“Sicherheit” in Smart Grid Control Networks

Michael Niedermeier, Hermann de Meer
michael.niedermeier@uni-passau.de
hermann.demeer@uni-passau.de

University of Passau
1. INTRODUCTION: “SICHERHEIT” IN CONTROL NETWORKS

2. SCADA NETWORKS
   2.1 History & Challenges
   2.2 Protocols

3. SECURITY
   3.1 Protocol & Challenges
   3.2 Protocol Security (IEC 62351)
   3.3 Additional Remarks

4. CONCLUSION
“Sicherheit” is a term that directly leads to two questions:

- **Meaning**
  - “Sicherheit” = Security
  - “Sicherheit” = Safety

- **Possibility**
  - “Sicherheit” = Possible
  - “Sicherheit” = Impossible
SCADA NETWORKS: History & Challenges

- SCADA = Supervisory Control And Data Acquisition
- Includes supervisory computers (with HMI), PLCs, and RTUs
- History of SCADA

1st generation
Monolithic

- Single mainframe
- No networking

2nd generation
Distributed

- Multiple stations
- Connected by LAN
- No standards for protocols
- Security not considered

3rd generation
Networked

- Multiple stations
- Connected by WAN
- First standards for protocols
- “Security by obscurity” still often used

4th generation
Internet of Things

- Usage of cloud technologies
- Connected by WAN
- Mostly standard protocols
- Includes security schemes from ICT (e.g., TLS)
• SCADA communication protocols
  – Many proprietary implementations (not covered here)
  – Several standards developed starting late 1970s

• Analysis of some well-known protocols
  – 1980: MODBUS
  – 1990: DNP3
  – 1990: IEC 60870-5-101
  – 2000: IEC 60870-5-104
  – 2010: IEC 61850

➔ How to judge protocol security?
Security often no key goal in SCADA protocols

High number of vulnerabilities

- **MODBUS**
  - Lack of confidentiality, weak integrity, no authentication

- **DNP3**
  - Originally also lacked confidentiality, weak integrity, no authentication
  - Revisions: DNPSec, DNP3 Secure Authentication

- **IEC 60870-5-101 & IEC 60870-5-104**
  - Lack of confidentiality, weak integrity, no authentication

- **IEC 61850**
  - Security directly based on IEC 62351 ➔ Explained next!
• Security for SCADA networks
  1. Security goals
  2. Adversary model
  3. Attack scenarios
  4. Countermeasure recommendation

• Covered by IEC 62351
• Includes solutions for:
  – DNP3
  – IEC 60870-5-101
  – IEC 60870-5-104
  – IEC 61850
IEC 62351 is a “well-balanced” security solution

- Threat scenarios / possible attack vectors
- Security recommendations for 60870-5-based protocols (HMAC, TLS, encryption)
- Access control model (role-based)
- Backward compatibility

However, IEC 62351 still lacks

- Advanced cryptographic algorithms (e.g., elliptic curve encryption, high key length)
- Accuracy and completeness (e.g., keys management recommendations)
- Performance considerations
- Application layer end-to-end security in multi-hop environments
Many other domains require security besides SCADA protocols

- Network architecture
- Personnel training
- Risk assessment and management
- Change and patch management
- Business continuity / disaster recovery planning
- Safety challenges

Luckily, standards exist that help here

- ISO/IEC 2700x: Information Security Management System
- ISO/IEC 31000: Risk management
- IEC/EN 61805: Functional Safety
Is “Sicherheit” in SCADA networks achievable?

- Many legacy devices
- 24/7 availability requirement
- Real-time constraints
- Rising attack numbers
- Financial strain for companies

- Advancing protocol standards
- Adoption of security concepts by IEC 62351
- Dedicated security solutions for SCADA available
- Standards available for both security and safety
- Long term benefits of security

„Sicherheit“ achievable, but not always achieved!
• Michael Niedermeier
  
  📧 michael.niedermeier@uni-passau.de
  
  📞 +49 851 509 3056

• Hermann de Meer
  
  📧 hermann.demeer@uni-passau.de
  
  📞 +49 851 509 3051
  
  📬 +49 851 509 3052