Informationssicherheit für SCADA-Systeme

Informatik Kolloquium an der FH Trier

23. Juni 2010

Prof. Dr. Konstantin Knorr

knorr@fh-trier.de

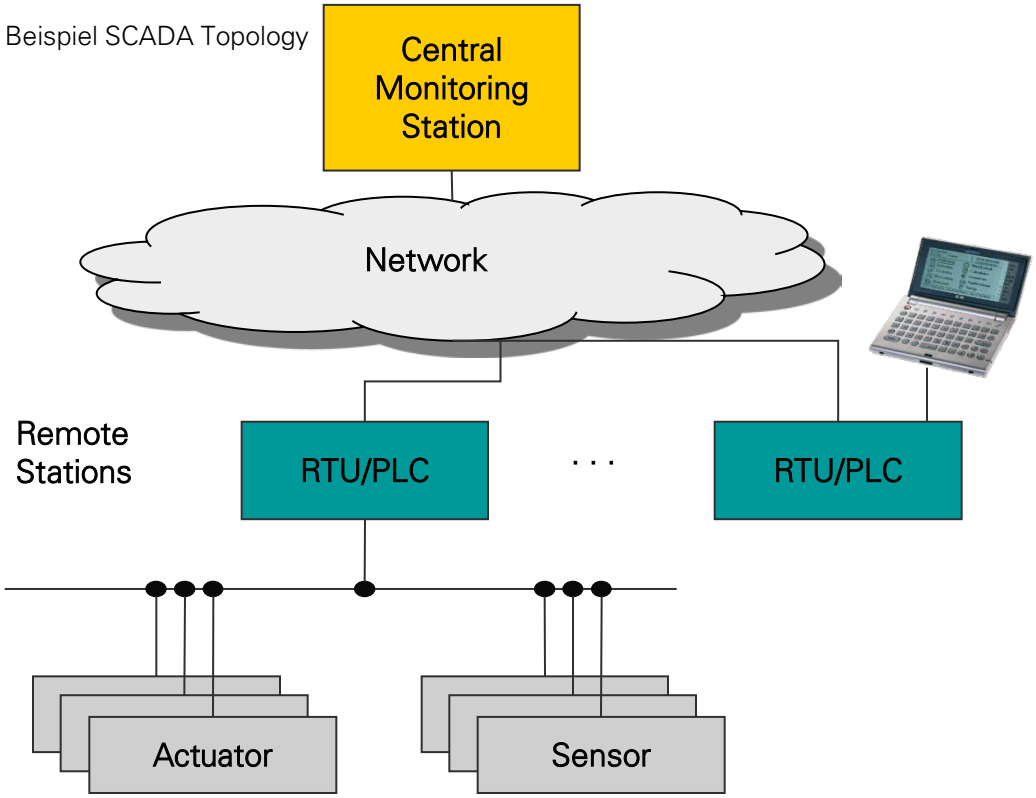
Gliederung

- Was sind SCADA-Systeme?
- Sicherheitsunterschiede zur Bürowelt
- Standardisierung
- Ausgewählte Sicherheitsanforderungen
  - Energie Automatisierung
  - Smart Grid
- Diskussion

Definition SCADA

(Supervisory Control and Data Acquisition)

Beispiel SCADA Topology



SCADA-Systeme werden zur Überwachung und Steuerung von oft stark automatisiert ablaufenden technischen Prozessen eingesetzt.

Sie werden z. B. in folgenden Umgebungen eingesetzt

- Chemiefabriken
- Pipelines (Öl & Gas)
- Raffinerien
- Energieerzeugung und –verteilung
- Eisenbahnüberwachung
- Wasserversorgung

und sind somit oft ein wesentlicher Bestandteil unserer kritischen Infrastrukturen.

SCADA	Supervisory control and data acquisition
PLC	Programmable Logical Controller
RTU	Remote Terminal Unit

SCADA Sicherheitsvorfälle

Australian Sewage Spill, 2000

SQL-Slammer Wurm in US Atomkraftwerk, 2003

Kritische Schwachstelle im SCADA-Protokoll ICCP, 2006

BCIT Industrial Security Incident Database

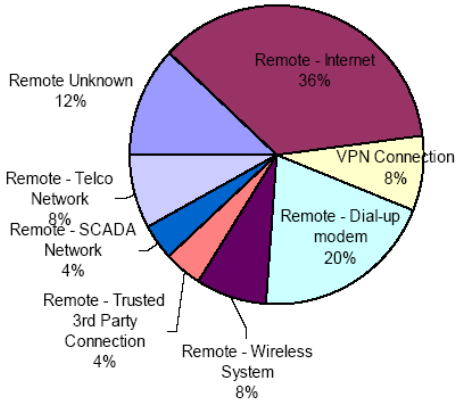


Fig 6: External Security Incidents by Entry Point

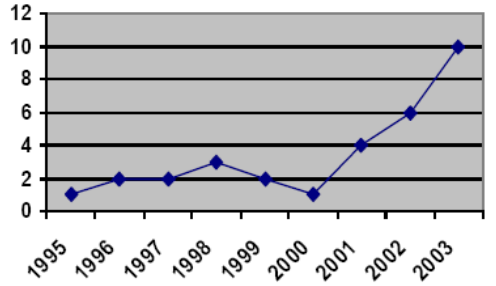


Fig. 2 Security Incidents between 1995 and 2003

SCADA Sicherheits-Herausforderungen

- Zunehmende Verwendung von Standardbetriebssystemen und Anwendungen wie z.B. Datenbanken und Web-Server in SCADA-Systemen
- Zunehmende Verwendung von TCP / IP und des Internets
- Zunehmende Verwendung von kabellosen Netzwerken
- Zunehmende Vernetzung früher isoliert betriebener Netzwerke

Unterschiede SCADA und Bürowelt

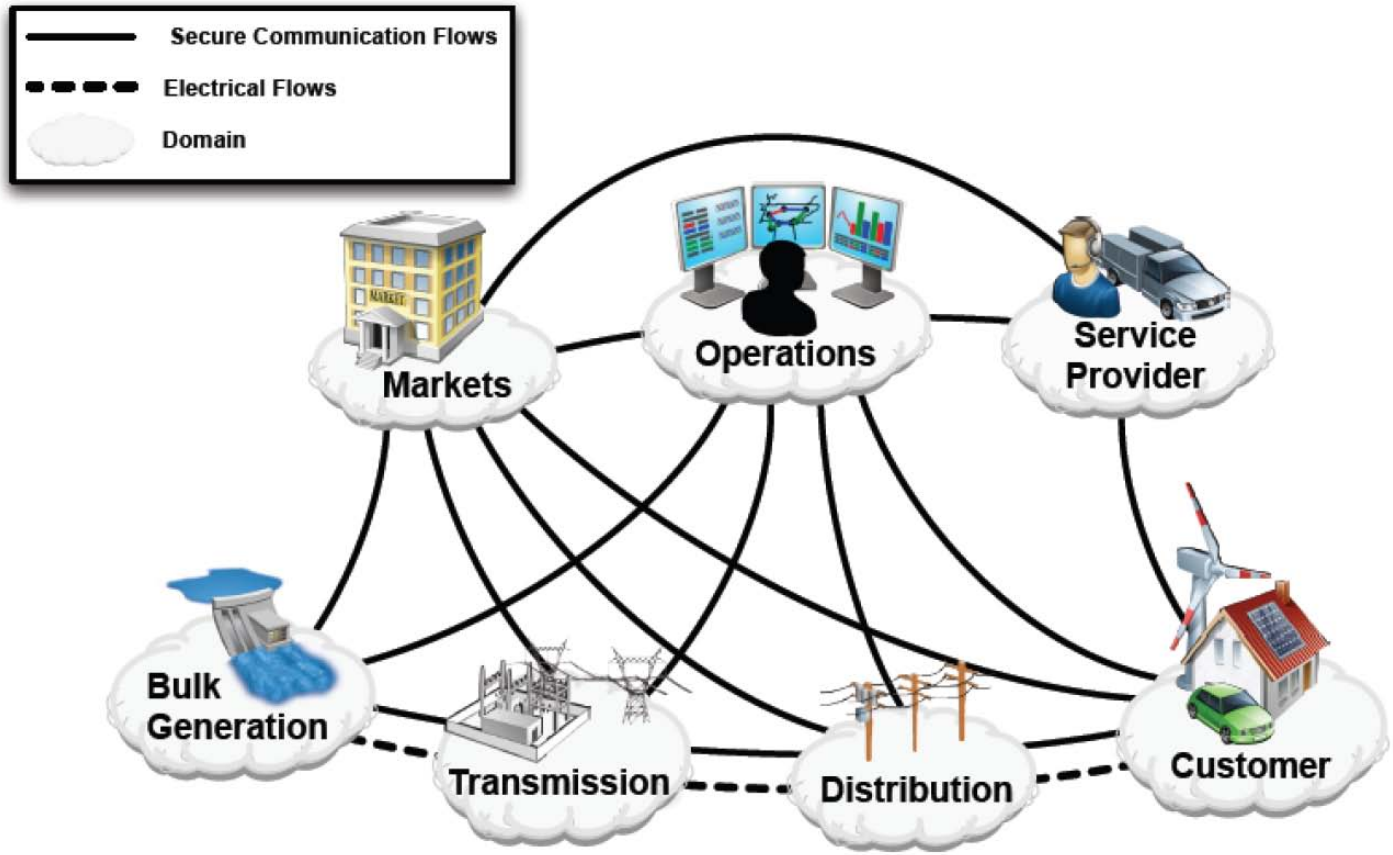
	IT-System in der Bürowelt	SCADA-System
Lebensdauer	Wenige Jahre	Bis zu 30 Jahren
IT-Kenntnisse / Benutzer	Grund-IT-Kenntnisse sind vorhanden	Benutzer haben oft anderen Ausbildungshintergrund
Performance-Anforderungen	Nicht-Echtzeit	Echtzeit
Verfügbarkeits-Anforderungen	Reboot nach Patchen OK	Reboot nach Patchen nicht OK
Sicherheitsfokus	1. Vertraulichkeit, 2. Integrität, 3. Verfügbarkeit	1. Safety, 2. Verfügbarkeit, 3. Integrität, 4. Vertraulichkeit
Kommunikation	standardisiert	Heterogen (Standardisierungsgrad, Protokollen, Hardware)

Weitere Informationen in NIST SP 800-82

Ausgewählte SCADA-Sicherheitsstandards

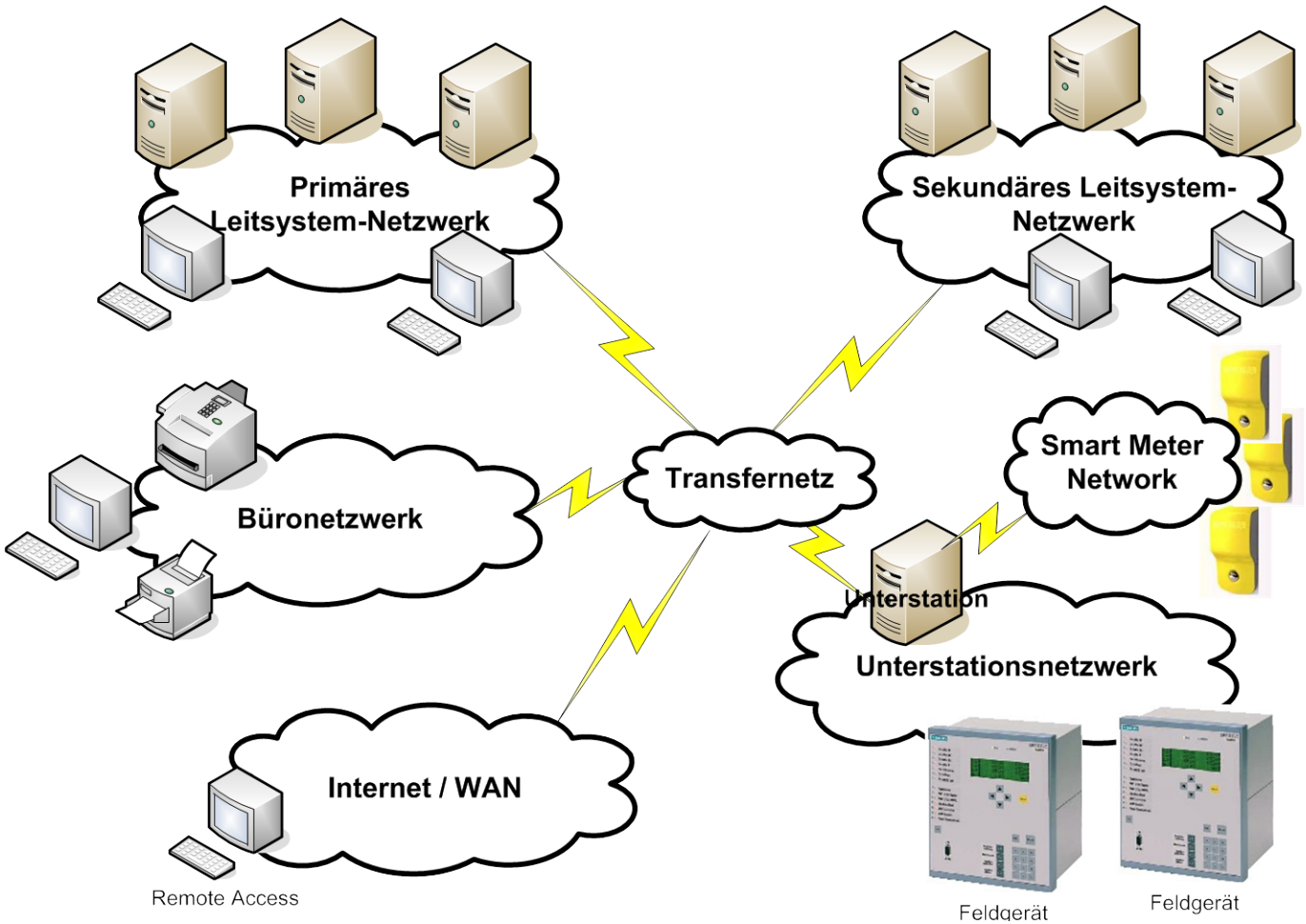
- NERC Critical Infrastructure Protection (CIP)
- ISA SP 99: Manufacturing and Control Systems Security
- BDEW Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
- ISO 270xx: Informationssicherheits-Management
- ISO 15408: Common Criteria for Information Technology Security Evaluation

Smart Grid Framework

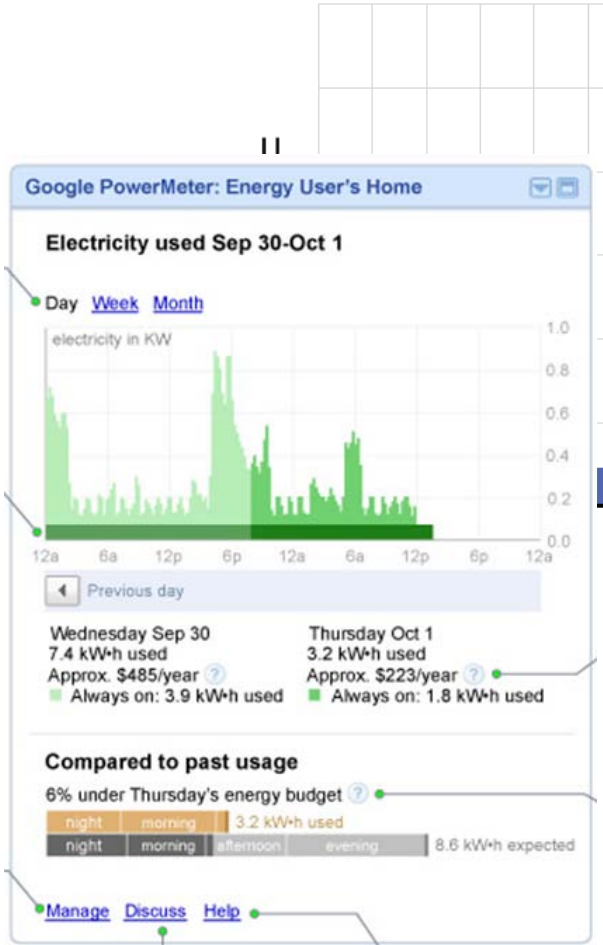


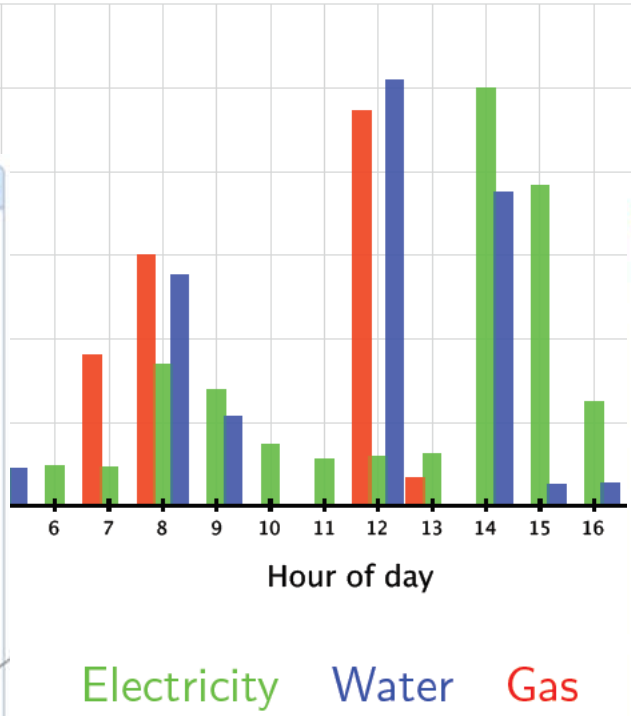
NIST Smart Grid Framework 1.0 January 2010

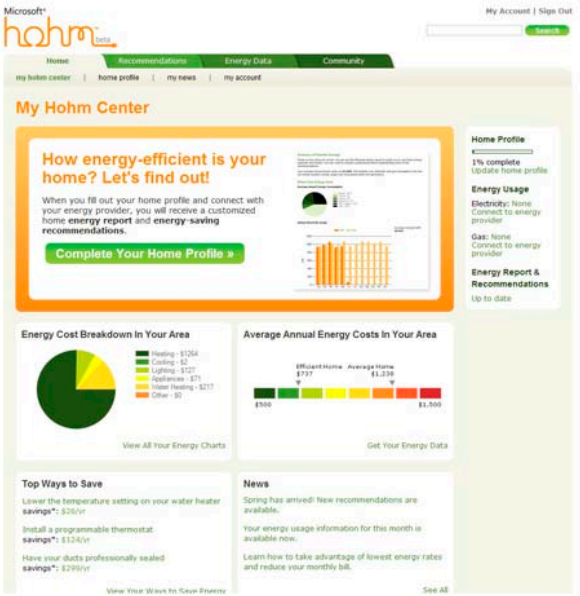
Bedrohungsanalyse: Kommunikationsnetzwerk eines Energieversorgungsunternehmens



Beispiel für Strom-, Wasser- und Gasverbrauch







Referenzen

- BDEW Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme,
- NERC Critical Infrastructure Protection (CIP) Standards
- Living Energy: „Ensuring the Integrity of Integrated Energy Networks", August 2010
- NIST Framework and Roadmap for Smart Grid Interoperability Standards
- NIST IR 7628: Smart Grid Cyber Security Strategy and Requirements
- NIST SP 800-82:Guide to Industrial Control Systems (ICS) Security

Diskussion