Cyber and physical security in Critical Energy Infrastructures

Nikolaus Wirtz, M. Sc.

ACS | Automation of Complex Power Systems

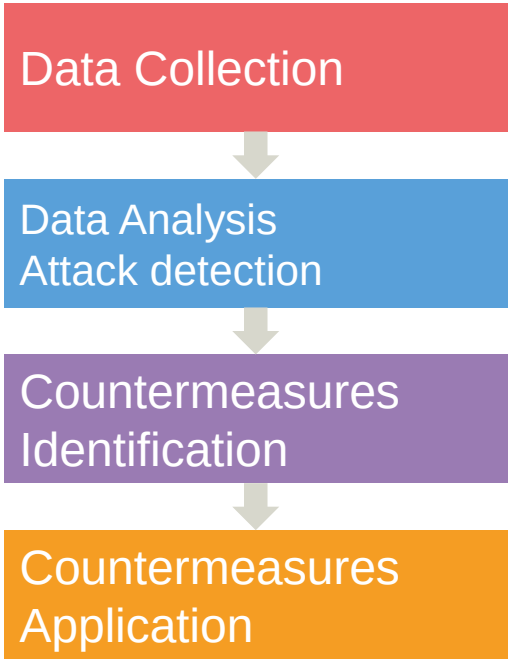
E.ON Energy Research Center

RWTH AACHEN UNIVERSITY

Cyber and physical security in SUCCESS and DEFENDER

Project	SUCCESS	DEFENDER
Research framework	H2020	H2020
Scope	Development of an overarching approach to threat and countermeasures analysis, focusing on vulnerabilities introduced by Smart Meters	Adaption, integration and validation of different technologies and operational blueprints to develop a new approach to safeguard existing and future European CEI operation over cyber-physical-social threats
Duration	05/2016-10/2018 30 months	05/2017-04/2020 36 months
Consortium	16 partners 9 countries	18 partners 9 countries
Further information	https://success-energy.eu/	http://defender-project.eu/

- Increase in number and sophistication of cyber security attacks
- Need to better secure the (currently insufficiently protected) smart CIs
- Preparation: identify security threats, design countermeasures
- Act: collect data, analyse data, detect attacks, apply countermeasures



ICT in Critical Infrastructures
Target of Cyber Attacks

IT

Level 4
Business Logistics Systems
Customer Information Systems
Billing Systems

DMZ, Firewall

Level 3
Operations Systems
Distributed Management System
Network Information System

DMZ, Firewall

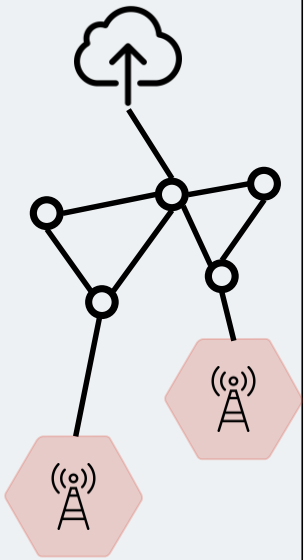
OT

Level 2 Supervisory Control Systems
SCADA
HMI
Data Collection
Energy Management System

Level 1
Intelligent Devices
Meter
Sensors
Controllers
Actuators

Level 0
Physical Process

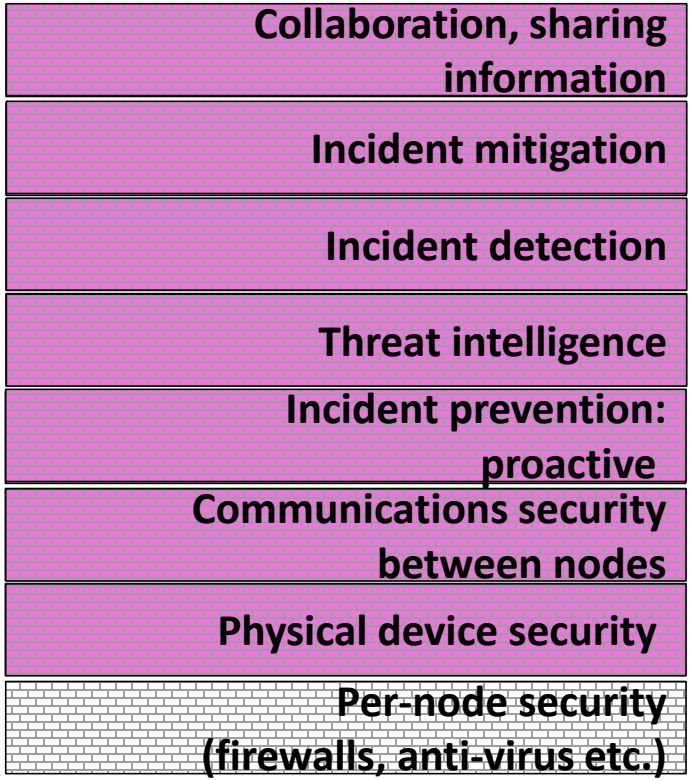
Cross-Cutting:
Communications Systems

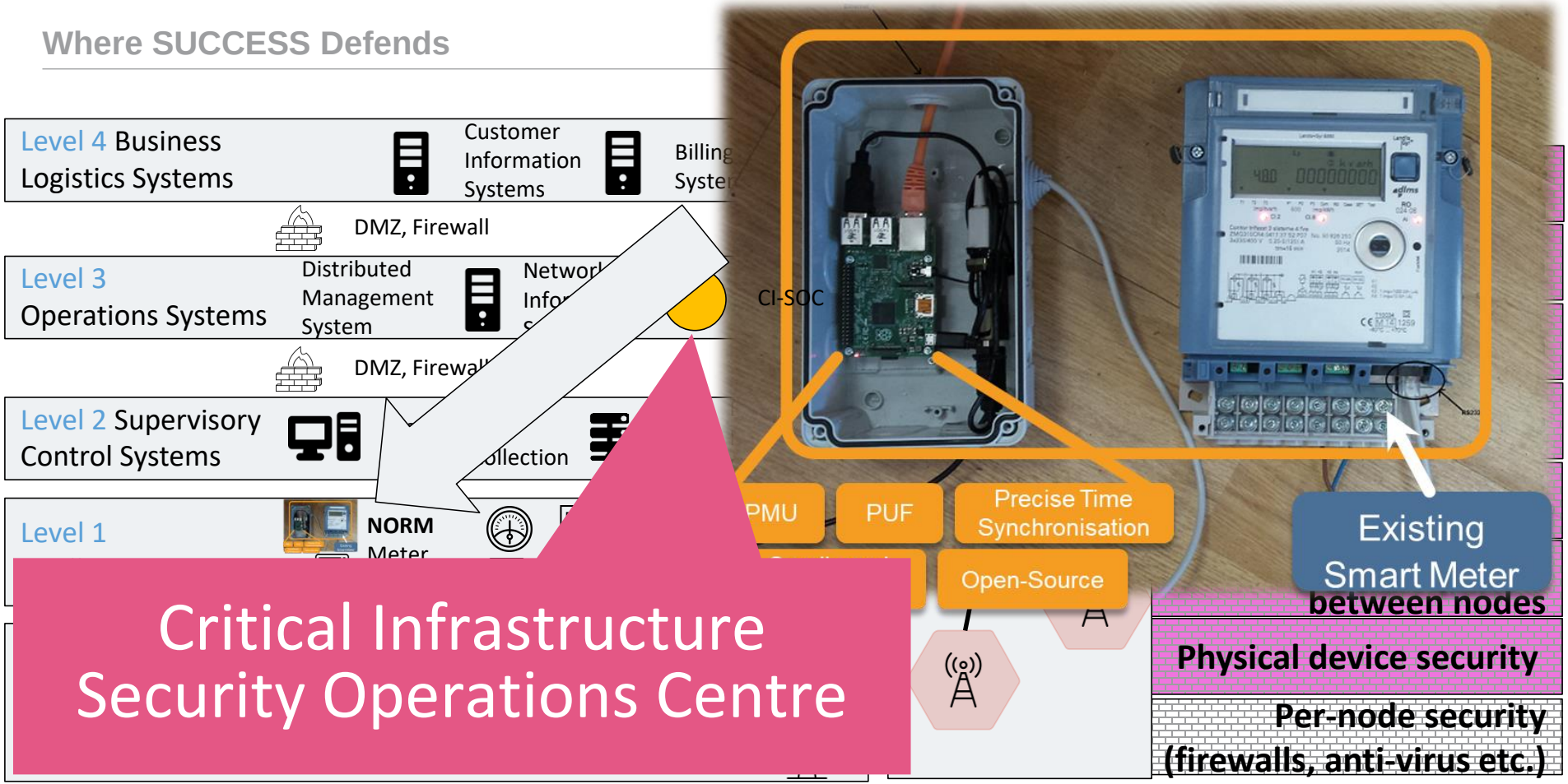


How Can We Defend Against Attacks?

- Can't hack back, limited to defence
- Security is intrinsic to system, architecture, protocols, must be executed according to scrutinised processes and operating procedures
- Need protection at each of the attack stages and in all system parts

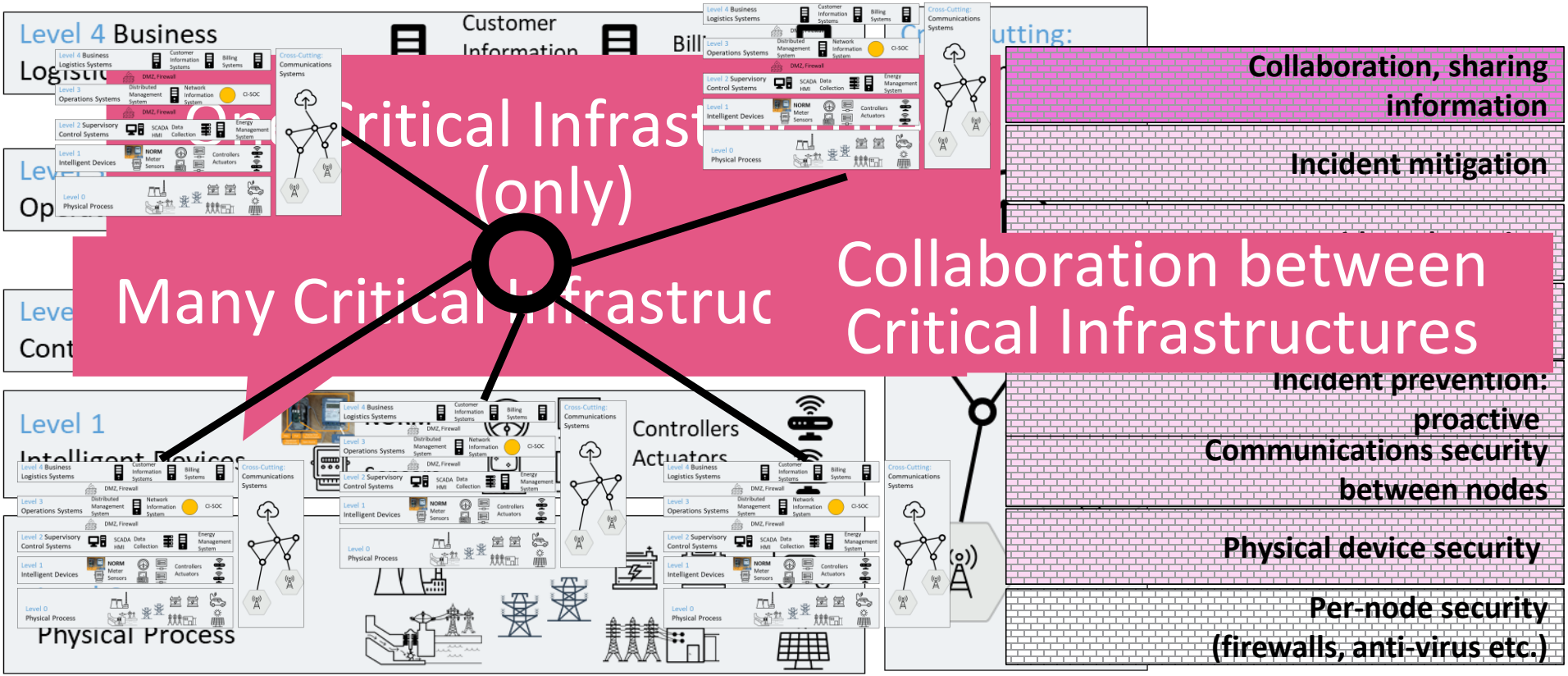
SUCCESS focus





Critical Infrastructure Security Operations Centre

Where SUCCESS Defends



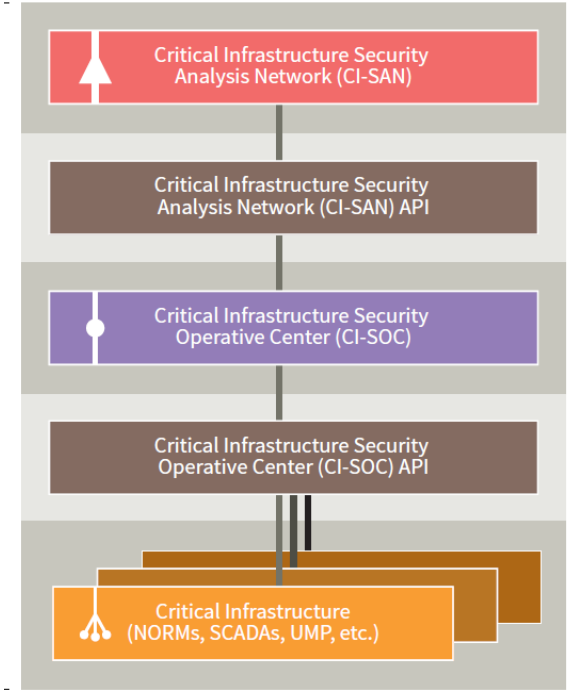
E.ON Energy Research Center | RWTH AACHEN UNIVERSITY

SUCCESS Security Solution

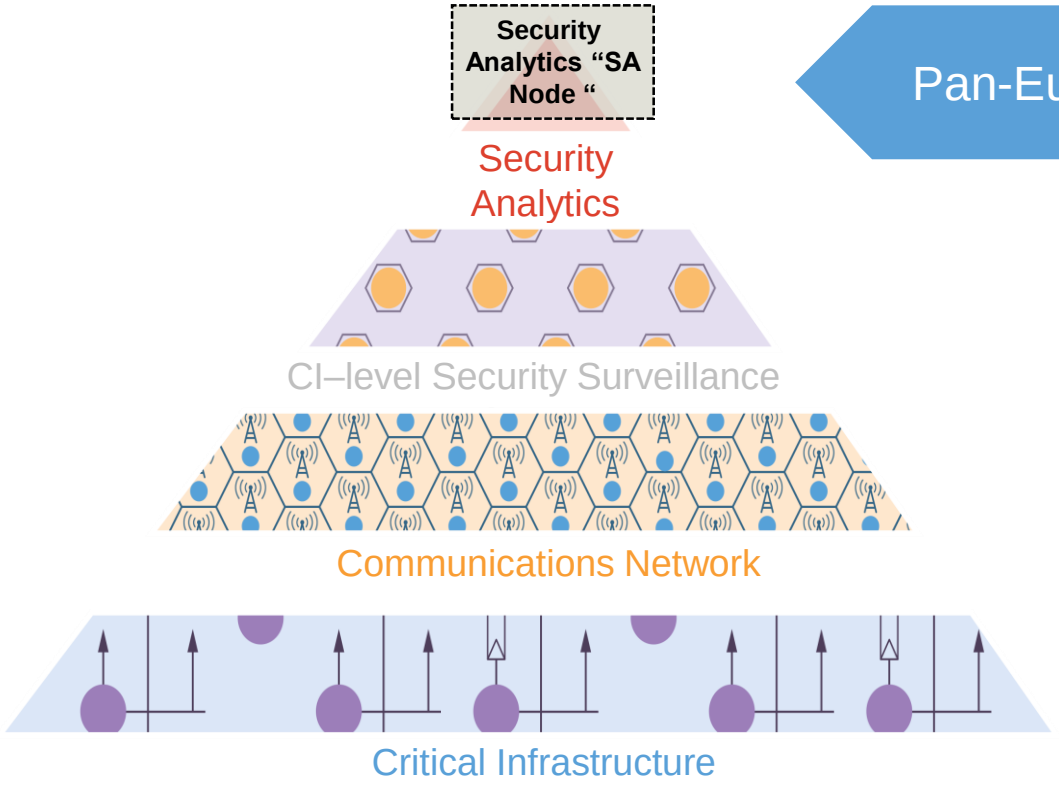
- Security framework tries to significantly reduce risks of cyber threats and attacks to CIs
  - Implementation focus on set of relevant use cases
  - Both for individual CIs and for wide areas by information sharing
- Emphasis on electrical infrastructure, fundamental for all CIs
  - Enhanced security features, techniques and components, in particular Smart Metering
  - Project field trials detects and mitigate set of cyber-attacks.

- Holistic approach to CI security
- Hierarchical structure, spanning from single CI to national and pan-European security monitoring centres
- Include security of communication channels for data integrity and privacy protection

TRiPLE S

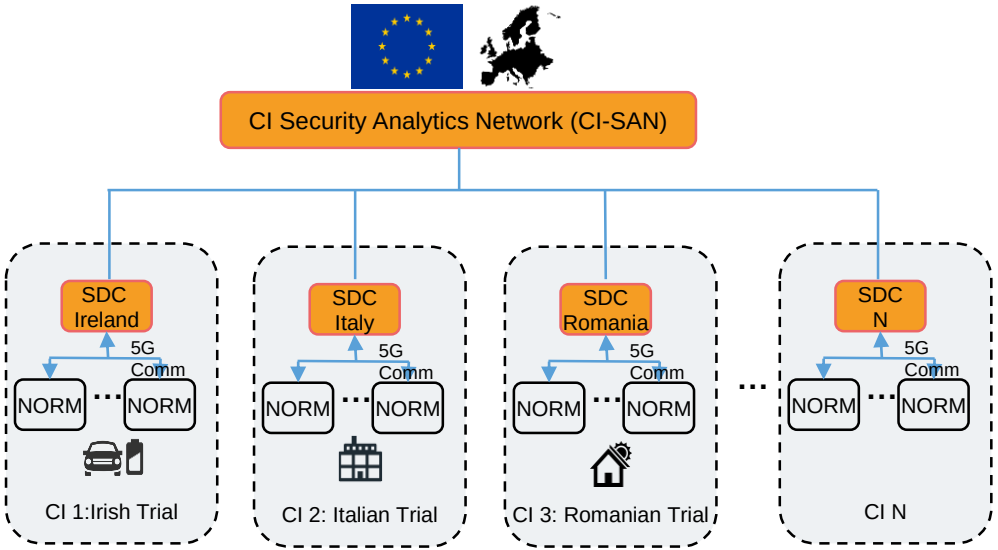


SUCCESS Security Solution



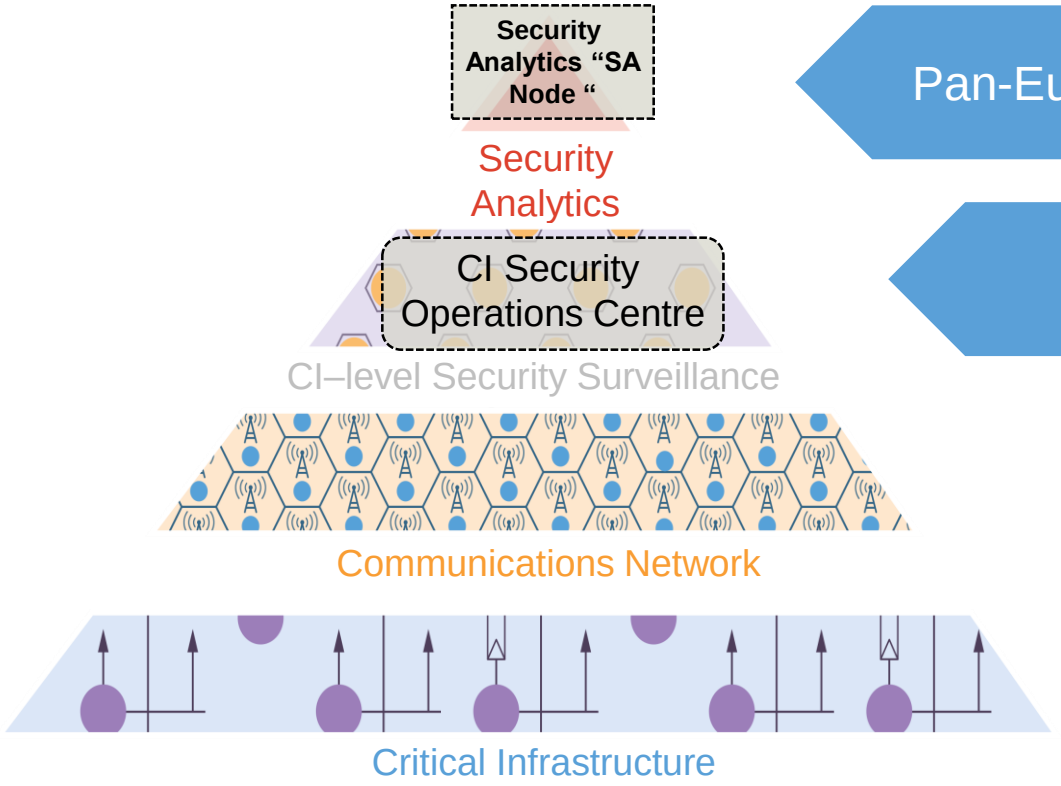
Pan-European Security Analytics Network

CI-SAN



- Security Analysis Node (SA-Node):
  - identifies threats in almost real-time and at the European level
  - informs all appropriate SDC instances about identified threats
  - suggests appropriate countermeasures
- Security Data Concentrators (SDC):
  - send aggregated and anonymized data to SA-Node
  - receive superior threat patterns from SA-Node

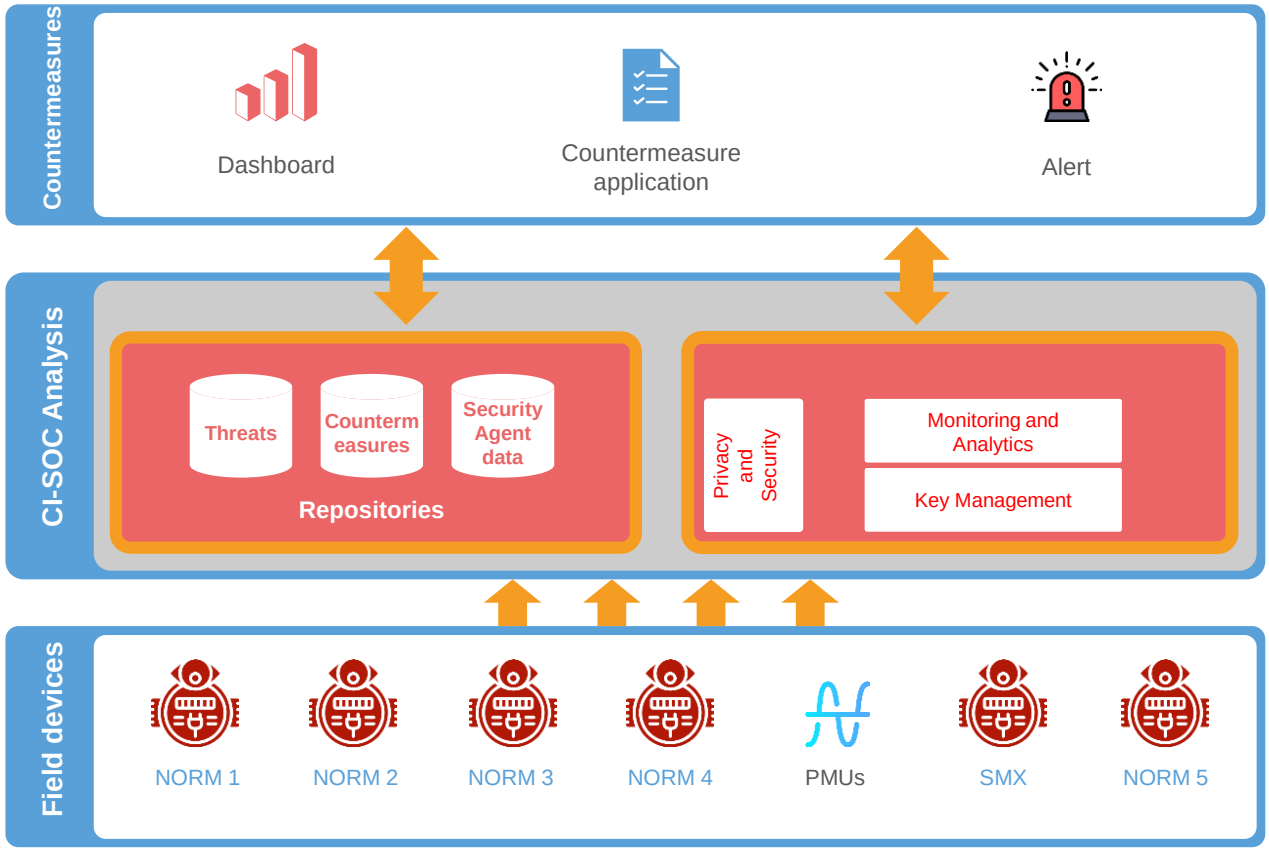
SUCCESS Security Solution



Pan-European Security Analytics Network

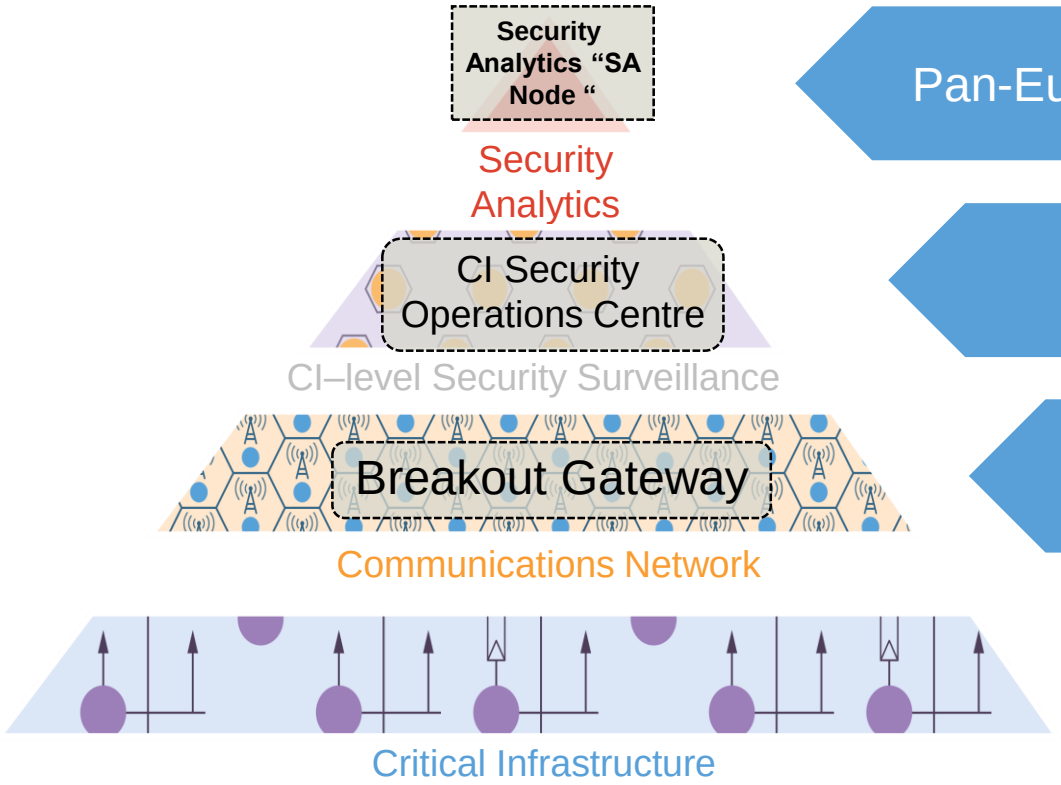
Security Monitoring, Analytics, Countermeasure Suggestions

Threat detection and countermeasures



- Collect data from field devices and run real-time incident detection
- Identify threats and corresponding countermeasures
- Apply countermeasures with automatic, semi-automatic or manual procedures

SUCCESS Security Solution

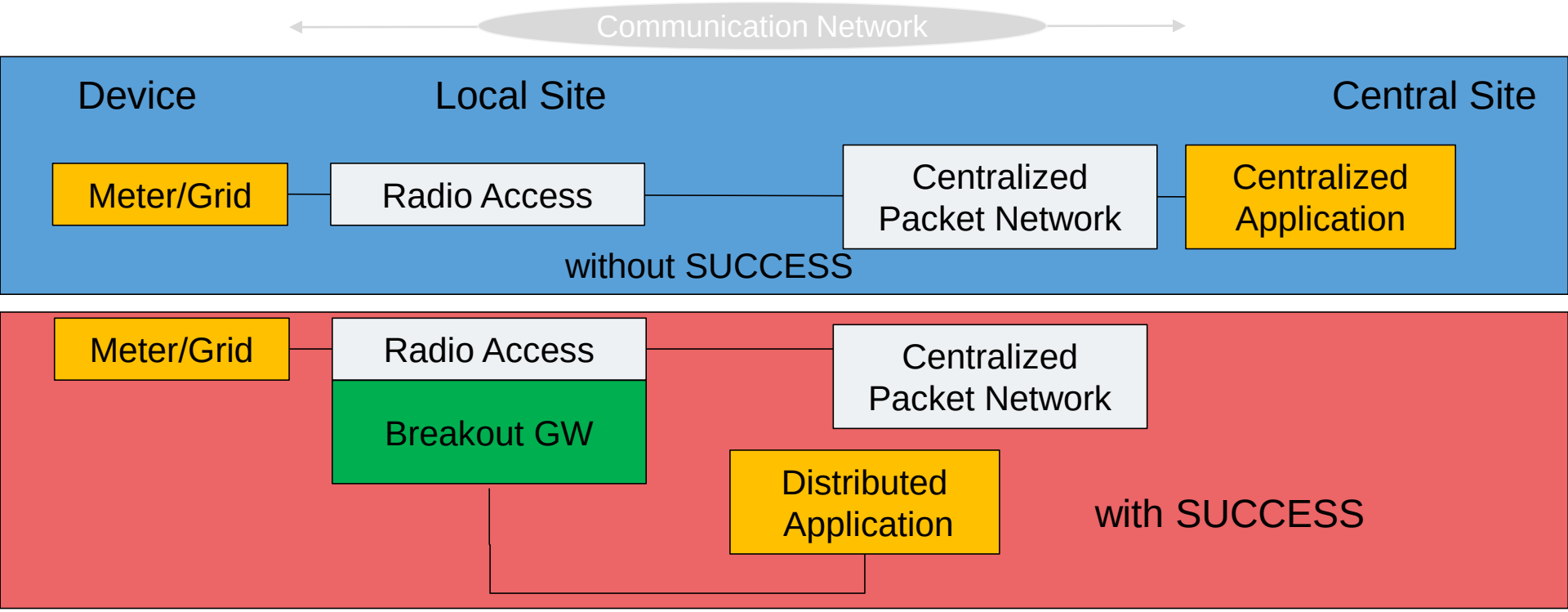


Pan-European Security Analytics Network

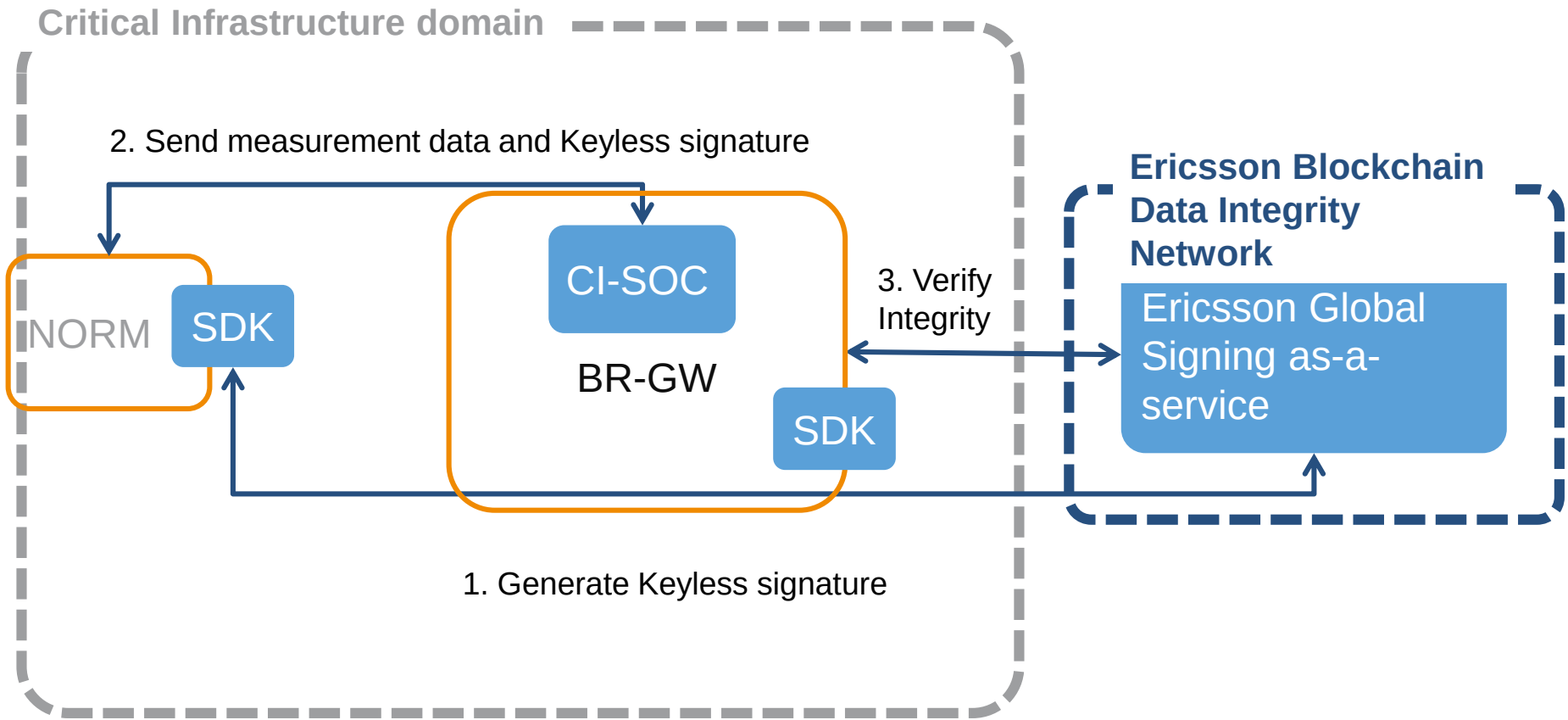
Security Monitoring, Analytics, Countermeasure Suggestions

Mobile edge computing with data tampering detection

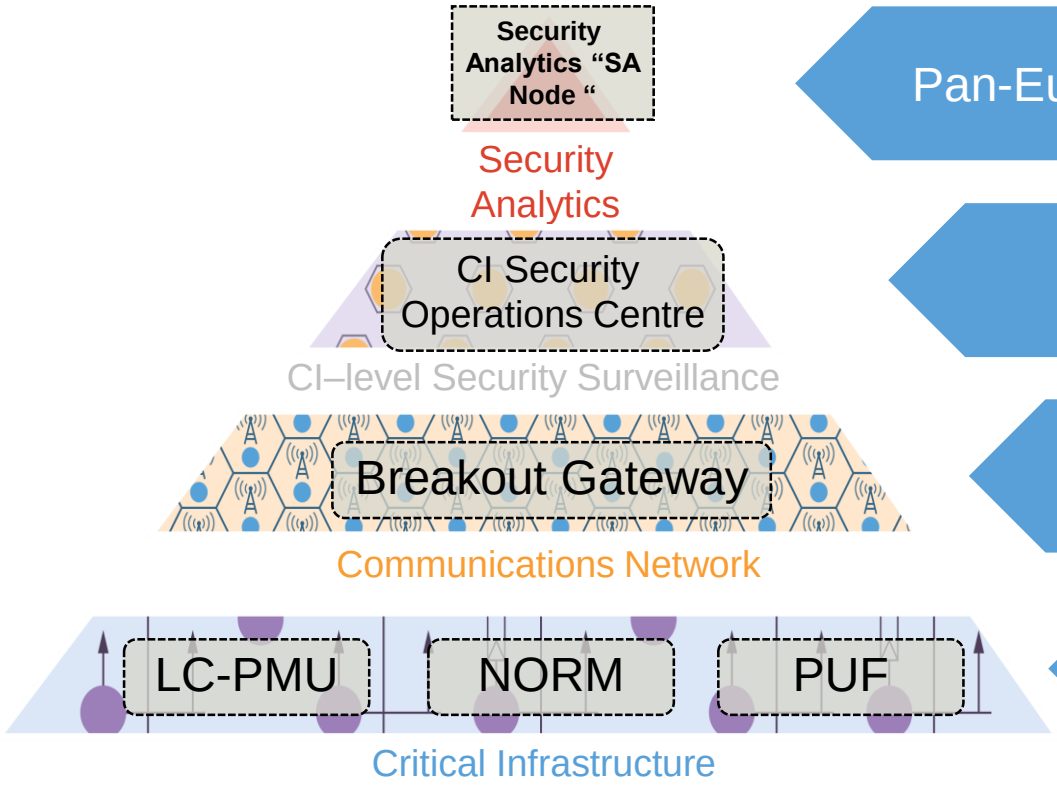
Breakout Gateway concept



Integration with SUCCESS Security Solution



SUCCESS Security Solution



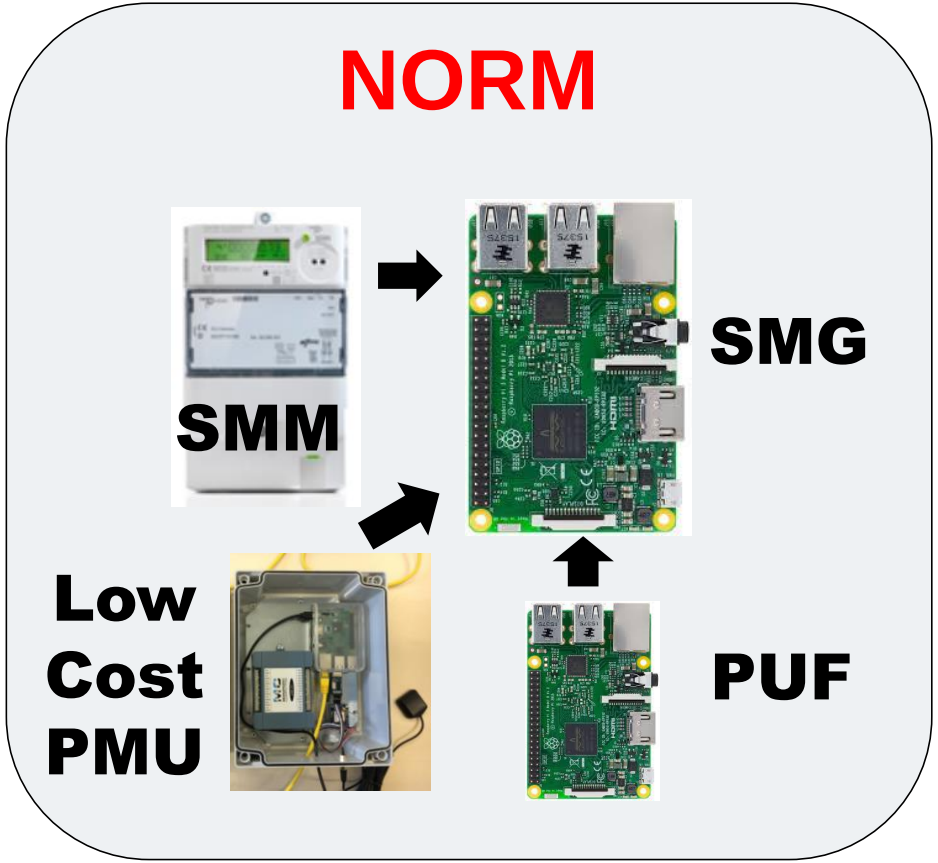
Pan-European Security Analytics Network

Security Monitoring, Analytics, Countermeasure Suggestions

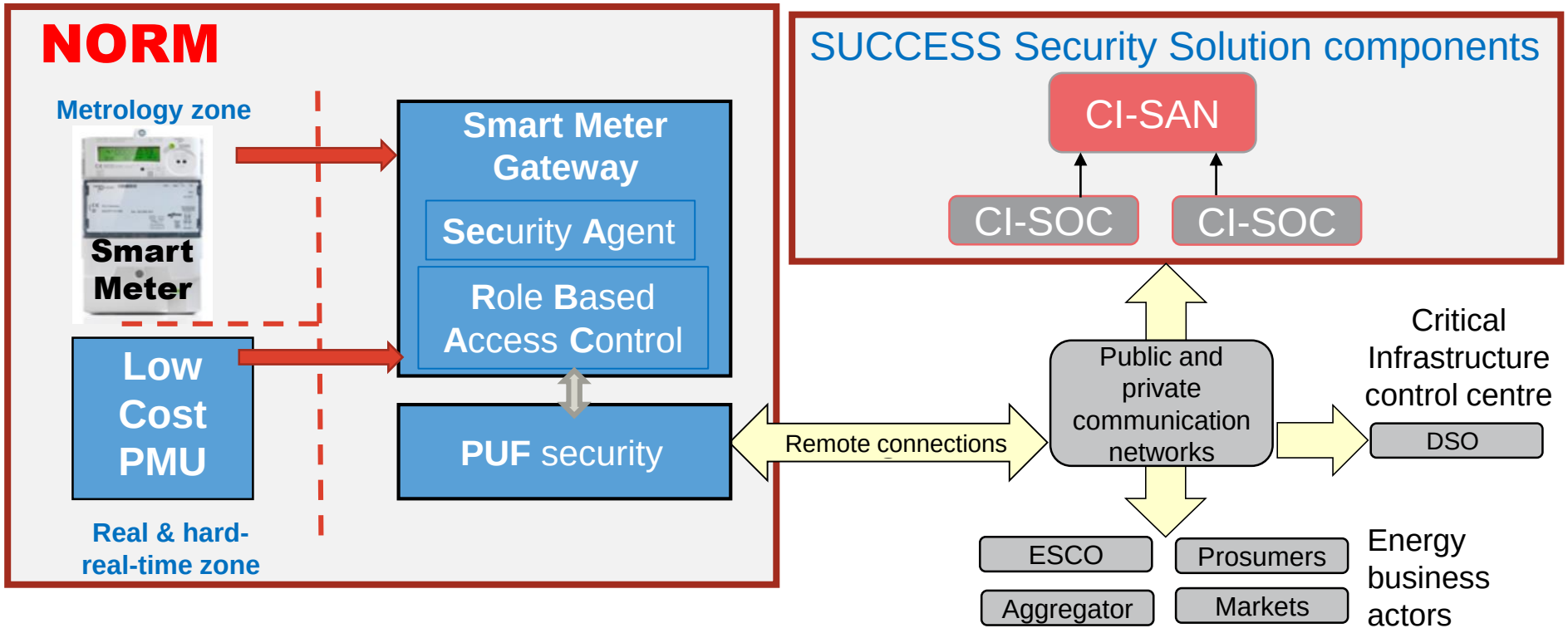
mobile edge computing with data tampering detection

NORM with enhanced security functions

- Key features
  - Enable new services in **Active distribution networks**
  - Implement SUCCESS Security Solutions
  - Data integrity check
  - Detecting tampering at device level
  - High level encryption
  - Unbundled meter concept



- Benefits: Increase Smart Grid cyber-security while preserving privacy



- **Data security assessment** on each level, using **real-time measurements**

- Checking consistency at each grid level (using redundancies):

Redundancy at NORM level:
- Frequency from meter (each 1 second)
- Frequency from PMU (each 1 second)

Redundancy at local grid level:
- Grid frequency from NORM_1
- ……
- Grid frequency from NORM_n

Redundancy at national and Pan-European level:
- Frequencies from regional/national grid 1
- ……
- Frequencies from regional/national grid n

DEFENDER scope

- „Defending the European Energy Infrastructures“
  - Focus on Critical Energy Infrastructure (CEI) Protection
  - Including the cyber, physical and social/human domain
  - Considering interdependencies and cascading effects

- Leveraging on SUCCESS results
  - CEI as cyber-physical-social systems (CPSS)
  - Utilization of cross-domain sensors and countermeasueres (HITL, drones), including existing infrastructure
    - = Interoperability provided by event layer & Complex Event Processing
  - Extension of situation awareness and incident detection components

DEFENDER structure and focus

- Risk assessment and analysis
  - Based on ENISA Threat Taxonomy
  - Identification of relevant threat scenarios in DEFENDER
- Reducing risk by design
  - Covering 4 CEI design objectives
  - Laboratory testing and concept work
- Situation Awareness and Incidents Mitigation
  - Development of a framework to provide situation awareness, and detect and mitigate incidents
- Validation in trials

Nuclear Power Plant

Transmission Network

Wind Farms

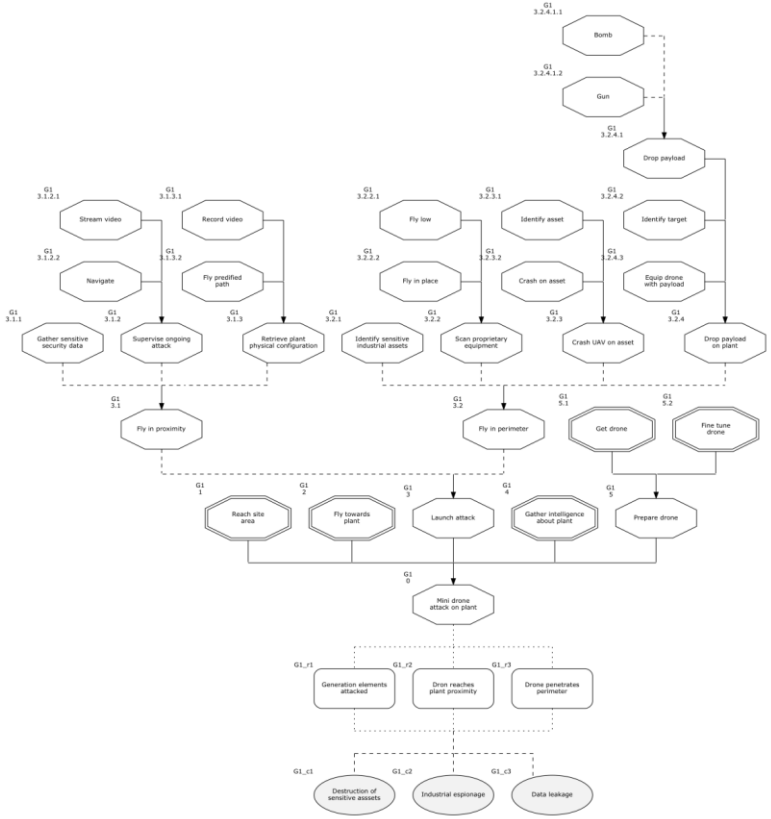
Distribution and Prosumer

Physical Protection
Cyber Protection
Human in the Loop

DEFENDER trial sites

DEFENDER threat scenarios

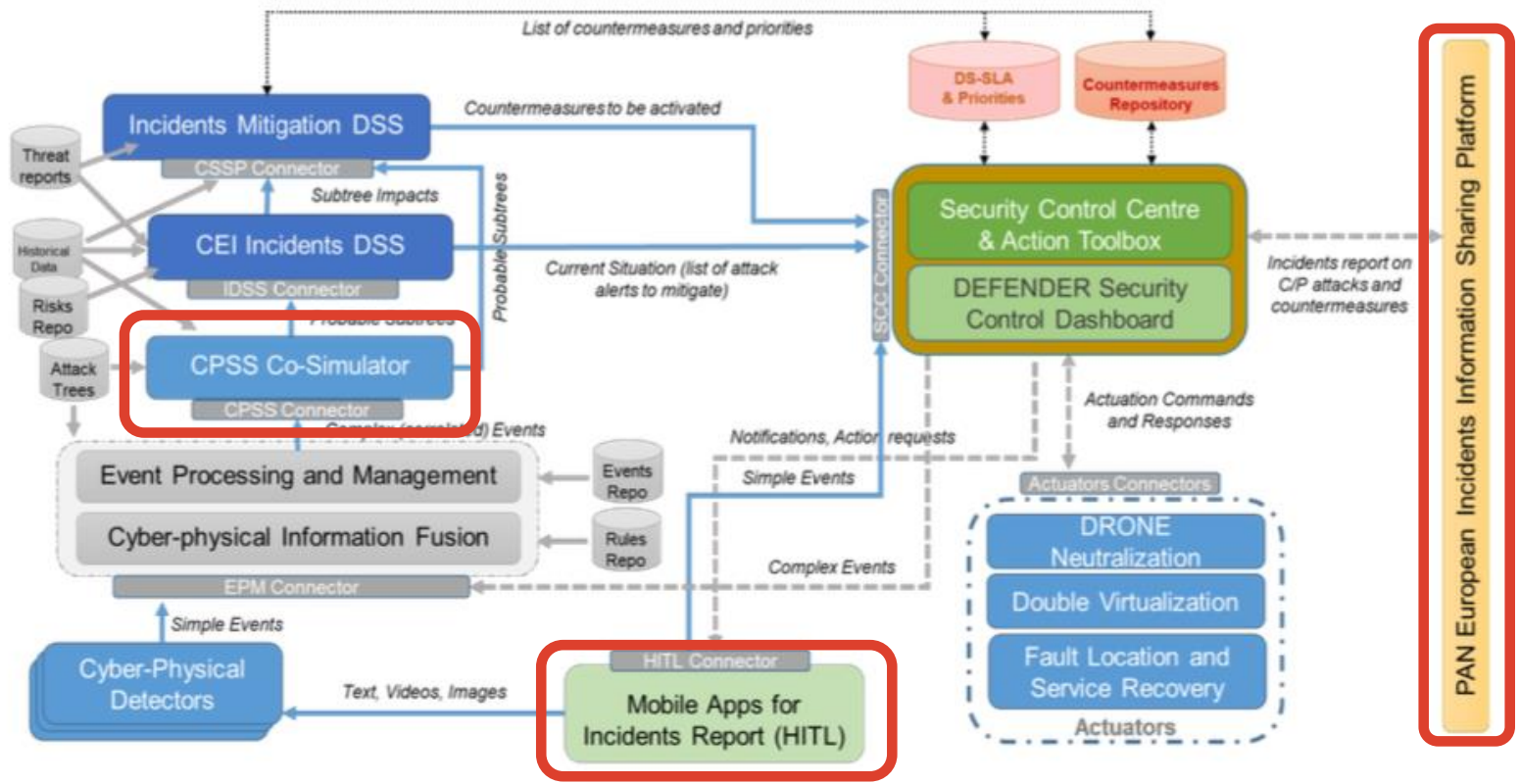
- Attack trees to describe threat scenarios
  - Paths in the tree show possible attack sequences to perform a successful attack
- Combining vulnerabilities from different domains
  - To include complex, multi-domain attack paths
- Showing possible results of a successful attack
  - Can include harmed persons, financial damage, reputation damage, …
- Countermeasures can be included as mitigation to certain (intermediate) attacks
  - Blocking certain paths in the attack tree



DEFENDER design objectives

- Security Lifecycle Assessment by design
  - 2-layer approach to security lifecycle assessment
  - Operational layer for maintaining or restoring the targeted service level
  - Strategic layer for long-term evaluation and efficient security resource allocation
- Resilience by design
  - Use of Double Virtualization to virtualize grid control and monitoring functions and databases
  - Separating functionality from specific hardware
  - Enabling migration of virtualized components for optimized resource allocation and in case of attacks or faults
- Self-healing by design
  - Acknowledge that incidents may always happen
  - Implementation of fault detection and localization algorithms to support countermeasures deployment
  - PMU deployment in power grids to enhance system observability and provide increased control functionality
  - Power grid reconfiguration to restore lost services in case of physical or cyber attacks and faults
- Data Protection by design
  - Ensure data privacy, considering e.g. metering data, access logs, CCTV footage, …
  - Ensure compliance with GDPR
  - Provide recommendations to DEFENDER system developers

DEFENDER Architecture Specification

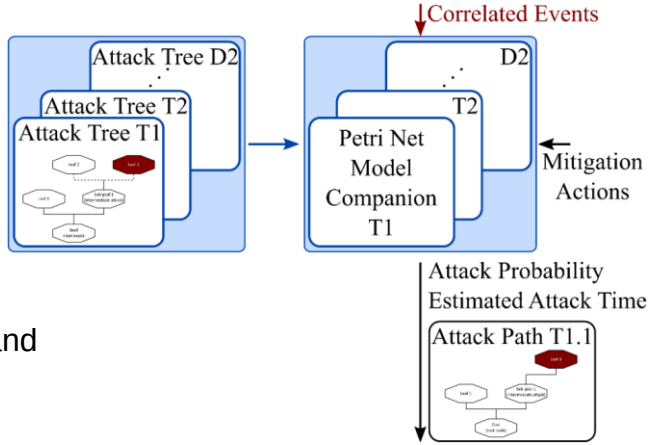


Critical Energy Infrastructure (CEI) Modelling

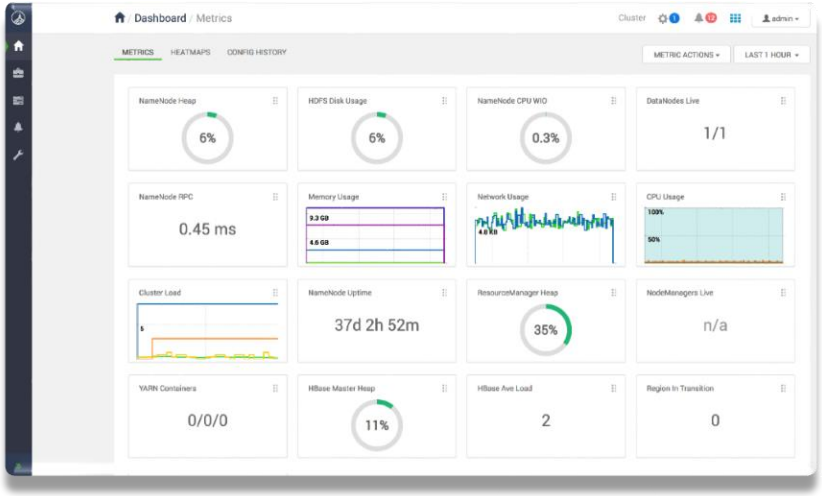
- Attack trees of threat scenarios
- Petri Net (PN) model companions and augmentation of attack trees

Cyber-Physical-Social System (CPSS) Co-simulator

- **Inputs**
  - **State of the Environment**: correlated events from the Event Processing and Management Module
  - **Mitigation actions** proposed from the Incident Mitigation Module
- **Simulation**: probabilistic and time-domain analysis of attack propagation
- **Outputs**:
  - **Situation Perception**: attack paths with associated probabilities and estimated time to attack
  - **Future Situation Projection**: prediction of effectiveness of mitigation actions in terms of attack probability and time to attack



Pan-European CEI Incidents Information Sharing Platform

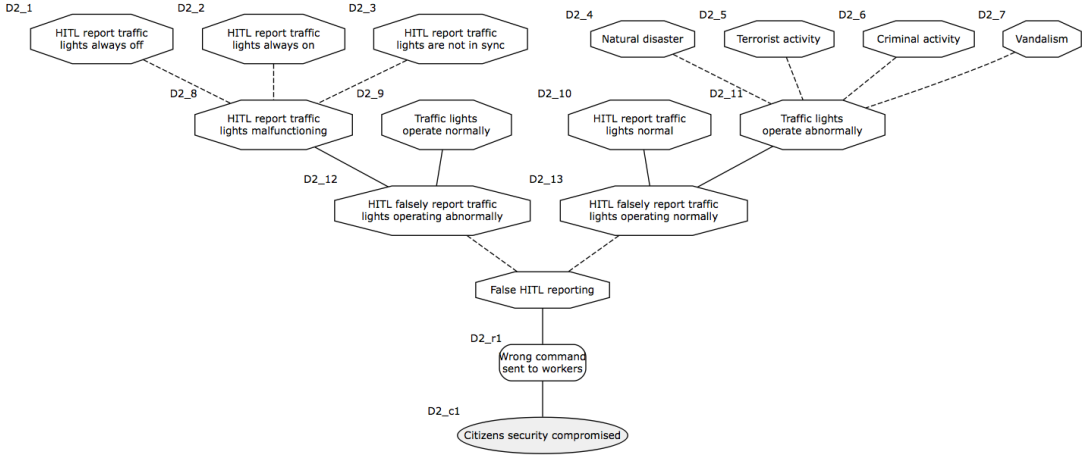


- **Scope**:
  - Design and implement the DEFENDER I2SP to enable controlled sharing of intel/info related to cyber-physical security of CEI Operators.

- Identified MISP project as core candidate for **interfacing with the public**
  - Community-based, EU-funded, features many taxonomies and is also NATO-compliant

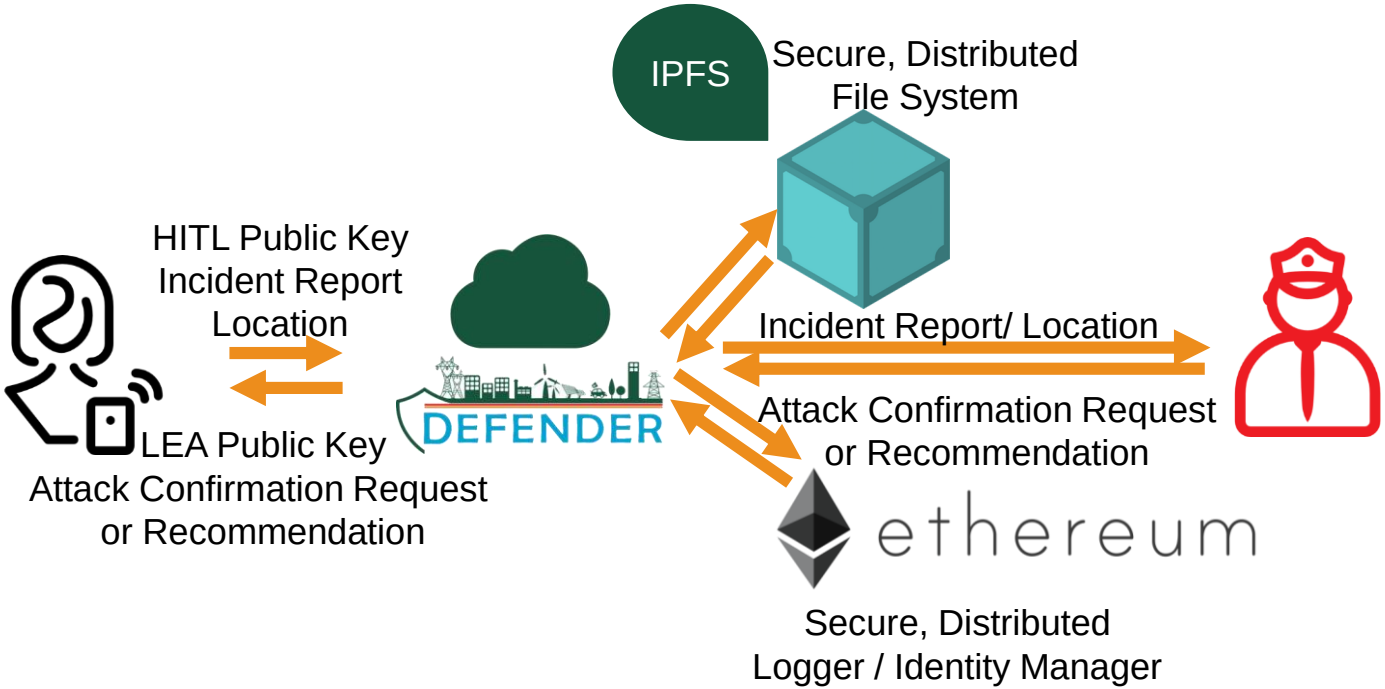
Human in the Loop – example scenario

- Human in the Loop (HITL)
  - Trusted volunteers as „human sensors“
  - Mobile app for information sharing
  - Uses structured and free text, pictures, videos



1. HITL user A notifies CEI operator that traffic lights are not operating properly
2. The CEI operator checks the message in the DEFENDER SCC and asks for verification from all HITL volunteers in the vicinity of the city centre
3. HITL user B (fraudulent) sends a message claiming that they are operating normally
4. HITL user A sends a photo showing all traffic lights closed
5. CEI operator bans HITL user B from the platform

Human in the Loop – architecture and information flow



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