen in Bezug auf Angriffswahrscheinlichkeit und “time-to-attack”



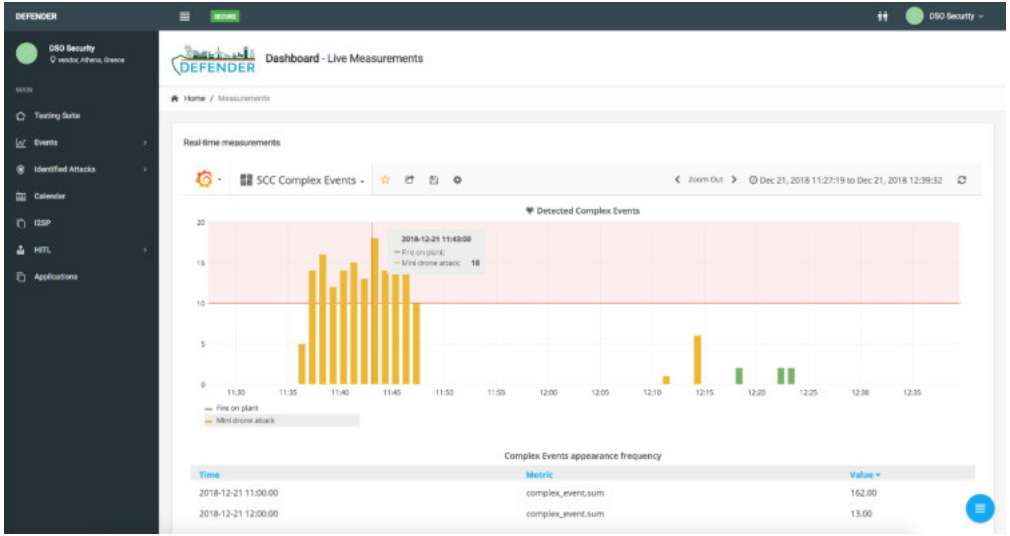
Incident Mitigation Decision Support System



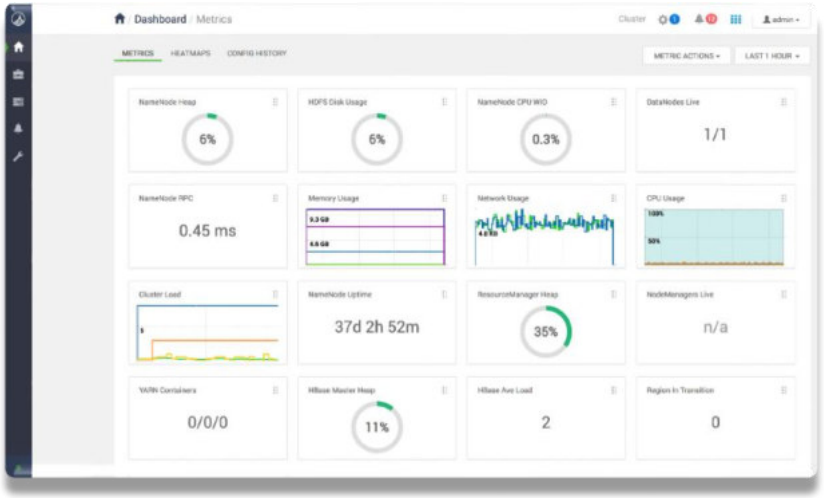
- Evaluierung der im Entscheidungsbaum dargestellten Gegenmaßnahme basierend auf Gegenmaßnahmen- und Angriffspfad-Kriterien
- Ergebnisse für Gegenmaßnahme und entsprechende Angriffsbäume wird dem „Incident Mitigation DSS“ bereitgestellt
- Berechnung eines Nutzenwerts für jedes Kriterium
- Die Wurzel des Baums korrespondiert mit dem Gesamt-Score der Gegenmaßnahme

CEI Security Control Centre

- Ermöglicht den Überblick des Sicherheitsstatus im Betrieb und die Aktivierung von Gegenmaßnahme im Angriffsfall
- Alarme und Karten zum Echtzeit-Monitoring von Ereignissen
- Ansicht historischer Daten zu Ereignissen und Angriffen



„Pan-European CEI Incidents Sharing Centre”



MISP
Threat Sharing

MISP - Open Source Threat Intelligence Platform &
Open Standards For Threat Information Sharing

- Ermöglicht den kontrollierten Austausch von Informationen zwischen CEI-Betreibern
- Nutzt das MISP-Projekt als Grundlage
  - Open-Source
  - Co-finanziert durch die EU
  - Unterstützt diverse Taxonomien
  - NATO-konform

Vielen Dank

Fragen?

M.Sc. Nikolaus Wirtz
Research Associate

T +49 241 80-49580
NWirtz@eonerc.rwth-aachen.de

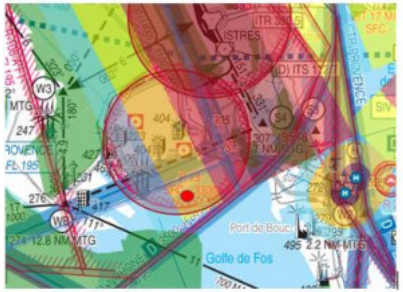
RWTH Aachen University
E.ON Energy Research Center
Institute for Automation of Complex Power Systems

www.eonerc.rwth-aachen.de

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 740898

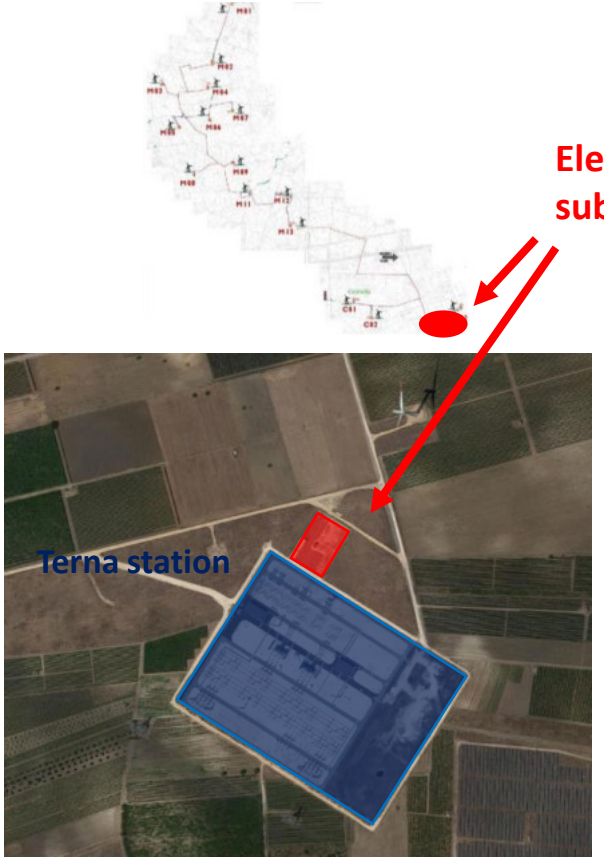
Bulk Energy Generation Trial

- **Pilot site:** Combigolfe plant at Fos-sur-Mer, France
- **Main focus:**
  - Human malicious attack via drone fleet
  - Drone fleet neutralization
- **Plant specifications :**
  - 424 MW NG power plant for electricity production
  - Located in Prohibited airspace → flight protocol with French Air Force
  - 22 fixed camera all around fences for intrusion detection, manned surveillance patrol
- **Threats scenario :**
  - R1 : Mini-drone attack & neutralization
  - R2 : Physical attack to gain network access
- **Surveillance proposal**
  - Autonomous drone coupled to GENETEC
  - Surveillance tour + doubt removal



Decentralized RES generation

- **Pilot site:** Erchie wind farm, Italy
- **Main focus:**
  - Infrastructure aging (structural collapse of wind tower) or natural hazard
  - Security gap between RES generator and DSO
- **Four threat scenarios:**
  - R1: Unauthorized access to the electrical substation
  - R2: Unauthorized access to the wind turbines
  - R3: Drone attack
  - R6: Stop time reduction
- **Implementation** in progress



TSO Network Trial

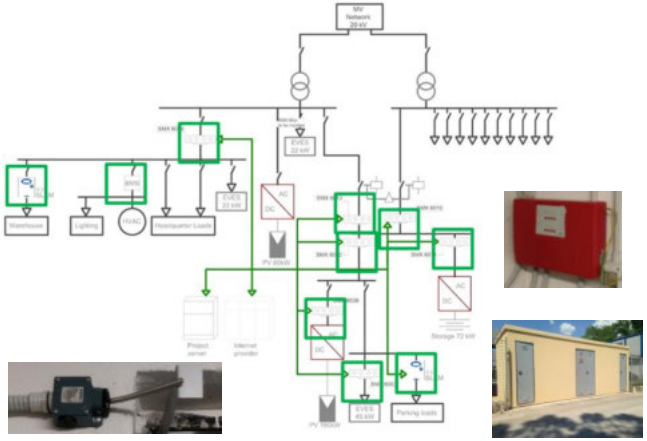
- **Pilot site:** Okroglo switching station, Slovenia
- **Main focus:**
  - Fault isolation and restore
  - Lack of coordination among different security platforms
  - Swarm of camera equipped drones for lifecycle assets management
- **Three threat scenarios:**
  - T1: Power line fault isolation and restore based on optical and communication network observations
  - T2: Lack of coordination between different access control systems, physical access control and SCADA network access control
  - T3: Implant monitoring and control element in the system, SCADA network centre
- **Additional effort:**
  - organisational improvements (all scenarios)
  - swarm of drones evaluation for preventive maintenance (T1 scenario)
- **Implementation** T1 & T2 and additions in progress

➢ The substation
- Two 400 kv and 110 kv transformers
- Two-story station consists of:building including a ICT control room
- SCADA control room and offices
- Secondary and backup powers systems
- Warehouse
- Switch yard

➢ The substation extends on 34.323,56m2

DSO Network & Prosumer Trial at Terni

D1 – a) Cyber-Physical

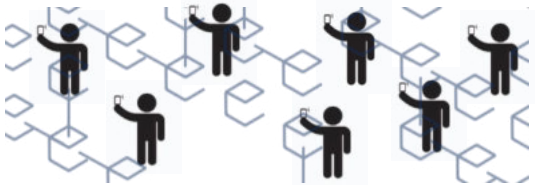


D1 – b) Fault localization and Power flow rerouting

PMU-based algorithm for fault localization

DEFENDER

D2 - HITL



- **Main focus:**
  - Physical threat to network assets
  - Security gap between DSO and RES
- **Implementation** in progress