Smart Power Grid Security: A Unified Risk Management Approach

Authors: Partha Datta Ray, Rajopal Harnoor, Dr. Mariana Hentea

Presenter: Yan Zhang

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

Overview

- 1. Introduction & Motivation
- 2. Implications for security implementations
- 3. Risk Management
- 4. Risk Strategies
- 5. Risk Assessment
- 6. General Conclusion
- 7. Future Work
- 8. Reference

Introduction and Motivation

- Power Grid Information Security and Protection

1. Industrial Control System (ICS)

2. Information Technology (IT)

Availability VS Confidentiality

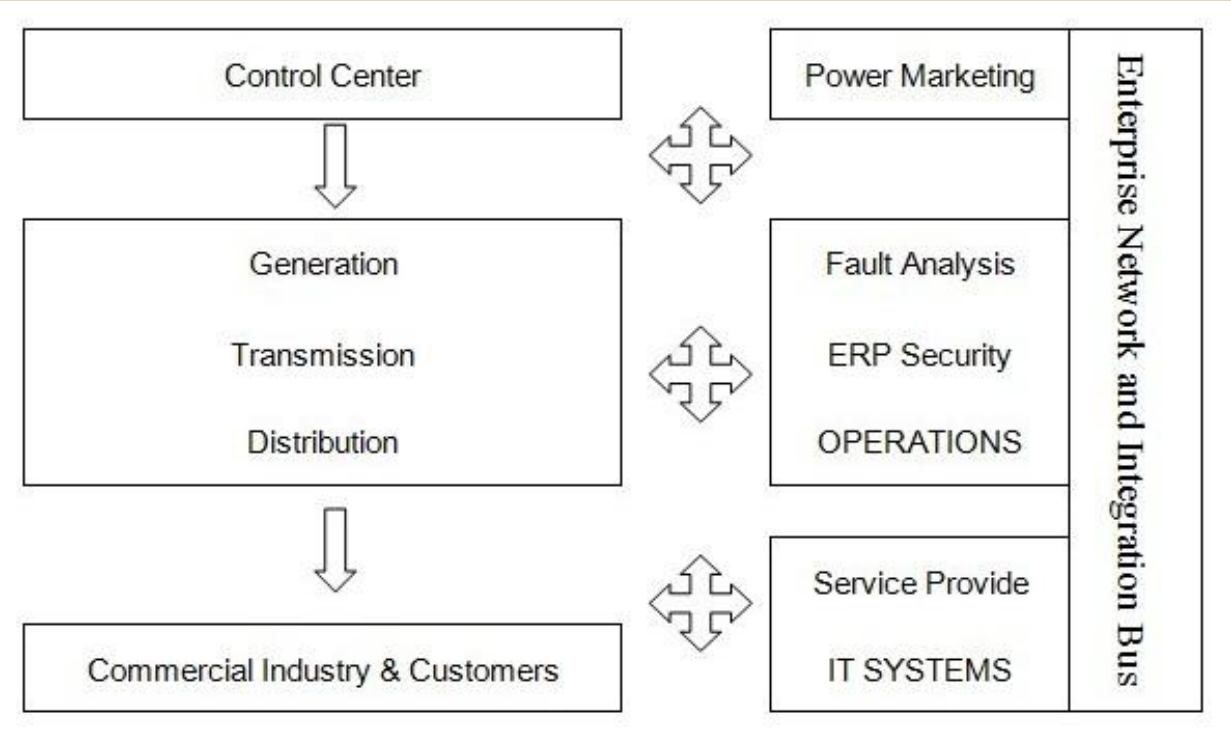
Motivation: Why Unified?

- The power grid operation systems have unique performance and reliability requirements.
- Without a formal and objective risk management…(Guidelines\Government)
- Unified Risk Management in other fields.(Finance, Aviation, Business)

How to approach?

- Such approaches need to provide frameworks which can consider all the interconnected vulnerabilities, different performance requirements and security priorities.
- Control Flow through the entire IT system should not adversely impact the various performance requirements and implantation limitations of smart grid.

Implications for security implementations of ICS and IT systems



SMART GRID: An emerging convergence of Operations Technology (OT) and Information Technology (IT)

Unified Security for Distinctive Platform

Security Characteristics	Control Systems	IT Systems
Physical Security	Less Secure when far flung, unmanned	Secure: Facility, Server
Connection Speed	Slow serial link	Fast broadband
Availability	Need timely authorized access 24/7/365	Can tolerate some delay in access
Integrity	Less assured	Assured
Confidentiality	Less important	Preservation is critical
Encryption Key, digital certificate and signature	Server access and local memory limitation	Extensively used

Difference in security environments

Risk Management

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and impact of unfortunate events in the smart grid system.

a. Risk & Vulnerabilities

- Vulnerabilities
- Tolerance
- Improve the integrity, repeatability and Timeliness of security measurements

Risk Management

- b. Risk Management Process Framework

PHYSICAL	1	Set security goal	Interaction Between Two Domains	1	Identify	PHYSICAL
	2	Identify Assets		2	Plan& Analysis	
CYBER	3	Assess Risks		3	Prioritize	CYBER
	4	Prioritize		4	Track& Control	
HUMAN ORGANIZAITONAL	5	Implement Protection		5	Communicate Document	HUMAN ORGANIZAITONAL
	6	Measure Effectiveness		6	Decision Support	
Operations Technology				Information Technology		

Unified Risk Management Framework for a Smart Grid

Risk Management

- c. Unified Risk Management & Risk Strategies

  A unified risk management approach lets organizations evaluate risks and protection measures across both domains (which often can be highly correlated) for all its assets using a common principle.

Risk Strategies

Risk Strategies	
Risk Avoidance	Take an alternative approach and re-assess risk, document & communicate to stakeholders
Risk Acceptance	Passive: Accept consequences Active: Prepare Contingency Plan and re-assess risk, document & communicate to stakeholders
Risk Mitigation	Apply countermeasures to reduce the risk while monitoring and re-assessing the risk on an ongoing basis. Document & communicate to stakeholders
Risk Transference	Transfer the risk with a deliberate intent. Re-assess risk, document & communicate to stakeholders
Contingency Plans & Workarounds	Workaround are short-term risk response actions. These are wish-list items for long-term solutions. Contingency plans are planned risk responses for short term or long term.

Risk Assessment

- Qualitative risk assessment

-Short time

-Small Budget

- Quantitative approaches

$$\text{Risk} = (1 - \text{SC}_{\text{Effectiveness}}) \times \sum_{\text{AttackType}} \text{P}_{\text{attack}} \times \text{C}^{r}$$

Risk Assessment

- Notionally, a non-linear function g1 could be constructed to capture the quantification of interrelationship between vulnerability V1 and threat T1 for different use cases, and systems.

$$\text{Risk: } R_1 = f_1(g_1(V1, T1), C_1)$$

- Extending the notion to compose overall risks for larger and unified systems, we could construct a non-linear composition function which would capture two component risks, their weighted contributions (α,β) and power indices (γ,μ)

$$\text{Unified Risk: } R_1 = F(\alpha R_1^{\gamma}, \beta R_2^{\mu})$$

General Conclusion

- Interconnection of Power Grid IT & ICS Systems
- Unified methodologies for automated risk management will comprehensively enhance the security and reliability aspects of the convergent smart grid information exchange system.
- Since threats and vulnerabilities to existing and emergent smart grid functionalities are continuously evolving, automated and adaptive methodologies should be better placed to make such frameworks robust.

Future Work

1. Unified models, methods, and technologies for risk and security that provide a correlated view of power system and cyber impacts

2. Automated and adaptive methodologies and tools:

- Newer grid simulation tools and techniques that incorporate device communication and modeling
- Security and reliability analysis

3. Risk management in Cyber-Physical Power System Security & Reliability

Reference

- [1] Ryan D J & Ryan J C H, Risk Management & Information Security, 11th Computer Security Applications Conference, New Orleans, Louisiana, December 19, 1995
- [2] Control Systems Cyber Security: Defense in Depth Strategies – Idaho National Labs, US DHS, INL-EXT-06-11478
- [3] Best Security Practices for SCADA systems utilizing ISO 17799 ISM Matrix – ISS Solutions
- [4] Jones, A. and D. Ashenden, Risk Management for Computer Security: protecting your network and information assets. 2005, Oxford: Elsevier.
- [5] Security Metrics for Communication Systems, Mark D. Torgerson, June 2007, Sandia National Laboratory

Q & A

- Thank you!