Hochschule Bremen
City University of Applied Sciences

HSB

Automated Monitoring of Operational Technology Security and Compliance for Power Grids - Enhancing Trust by Continuous Security Configuration Monitoring

Karlsruhe 4th April 2022 – Bastian Fraune M.Sc. Informatik, City University of Applied Sciences Bremen

Inhalt

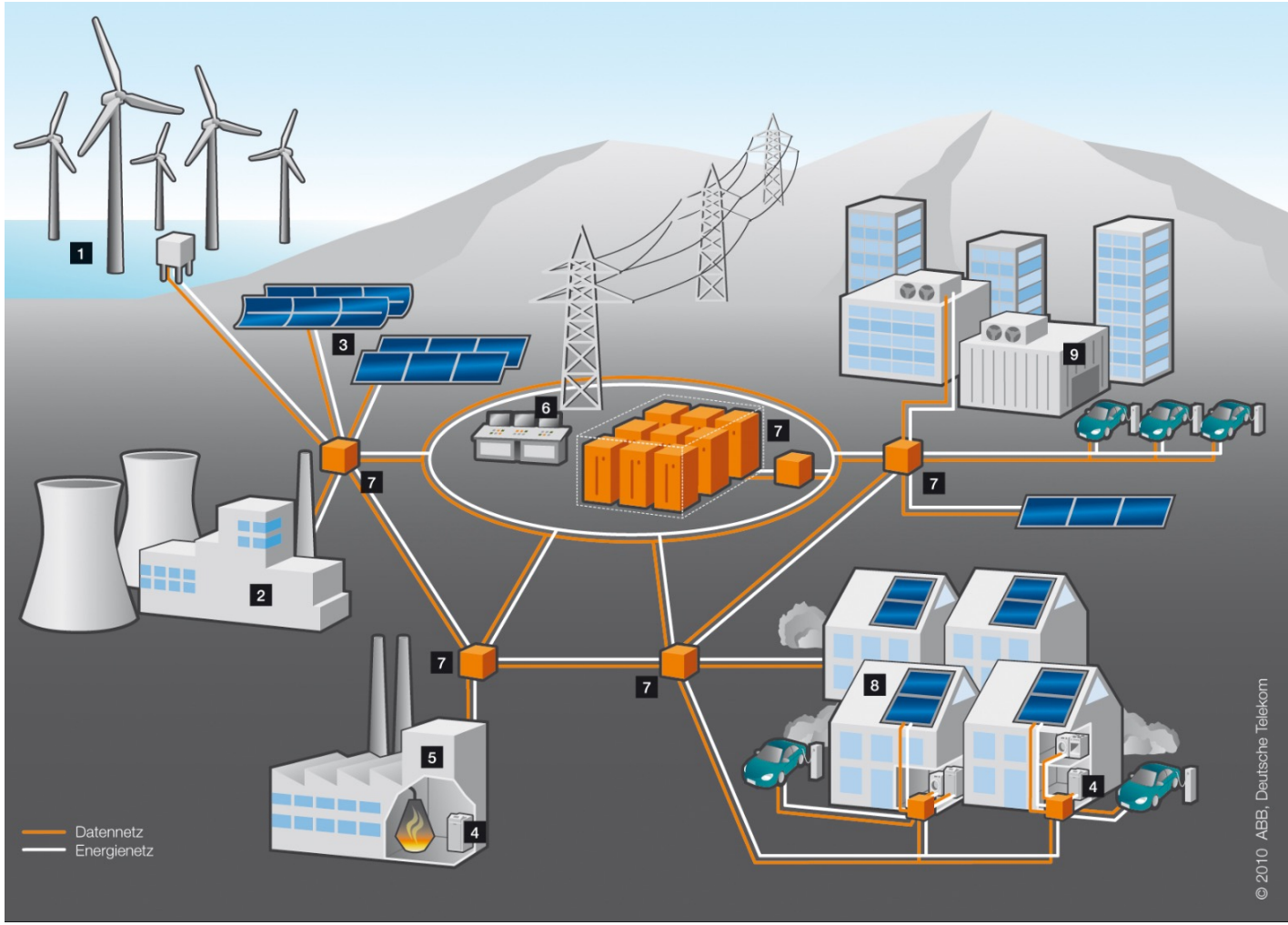
Power Grid Transition

Energy transition

- Decentralized generation
- „Prosumers“: generate and consume energy
- Requires much more (intelligent) digital coordination

Cybersecurity

- Broader attack surface
- ICT is backbone of Smart Grids [Bu20]



Physical- and Information Flow in Energy Domain

Electrical Flow

- Manged by SCADA systems

Information Flow

- Strong linkage between
  - Market
  - Operations, Service
  - Electrical Grid
- ICT is backbone of Smart Grids [Bu20]

Cyber-Attacks

"High-Wattage" Botnets [Sh21]

- Botnet controls high-wattage devices
- Spontaneously raise the energy consumption
- Currently: Theoretical calculations

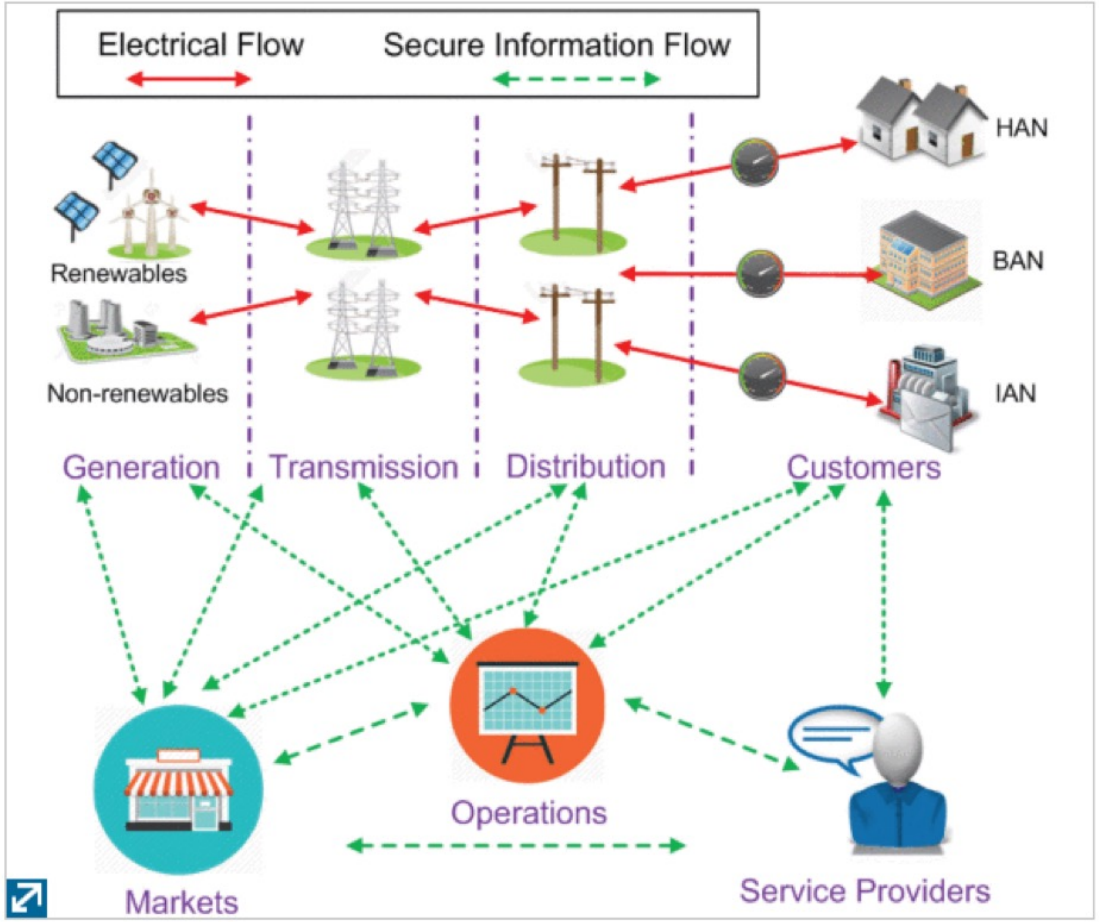


Figure 1: NIST Smart Grid Referencemodel [2]

Typical Issues in Industrial Controllable System's Components

Typical issues

According to BSI ICS Security Compendium [Bu21]

- Insecure configuration
- Insufficient documentation
- Inadequate monitoring
- Insufficient access control
- Manipulation and sabotage of ICS components
- Manipulated firmware
- Insufficient user- and authorisation management
- Insufficient logging
- Application of unsecure protocols
- Denial-of-Service (DoS) attacks
- Malware
- Information spying
- Insufficient safety requirements in procurement

Standards as Countermeasures

ISO 27001 [IS17]

- Process to manage information security
- Defines requirements
- Forced §11 section 1b German „Energiewirtschaftsgesetz“

IEC 62351

- Standard for Operatin Technology in Power Grid
- Security requirements
- Technical

ISO 27001 and NIST SP800-53

- Require the monitoring of configurations
- Require a configuration management and process

NIST SP 800-128:

- “*Monitoring the configuration of systems to ensure that configurations are not inadvertently altered from the approved baseline*” [NIST SP 800-128, Ch. 3]

Research Questions

Objectives

- Automate security configuration assessment of devices within the smart grid

PhD focus on

- Collection of security configurations for substation devices
- Data transmission via common IEC protocols
- Provide assessment data for control center (i.e. IEC 61970)

Future vision

- Integrate assessment into ICTmonitoring systems
- Use for automated security audits (~ ISO 27001)
- Use for trust between devices

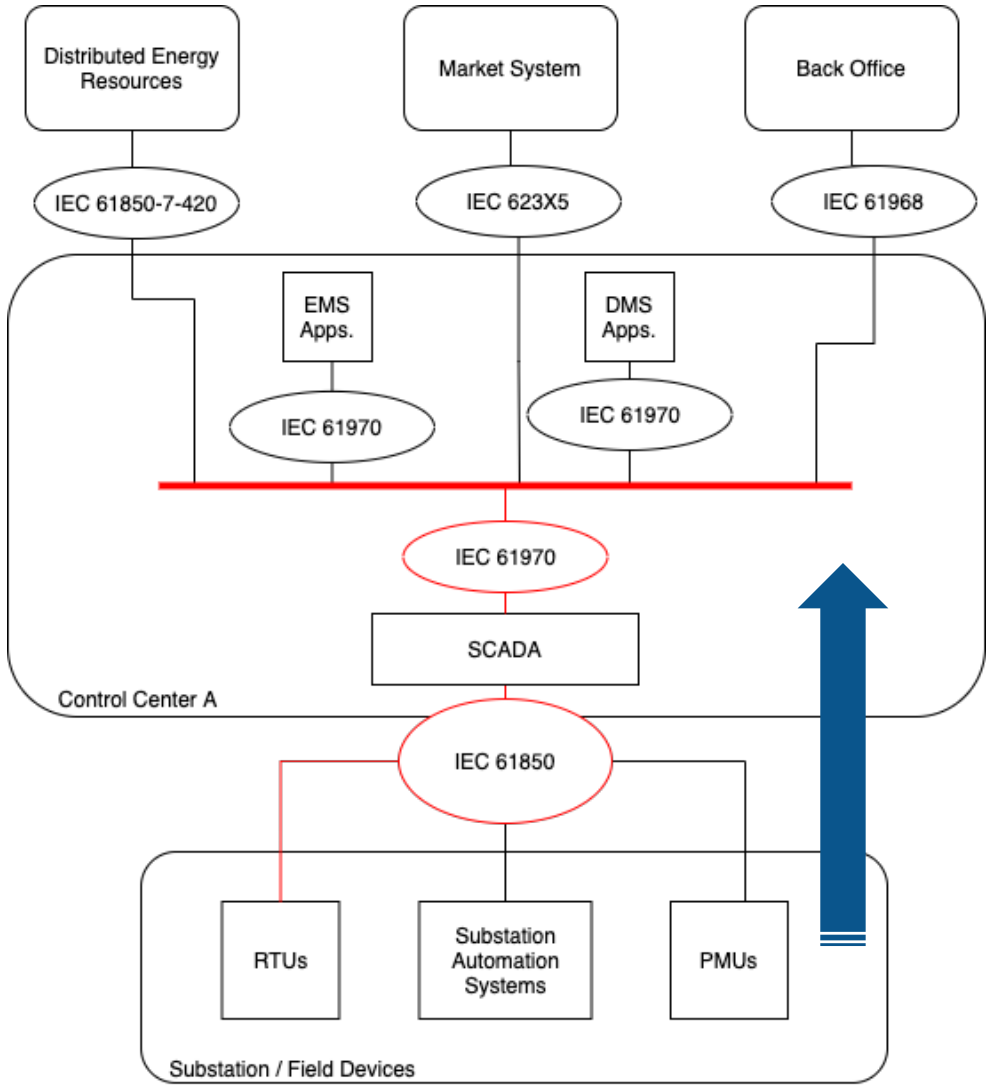


Figure 1: Simplified TC 57 Model Architecture, depiction: own, source: IEC 62357 (TC 57 SIA),

Research Question

How can automated monitoring of technical security configurations,

for SCADA components in the energy distribution domain, be enabled?

RQ 1
Which security features are relevant from the view of existing domain standards?

RQ 2
How can existing information models from ICT monitoring be considered?

RQ 3
How can concepts of Trusted Computing support this?

How will I achieve it / My Concept

RQ 1: Which security features are relevant from the view of existing domain standards?

1. Identify relevant standards / requirements by extensive literature and standards research
2. Derive security features requirements
3. Map requirements to measurable entities

RQ 2: How can existing information models from ICT component monitoring be considered?

1. Identify relevant information models by literature research

RQ 3: How can concepts of Trusted Computing support this?

1. Integration of root of trust into energy standards
2. Propose data and information model
3. Prototyping

Design Science Research Process (DSRP)

Design Science Research Process from Peffers et. Al [Pe20]

- Extension of Hevner et. al's version

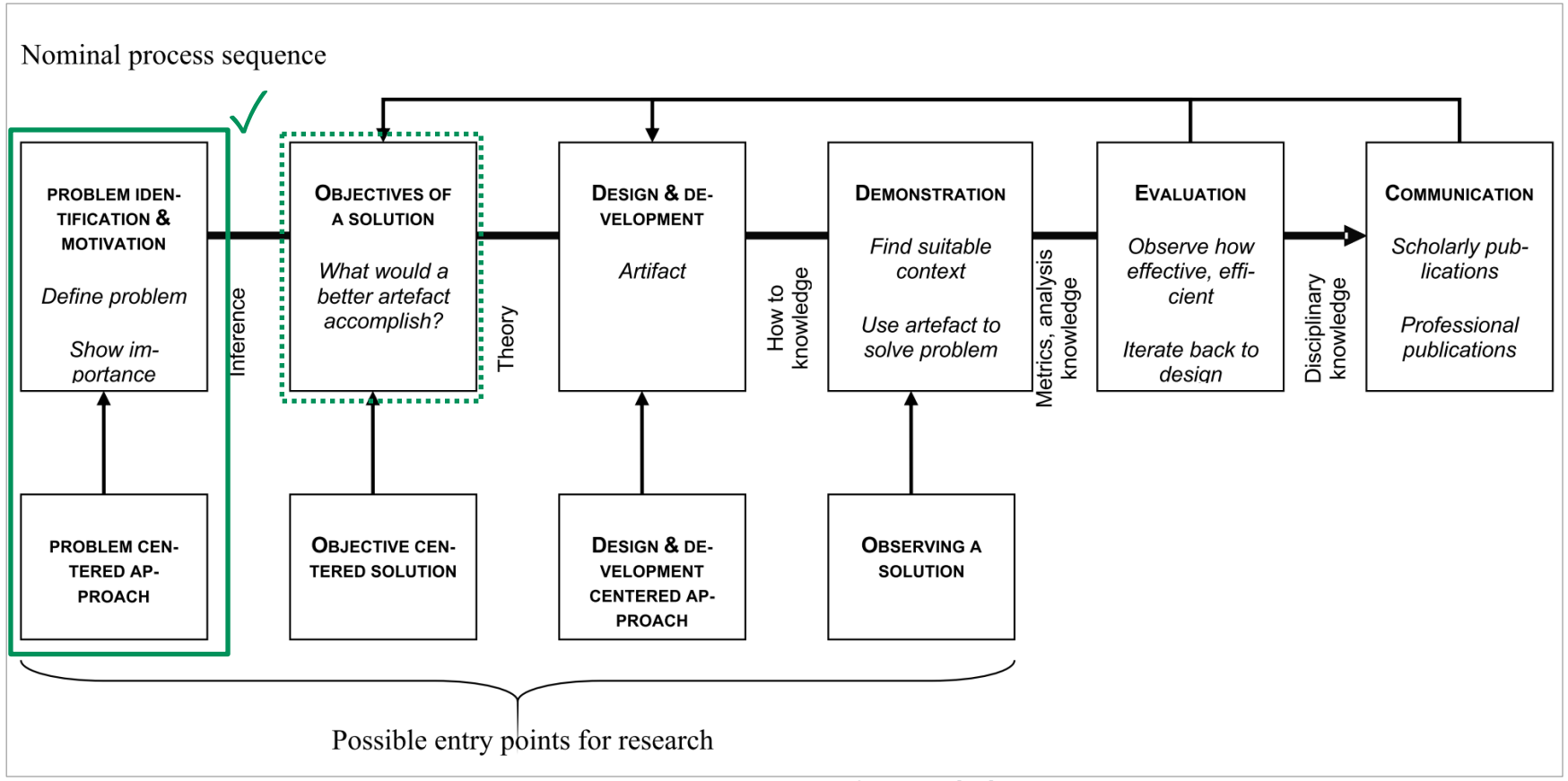


Figure 11: Design Science Research Process, Peffers et. al [14]

Related Work

What have others done?

Security Configuration Assessment for Android [Na18]

- Tool extracts 41 security related settings
- No common information model
- No specified software interface

→ Android only

Simple Network Management Protocol (SNMP)

- Standardised in RFC 3410-3418
- Original purpose
  - Management of network devices
  - Configuration of network devices

→ Can it be used? / What could be used?

Security Protocol and Data Model Specification []

For hardware components

- Message exchange for security capabilities
- Identity authentication
- Firmware and configuration measurement
- “Secure Sessions”
- Mutual authentication
- Made for office computer / technologies

→ Which components are suitable for energy informatics?

What have others done?

Information Security Automation: How Far Can We Go?

- Investigated ISO 27001 + NIST SP 800-53
- ISO 27001: 37 controls (27,8%)
- NIST SP 800-53: 62 controls (31,3%)

- Reflect controls where no human intervention is necessary
  - Audit logging
  - Network connection control
  - Physical entry control
  - Backup scheduking / automation
  - Access control logging

→ Office IT

Security Content Automation Protocol

- U.S. standard maintained by NIST
- Exchange security automation content
- Assess configuration compliance
- According framework is OpenSCAP
- Suite of specifications

→ Office IT

Research Gaps

- No (common) information model for security configurations
- Linking trusted computing technologies with security configurations
- How to derive a data model that can be used within current protocols
- Which existing information models can be adopted for the energy domain
- Which components need to be newly designed?

Summary & Discussion

Summary / Discussion points

Main problem

- Security configurations not considered for device assessment
- Requirements (derived) from standards cannot be assessed in an automatic way

OT device configurations need to be monitored

- Required by security standards
- No standard to achieve it in an automatic way

Dissertations objectives

- Enable automatic monitoring of security configurations on OT devices
- Provide a secure standardised solution
- Supports the automation of compliance monitoring

Discussion

- Which measures for a successful evaluation?
- What about security metrics? Which and how…?

Bibliography / Sources

[Sh21] T. Shekari, C. Irvene, A. A. Cardenas, and R. Beyah, “MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets,” *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1338–1356, 2021.

[Bu20] B. M. Buchholz and Z. A. Styczynski, “Advanced Information and Communication Technology: The Backbone of Smart Grids,” in *Smart Grids*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2020, pp. 297–366.

[Bu21] Bundesamt für Sicherheit in der Informationstechnik (BSI), “IT-Grundschutz-Kompendium 2021,” 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5.

[IS17] ISO Central Secretary: Information technology - Security techniques - Information security management systems - Requirements. Standard ISO/IEC 27001:2017, International Organization for Standardization, Geneva, CH, 2017.

[Pe20] K. Peffers *et al.*, “Design Science Research Process: A Model for Producing and Presenting Information Systems Research,” Jun. 2020.

[Na18] National Institute of Standardization and Technology (NIST): , Security Content Automa- tion Protocol - Project Overview, 2018.

Hochschule Bremen
City University of Applied Sciences

HSB

Automated Monitoring of Operational Technology Security and Compliance for Power Grids - Enhancing Trust by Continuous Security Configuration Monitoring

Karlsruhe 04. April 2022 – Bastian Fraune M.Sc. Informatik, City University of Applied Sciences Bremen