EPRI | ELECTRIC POWER RESEARCH INSTITUTE

QUICK BRIEF: CRITICAL INFRASTRUCTURE INTERDEPENDENCIES ON GENERATION CAPACITY—MANAGING RISK

Malware and Ransomware Expose Critical Interdependencies for Generation Plants

Generation plants contain various interdependencies from critical infrastructure that can impact their capacity to generate power. Some of the interdependencies are external to the utility, and others are internal to plant support. These interdependencies remain the focus in many recent ransomware and malware attacks on critical infrastructure companies. As reported recently, Colonial Pipeline became the victim of a ransomware attack. Cyber threat actors known as *DarkSide* developed the ransomware, which caused Colonial Pipeline to proactively curtail operational technology (OT) operations on its pipeline. Because critical billing services were impacted, its ability to account for fuel distribution [1] was limited. If critical communications are needed between an information technology (IT) network and an OT network and one of them has been compromised, that internal interdependency could become a limiting factor that could cause a forced outage.

External interdependencies also exist. Examples of external generation plant interdependencies include fuel pipelines, transportation systems, water supplies, and communications systems. There are many examples where external interdependencies have forced an outage at a power plant. In many cases, generation plants rely on fuel supplies from natural gas pipelines or transportation systems. If the pipeline were not able to deliver fuel, rail transportation were unavailable, or barging were halted, fuel would not be able to make its way to the plant. Many coal power plants stockpile coal for emergency use to ensure continued operations, but this is limited to days, not indefinitely. Combined-cycle power plants are limited to fuel being transported within the pipeline, and many do not have active storage on-site.

Determining the Risk Associated with Internal and External Interdependencies

Cyber security risk consists of the likelihood and consequence of a successful attack. The risk level differs for a successful attack in an IT network versus an OT network. Within an OT network, the risk level is different from system to system. Understanding the internal and external interdependencies on the IT network (business operations) and the OT network (plant operations) is an important component to determining risk. There are several use cases for OT system operations that traverse the IT/OT boundary. If IT systems are compromised, OT operations, such as the following, could be impacted:

- Monitoring and diagnostics of plant conditions
- Physical and cyber security operations
- Integrated identity management
- Vendor and utility remote access
- Continuous emissions monitoring systems
- Remote control and operations

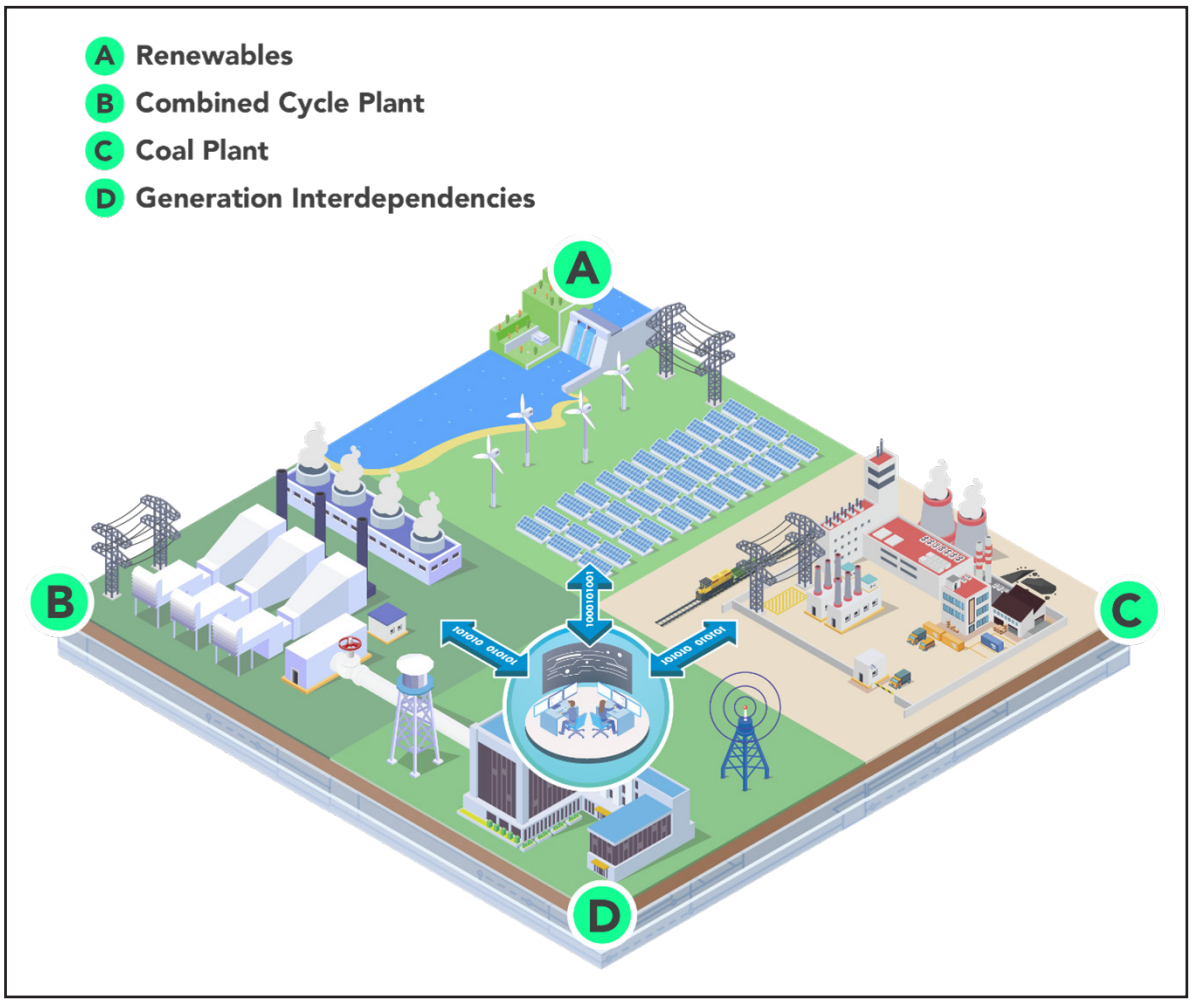

Figure 1: Generation plants and interdependencies

Loss of any of these functions further impacts either short- or long-term operations. Understanding the consequence of a compromise of these functions is the first step in developing a cyber defense-in-depth strategy.

What also became apparent from the Colonial Pipeline ransomware compromise was that the curtailment of OT pipeline operations caused a large gap in fuel delivery service for a large portion of the Southeastern United States. It was evident that the gap in service exposed a lack of resiliency and diversity in the impacted area. It led to localized gas shortages, hoarding, and negative sentiment for the company. These impacts should be taken into consideration when determining overall risk. For generation plants, multiple regional concurrent plant outages caused by impacts from interdependencies could have varied results. If multiple plants are impacted at once in a region, this could cause destabilization of the grid or brownouts/blackouts.

Figure 1 illustrates how generation assets have external and internal interdependencies with data networks, fuels supplies, communications systems, water supplies, etc.

When determining risk, cyber security organizations can ask questions such as the following:

- Is my plant's OT network architecture segmented so that an IT compromise cannot compromise OT devices across the IT/OT boundary?
- What are my network bypasses, and can they be leveraged by an adversary or malware?
- How long can my plant operate if my critical infrastructure service providers (interdependencies) have a disruption?
- If my plant (and others in the fleet) are in a forced outage, what could be the downstream impacts to critical loads, customers, and other critical infrastructure sectors?

EPRI worked with the National Energy Technology Lab to develop a Fossil Power Plant Cyber Security Life-Cycle Risk Reduction Framework [2]. The framework can be used for all power generation as a tool to understand facility risk, identify potential vulnerabilities, and allocate cyber security control to mitigate the vulnerabilities.

Mitigating Risks Associated with Generation Interdependencies

Identifying the risk level and the utility's acceptable risk tolerance is the first step toward mitigation. A defense-in-depth approach is recommended to ensure that controls perform the following functions:

1. Protect against a cyber attack
2. Detect when a cyber compromise is ongoing
3. Respond to a cyber attack
4. Recover after the compromise has been eradicated

This seems simplistic, but no one cyber security function stands alone and there are no singular controls that are all-encompassing. These functions work together to provide a holistic defense-in-depth cyber security strategy that is the basis of a mature OT cyber security program. The cyber security control allocation can be further broken down to be effective in mitigating impacts from external and internal interdependencies. For example, EPRI's Cyber Security Procurement Methodology [3] can help ensure that external critical infrastructure interdependencies and impacts are minimized through contractual requirements and mandatory cyber security control application in suppliers' OT environments. In addition, the critical function controls help to limit or eliminate downstream impacts by avoiding a forced outage.

EPRI's Cyber Security Technical Assessment Methodology [4] is a tool that utilities use to identify and mitigate vulnerabilities through cyber security control application at the device level, system level, or even facility level—and considers the *Protect, Detect, Respond,* and *Recover* functions listed previously. Other EPRI guidance that is focused on cyber security control applications in generation plants helps to identify an effective control strategy and determine which controls can be used for a layered defense. By layering the critical function controls, mission-critical assets inherit control efficacy from higher-level controls within the application, endpoints, network, and network perimeter. See Figure 2 for an illustration of a layered defense.

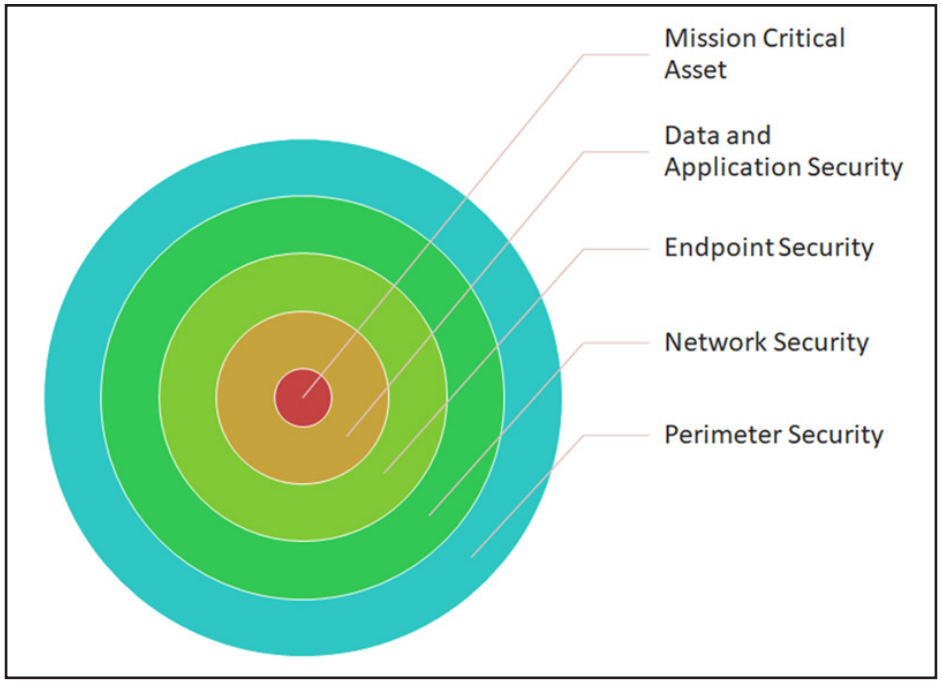

Figure 2: Layered control approach for generation assets

Working with Generation Utilities to Identify Challenges and Research Gaps

EPRI generation sector cyber security subject matter experts (SMEs) and researchers are working with electric utilities to understand where industry challenges exist and what research needs to be prioritized to address gaps. The Cyber Security for Generation Assets program develops applied solutions such as technology, tools, software, and field guides that are used by utilities to provide immediate value. This program researches tactical issues impacting generation plants today and strategic issues that will impact generation utilities in the future, to help utilities build robust and agile generation OT cyber security programs.

Identified gaps include the following:

- Protect
  - Wireless security
  - Virtual machine security
  - OT network microsegmentation
- Detect
  - Inspection of OT protocols
  - Security data integration and analysis
- Respond
  - Incident response scenario development
  - Playbook development
  - Testing and drills
- Recover
  - Incident response team training
  - Recover agreements for vendors and contractors

Although EPRI SMEs work with utilities to prioritize and sponsor this identified research, there are numerous resources available to help determine a plant's risk level and risk acceptance, determine the correct control to mitigate vulnerabilities, and build the capability of the generation OT cyber security program. More information can be found at https://www.epri.com/research/programs/112046/results.

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com)

Technical Contact

Jason Hollern, 704.595.2579 (jhollern@epri.com)

References

1. https://www.mediaite.com/news/colonial-pipeline-shut-down-distribution-because-it-couldnt-bill-customers-report.
2. *Fossil Power Plant Cyber Security Life-Cycle Risk Reduction: A Practical Framework for Implementation*. EPRI, Palo Alto, CA: 2020. 3002019700.
3. *Cyber Security in the Supply Chain: Cyber Security Procurement Methodology, Revision 2*. EPRI, Palo Alto, CA: 2018. 3002012753.
4. *Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1*. EPRI, Palo Alto, CA: 2018. 3002012752.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together . . . Shaping the Future of Electricity

3002022287 June 2021

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA • 800.313.3774
• 650.855.2121 • askepri@epri.com • www.epri.com