Towards a Cyber-Physical Resilience Framework for Smart Grids

Ivo Friedberg[1,2(✉)], Kieran McLaughlin[1], and Paul Smith[2]

[1] Queen's University Belfast, Belfast, UK
{ifriedberg01,kieran.mclaughlin}@qub.ac.uk
[2] AIT Austrian Institute of Technology, Vienna, Austria
firstname.lastname@ait.ac.at

Abstract. As modern power grids move towards becoming a *smart grid*, there is an increasing reliance on the data that is transmitted and processed by ICT systems. This reliance introduces new digital attack vectors. Many of the proposed approaches that aim to address this problem largely focus on applying well-known ICT security solutions. However, what is needed are approaches that meet the complex concerns of the smart grid as a *cyber-physical system*. Furthermore, to support the automatic control loops that exist in a power grid, similarly automatic security and resilience mechanisms are needed that rely on minimal operator intervention. The research proposed in this paper aims to develop a framework that ensures resilient smart grid operation in light of successful cyber-attacks.

1 Introduction

Power systems are one of the most critical infrastructures in our society. Priority lies on the stable operation of any power system, ensuring *(i)* human safety, *(ii)* availability and *(iii)* equipment safety [10]. With the shift towards distributed, renewable energy sources, extensive use is made of information and communication technology (ICT) infrastructures to enable enhanced control strategies and energy services. Embedded systems that once worked independently now form an interconnected and interdependent part of the *smart grid*. However, systems such as smart grids, where ICT components control the operation of physical entities – so called cyber-physical systems – are increasingly being targeted by sophisticated cyber-attacks [4]. Thus, to provide resilience – the ability to maintain acceptable operation in the face of faults and challenges [5] – during successful cyber-attacks on smart grids is an operationally critical problem.

This cyber-physical nature of the smart grid introduces a range of new challenges to ensure grid stability in light of cyber-attacks. One especially hard problem lies in managing both the physical (power) system and the cyber system, in order to provide a comprehensive resilience strategy. Without addressing this problem it is not possible to effectively address the risks caused by the interdependency between both systems. However, current research in the area is either focused on ensuring the robustness of control loops for the physical power

S. Latré et al. (Eds.): AIMS 2015, LNCS 9122, pp. 140–144, 2015.
DOI: 10.1007/978-3-319-20034-7_15

system (e.g., [9]) or securing the ICT systems. Efforts to secure the ICT systems in this domain largely focus on the prevention [8] or detection [12,3] of cyber-attacks – limited attention is paid to what steps should be taken to ensure grid stability when an attack is successful. In ICT systems, this problem is often left to be solved by human operators. The control loops in power grids – e.g., the Automatic Generation Control (AGC) in Energy Management Systems (EMSs) – currently issue control commands on the order of seconds [6]. This makes timely manual intervention by human operators quite difficult, if not impossible.

Ten *et al.* [7] propose an integrated security framework for power grids. The authors highlight operational blocks of the framework, but the interaction between these blocks is not clearly defined. A data model is needed to tailor the framework to a concrete infrastructure. Furthermore, the authors limit the analysis of the monitored data to anomaly detection. This approach is limiting because current power systems and ICT systems have well-known (non-anomaly based) security and detection mechanisms in place. Sridhar and Manimaran propose an automatic attack mitigation approach that addresses attacks on the AGC control loop [6]. While the described attack scenario leverages the cyber-physical design of the system under evaluation, the mitigation approach operates only on measurement data from the physical part of the system. Furthermore, a broader approach is needed to extend resilient operation to different control loops.

In this paper, we propose a novel cyber-physical resilience framework for smart grids. The framework aims to ensure acceptable levels of grid operation, even in the case of successful and targeted cyber-attacks. The novelty of our work lies in the integration of a synergistic approach linking the cyber and physical systems of a smart grid and in particular deriving a method intended for response and mitigation, rather than prevention and detection. In particular the focus lies on response and mitigation, rather than prevention and detection of the negative effects from successful cyber-attacks on physical system components or their control loops.

2 Proposed Research: A Cyber-Physical Resilience Framework

Our cyber-physical resilience framework consists of a *system model* and a *resilience control loop*. The system model has two main parts: *(i)* a *generic* system model that is provided with the framework; and *(ii)* a *specific* system model that has to be derived from the generic model when the framework is applied to a target infrastructure. The purpose of the model is to describe the necessary domain knowledge to realise the framework and to define the data structures that are transferred between the functional blocks that realise the control loop. The development of the generic model will be one major challenge for this research.

The operation of the grid is managed by the resilience control loop, which is depicted in Fig. 1. It interacts with both the ICT and physical systems of a smart grid to detect and mitigate cyber-attacks. Its functionality can be described as follows. Both the physical and ICT systems of the *Grid* will be monitored using

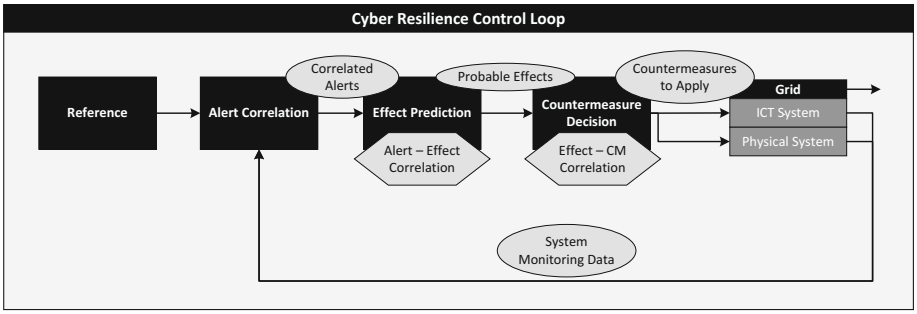

Fig. 1. The control loop at the center of our resilience framework. Rectangular blocks indicate the functional blocks in the loop, while ellipses (transferred data) and hexagons (domain knowledge) mark where parts of the system model will be used.

various systems. For example, for the ICT systems, existing security solutions will be used, such as intrusion detection systems. Meanwhile, for the physical systems various parameters (e.g., voltage, active and reactive power, frequency or phase) will be monitored. Additionally, existing security algorithms in the EMS (e.g., state estimation or bad data detection) [11] can be used to trigger alerts in the case of unexpected behaviour. We foresee one of the major challenges is choosing the right monitoring techniques at the different points of the cyber-physical system. This monitoring needs to be extensive, in order to get a comprehensive view of the whole cyber-physical system, but as limited as possible to make real time correlation feasible.

All *System Monitoring Data* is transferred to the *Alert Correlation* function. Additional information about operational metrics is provided from the *Reference*. The reference data is used to understand the status of the power system based on the collected physical measurements. It contains optimal, acceptable and critical ranges for the various physical measurements as well as operational constraints of the system. In the *Alert Correlation* function, information provided from both parts of the cyber-physical system is analyzed and correlated. The result of this phase is a set of alerts. An alert in this context is a signal that indicates a deviation from optimal system behaviour. The set of possible alerts is defined in the system model. The main challenges associated with realising the *Alert Correlation* function include determining the correct interpretation of physical measurement values during the course of operation, and the timely correlation of monitoring data from the ICT domain and physical domain.

The *Effect Prediction* functionality processes the correlated alerts and predicts the operational behaviour of the grid to detect potentially critical developments, so called effects. An effect is seen as a critical operational state that, if reached, would violate the definition of resilient operation, as defined by the *Reference*. Here we see the major challenge to be the development of an algorithm that estimates the future state of the grid, based on the alerts triggered by the current system state.

Finally, the predicted effects are transmitted to the *Countermeasure Decision* function. Here the available countermeasures are evaluated based on the set of

predicted system effects. A decision is taken on which countermeasures to apply. Arguably, for resilient operation it is not required to tackle the root cause of a problem. It can be a valid strategy to do so, but often the root cause cannot be automatically detected or eliminated. Rather, the highest priority of the applied countermeasures (to both the cyber and physical systems) is to mitigate the imminent threat to stable system operation. One challenge will be to identify applicable and effective countermeasures in each domain. Furthermore, applying an automatic countermeasure could result in the non-optimal operation of the grid. Therefore, the decision needs to aim for the least limiting countermeasure that is sufficient to mitigate the effect.

3 Research Methodology

We propose to take a practical approach to evaluating the resilience framework. A test setup, including a power generator and a Phasor Measurement Unit (PMU), will be developed, based on the work of Best *et al.* [2]. The goal will be to detect a set of attacks on a synchronized, but islanded generator. The effects of such attacks can range from outages in the island to equipment damage when the generator is reconnected to the mains supply whilst not synchronized. Countermeasures will be developed to automatically mitigate these risks. To ensure that the lab experiments are representative for attacks in the wild, they will be based on officially published threat scenarios (e.g. the *Electric Sector Failure Scenarios and Impact Analyses* by NESCOR [1]) and performed with modern protocols like IEC 61850. Measuring the effectiveness of the proposed framework will be performed in two ways. Physical (e.g., phase, current or frequency) and operational metrics (e.g. thresholds or set-points) will be used to evaluate the timely effectiveness of the framework in countering the critical effects of successful cyber-attacks. Second, we will develop experimental scenarios that will allow us to compare our framework to related work, such as that discussed earlier.

4 Conclusion

In this paper, we have argued for the need for a cyber-physical resilience framework for smart grids, and presented our initial findings for developing such a framework. The expected impact of this research is an increased resilience of future power systems against cyber-attacks. This resilience is needed to successfully realize the vision of a smart grid. Without it, smart grids will either be realized in a limited way, or the increased use of ICT technology in the power domain will open the means for cyber-attacks with significant societal impact. From a scientific point of view, this research aims to make new advances in cyber-physical system resilience. Results of this research could be extended to address emerging threats or applied to other application domains of cyber-physical systems.

Acknowledgments. This research is funded by the EU FP7 SPARKS project.

References

1. Technical Working Group 1. Electric Sector Failure Scenarios and Impact Analyses. Technical report, NESCOR (June 2014)
2. Best, R.J., Morrow, D.J., Laverty, D.M., Crossley, P.A.: Synchrophasor Broadcast Over Internet Protocol for Distributed Generator Synchronization. IEEE Transactions on Power Delivery 25(4), 2835–2841 (2010)
3. Friedberg, I., Skopik, F., Settanni, G., Fiedler, R.: Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security 48, 35–57 (2015)
4. Lee, R., Assante, M., Connway, T.: ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack. Technical report, SANS ICS (December 2014)
5. Smith, P., Hutchison, D., Sterbenz, J.P.G., Scholler, M., Fessi, A., Karaliopoulos, M., Lac, C., Plattner, B.: Network Resilience: A Systematic Approach. IEEE Communications Magazine 49(7), 88–97 (2011)
6. Sridhar, S., Govindarasu, M.: Model-Based Attack Detection and Mitigation for Automatic Generation Control. IEEE Transactions on Smart Grid 5(2), 580–591 (2014)
7. Ten, C.-W., Manimaran, G., Liu, C.-C.: Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 40(4), 853–865 (2010)
8. Vukovic, O., Sou, K.C., Dan, G., Sandberg, H.: Network-layer Protection Schemes Against Stealth Attacks on State Estimators in Power Systems. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 184–189 (October 2011)
9. Wang, D., Guan, X., Liu, T., Gu, Y., Shen, C., Xu, Z.: Extended Distributed State Estimation: A Detection Method Against Tolerable False Data Injection Attacks in Smart Grids. Energies 7, 1517–1538 (2014)
10. Wei, D., Lu, Y., Jafari, M., Skare, P., Rohde, K.: An Integrated Security System of Protecting Smart Grid Against Cyber Attacks. In: Innovative Smart Grid Technologies (ISGT 2010), pp. 1–7 (January 2010)
11. Wood, A.J., Wollenberg, B.F.: Power Generation, Operation, and Control, 3rd edn. John Wiley & Sons (2012)
12. Zhu, B., Sastry, S.: SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy. In: Proceedings of the 1st Workshop on Secure Control Systems, (SCS) (2010)