SOC Development for IDS

Exploring approaches to embedding IDS into a variety of SOC frameworks to ensure full preparedness for timely and constructive responses to anomalies

Nikolaus Wirtz, M. Sc.

ACS | Automation of Complex Power Systems

E.ON Energy Research Center

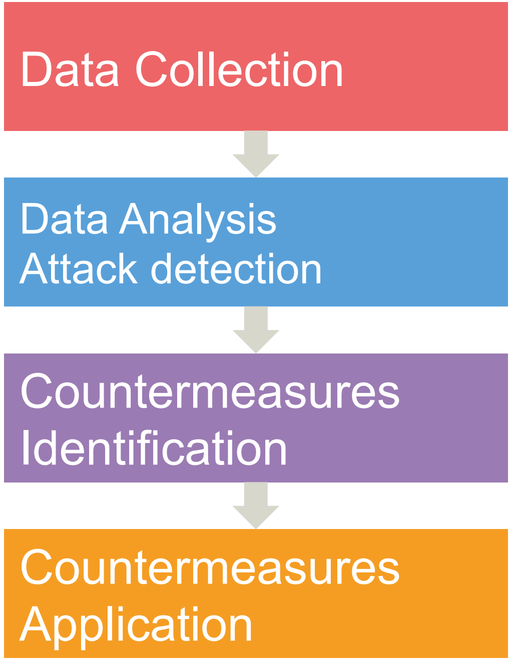
RWTH AACHEN UNIVERSITY

SOC development for IDS 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/

Cyber-security for next generation Smart Critical Infrastructures

- 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

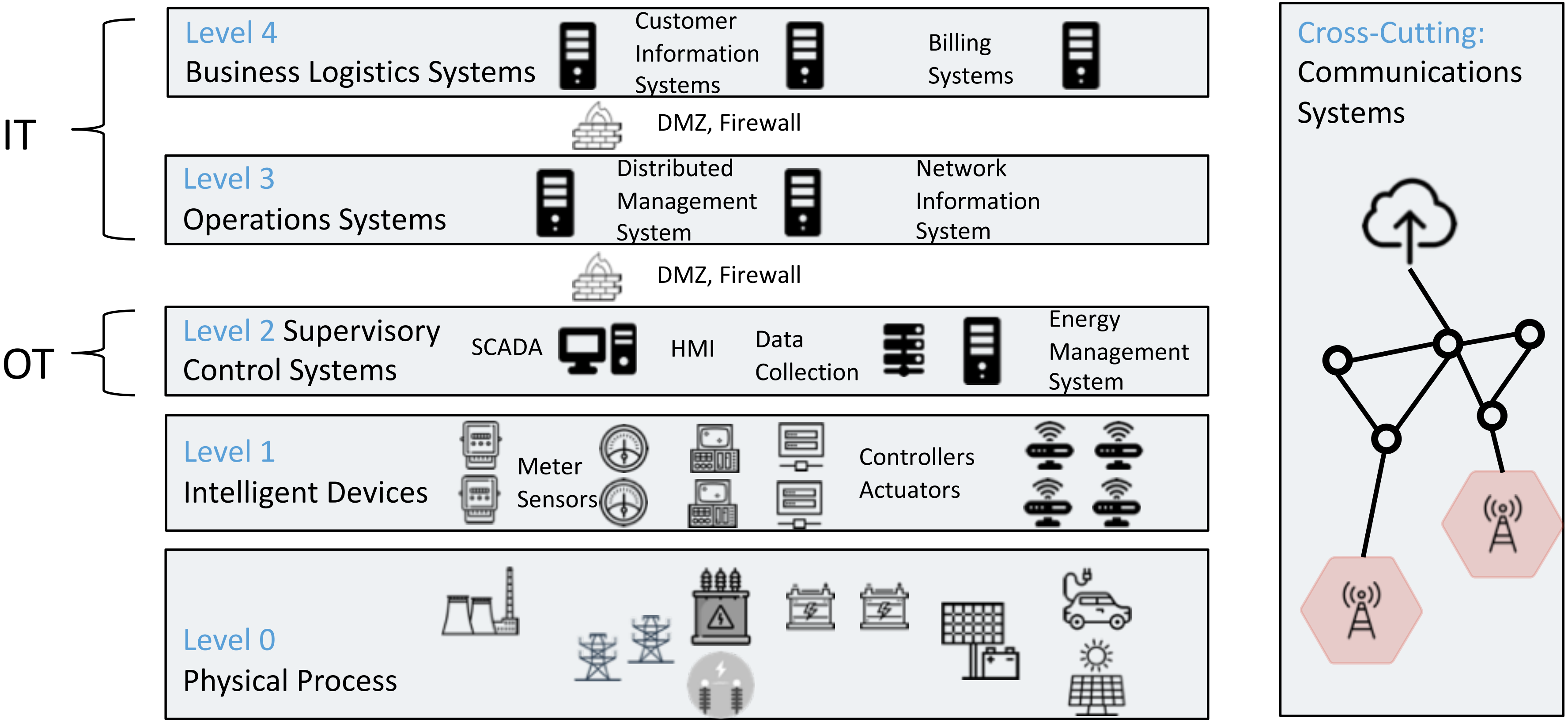

Data Collection

Data Analysis
Attack detection

Countermeasures
Identification

Countermeasures
Application

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

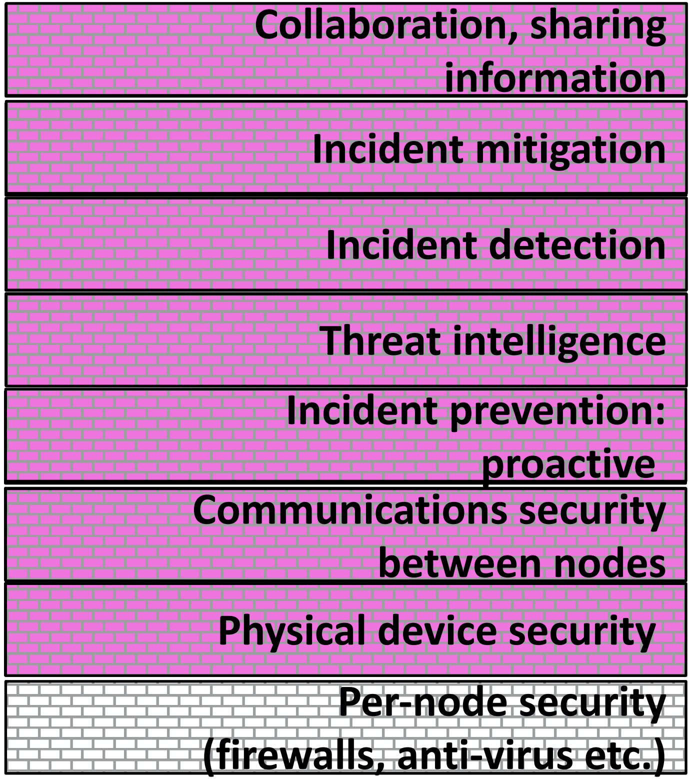
Level 0
Physical Process

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



Collaboration, sharing information

Incident mitigation

Incident detection

Threat intelligence

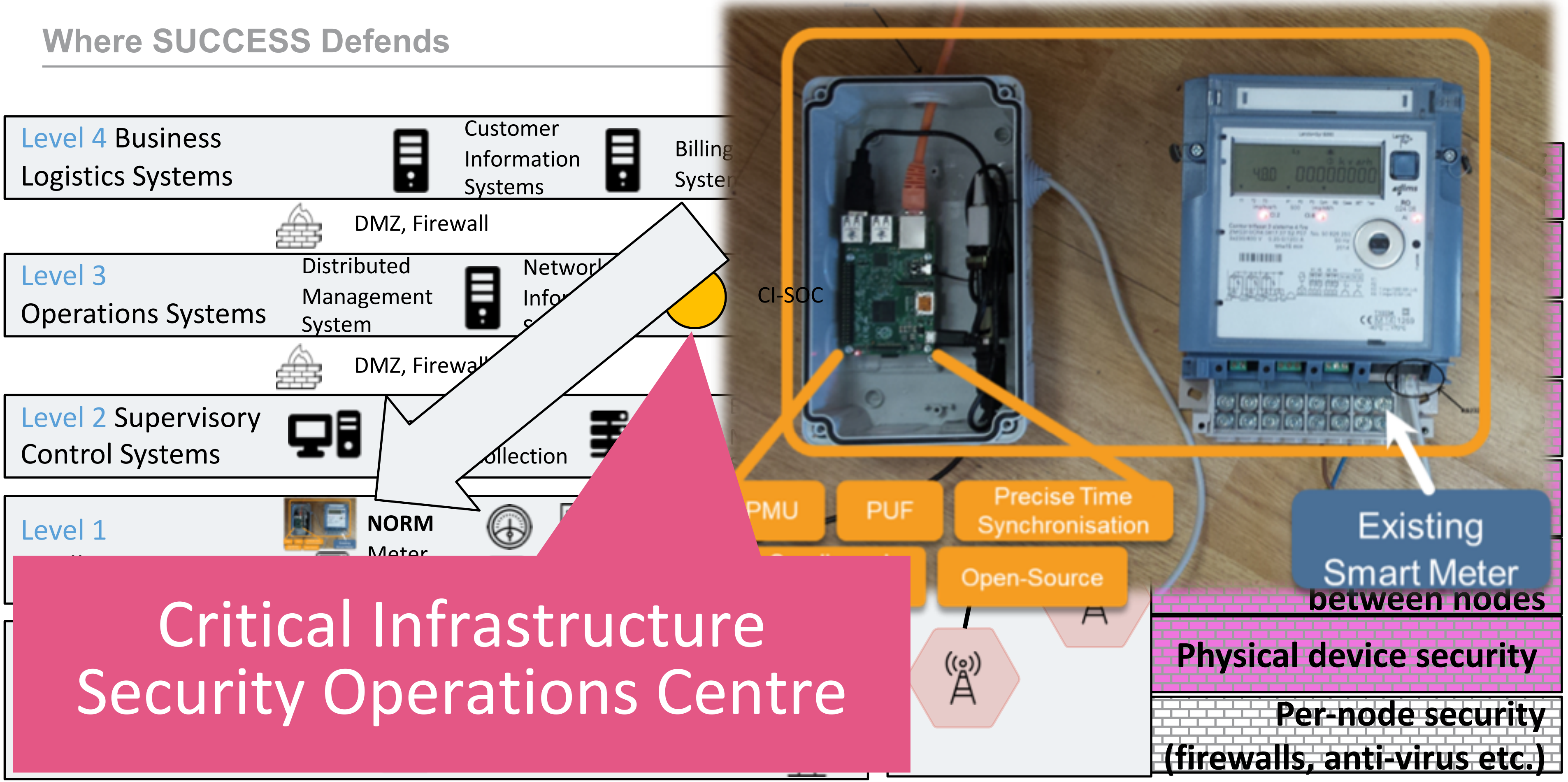
Incident prevention: proactive

Communications security between nodes

Physical device security

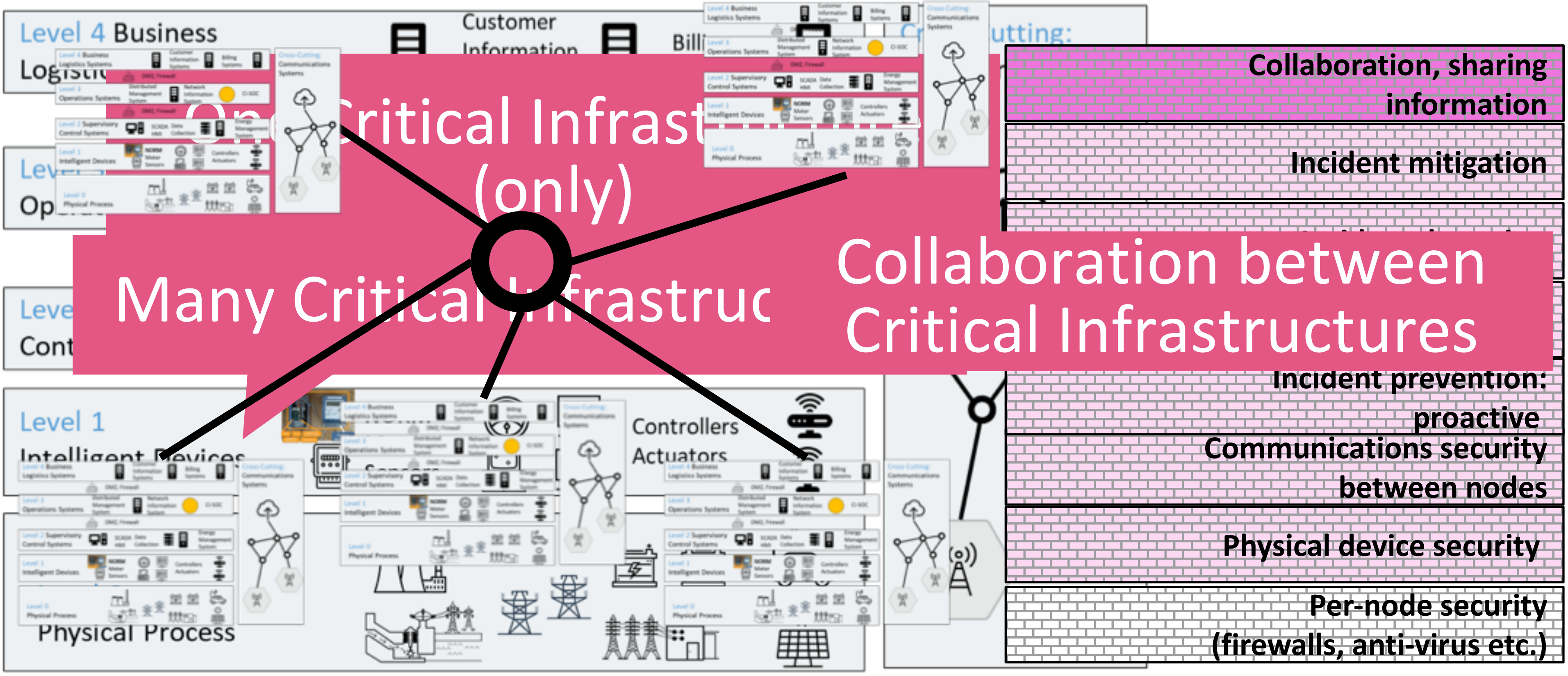
Per-node security (firewalls, anti-virus etc.)

Where SUCCESS Defends


Level 4 Business Logistics Systems
Customer Information Systems
Billing Systen
DMZ, Firewall
Level 3 Operations Systems
Distributed Management System
Network Info
CI-SOC
DMZ, Firewal
Level 2 Supervisory Control Systems
ollection
Level 1
NORM Meter
PMU
PUF
Precise Time Synchronisation
Open-Source
Existing Smart Meter
between nodes
Physical device security
Per-node security (firewalls, anti-virus etc.)

Critical Infrastructure Security Operations Centre

Where SUCCESS Defends



One Critical Infrast (only)

Many Critical Infrastruc

Collaboration between Critical Infrastructures

Collaboration, sharing information

Incident mitigation

Incident prevention: proactive

Communications security between nodes

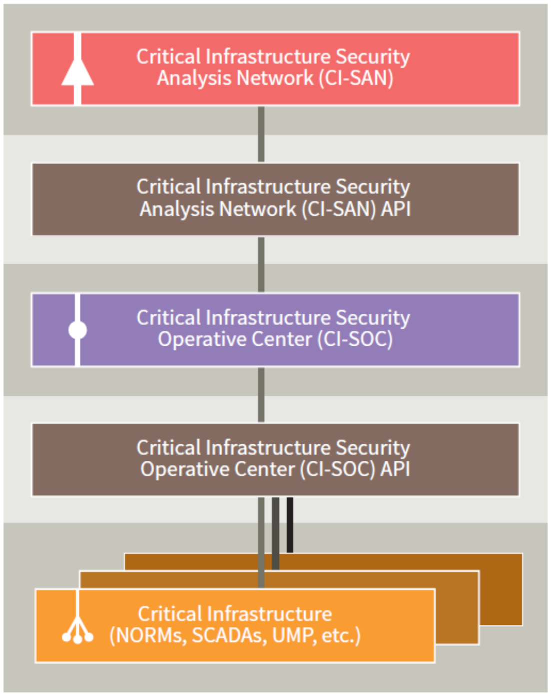
Physical device security

Per-node security (firewalls, anti-virus etc.)

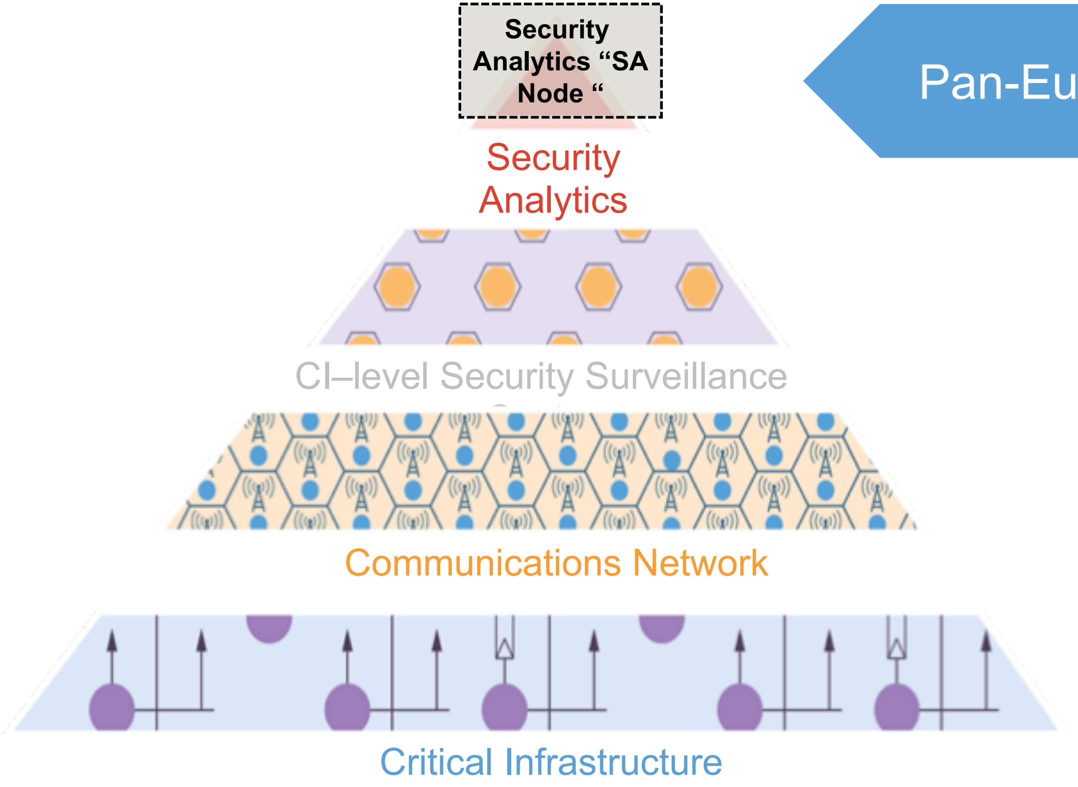
SUCCESS Security Solution

- 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
Critical Infrastructure Security Analysis Network (CI-SAN)
Critical Infrastructure Security Analysis Network (CI-SAN) API
Critical Infrastructure Security Operative Center (CI-SOC)
Critical Infrastructure Security Operative Center (CI-SOC) API
Critical Infrastructure (NORMs, SCADAs, UMP, etc.)

SUCCESS Security Solution



Security Analytics “SA Node “

Security Analytics

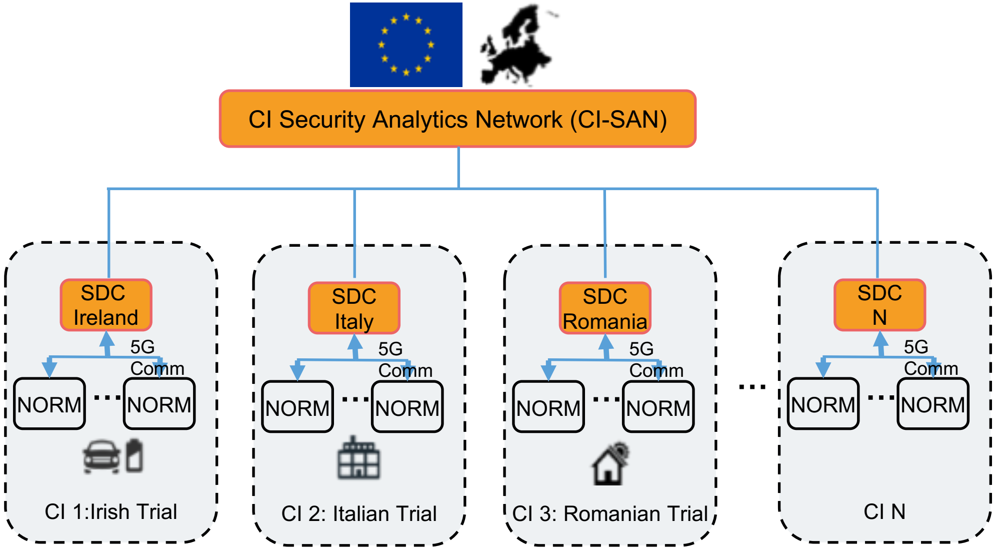
CI–level Security Surveillance

Communications Network

Critical Infrastructure

Pan-European Security Analytics Network

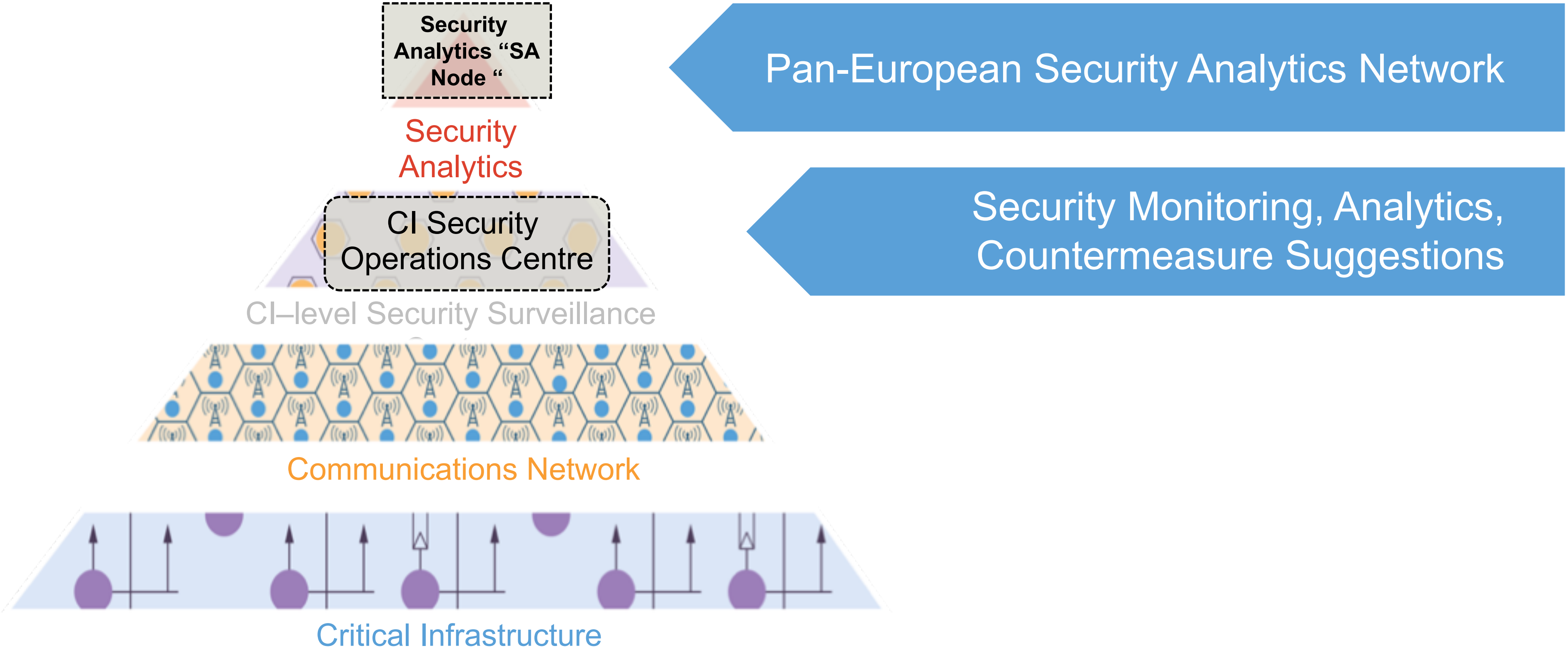
CI-SAN



- 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



Security Analytics "SA Node "

Security Analytics

CI Security Operations Centre

CI–level Security Surveillance

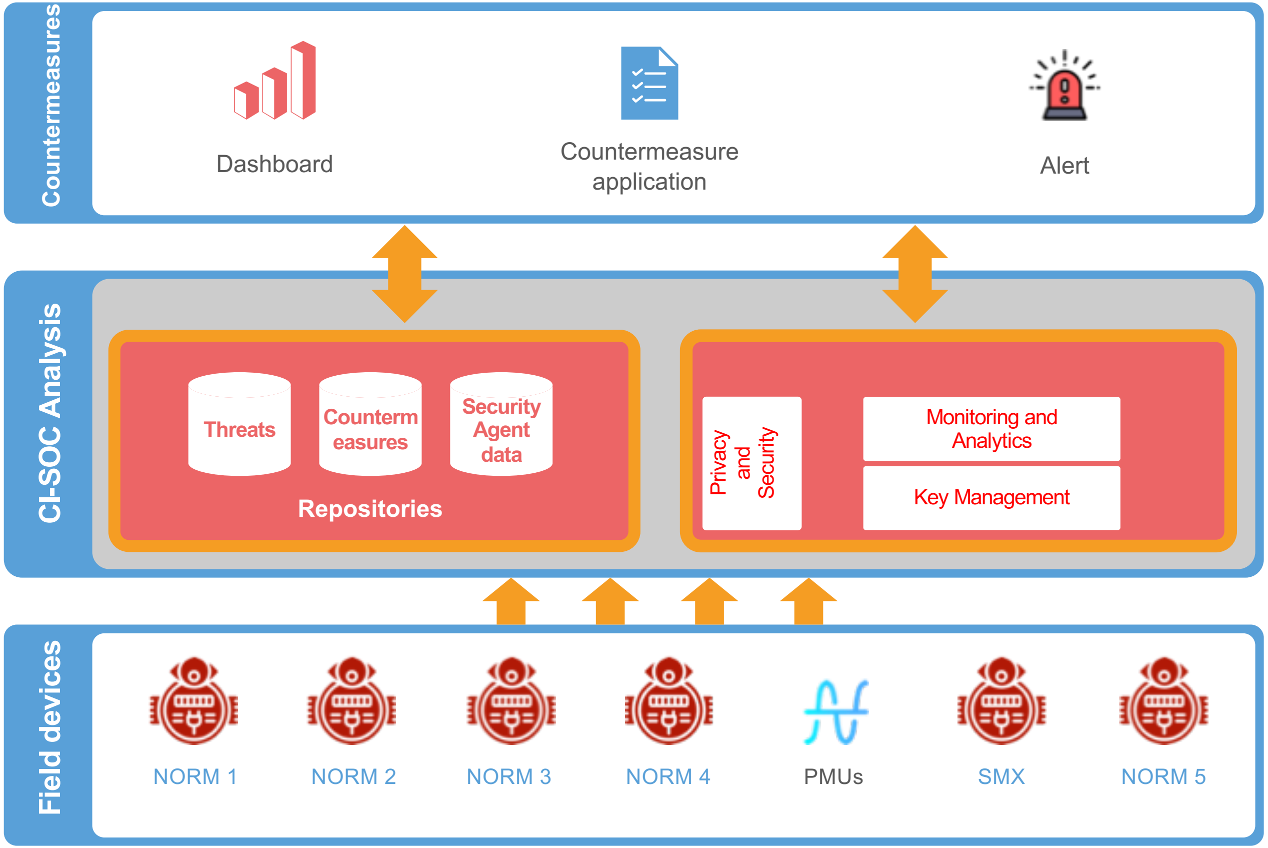
Communications Network

Critical Infrastructure

Pan-European Security Analytics Network

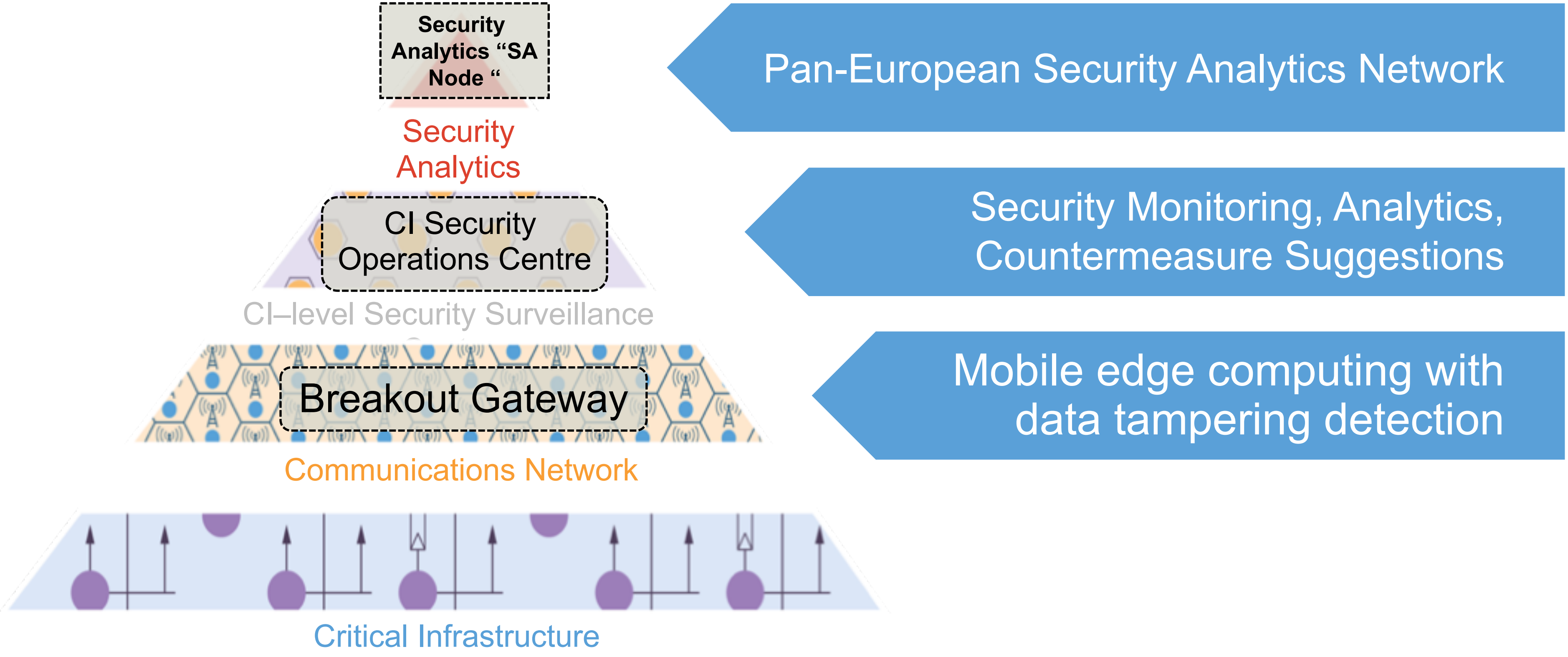
Security Monitoring, Analytics, Countermeasure Suggestions

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



Security Analytics “SA Node “

Security Analytics

CI Security Operations Centre

CI–level Security Surveillance

Breakout Gateway

Communications Network

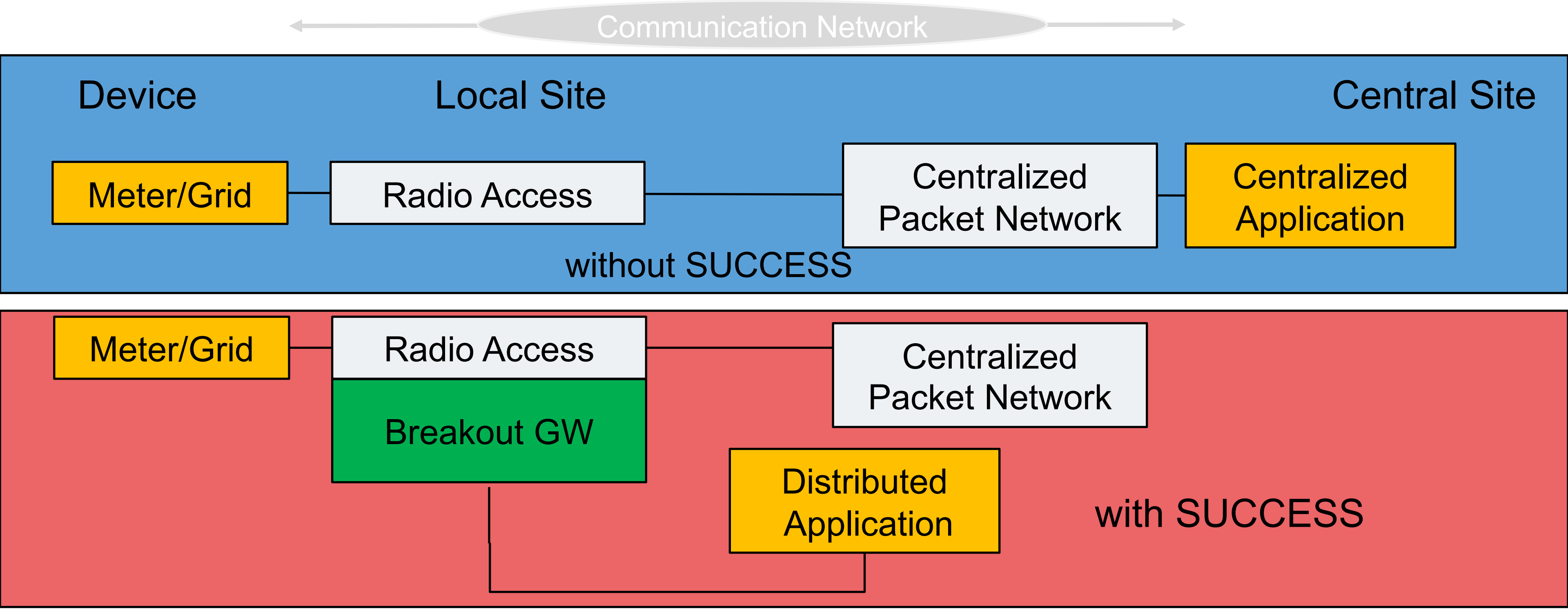
Critical Infrastructure

Pan-European Security Analytics Network

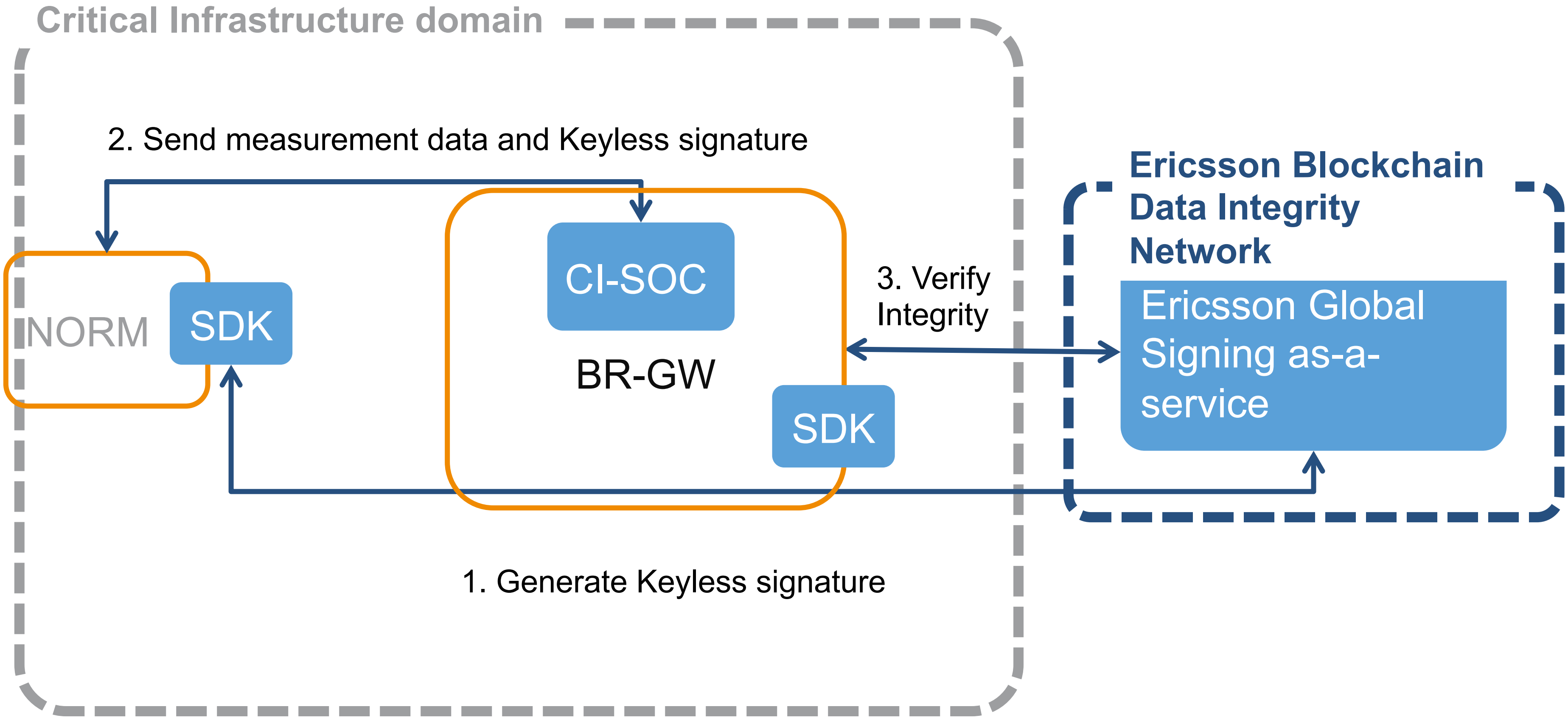
Security Monitoring, Analytics, Countermeasure Suggestions

Mobile edge computing with data tampering detection

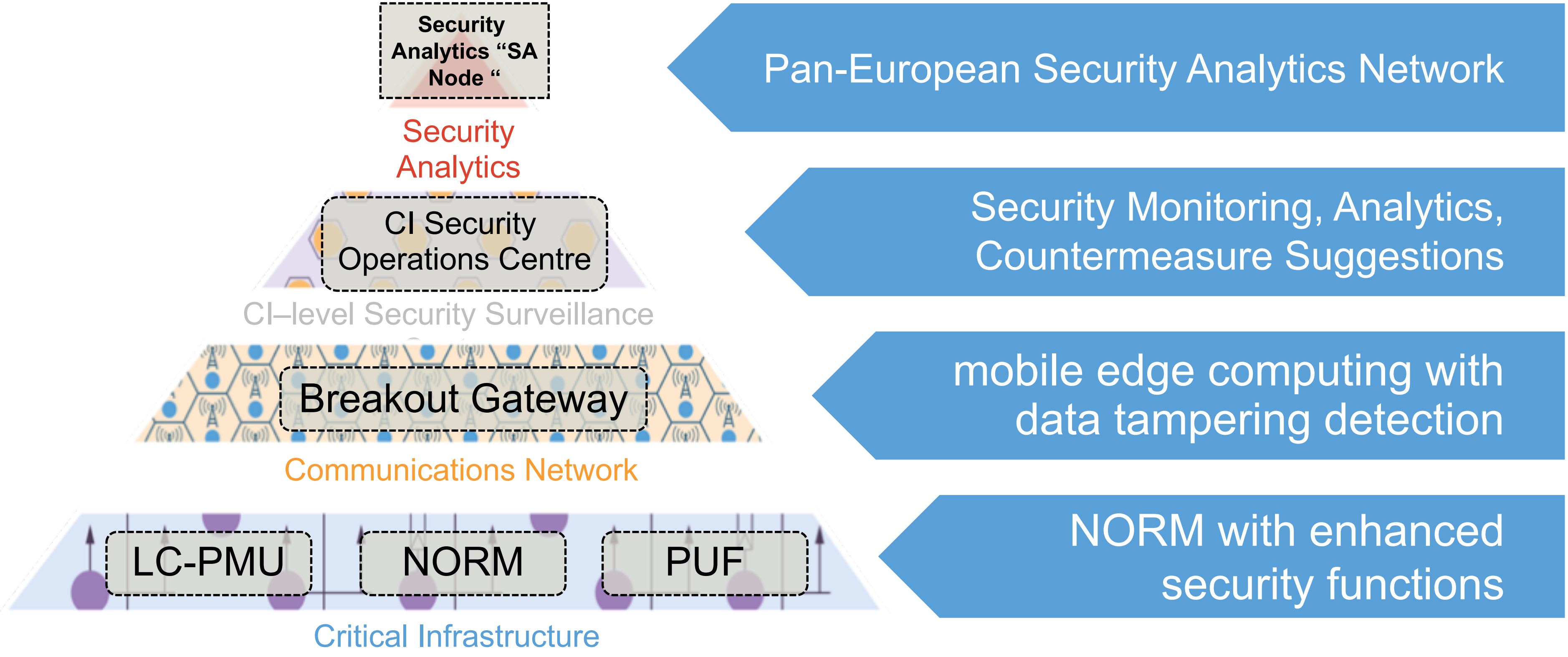
Breakout Gateway concept



Integration with SUCCESS Security Solution


Critical Infrastructure domain
2. Send measurement data and Keyless signature
NORM
SDK
CI-SOC
BR-GW
SDK
3. Verify Integrity
Ericsson Blockchain Data Integrity Network
Ericsson Global Signing as-a-service
1. Generate Keyless signature

SUCCESS Security Solution



Security Analytics "SA Node "

Security Analytics

CI Security Operations Centre

CI–level Security Surveillance

Breakout Gateway

Communications Network

LC-PMU

NORM

PUF

Critical Infrastructure

Pan-European Security Analytics Network

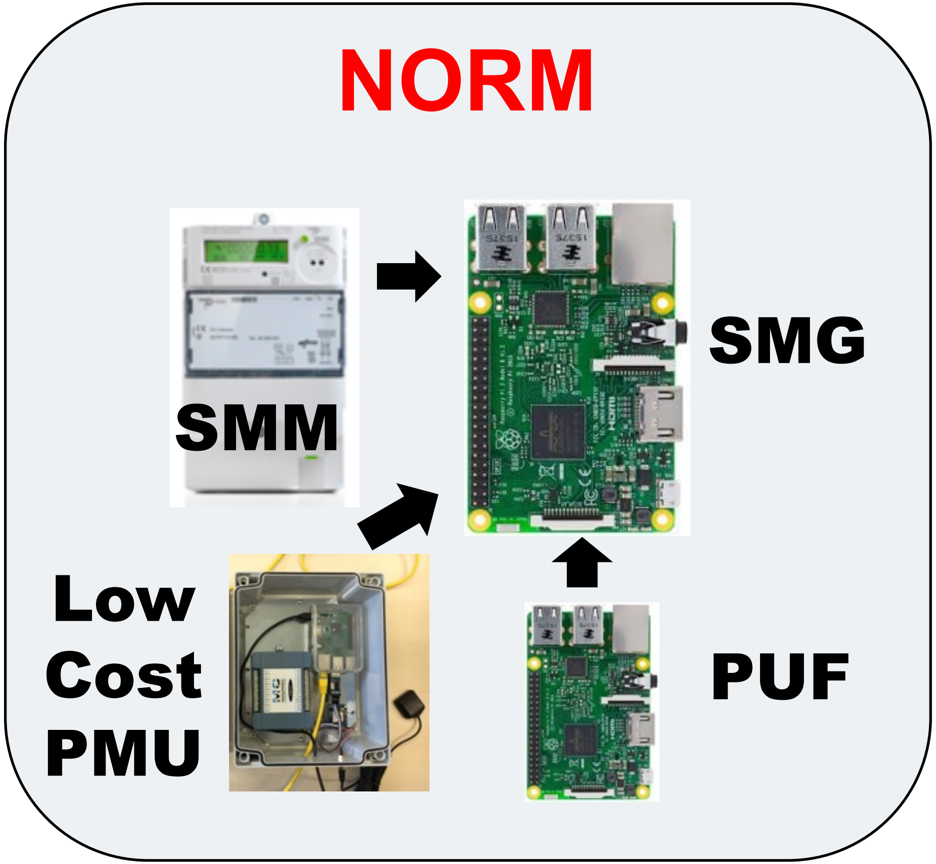
Security Monitoring, Analytics, Countermeasure Suggestions

mobile edge computing with data tampering detection

NORM with enhanced security functions

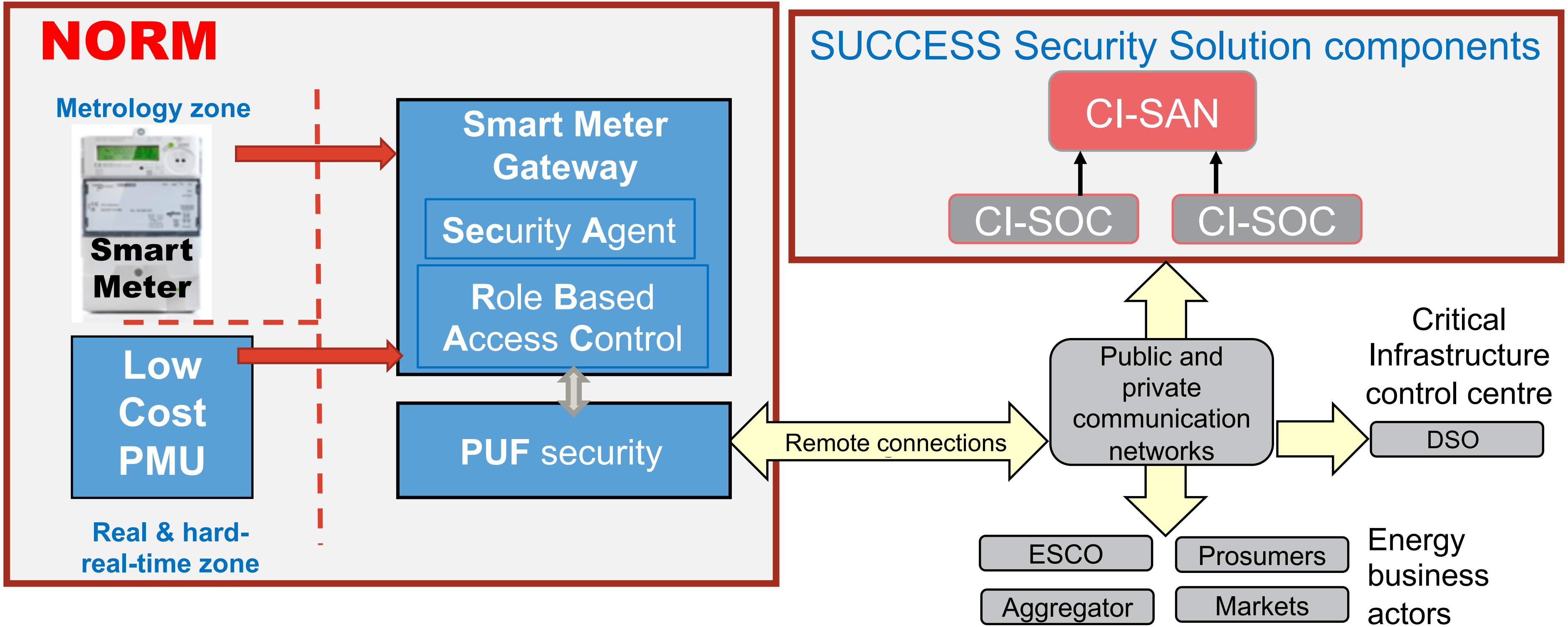
Next Generation Open Real-Time Meter

- 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



Integration with SUCCESS Security Solution

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



Integration with SUCCESS Security Solution

- **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

🟩 Physical Protection
🟨 Cyber Protection
⬜ Human in the Loop

ENGIE Ineo

🟩 Nuclear Power Plant

🟩🟨 Transmission Network

ELES

BFP

🟩🟨 Wind Farms

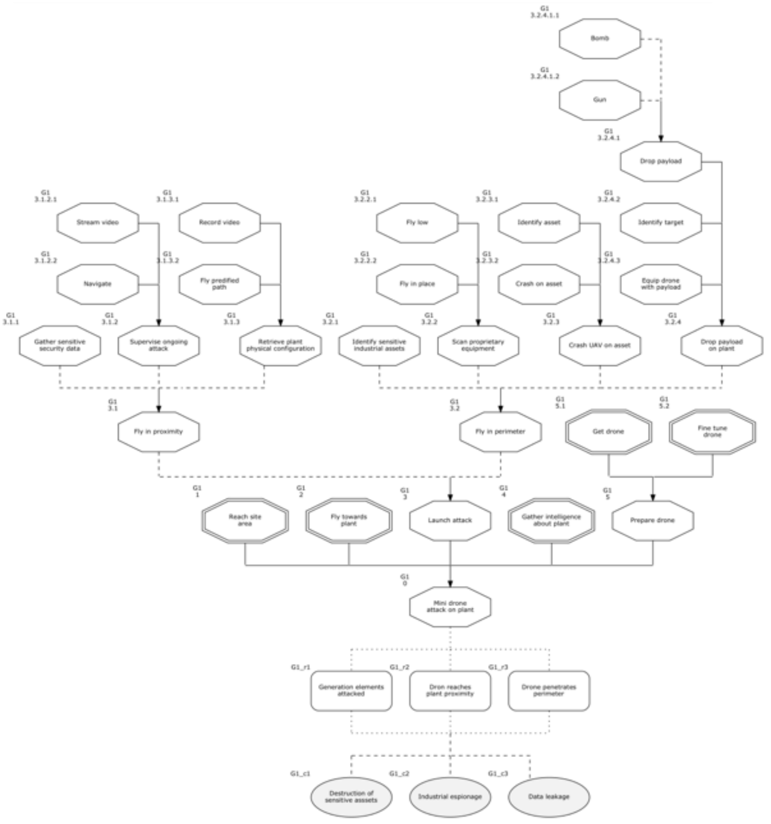
🟨⬜ Distribution and Prosumer

ASM Terni S.p.A.

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

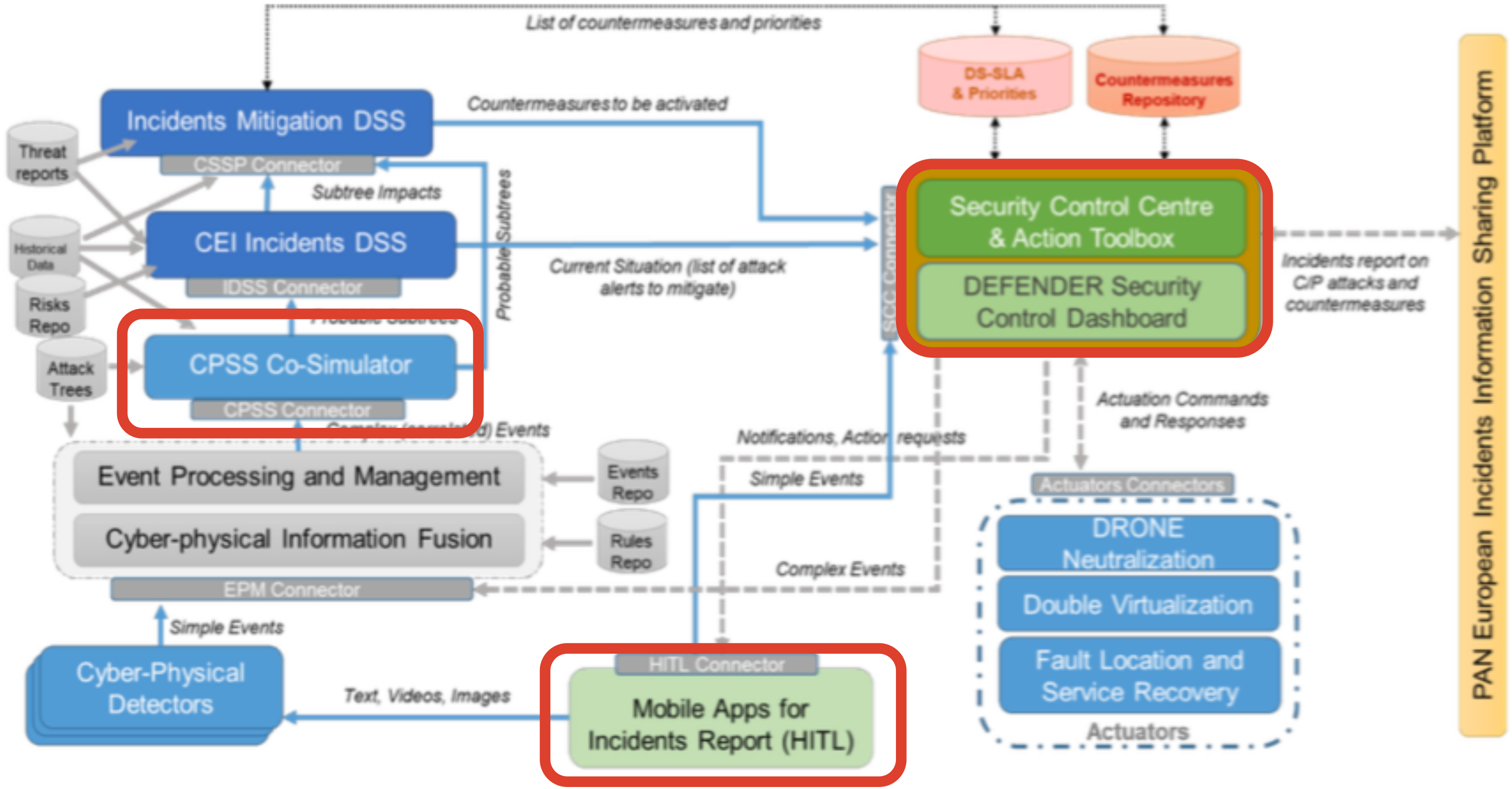
- Security Lifecycle Assessment by design
  - 2-layer approach to security lifecycle assessment
  - Operational layer for maintaining or restoring the targeted service level
  - Strategic layer for long-term evaluation and efficient security resource allocation

- 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



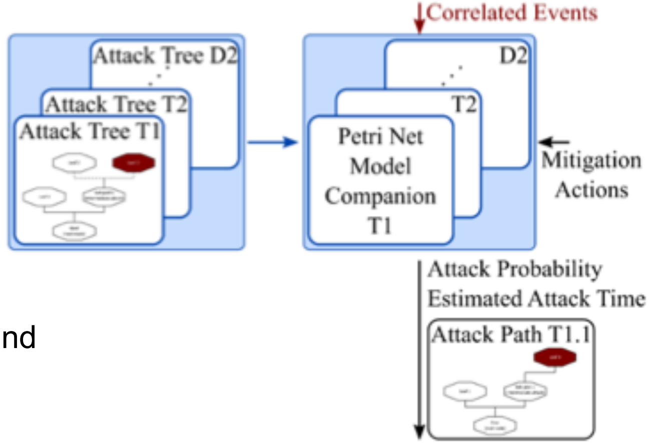
List of countermeasures and priorities
DS-SLA & Priorities
Countermeasures Repository
Incidents Mitigation DSS
Countermeasures to be activated
Threat reports
CSSP Connector
Subtree Impacts
Probable Subtrees
CEI Incidents DSS
Historical Data
IDSS Connector
Current Situation (list of attack alerts to mitigate)
Risks Repo
Probable Subtrees
SCC Connector
Security Control Centre & Action Toolbox
DEFENDER Security Control Dashboard
Incidents report on CIP attacks and countermeasures
PAN European Incidents Information Sharing Platform
Attack Trees
CPSS Co-Simulator
CPSS Connector
Complex (correlated) Events
Notifications, Action requests
Actuation Commands and Responses
Event Processing and Management
Events Repo
Simple Events
Actuators Connectors
Cyber-physical Information Fusion
Rules Repo
DRONE Neutralization
Double Virtualization
Complex Events
EPM Connector
Fault Location and Service Recovery
Simple Events
Actuators
HITL Connector
Cyber-Physical Detectors
Text, Videos, Images
Mobile Apps for Incidents Report (HITL)

Critical Energy Infrastructure (CEI) Modelling

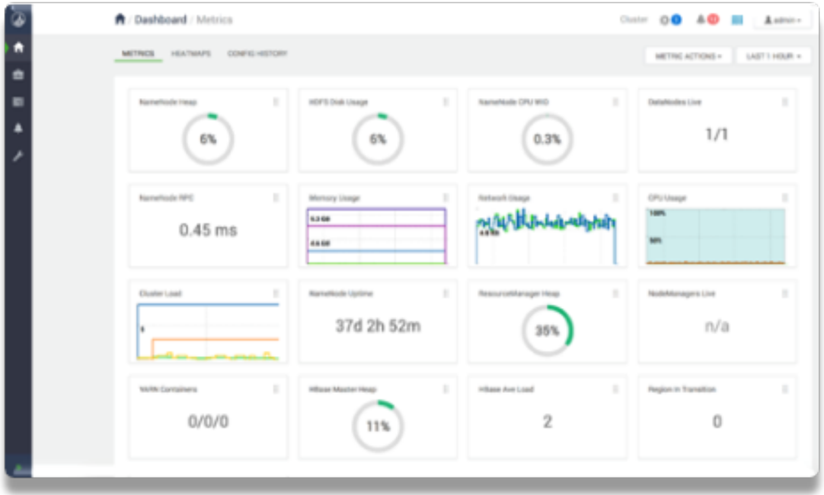
- Attack trees of threat scenarios
- Petri Net (PN) model companions and augmentation of attack trees

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

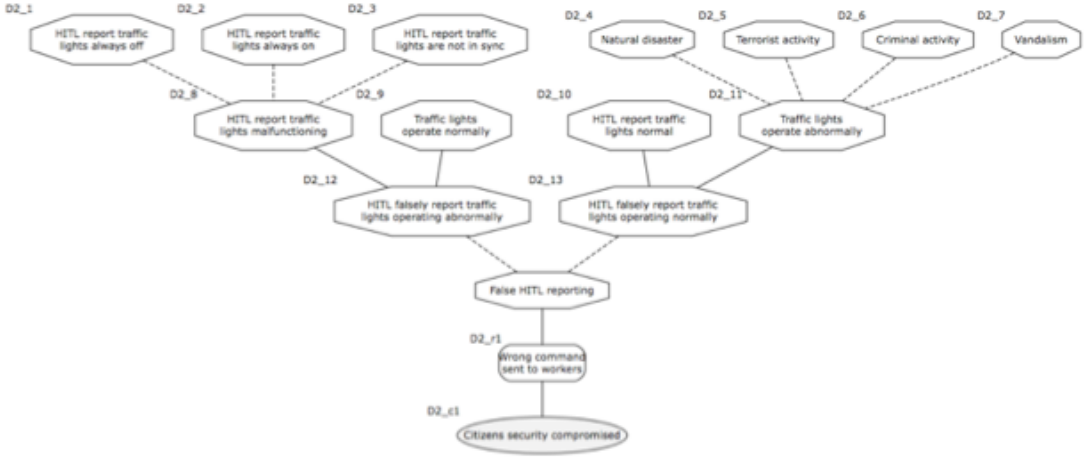


MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

- **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

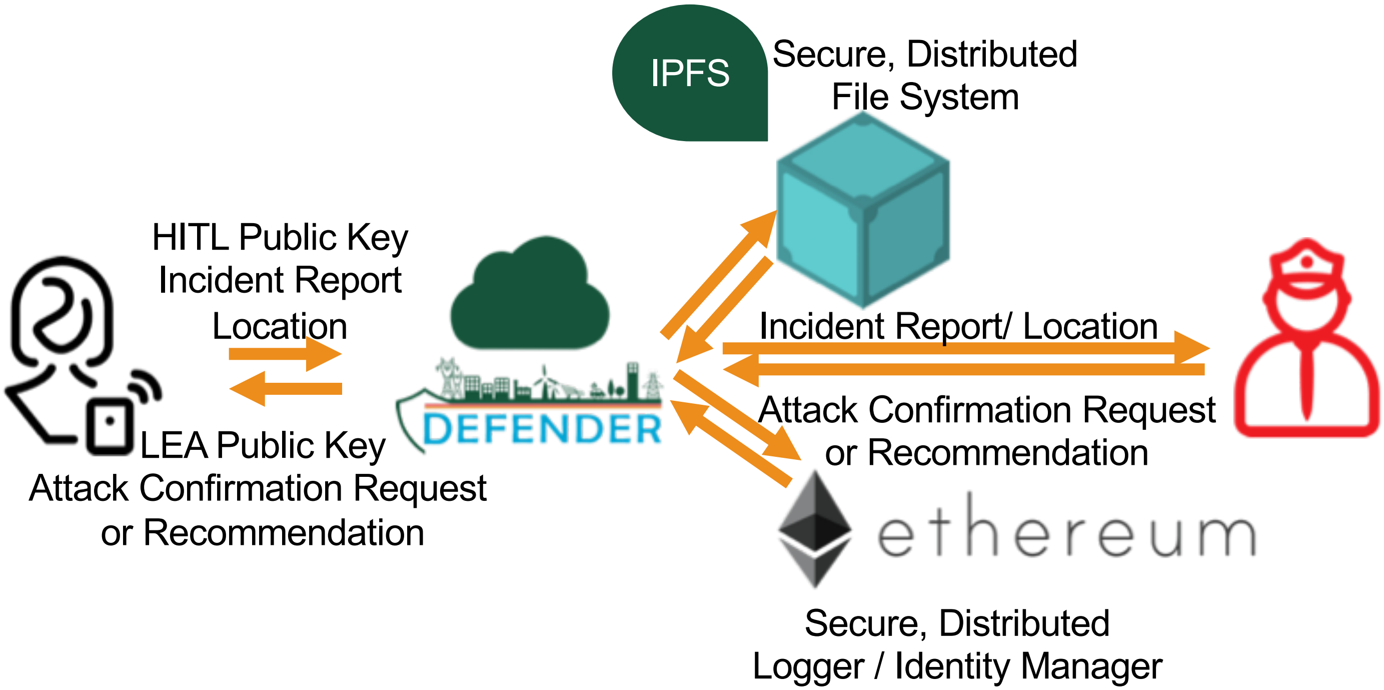
Human in the Loop – example scenario

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


D2_1
HITL report traffic lights always off
D2_2
HITL report traffic lights always on
D2_3
HITL report traffic lights are not in sync
D2_4
Natural disaster
D2_5
Terrorist activity
D2_6
Criminal activity
D2_7
Vandalism
D2_8
HITL report traffic lights malfunctioning
D2_9
Traffic lights operate normally
D2_10
HITL report traffic lights normal
D2_11
Traffic lights operate abnormally
D2_12
HITL falsely report traffic lights operating abnormally
D2_13
HITL falsely report traffic lights operating normally
False HITL reporting
D2_r1
Wrong command sent to workers
D2_c1
Citizens security compromised

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



IPFS
Secure, Distributed File System
HITL Public Key
Incident Report
Location
DEFENDER
Incident Report/ Location
LEA Public Key
Attack Confirmation Request or Recommendation
Attack Confirmation Request or Recommendation
ethereum
Secure, Distributed Logger / Identity Manager

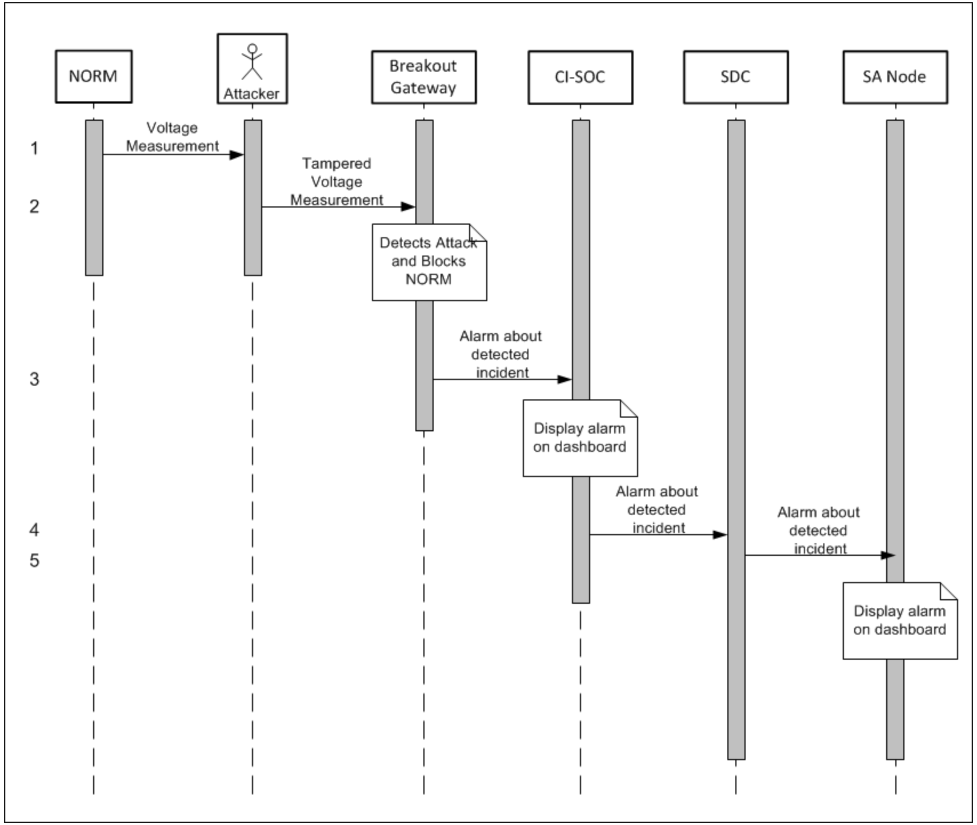
M.Sc. Nikolaus Wirtz
Research Associate

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

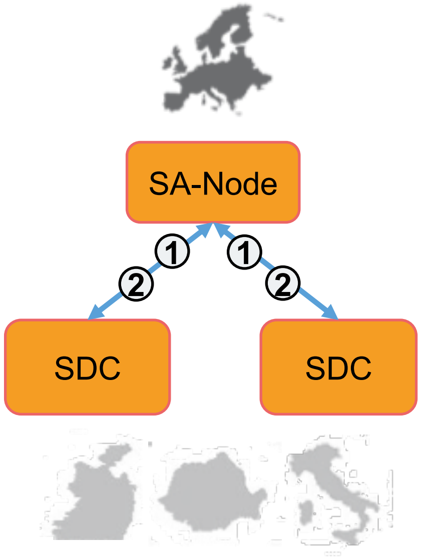
Man-in-the-Middle Attack Detected by Breakout Gateway


NORM
Attacker
Breakout Gateway
CI-SOC
SDC
SA Node
1
Voltage Measurement
2
Tampered Voltage Measurement
Detects Attack and Blocks NORM
3
Alarm about detected incident
Display alarm on dashboard
4
Alarm about detected incident
5
Alarm about detected incident
Display alarm on dashboard

Architecture and Roles

Security Data Concentrators (SDC):

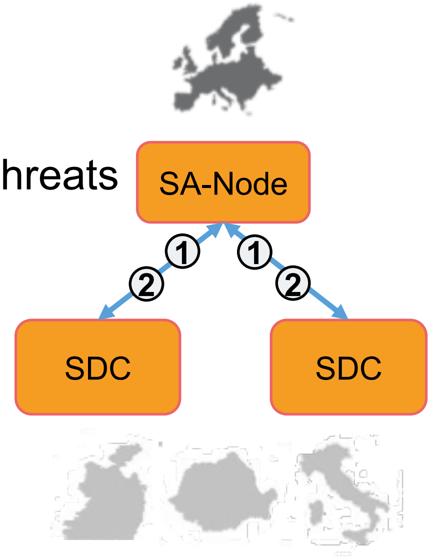
- sends **aggregated** data to SA-Node (1), to not overburden the communication channel due to a potential high number of registered SDC instances in the system
- sends **anonymized** data to SA-Node (1), to not violate country-specific privacy issues; SCC instances are hosted by DSOs/TSOs and therefore are country-related
- receives superior **threat patterns** from SA-Node (2), as SA-Node has an comprehensive view an the threat landscape of Europe



Architecture and Roles

- Security Analysis Node (SA-Node):

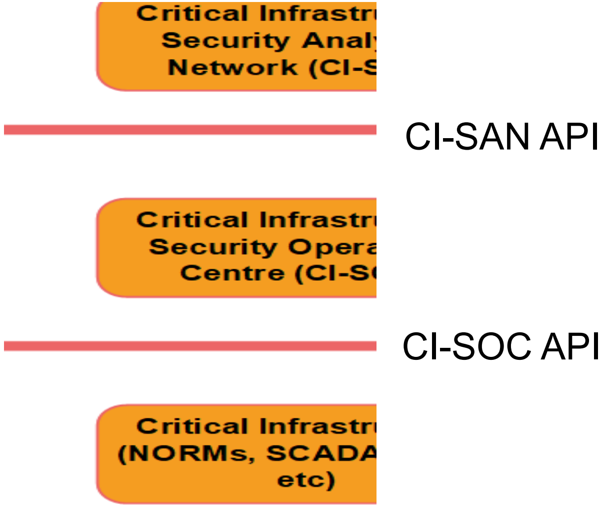
- **identifies threats** by combining aggregated data from SDC instances; threats can be identified in almost **real-time** and **only at the European level**
- **informs** all appropriate SDC instances about found threats (2)
- **suggests** appropriate countermeasures (2) to DSOs/TSOs to prevent threats



Interface and other critical infrastrutures

Interface

- CI-SAN **API**: security incidents, counter-measures, further payload between the SUCCESS components.
- Based on IODEF/IDMEF format



Critical Infrastr
Security Anal
Network (CI-S

CI-SAN API

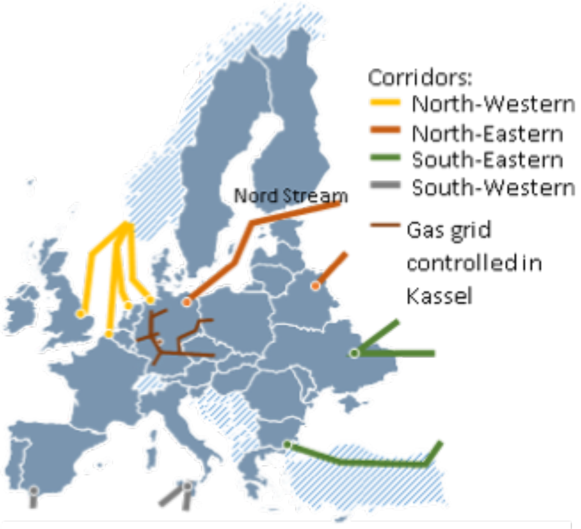
Critical Infrastr
Security Opera
Centre (CI-S

CI-SOC API

Critical Infrastr
(NORMs, SCADA
etc)

(see SUCCESS Deliverable D4.6 Description of Available Components for SW Functions, Infrastructure and Related Documentation)

- **Other Critical Infrastructures**
- Study about applying CI-SAN to **other critical infrastructures**: gas, oil, water, transport and traffic, health, finance, food, government, media, culture



(see SUCCESS Deliverable D4.3 Solution Architecture and Solution Description)

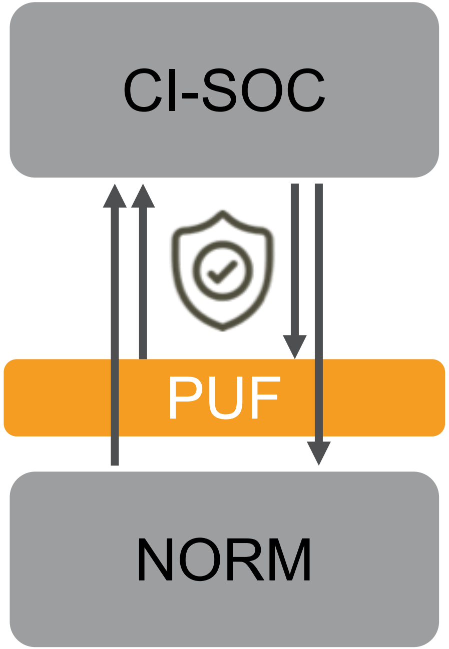
Physical Unclonable Function

- PUF – a **unique hardware fingerprint generator** only dependent on the physical characteristics of the device
- Uses of PUF in SUCCESS:
  - Authentication mechanism
  - Identification mechanism
  - Hardware changes tracker
  - Hardware encryption services
- PUF prototype for NORM protection was developed in SUCCESS

PUF - How it works

- Exploits the physical variations which occur naturally during manufacturing to ensure **uniqueness** of the hardware
- Physically connected to a NORM, this uniqueness feature is used as an enabler for:
  - Determining PUF **authenticity**
  - **Securing** NORM <=> CI-SOC communications

- If an adversary attacks the PUF (or the NORM hardware), CI-SOC will immediately notify the Utility



Low Cost PMU

- PMU are power systems measurement devices that, by exploiting GPS time reference, provide synchrophasors, frequency and ROCOF of current and voltage

Computation

- Raspberry PI 3
- MicroSD 32 GB storage
- Power Supply

Data acquisition

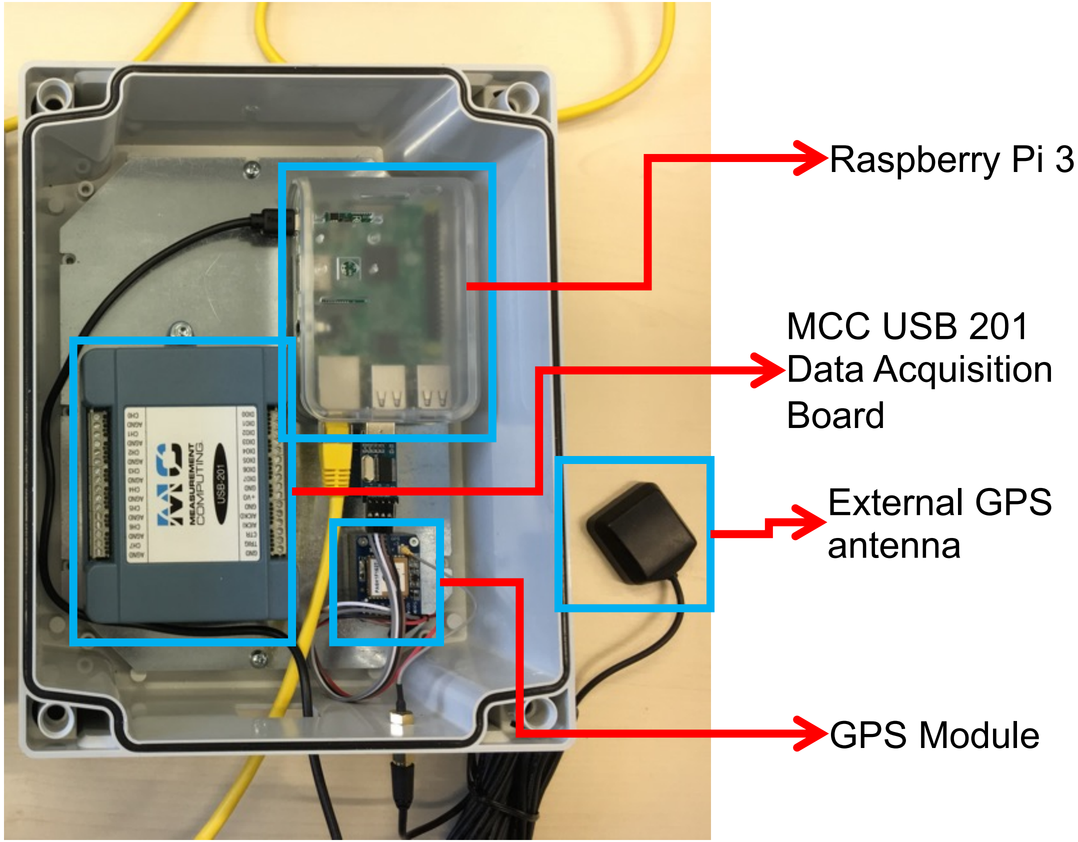
- MCC USB 201 Data Acquisition Board

Time synchronization

- GPS MTK 3339
- External GPS antenna

Electrical connections and box

- Screw terminal connector
- PVC enclosure witgh IP61 protection
- Aluminum EMI shield



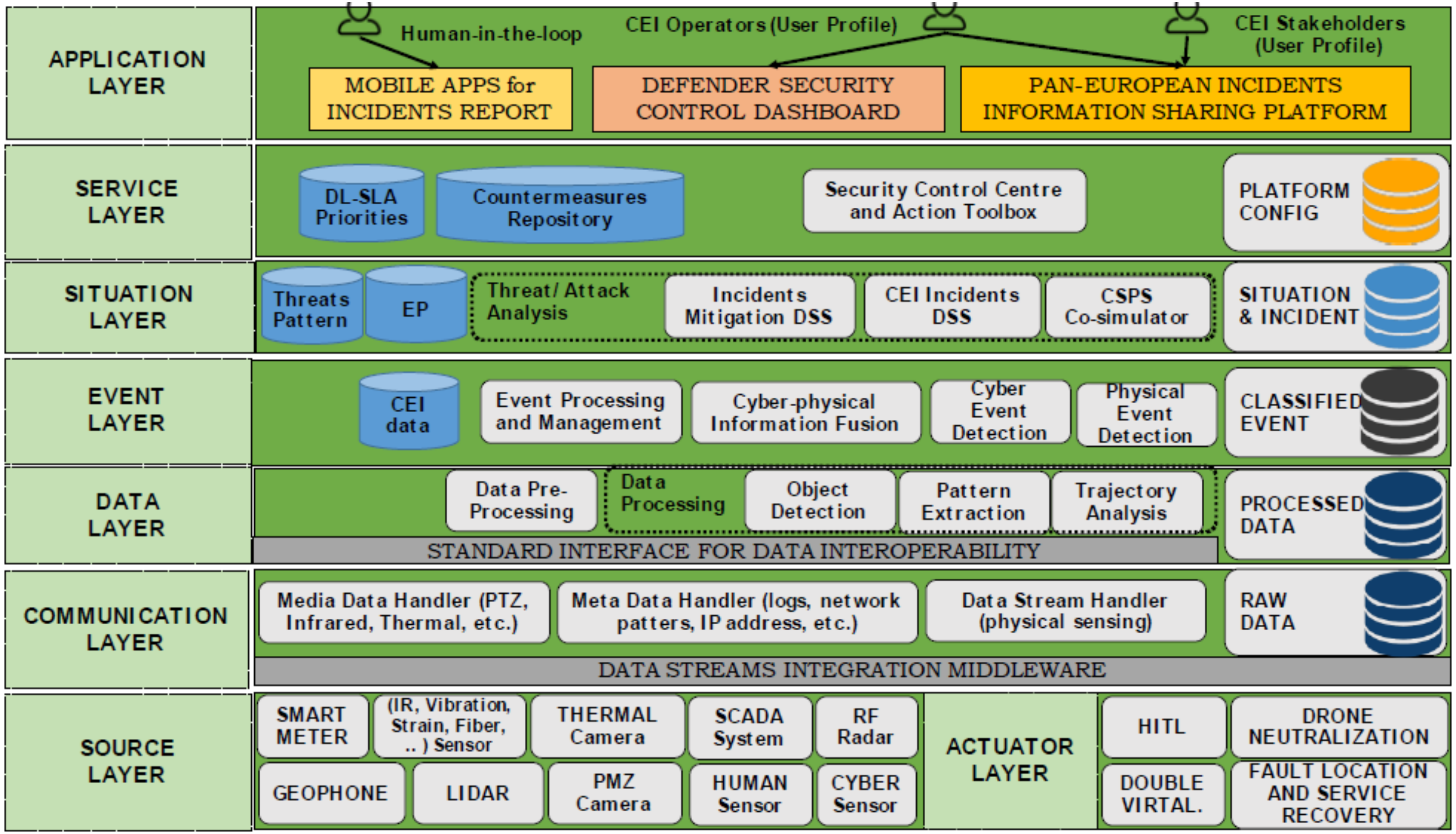
Raspberry Pi 3

MCC USB 201 Data Acquisition Board

External GPS antenna

GPS Module

DEFENDER Architecture Specification



APPLICATION LAYER
- Human-in-the-loop
- CEI Operators (User Profile)
- CEI Stakeholders (User Profile)
- MOBILE APPS for INCIDENTS REPORT
- DEFENDER SECURITY CONTROL DASHBOARD
- PAN-EUROPEAN INCIDENTS INFORMATION SHARING PLATFORM

SERVICE LAYER
- DL-SLA Priorities
- Countermeasures Repository
- Security Control Centre and Action Toolbox
- PLATFORM CONFIG

SITUATION LAYER
- Threats Pattern
- EP
- Threat/ Attack Analysis
- Incidents Mitigation DSS
- CEI Incidents DSS
- CSPS Co-simulator
- SITUATION & INCIDENT

EVENT LAYER
- CEI data
- Event Processing and Management
- Cyber-physical Information Fusion
- Cyber Event Detection
- Physical Event Detection
- CLASSIFIED EVENT

DATA LAYER
- Data Pre-Processing
- Data Processing
- Object Detection
- Pattern Extraction
- Trajectory Analysis
- PROCESSED DATA
- STANDARD INTERFACE FOR DATA INTEROPERABILITY

COMMUNICATION LAYER
- Media Data Handler (PTZ, Infrared, Thermal, etc.)
- Meta Data Handler (logs, network patters, IP address, etc.)
- Data Stream Handler (physical sensing)
- RAW DATA
- DATA STREAMS INTEGRATION MIDDLEWARE

SOURCE LAYER
- SMART METER
- (IR, Vibration, Strain, Fiber, ..) Sensor
- THERMAL Camera
- SCADA System
- RF Radar
- GEOPHONE
- LIDAR
- PMZ Camera
- HUMAN Sensor
- CYBER Sensor

ACTUATOR LAYER
- HITL
- DRONE NEUTRALIZATION
- DOUBLE VIRTAL.
- FAULT LOCATION AND SERVICE RECOVERY