

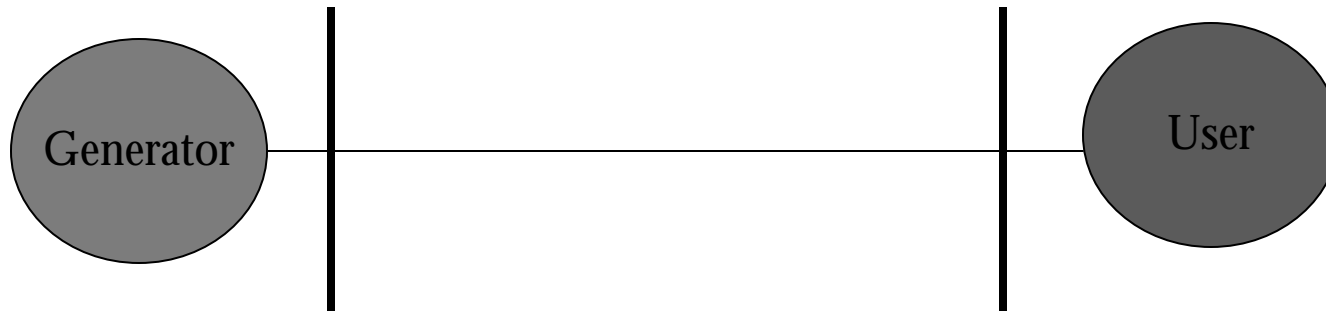
# **Network Security in Power Systems**

Maja Knezev and Zarko Djekic

# Outline

- Introduction
- Protection control
- EMS, SCADA, RTU, PLC
- Attacks using power system
- Vulnerabilities
- Solution
- Conclusion

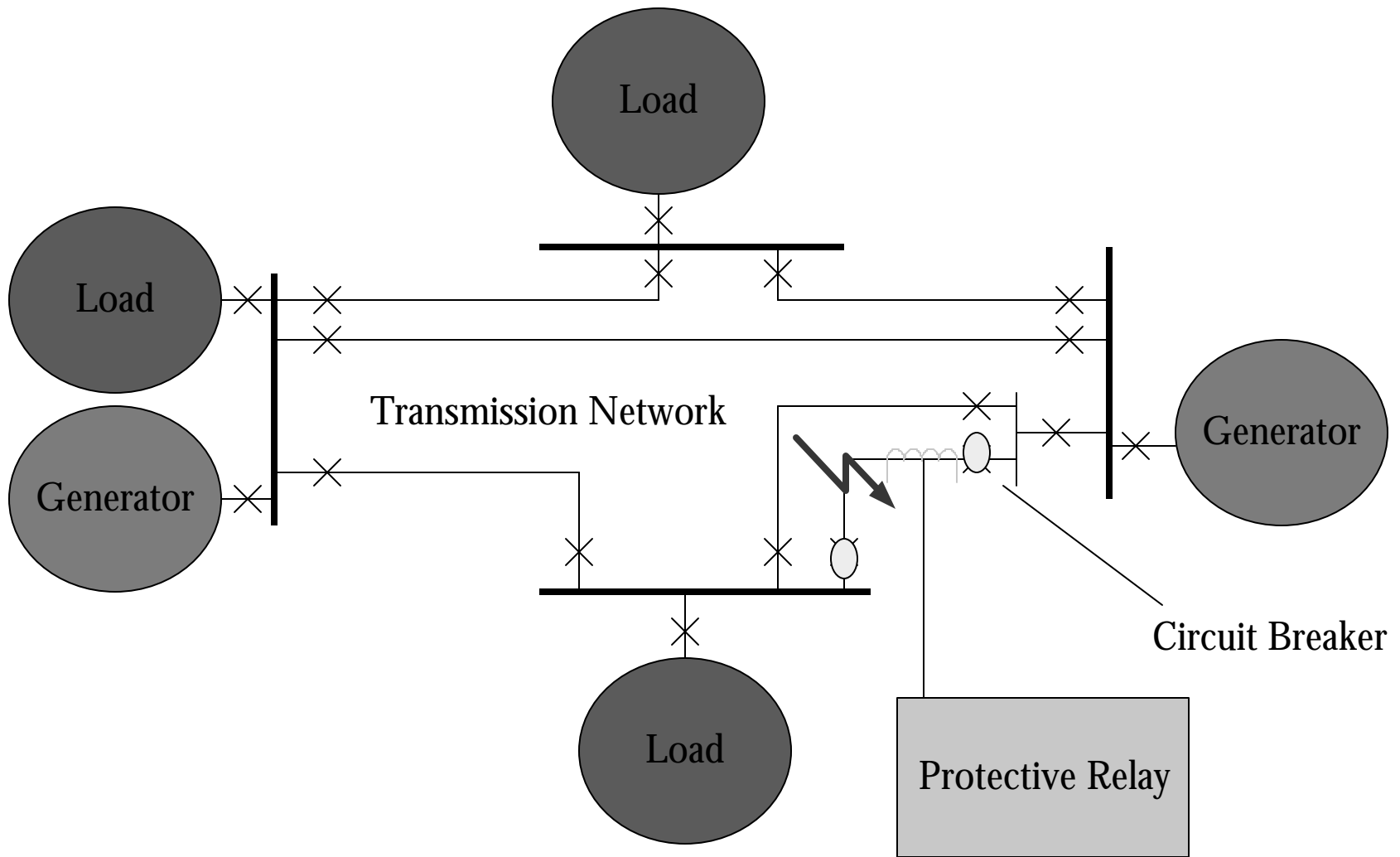
# Introduction



- Providing electrical energy in the power system at a minimal cost with a due respect to safety and reliability.

# Protective control

- Protective relays are designed to respond to system faults such as short circuits.  
Transmission relaying must locate and isolate a fault with a sufficient speed to preserve stability, to reduce fault damage and to minimize the impact on the rest of the system.



- Relays should respond when fault occurs but they should not respond in any other situation

# EMS(Energy Management System)

- CONSISTS OF computers, display devices , software, communication channels and remote terminal units that are connected to RTUs, control actuators in power plants and substations.
- PURPOSE: to manage the production, purchase, transmission, distribution and sale of electrical energy in the power system. It provides status of huge area to operator who makes decisions and it is capable of making decisions automatically by itself.

# **System Control And Data Acquisition**

## **SCADA**

- CONSISTS OF one or more computers with appropriate applications software connected by a communications system to a number of RTUs placed at various locations to collect data. Communication protocols differ from substation to substation.
- PURPOSE: provides three critical functions
  - Data Acquisition
  - Supervisory control
  - Alarm Display and Control
  - Supports operator control of remote (or local) equipment

- RTU(Remote Terminal Unit)

RTUs are microprocessor based computers which contain ADC and DAC, digital inputs for status and digital output for control.

- PCL (Programmable Logic Controller)

PCLs have extended I/O and control outputs can be controlled by software residing in PLC as well as via remote commands from a SCADA. The PLC user can make changes in the software without major hardware or software changes.

- Both have many real time communication links inside and outside the substation or plants

# Attacks using power system

- Attacks upon the power system

Attacking two substations simultaneously in order to cause a black out

- Attacks by the power system

Using dangerous nature of power plants for generating attack (chemical, biological agents)

- Attacks through the power system

Using some installations of the power system to attack civil infrastructure. For example by coupling an electromagnetic pulse through the grid computer and telecommunications infrastructure could be damaged

# SCADA system attacks

- On the Ohio Davis-Besse nuclear power plant process computer, a 2003 Slammer worm attack, which disabled a nuclear safety monitoring system over five hours
- A wireless link to the SCADA system for the Queensland, Australia, Maroochy Shire sewage control system in 2000 was exploited by one Vitek Boden. This attack caused millions of gallons of sewage to be dumped into Maroochy waterways over a four-month period.
- Security consultant Paul Blomgren and his associates were hired to assess SCADA vulnerabilities at a large southwestern power utility, they were able to penetrate the power station's operational control network and computer systems through wireless connections from laptops in a vehicle parked outside of the plant.

# **SCADA/EMS vulnerabilities**

- **Network Architecture vulnerabilities**
- **Physical connection vulnerabilities**
- **RTUs and IEDs vulnerabilities**
- **Protocol vulnerabilities**

# **Network Architecture vulnerabilities**

- **20 years ago - separated Administrative and Control networks**
- **Today networks are tightly coupled**
- **Connection between SCADA and other corporate networks are not protected by strong access controls**

# **Physical connections vulnerabilities**

- **Internet connection between remote devices and control center in order to avoid more expensive private lines**
- **Wireless connections**
- **Dial up telephone lines**

# **RTUs and IDEs vulnerabilities**

- **Physical security**
- **Many RTUs and IDEs have no password protection**
- **Many actuators (breakers, pumps) have its own network connection**

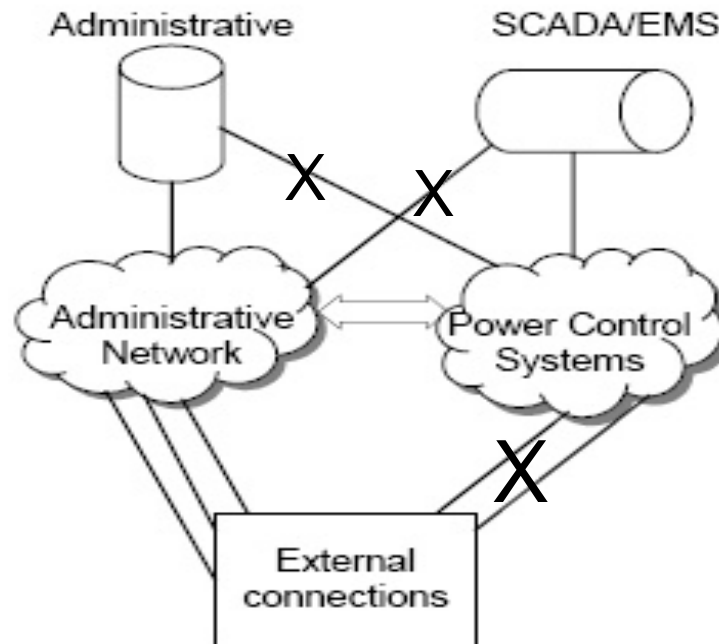
# Protocol vulnerabilities

- **Many plain-text SCADA protocols are developed for private serial networks in 60s and 70s and today they have been adapted to function over TCP/IP (MODBUS, FIELDBUS, DNP3)**
- **Standard wireless protocols vulnerabilities (IEEE 802.11b)**

# Solutions

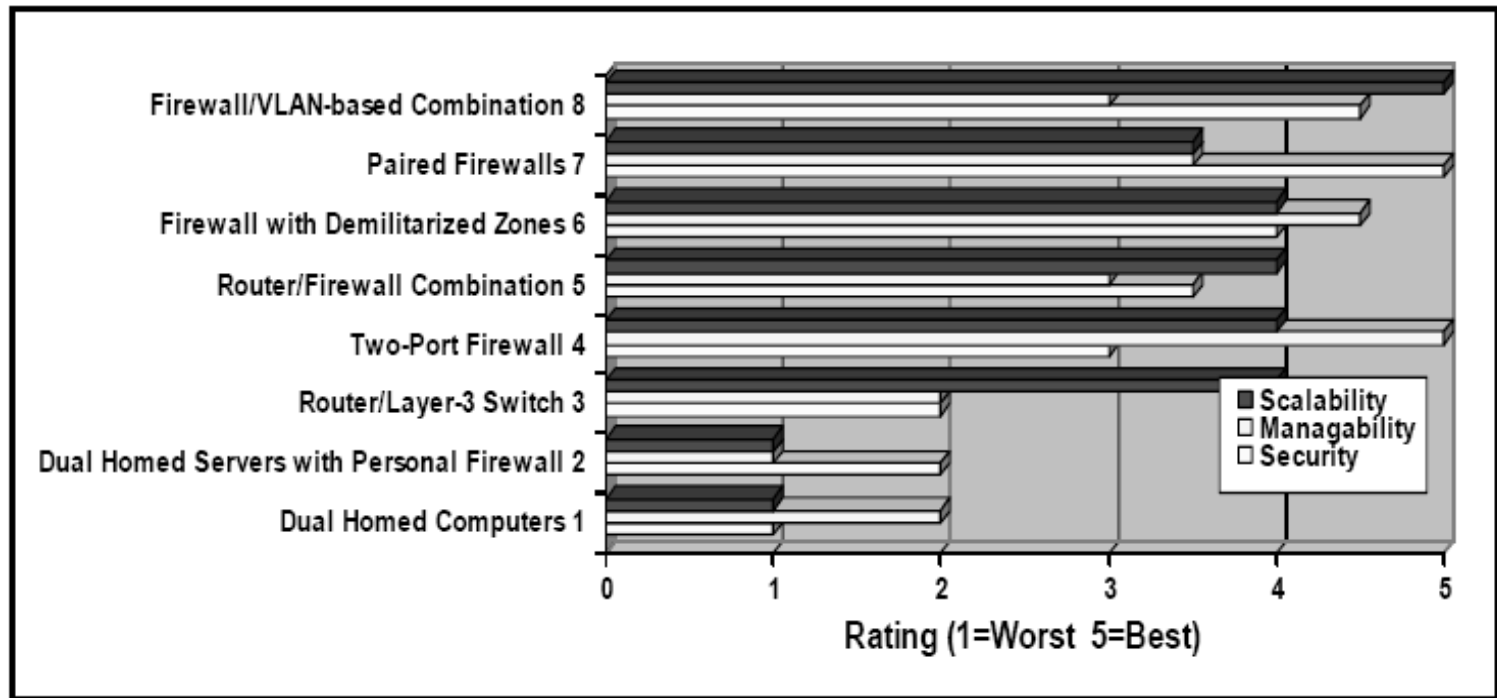
## Physical network insulation

- **Separate intranet (SCADA/EMS) network and external network physically**



# Firewall Technique

- **Firewalls** - between enterprise network and Internet
  - **Intrawalls** - between enterprise and process control network
- NISCC, BCIT; Firewall Deployment for SCADA and Process Control Networks, February 2005*



# Physical connections

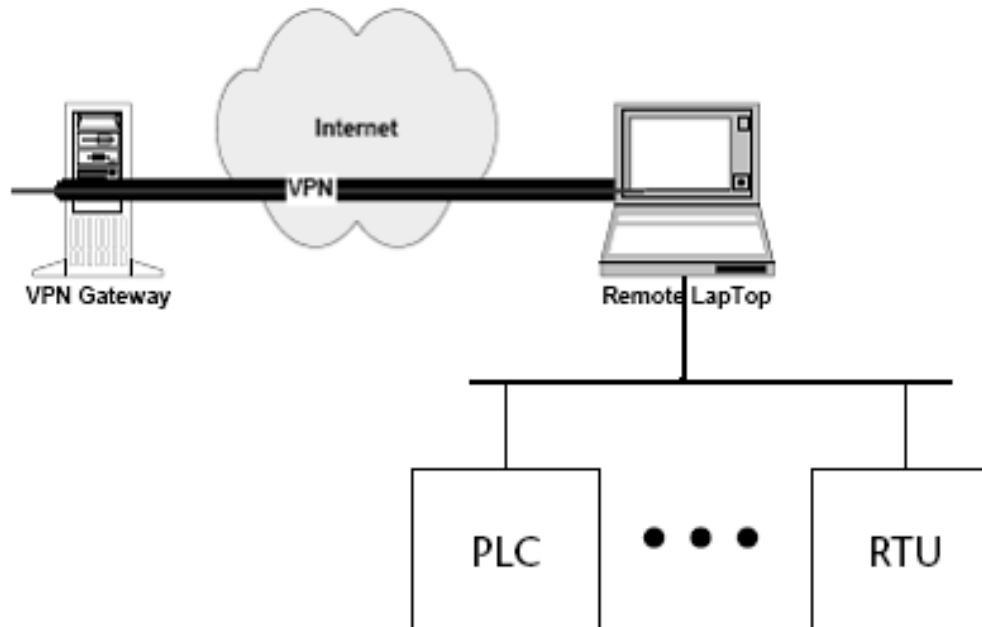
- **Private lines**
- **Dial back modems**
- **Private wireless protocols**
- **VPN (Virtual private network)**
  - IPsec**
  - PPTP (Point-to-Point Tunneling Protocol)**

# RTUs and IDEs

- **Assure physical security of all remote sites connected to network**
- **Do not allow “live” network access point at remote, unguarded sites**
- **Disable all necessary connections to RTUs, IDEs and actuators**
- **Update firmware**

# RTUs and IDEs

- **Interface between network and devices**



# Security Policies

- **Password policy**
- **Identification and Authentication of Users**
- **Secure E-mail (PGP, PEM)**
- **Intrusion detection**
- **System Redundancy**
- **System Backup and Recovery plan**

# Conclusion

- **SCADA/EMS networks were initially designed to maximize functionality and reliability, with little attention paid to security**
- **SCADA/EMS networks can be very vulnerable and that could result huge consequence to public safety and disruptions in the nation's critical infrastructure.**
- **No unique and entire solution – every network is different and requires custom solution**

# References

- [1] Ronald L. Krutz; **Securing SCADA Systems**; Wiley Publishing, Inc. 2006
- [2] George D. Jelatis, **Information Security Primer**, EPRI 2000
- [3] **21 Steps to Improve Cyber Security of SCADA Networks**, President's Critical Infrastructure Protection Board , U.S. Dept. of Energy, 2002
- [4] A. Creery, E.J. Byres, **Industrial Cybersecurity for Power System and SCADA**, IEEE Paper No. PCIC-2005-34
- [5] M.T.O. Amanullah, A. Kalam, A. Zayegh, **Network Security Vulnerabilities in SCADA and EMS**, IEEE/PES 2005
- [6] Yongli Zhu, Baoyi Wang, Shaomin Zhang; **The Analysis and Design of Network and Information Security of Electric Power System**, IEEE/PES 2005
- [7] Göran N. Ericsson, **On Requirements Specifications for a Power System Communications System**, IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 20, NO. 2, APRIL 2005
- [8] Alan S. Brown, **SCADA vs. the Hackers**, Mechanical Engineering Dec. 2002
- [9] NISCC, BCIT; **Firewall Deployment for SCADA and Process Control Networks**, February 2005