AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Security Challenges in Smart Distribution

Thomas Bleier

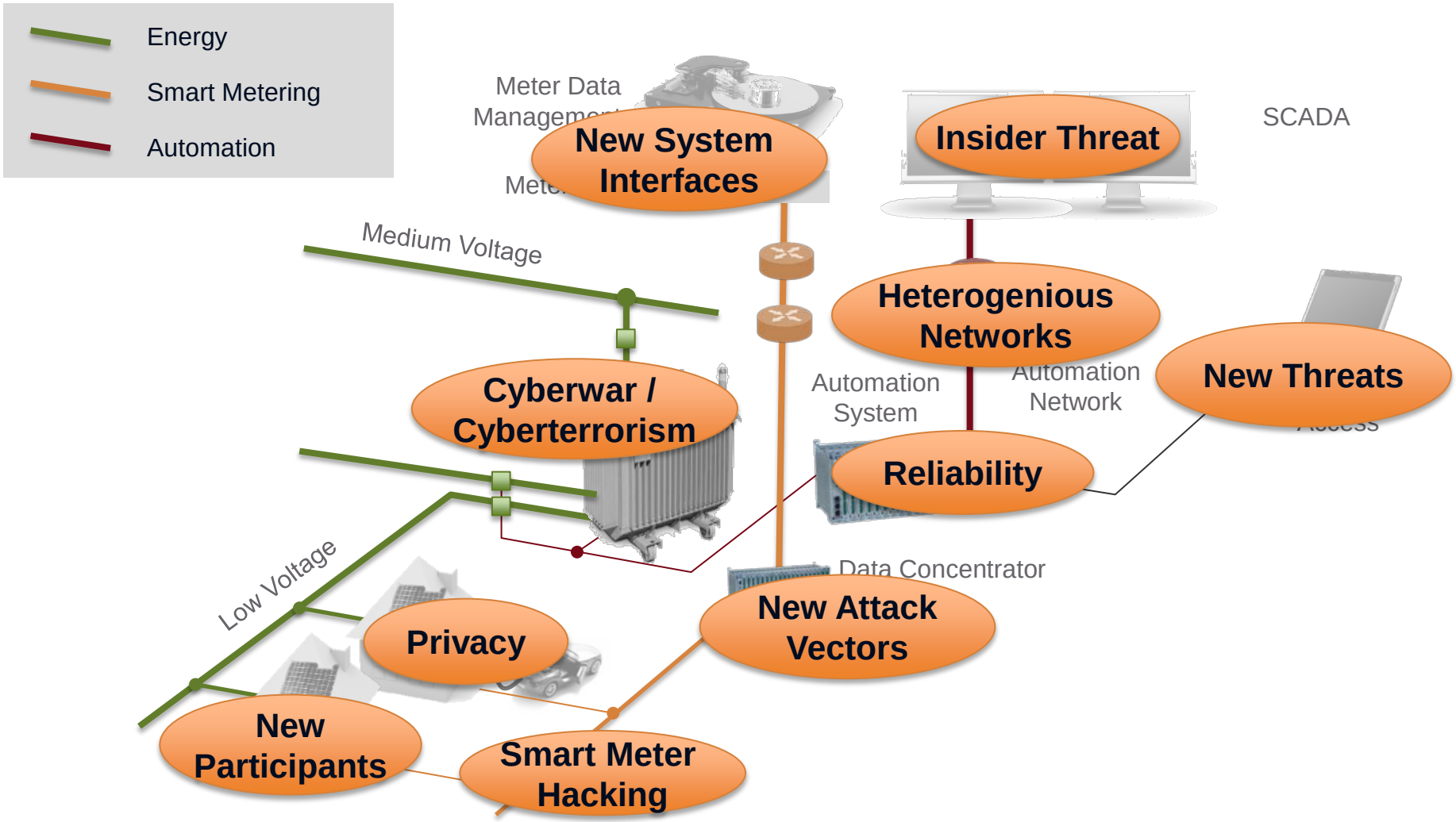
Dipl.-Ing. MSc zPM CISSP CEH CISM

Thematic Coordinator ICT Security

Safety & Security Department

AIT Austrian Institute of Technology GmbH

Smart Secondary Substation



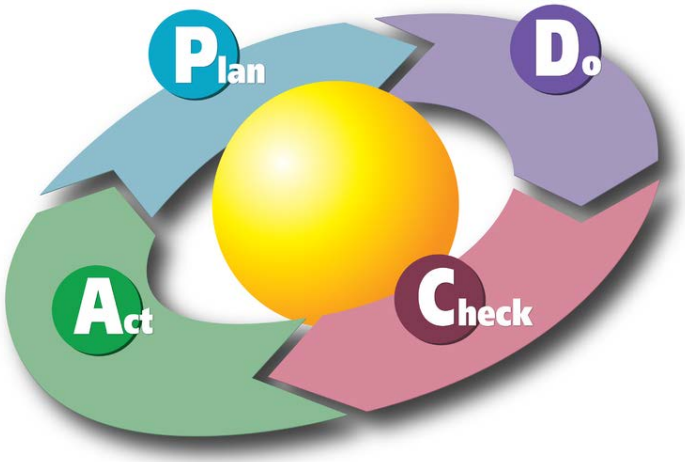
Security Challenges in Smart Distribution

- Processes and Organizing Security
- Secure Development and Comissioning
- Secure Communication
- Secure Operation
- Physical Security
- Incident Management

Based on existing Standards and Best Practices like ISO 27002, ENISA Appropriate security measures for Smart Grids,
NIST Guidelines for Smart Grid Cyber Security, NERC CIP, IEC 62443, etc.

Processes and Organizing Security

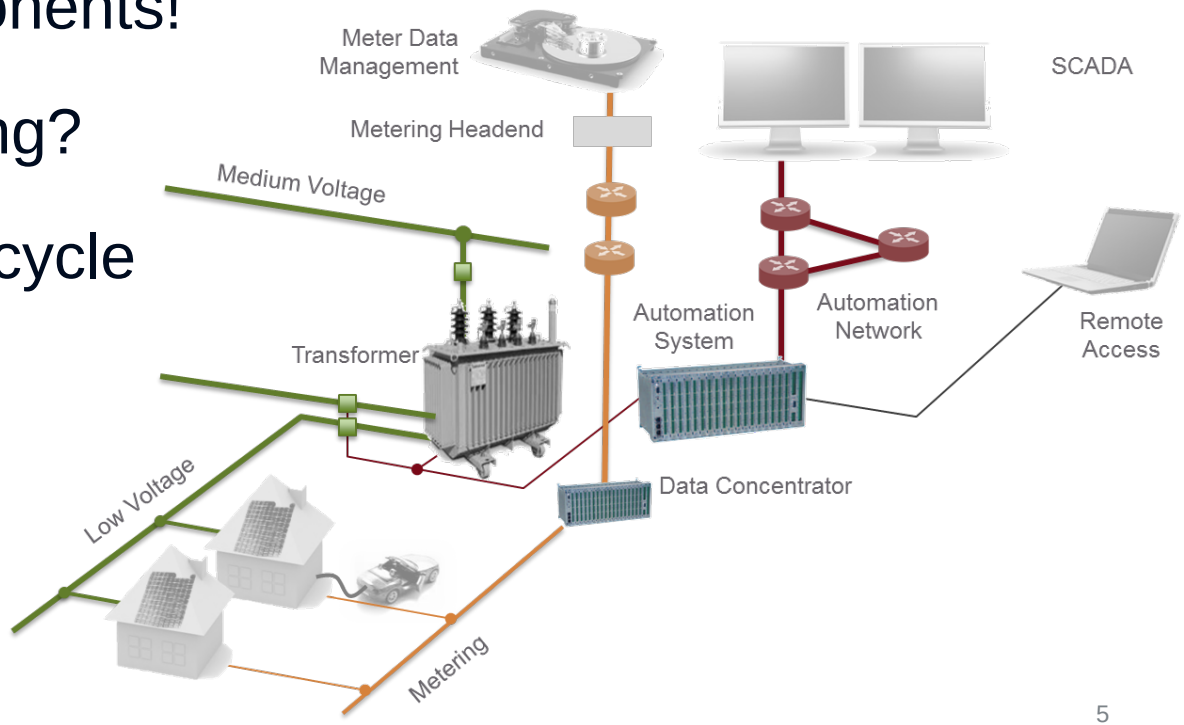
- Information Security Management
  - General Purpose IT: ISO 2700x, BSI Grundschutz, NIST SP 800-53
  - Industrial Automation: ISA 99 / IEC 62443, NIST SP 800-82
  - (Smart) Grid: ISO 27019, NERC CIP, BDEW, ENISA, OE, etc.
- Risk Management
- Compliance and Certification
  - ISO 27001, NERC CIP or specific standards?
  - Mandatory?



Wikimedia Commons - Diagram by Karn G. Bulsuk (http://www.bulsuk.com)

Secure Development and Comissioning

- Secure Development Processes
  - NIST SDL, MS-SDL, ISSECO, etc.
  - Requirements, Threat Modelling, Code Analysis, Penetration-Tests, Incident Response Processes, etc.
- For all new components!
- What about existing?
- Comissioning/Lifecycle



Secure Components

- COTS vs. Industry components
- Internet-Technology vs.
  Industrial Automation
- Functional Safety (IEC 61508) vs.
  IT Security (ISO/IEC 15408 Common Criteria)
- Cryptography – Lifecycle, Low Power, etc.
- Tests and Certification
- Supply Chain Management

© c't

Secure Communication

- Protocols from the Automation/Energy World
  - IEC 61850, IEC 60870, DNP3, etc.
- vs. Protocols from the Internet/Business IT
  - HTTP, SOAP, REST, etc.
- Security-Extensions…
  - SSL/TLS, IEC 62351, IPsec, SAML, XACML, etc.
- Availability vs. usage in practical applications
- Protocol design goals vs. application scenarios
- Privacy-Requirements vs. Functionality

Secure Operation

- Complexity (Operating Personell)
- Vulnerability Management, Patch Management
  - → Configuration Management
- Third Parties, Suppliers
  - Responsibilities
- Access Control – Authentification, Authorization, Audit
- Separation of Duties, Least Privilege
- Safety vs. Security – Availability vs. Integrity/Confidentiality

Physical Security

- → Next Talk
- Basic principles stay the same
- But: increase in volume, new technologies available, new challenges
- Important part of a holistic security concept

Incident Management

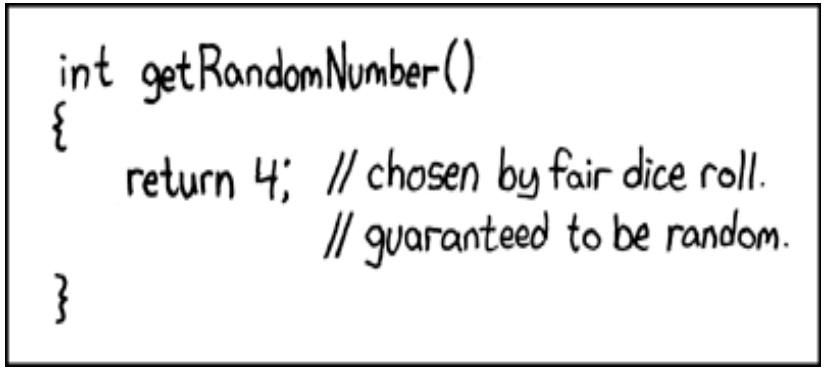
- Response to incidents is key!
- Logging, Monitoring
- Situational Awareness
- Incident Management
- Information Sharing
- Culture – learning from incidents
- Obligatory Reporting?

Appropriate solutions are needed…

- … but don‘t reinvent the wheel!
- Specific Requirements:
  - Risk vs. Security vs. Cost
  - Safety & Security
  - System Lifecycle
- **Appropriate** security levels
  - Not every substations needs to be Fort Knox!
  - But it also should not become an archilles heel…

Security is a joint responsibility…

- … between manufacturers and operators!
- Secure components are **not enough!**
- Secure **commissioning** and **operation**
- Reliance on the security of specific components
- Responsibilities for specific security aspects need to be defined



Prevention, detection and reaction…

- Protection mechanisms are useless without detection of attacks and reaction to them
- System complexity problem
- Responsibility vs. competence
- Situational awareness
- Information Sharing, Reporting

Smart Grid Security Research @ AIT

Research Topics:

- Risk analysis and management for Smart Grids
- Secure architectures for resilient Smart Grids
- Security Lifecycle Tools
- Situational awareness – anomaly detection, incident information sharing

Selected reference projects:

- **SG2** | national (coord) | Smart Grid Security Guidance
- **PRECYSE** | EU FP7 SEC | Prevention, protection and reaction to cyberattacks to critical infrastructures
- **SPARKS** | FP7 SEC (coord) | Smart Grid Protection against Cyber Attacks
- **HYRIM** | FP7 SEC (coord) | Hybrid Risk-Management for Utility Providers

Selected research partners:

AIT Austrian Institute of Technology

your ingenious partner

Thomas Bleier

Dipl.-Ing. MSc zPM CISSP CEH CISM

Thematic Coordinator ICT Security

Research Area Future Networks and Services

Safety & Security Department

thomas.bleier@ait.ac.at | +43 664 8251279 | www.ait.ac.at/ict-security