The Challenges of Risk Assessment for Smart Grid

Lucie Langer and Paul Smith
firstname.lastname@ait.ac.at
AIT Austrian Institute of Technology

ComForEn Workshop
Monday 29th September, 2014
Risk Assessment: The Basics

- Risk assessment is concerned with understanding the probability of a cyber-attack and its impact

\[ \text{risk} = \text{probability} \times \text{impact} \]

Based on an understanding of **threats** and **vulnerabilities**

For example, financial loss, damage to equipment, loss of power, …

- The basis for prioritising how to mitigate threats and apply resources for cybersecurity
Breakout Session

- Split into groups of three people and appoint a spokesperson

- For ten minutes discuss the challenges of risk assessment for smart grid in your group
  - Write these down on post-it notes and stick on the wall

- Spokesperson presents to the workshop and discuss
The Challenges We See …

- We have identified five key challenges with carrying out a risk assessment for smart grid:
  
  1. Managing safety and security risks
  2. Analysing cyber-physical risks
  3. Understanding risks to legacy systems
  4. Complex organizational dependencies
  5. Understanding cascading effects

- These are not unique to smart grid, but all exist, making risk assessment particularly challenging
Managing Safety and Security Risks

- Safety analysis methods are widely used in the energy domain
  - Examples include HAZOP, fault-tree analysis, event-tree analysis, FMEA, STAMP/STPA, …

- There are parallels in the security domain, e.g., attack trees

- Benefits can be had by performing security and safety co-analysis
  - Reuse of results across analyses
  - Ability to consistently prioritise different types of threats, i.e., attacks versus faults
Analysing Cyber-physical Risks

- The smart grid is a cyber-physical system
  - *Power system* and *ICT infrastructure* is tightly coupled through SCADA and control systems

- Traditional IT security provides necessary tools
  - but not sufficient to secure cyber-physical systems

- Need for tools and strategies to understand and mitigate attacks:
  - Which threats should we care about?
  - What impact can we expect from attacks?
  - Which resources should we protect (more)?
Understanding Risks to Legacy Systems

- The smart grid will consist of legacy systems and new ICT components that implement advanced measurement and control functions.

- It is often not clear what impact new components will have on legacy systems, and vice versa.

- Legacy industrial control systems are known to be fragile to active security testing techniques.

- A risk assessment method should account for these characteristics of the smart grid.
In a liberalised European energy market there are many actors
- Energy producers, Transmission and Distribution System Operators (TSOs and DSOs), and Energy Suppliers

Others from the ICT sector are emerging as being important
- E.g., telecommunications operators and cloud providers

Energy consumers become providers, potentially as part of virtual power providers

A diverse and complex supply chain is emerging

This complex web of dependencies can make risk assessment challenging
Understanding Cascading Effects

- The smart grid consists of a number of sub-systems that support an underlying grid infrastructure.
- The failure of a sub-system could cascade into another
  - This problem is closely related to cyber-physical impact analysis.
- A pathological case:
  1. A cyber-attack causes a failure in the energy grid, resulting in a blackout.
  2. ICT systems start to run on Uninterruptable Power Supply (UPS).
  3. The UPS runs out before the grid has recovered.
  4. ICT systems fail.
Conclusion

- SPARKS is aiming to develop a risk assessment framework that accommodates these challenges.
- Suitable analysis techniques can be “plugged into” the framework to address the challenges.
- Starting point is to consider the suitability of the SGIS toolbox.
- We have a position paper in the main symposium tomorrow that describes these issues …

Cybersecurity Risk Assessment in Smart Grids

Thomas Hecht, Lucie Langer, Paul Smith

AIT Austrian Institute of Technology
Safety and Security Department
firstname.lastname@ait.ac.at

Abstract – Smart grids will make extensive use of information and communication technology (ICT) to enable the integration of renewable energy sources. Consequently, future power grids
Questions?