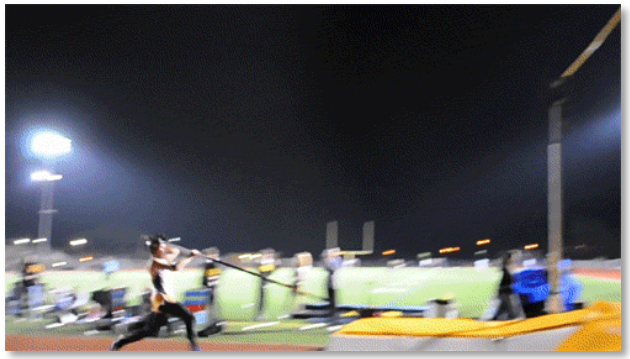
SMART GRID PROTECTION AGAINST CYBER ATTACKS

# SPARKS Cybersecurity Technology and the NESCOR Failure Scenarios

Lucie Langer and Paul Smith
firstname.lastname@ait.ac.at
AIT Austrian Institute of Technology

ComForEn Workshop
Monday 29th September, 2014




EU FP7 Programme Contract No. 608224

# SPARKS Security Technologies

- The SPARKS project will develop a number of security and resilience technologies

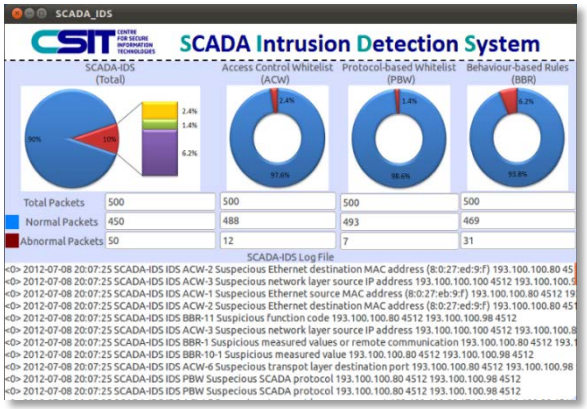
1. SCADA-specific intrusion detection systems
2. Physical Uncloneable Functions (PUFs) for smart meters and gateways
3. Security analytics approaches
4. Resilience control systems


EU FP7 Programme Contract No. 608224

# SCADA-specific intrusion detection systems

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Target is AIT SmartEST Lab demonstration
  - Focus on IEC 61850 protocol
  - Custom SCADA IDS
  - Also develop attack use cases



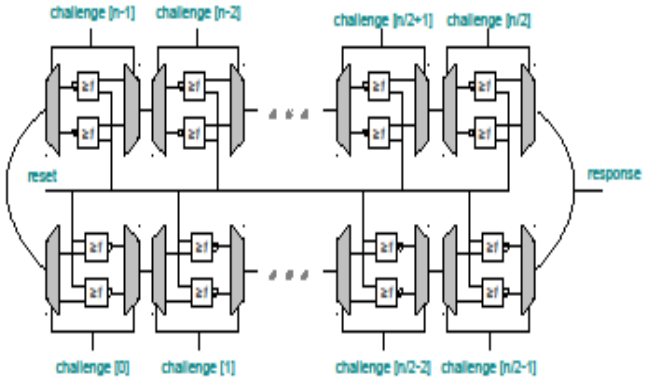

- Development of a multi-attribute SCADA-IDS
  - Identify permitted and non-permitted devices, connections, and protocols
  - Enhanced payload inspection to detect permitted and non-permitted operations and behaviours
  - Whitelist, stateful and behavioural analysis based on 61850 features and SmartEST demo physical system attributes


EU FP7 Programme Contract No. 608224

# Physical Uncloneable Functions (PUFs) for smart meters and gateways

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Physical uncloneable functions
  - use intrinsic physical properties of e.g. hardware to derive a unique uncloneable function
  - can be used as identity, secret key, etc.



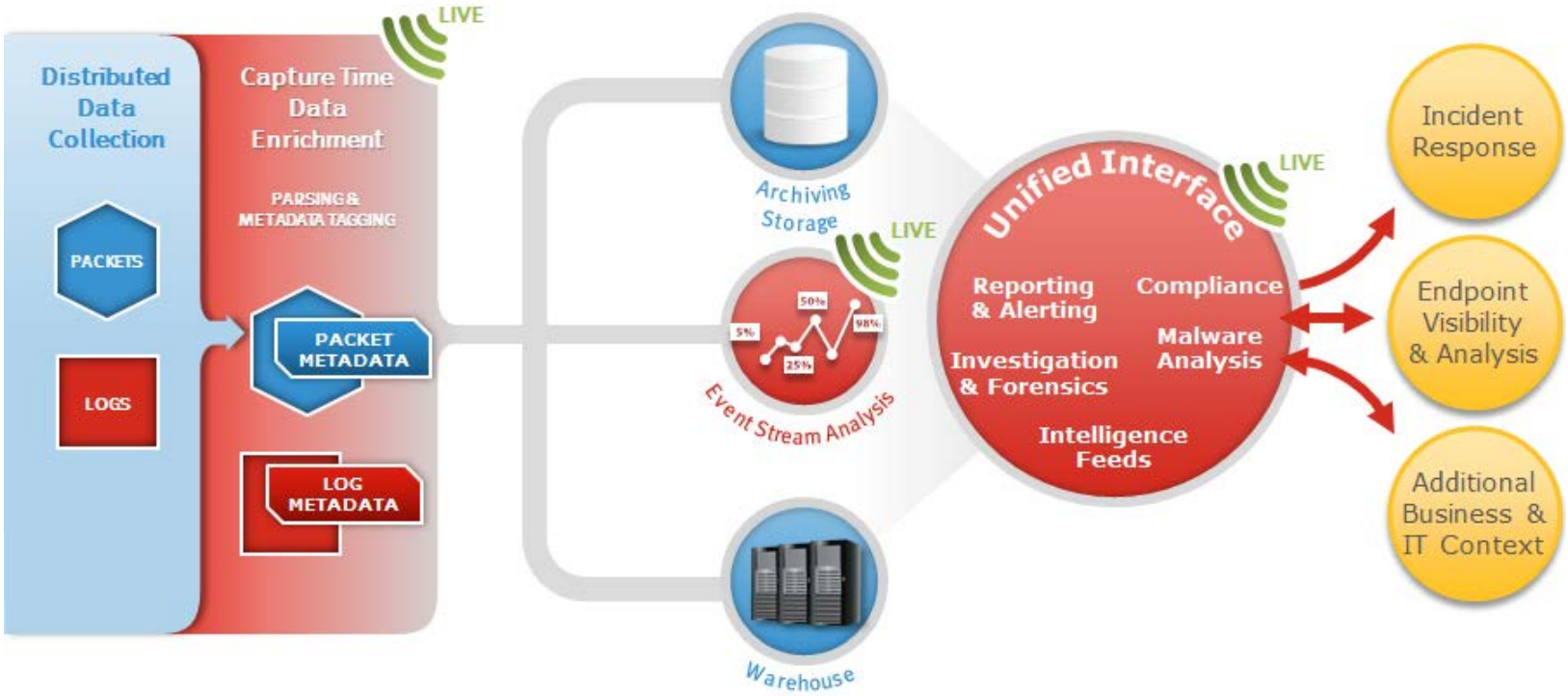

- Smart meters
  - exposed to physical attacks
  - PUF can act as a security anchor without dedicated security module



EU FP7 Programme Contract No. 608224

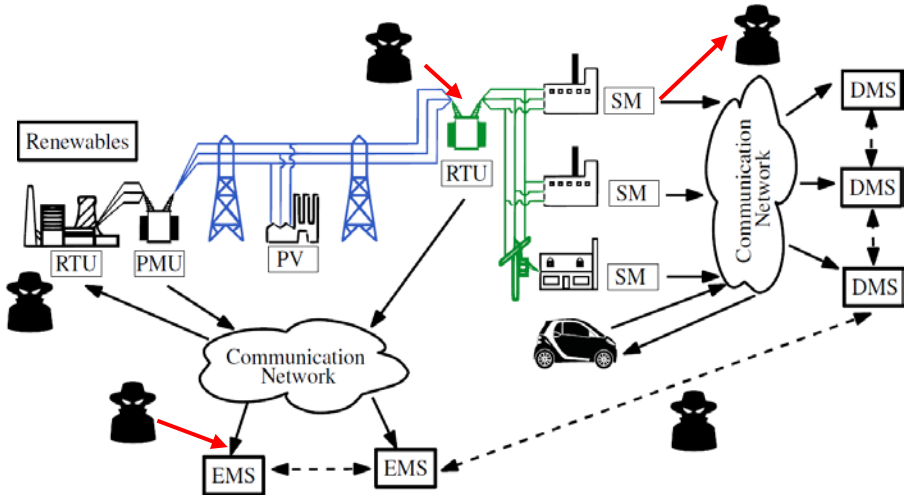
# Security analytics approaches

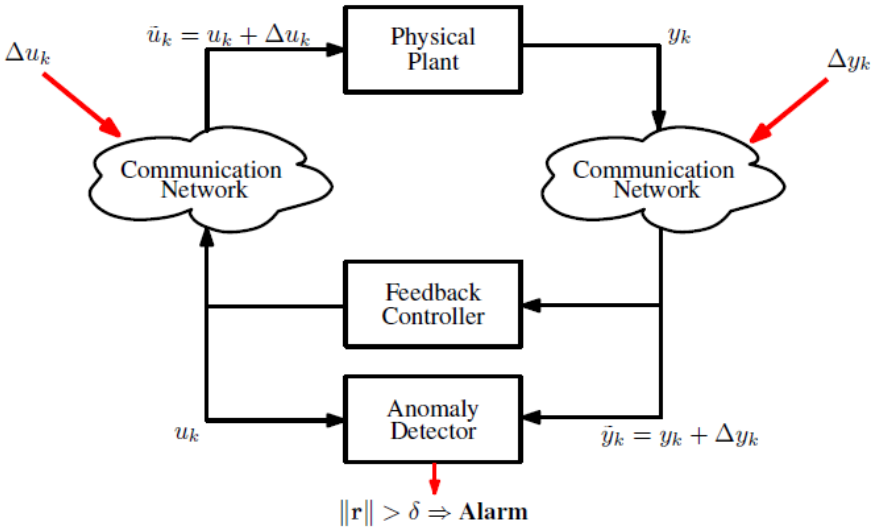
- Machine learning algorithms of big data to identify anomalous operation



# Resilient Control Systems

- Resiliency to disturbances and malicious threats
  - Maintain state awareness
  - Accepted level of performance




- Obtained through
  - automated fault detection
  - controller reconfiguration (islanding, for example)

# NESCOR (National Electric Sector Cybersecurity Organization Resource) Cyber Security Failure Scenarios

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Intended to be used by utilities for risk assessment, planning, training, security testing
- Realistic events in which the failure to maintain C-I-A of cyber assets has a negative impact on the generation, transmission, and/or delivery of power
- Organised in six categories (see NIST SP 1108):
  - **AMI**: Advanced Metering Infrastructure
  - **DER**: Distributed Energy Resources
  - **WAMPAC**: Wide Area Monitoring, Protection, and Control
  - **ET**: Electric Transportation
  - **DR**: Demand Response
  - **DGM**: Distribution Grid Management

# Example: Inadequate Access Control of DER Systems Causes Electrocution (DER.1)

- Description:
  The DER owner fails to change the default password or not set a password for the DER system user interface. A threat agent (inept installer, hacker, or industrial spy) gets access through the user interface and changes the DER settings so that it does not trip off upon low voltage (anti-islanding protection), but continues to provide power during a power system fault.

- Relevant Vulnerabilities:
  - Lack of access control,
  - Lack of mandatory change from default password,
  - Poor configuration design of the DER system that permits unauthorized changes to anti-islanding protection,
  - Insecure communication protocol between the user interface and the DER system that allows unauthenticated changes to sensitive parameters.

- Impacts:
  - DER system suffers physical damage due to feeding into a fault,
  - A utility field crew member may be electrocuted,
  - The utility experiences damage to its reputation due to smart grid anomalies.

# Ranking Method

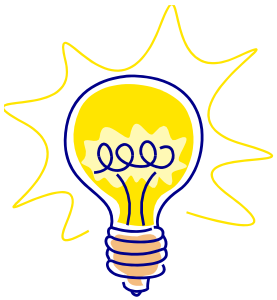
- Used for prioritising the failure scenarios in terms of „attractiveness“ for the adversary
- Two criteria:
  - Impact
  - Cost to the adversary
- Possible scores: 0 (0.1); 1; 3; 9
- Ranking = Impact / Cost

# Assessment Criteria (Examples)

- Impact
  - 0: one customer out of power for 15 mins, petty cash expenses
  - 1: small generation plant offline
  - 3: 20% of customers experience defect from smart meter deployment
  - 9: large transformer destroyed and major city out of power for a week

- Cost to the adversary
  - 0.1: failure scenario can be triggered easy and at almost no cost
  - 1: a bit of expertise and planning needed (e.g. .capture keys off unencrypted smart meter bus)
  - 3: serious expertise and planning needed
  - 9: needs nation-state resources (e.g. Stuxnet)

# Breakout Session



- Split into groups of two and appoint a spokesperson
- Assess the NESCOR cybersecurity failure scenarios for impact and threat agent cost
  - Impact: 0, 1, 3 and 9
  - Cost to the adversary: 0.1, 1, 3 and 9
- Consider whether each failure scenario would be possible in EU / Austria
- Discuss your assessments with the group

# Acronyms

- AMI: Advanced Metering Infrastructure
- CAN: Car Area Network
- DERMS: Distributed Energy Resources Management System
- DGM: Distribution Grid Management
- DMS: Distribution Management System
- DRAS: Demand Response Automation Server
- EVSE: Electric Vehicle Service Equipment
- PMU: Phasor Measurement Unit
- WAMPAC: Wide Area Monitoring, Protection, and Control


EU FP7 Programme Contract No. 608224