IT-Security for Smart Grids in Germany: Threats, Countermeasures and Perspectives

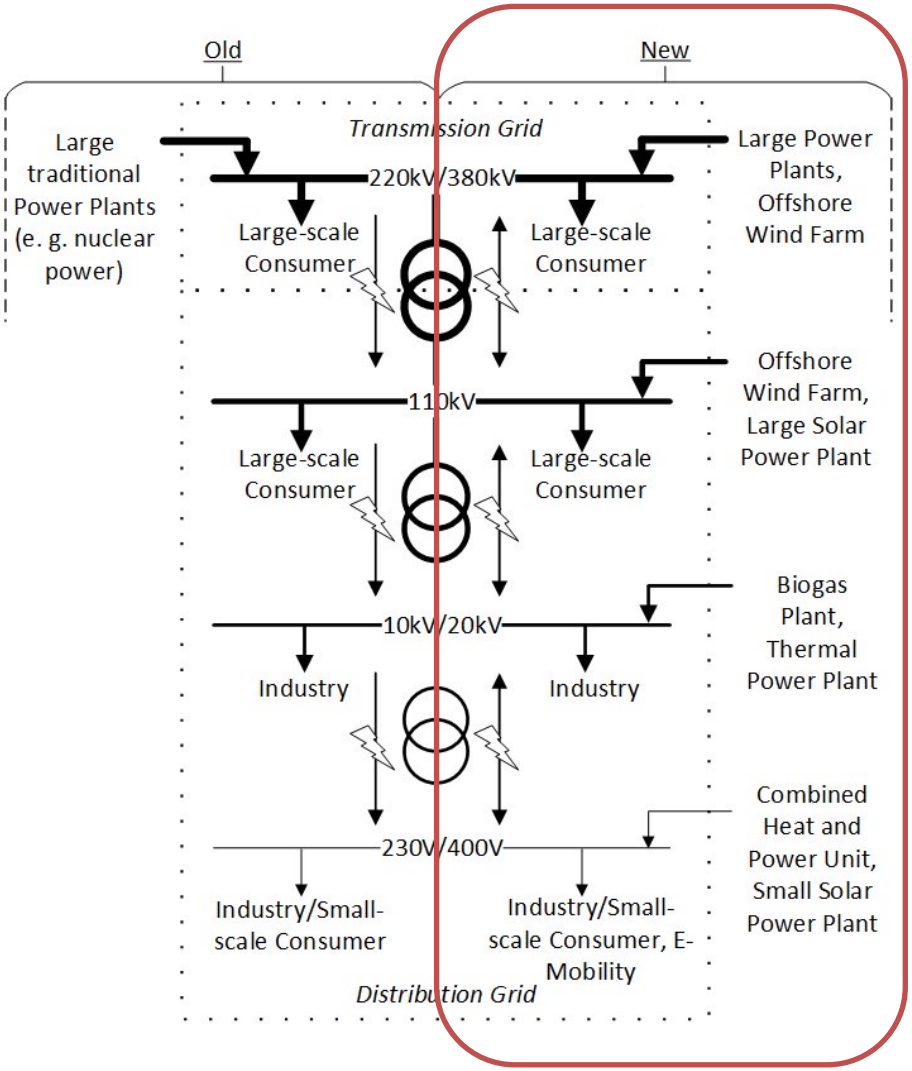
Carl-Heinz Genzel, Olav Hoffmann, Richard Sethmann
University of Applied Sciences Bremen
Flughafenallee 10, 28199 Bremen, Germany

Index

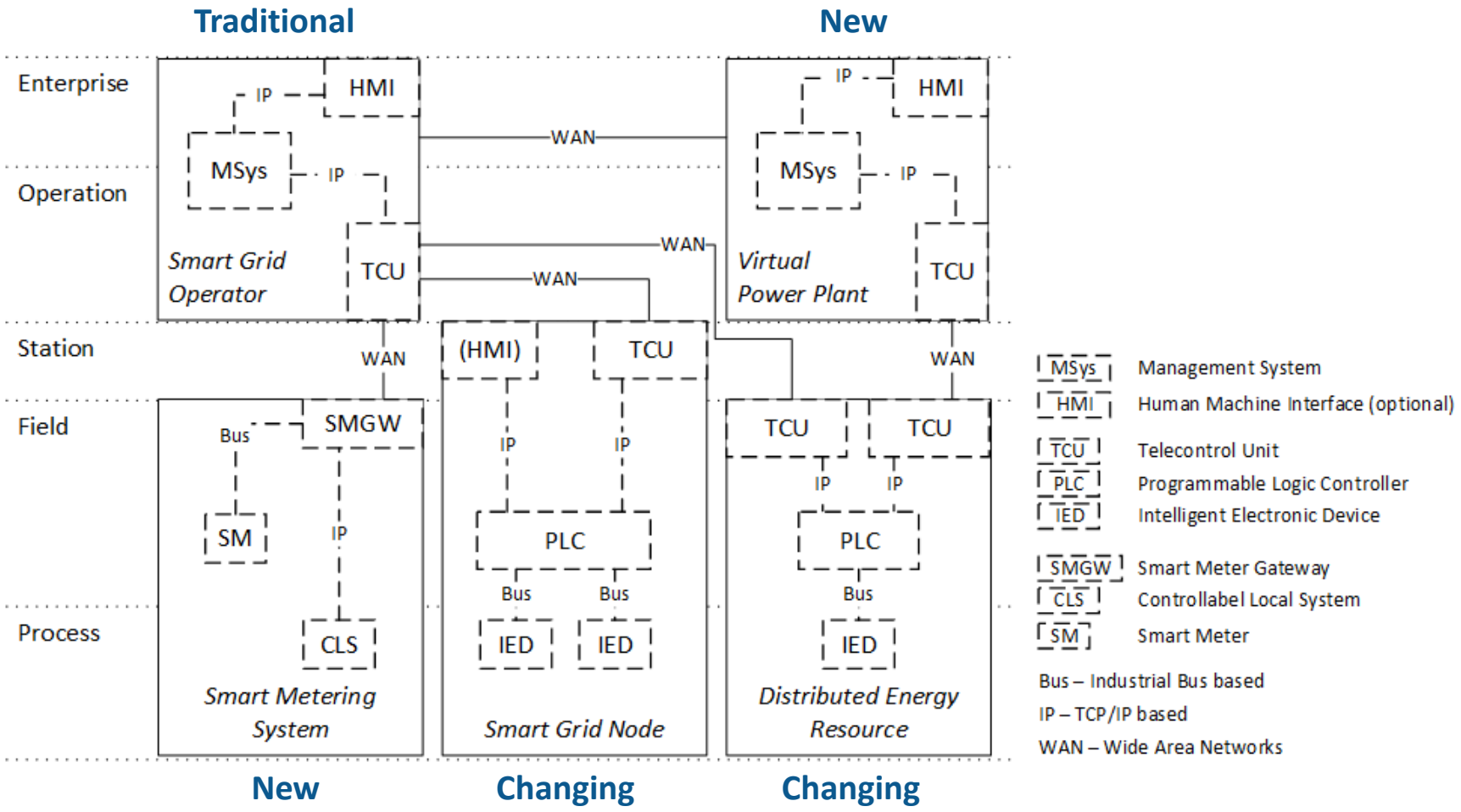
1. Introduction
2. Near future distribution grid
3. Threat modelling
4. Security recommendations
5. Conclusion
6. Prospects

Introduction

- Sustainable energy transition changes traditional energy flows
  - Renewable energy resources are connected to the distribution grid
  - Renewal energy resources are often volatile and unreliable
- Distribution grids must become intelligent for a successful transition
  - Intelligent and interconnected ICT systems are needed for grid stability
  - Trend towards standardized hard- and software to improve ICT stability
- **Security threats from the traditional ICT field become applicable in distribution grids**



Near future distribution grid



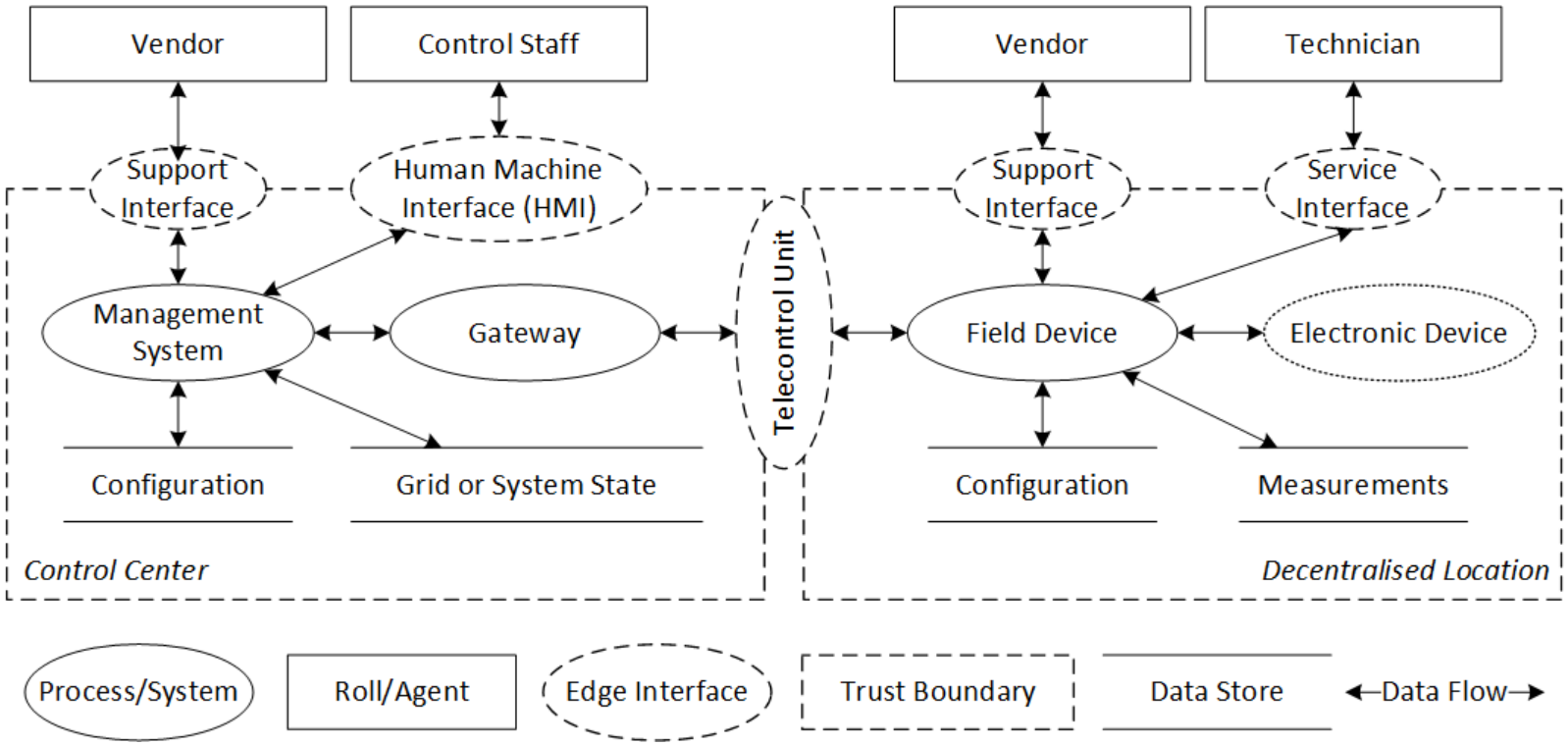
Threat modelling: Methodology

- Threat modelling using STRIDE based on OWASP Application Threat Modelling

- Approach
  - Scope definition
  - System model creation (data flow model)
  - Threat modelling (qualitative approach)
  - STRIDE categorisation
  - Comparison with existing threat considerations

Threat category	Security control
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Threat modelling: Scope



Control Center

- Distribution grid operator
- Virtual power plant

Decentralised Location

- Grid node (e. g. substation, cable cabinet)
- Distributed energy resource or distributed energy storage

Threat modelling: Scope

- Threat categories
  - Acts of god -> not included: no malicious attempt
  - Organisational flaws -> not included: ISO/IEC 27001 must be applied in Germany
  - Human mistakes -> not included: ISO/IEC 27001 must be applied in Germany
  - **Malicious acts -> included: malicious attacks are likely with new technologies**
  - **Technical malfunction -> included: new technologies are susceptible to malfunction especially at the beginning**
- Emphasis on external attackers

Threat modelling: Constraints

- Focus on threats that compromise the security perimeter and interfaces of decentralized locations
- Systems should be up to date and under regular maintenance
- Administrators and system vendors must be trustworthy
- System vendors need to fulfil the same security requirements as grid operators, if they need access
- System vendor access is explicitly controlled by the grid operator
- Decentralised locations are physically separated from the open space (e.g. fence, building, room, etc.)
- Local service ports are not reachable from remote
- Physical denial of service is out of scope

Threat modelling: Results

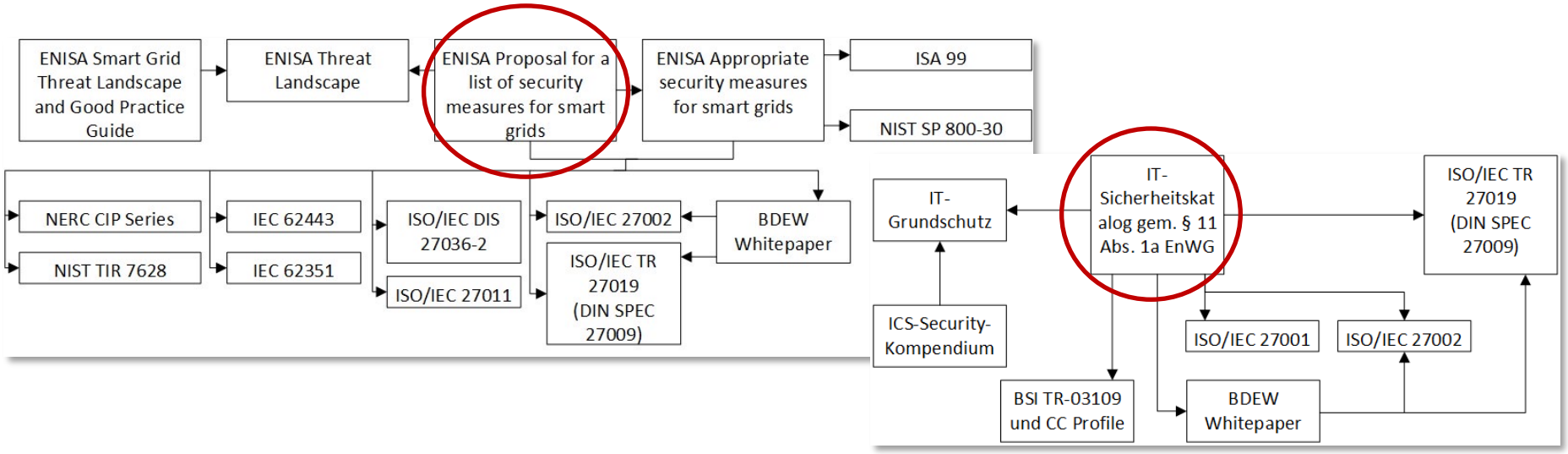
- 58 threats deduced in total
- Decentralised energy resources have special access requirements (9 threats)
- Field devices are most vulnerable (19 threats)
  - Field devices have the least security measures in place
  - Functionality is more important than security
- Most threats refer to information disclosure (18 threats) and tampering (11 threats)
  - Cryptographic and security measures are still under development

Threat modelling: Results

1. Integrity: Manipulation of control and measurement data can cause a faulty grid state and a power breakdown is likely.
2. Confidentiality: National laws about IT security and privacy must be met but power breakdown is unlikely.
3. Availability: Systems in the field are self-sufficient to a certain degree and able to maintain a stable distribution grid state without a control centre for a limited amount of time.

Security recommendations: Standards

- Most threats can be mitigated, if different security standards are applied together properly; especially:
  - Summary of important international standards by the European Network and Information Security Agency
  - German “IT-Sicherheitskatalog” with mandatory security requirements for energy grid operators



Security recommendations: Monitoring

- Grid status is closely monitored, but ICT components are often left out
  - “Blind Spot” -> ICT failures are not distinguishable from electronical failures
  - Diagnosis becomes more complicated -> loss rates increase
- “Blind Spot” due to inadequate systems and know how
  - Field devices do not support common ICT monitoring protocols in many cases
  - Especially smaller energy grid operators do not have enough ICT know how to establish proper ICT monitoring
- Monitoring of ICT components must be part of the grid operation for an efficient failure diagnosis
  - In Germany it is also required by law in regard to the “IT-Sicherheitsgesetz”

Security recommendations: Access & Integrity

- Decentralised locations are easier to attack
  - Decentralised locations are harder to supervise and protect, in general
  - Unauthorized access to decentralised locations and systems is often easier than to central company premises
  - Decentralised energy resources need to be accessible by different stakeholders, with different interests
- Access protection is needed on a physical and logical level
  - E.g. separate rooms, closets, AAA measures, IEEE 802.1X, etc.
- Integrity of a system must be accountable at any time physically and/or logically
  - E.g. official seals, Trusted Computing, etc.

Conclusion

- Distribution grids are mainly affected by the transition to smart grids
- ICT in decentralised locations create new security risks
- Integrity is the most important security aspect in energy grids
- Most security issues do exist, because existing security standards are not properly recognised
  - System/device vendors are as responsible as well as energy grid operators
- ICT monitoring capabilities have to be improved to avoid a “Blind Spot”
- Physical and logical integrity protection and access control is needed for the new components
  - especially in shared decentralised locations

Prospects

- Provide education
  - Summary of standards for energy grid operator staff, new to ICT security
  - Prioritisation of countermeasures according to our results about risks and core threats
- Develop secure systems
  - Adaptation of known ICT security solutions for this field of application
  - Addition or integration of security measures into field devices (Next Generation Industrial Control System)
  - Development of domain specific monitoring concepts

Thank you

Questions?