Cyber Security and Power System Communications – Essential Parts of a Smart Grid Infrastructure

Author: Goran N. Ericsson, Senior Member, IEEE

Talal El Awar

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Outline

- Introduction
- Classification of Power Systems Communications
- Development of Power System Control Systems
- Cyber Security Issues
- Smart Grid
- Assessment of Smart Grid Cyber Security
- Conclusion

Introduction

- Use of electricity is essential to our society.
- Physical security has been historically addressed but now digital threats are increasing.
- Using PSC capabilities and supervisory control and data acquisition systems (SCADA) substation are now interconnected with other systems.

Introduction

- Generally, vendors use commercially off the shelf products as part of their SCADA/EMS system.
- This use of standard products opens up new possibilities and threats.
- Security-by-obscurity principle does not apply to the same extent.
- A better choice of adequate technical solutions should be made when deploying a new SCADA system.

Purpose

- The purpose of this paper is to emphasize the role of cyber security and PSC systems in the smart grid infrastructure.
- Presents a historical development of the PSC systems of today.
- Highlight access points of a substation.
- Introduce information security domain modeling.

Outline

- Introduction
- Classification of Power Systems Communications
- Development of Power System Control Systems
- Cyber Security Issues
- Smart Grid
- Assessment of Smart Grid Cyber Security
- Conclusion

Classification of Power System Communication

- Real Time Operation Communication
- Administrative Operation Communication
- Administrative Communication

Real Time Operational Communication

Real time operational data communication encompasses:

- Tele-protection

  Should be transmitted within a very short time (12-20ms). This is because fault current disconnection shall function in 100ms.

- Power System Control

  PSC mainly includes supervisory control of the power system process on secondary levels. These include SCADA/EMS systems. Measured values arrive in 15s.

Real Time Operational Communication

Real time operational voice communication encompasses traditional telephony where voice communication has operational purposes.

Voice communication facilitates switching sequence orders and has other functional operation uses.

Administrative Operational Communication

- This communication is characterized by that it does not need to take place in real time.
- Includes information that is needed, in more detail with support description of what happened in the power system.
- Examples are interactions with local recorders, disturbance recorders and power swing recorders.

Administrative Operational Communication

Includes the following functions:

- Asset management
- Fault location
- Metering and transfer of settlement information
- Security systems
- Substation camera supervision

Administrative Communication

Includes voice communication within the company.

Communication to and from the company where the communication has administrative purposes.

Outline

- Introduction
- Classification of Power Systems Communications
- Development of Power System Control Systems
- Cyber Security Issues
- Smart Grid
- Assessment of Smart Grid Cyber Security
- Conclusion

Power System Control Systems

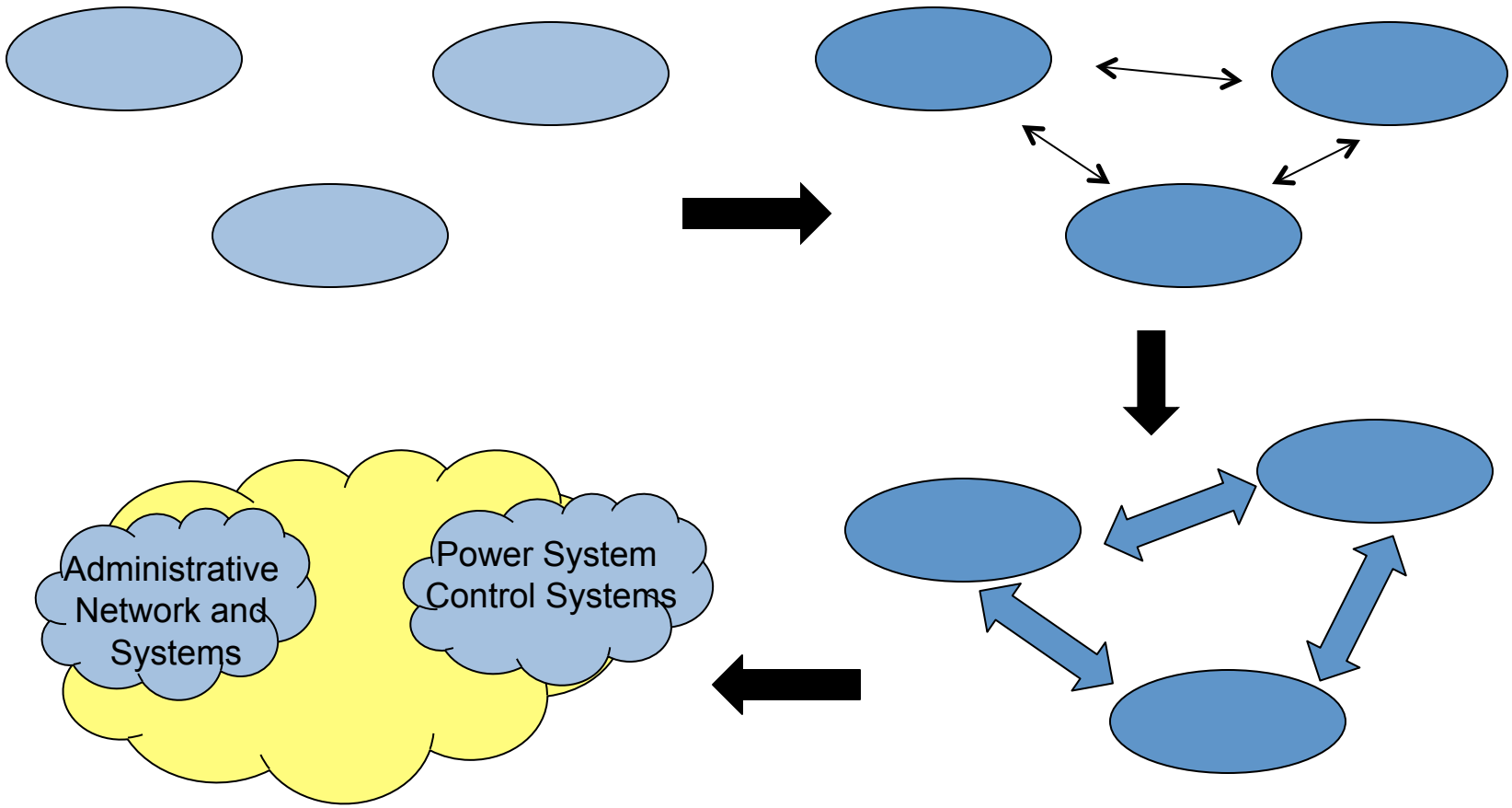
- PSC systems are the life nerve of the power system.
- Essential systems for adequate operation and control of a power system.
- Also, focus will increase on the communication system based on the new requirements for information and IT security.

Power System Control Systems

- Data communication systems have developed from proprietary solutions to standardized off the shelf solutions.

- Therefore, power system control systems that used to be islands of automation, now have developed to interconnected and integrated.

Power System Control Systems



Power System Control Systems

- In the 1990s and 2000s several of the systems were procured with the requirement of obtaining openness in the PSC system.
- However, there was no requirement for cyber security, thus limited security was incorporated into the systems.
- Therefore, utilities now have information and IT problems to tackle.

Outline

- Introduction
- Classification of Power Systems Communications
- Development of Power System Control Systems
- Cyber Security Issues
- Smart Grid
- Assessment of Smart Grid Cyber Security
- Conclusion

Cyber Security Issues

Based on the history of PSC systems and limited concern over cyber security new issues have arisen:

- Decoupling between operational SCADA/EMS and admin IT
- Threats and possibilities
- SCADA systems and SCADA security
- Government Coordination in Sweden on SCADA Security
- Information Security Domains

Decoupling Between Operational SCADA/EMS and Admin IT

- As an existing SCADA system is being updated, the information and IT issues should be taken into account.
- Operational SCADA/EMS part should be separated from the administrative part.
- Such that the operational part is protected from the digital threats that are possible over an internet connection.

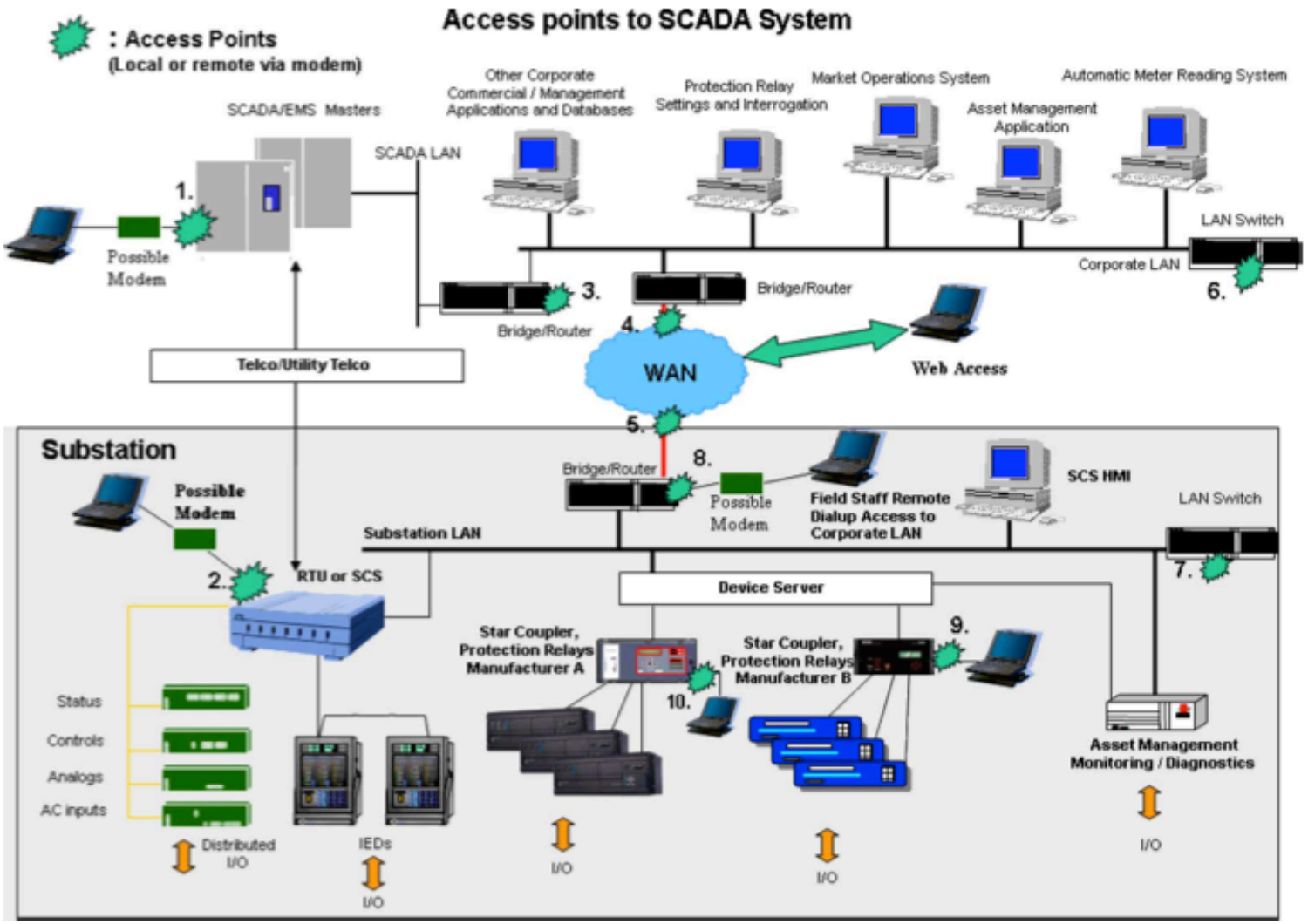
Decoupling Between Operational SCADA/EMS and Admin IT

- When updating a SCADA/EMS system a whole system structure update should be considered.
- A more secure state would be to de-couple the operational SCADA system and the administrative IT system.
- Another solution would be to secure the firewalls between operational and administrative parts.

Threats and Possibilities

- The integration of SCADA/EMS systems with external system creates new vulnerabilities and threats.
- There is a large number of access points where a SCADA system is vulnerable to such attacks.

Threats and Possibilities



Taken from [1]

SCADA Systems and Security

- Since, SCADA systems now use off-the-shelf products and becoming increasingly connected over the internet, these systems are being exposed to the same vulnerabilities as our home PCs.

- The protection of such a digital structure is called “critical information infrastructure protection (CIIP)”

Governmental Coordination in Sweden on SCADA Security

- In Sweden, a government coordination has taken place focusing on SCADA security.
- Different power utilities which have SCADA systems as critical part of operations gathered experiences in an attempt to design a secure SCADA system.
- As a result the SCADA Security Guideline was developed.

Information Security Domains

- Since the SCADA/EMS systems have become more integrated, it becomes hard to treat the system structure in terms of parts or subsystems.
- It is more natural to treat the system in terms of domains.
- A domain is an area where specific business operations are going on and they can be grouped together.

Information Security Domains

- Public, supplier, maintainer domain
- Power plant domain
- Substation domain
- Telecommunication domain
- Real-time operations domain
- Corporate IT domain

Information Security Domains

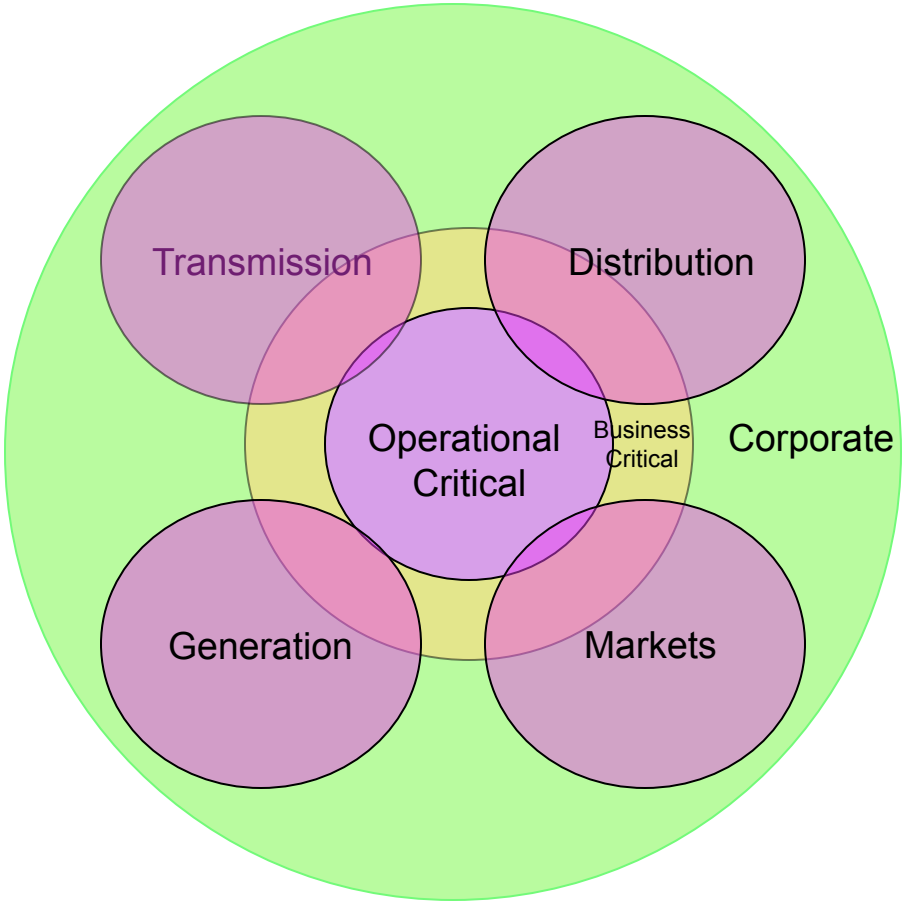
- Security is treated within each domain, and there is one security policy and one authority responsible for security within one domain.
- The authority should guarantee a minimum level of security.
- Security level of the individual domains must be classified and could vary from.

Information Security Domains

- A power utility should define the policy structure depending on the topology and importance of resources in the tele-control network.

- Also, an electric power utility (EPU) could define each domain according to the level of protection required by the organization.

Information Security Domains



Outline

- Introduction
- Classification of Power Systems Communications
- Development of Power System Control Systems
- Cyber Security Issues
- Smart Grid
- Assessment of Smart Grid Cyber Security
- Conclusion

Smart Grids

The development of power communication systems is a key factor for actually having a power grid that is smart.

Moreover, information and IT security considerations will soon be considered essential for such a smart grid.

- Smart Meters
- Smart Grid systems – Usage of Wind power

Smart Meters

- Broadband connections make it easier to transfer data faster across the network.
- This allows for the utility to remotely read the consumers consumption at each household.
- Moreover, utility companies are interested in transferring data to the household such as electricity prices.

Smart Meters

- A critical issue in this new control and information flow scheme is accountability.
- Who is responsible if there was a mistake or intentional digital tampering with the smart meters?

Smart Grid Systems
Use of Wind Power

- Introduction of wind power is becoming more evident.
- The intermittent power production while maintaining power balance is a very delicate issue.
- Smarter solutions will allow for such integration to form a smart grid system.

Outline

- Introduction
- Classification of Power Systems Communications
- Development of Power System Control Systems
- Cyber Security Issues
- Smart Grid
- Assessment of Smart Grid Cyber Security
- Conclusion

Assessment of Cyber Security and PSC Systems

- Gave a complete description of PSC systems from an infrastructure level.
- Introduced information security domains.
- Author did not present solutions or recommendations for most of the problems presented.
- Author failed to give test scenarios of information security domains.
- Failed to discuss state estimation as an essential part of the future smart grid. In addition to the “special” security issues of state estimation.

Outline

- Introduction
- Classification of Power Systems Communications
- Development of Power System Control Systems
- Cyber Security Issues
- Smart Grid
- Assessment of Smart Grid Cyber Security
- Conclusion

Conclusion

- PSC and cyber security issues are vital parts of the critical information infrastructure, such as a smart grid system.
- Also, the paper discussed the development from islands of automation to fully integrated systems.
- The openness that was required has opened up new vulnerabilities and created cyber security issues to be addressed.

References

[1] G.N. Ericsoon, "Cyber Security and Power System Communication -- Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501-1507, July 2010.

[2] P. Roche, "Cyber security considerations in power system operations,"*CIGRÉ Electra No. 218, Feb. 2005.*

[3] *Risk Management—Vocabulary, ISO/IEC CD 2 Guide 73, Concept,* Apr. 2008.

[4] M. Tritschler and G. Dondossola, "Information security risk assessment of operational IT systems at electric power utilities," presented at the CIGRÉ D2 Colloq., Fukuoka, Japan, Oct. 21–22, 2009, Paper D2-01 D03.

[5] G. Ericsson, "Classification of power systems communications needs and requirements: Experiences from case studies at swedish national grid," *IEEE Trans. Power Del., vol. 17, no. 2, pp. 345–347, Apr. 2002.*

[6] G. Ericsson and T. Rahkonen, "Openness in communication for power system control, a state-of-the-practice study," in *Proc. IEEE Power Tech, Stockholm, Sweden, Jun. 1995.*