Cyber-security Role in Enhancing Resilience

Cvetkovic, Milos; Palensky, Peter

Publication date
2018

Document Version
Accepted author manuscript

Citation (APA)
Cvetkovic, M., & Palensky, P. (2018). Cyber-security Role in Enhancing Resilience. https://smartgrid.ieee.org/newsletters/september-2018/cyber-security-role-in-enhancing-resilience

Title: Cyber-security Role in Enhancing Resilience

Authors: Milos Cvetkovic, Peter Palensky

Cyber-threats are challenging the resilience of power systems in ways uncommon to 'classic' operational risks of equipment failures and natural disasters. As an example, consider an attacker who monitors operator actions after a cyber-attack and who persistently blocks any operator attempt to mitigate the impact of the attack. Such immediate reply to operator actions is deliberately constructed, thoroughly thought of, and, typically, well-funded by malicious sources. To accommodate such cyber-attack characteristics, the resilience thinking must expand into the cyber-physical domain in which power systems, information technology (IT) and operational technology (OT) are considered as one system under scrutiny.

Until now, the power system community has coined terms of operational and infrastructure resilience to differentiate between service-disrupting and infrastructure-damaging events and the respective resilience measures. According to many studies, the operational resilience of power systems refers to operational strength to sustain system-threatening events, ensuring uninterrupted supply to customers and sufficient availability of generation capacity. The infrastructure resilience refers to the capability to cope with the nonfunctional parts of the grid, due to severe damage of one or more pieces of equipment. The dedication of the community to these two directions is embodied by the CIGRE working groups C2.25 and C4.47, that address them, respectively. In this article, we reflect on characteristics of cyber-attacks in relation to power system resilience.

A well-orchestrated cyber-attack consists of multiple actions that are targeted at infiltrating the industrial control system (ICS), weakening the defense and response measures, reducing the operator awareness to the true state of the system and maximizing the impact of the attack, all while ensuring the attacker cannot be traced. The attacks are performed by utilizing IT and OT systems of the grid operator, such as the corporate enterprise network and the ICS that include Supervisory Control And Data Acquisition (SCADA) and Wide Area Measurement, Protection and Control (WAMPAC) systems. At times, the attackers target supporting services, such as the emergency call line in the case of the Ukraine attack. The typical attacks are launched at the lower network layers as denial of service attacks, and at higher network layers as data integrity attacks. To successfully launch such attacks, ICS specialized malware is deployed after gaining access to the corporate network, control room and work stations in the field, or maintenance crew terminals.

Once the access to the ICS system is obtained, there is a multitude of options at the attacker disposal. Any of the operational processes can be scrambled, from indirectly toying with measurement systems and the state estimators, causing false grid observability, to directly dispatching malicious commands to the field devices in operation. In addition, the grid protection and restoration systems could be disarmed rendering the control room helpless during emergencies.

Since remaining untraceable until the moment of the attack is always one of the key attacker's goals, *intrusion detection* plays a crucial role in ensuring resilience. The intrusion detection systems (IDS) monitor the IT and OT systems for malicious activity and policy violations. The IDS deploys signature-

based and anomaly-based detection to identify corrupted packets and the deviations from the nominal traffic patterns. And yet, today's off-the-shelf IDS analyze network activity without taking ICS process semantics into account. Since power systems are industrial processes with highly rich semantics, i.e. well-established operational procedures and methods, there is ample opportunities to enhance the existing IDS. For example, including the output of the state estimation into the IDS would reduce the attack space that is available to the adversary and increase the probability of the detection, making the attack more difficult to launch. The enhancements such as this one would surely improve resilience in terms of robustness.

Furthermore, cyber-attacks have certain characteristics which make them peculiar in the context of resilience. For example, an attack is not necessarily confined to a certain geographical area, and could be launched simultaneously in various, distant parts of the grid. This is in contrast to natural disasters, which are usually spatially concentrated. Hence, designing self-sufficient grid partitions and superb islanding schemes would improve resistance to and recovery from a resilience-threatening event. Next, the attacker often looks to minimize resources to infiltrate the system, while maximizing the expected impact on the infrastructure. Thus, reinforcing the weakest links in the security chain, the electricity grid infrastructure and the power system operation procedures, are the necessary steps towards higher robustness. The human factor is also to be included. Since, historically, information security has not played a big role in the energy area, the information-safety mindset should be cultivated within the grid stakeholder organizations. Finally, an attacker could have means of countering operator actions, which could prolong the attack and increase its impact. Thus, the redundant and diversified defense measures and highly-skilled personnel in incident response are needed for higher level of resilience in the face of cyber-threats.