Operational Technology (OT) Security in Substations

by **Bryan J. Gwyn**
and **Sagar S. Singam**

Operational Technology (OT) is a broad category of programmable systems or devices that interface with or manage equipment that interacts with the physical environment [1]. Organizations have tended to deploy specialized point solutions to solve specific challenges, as digital innovation has spread IT and OT networks have fused. These approaches to OT security resulted in a complex network in which the solutions could not communicate information and give complete visibility. Network OT typically reports to the COO, and IT to the CIO, resulting in two network security teams, each covering half of the network. There are several ways to manage OT security, and this article focuses on asset management and the need to patch those assets using a typical architecture.

Photo: AdobeStock

Bryan J. Gwyn is Doble's Senior Director of Solutions at Doble, with over 30 years of international experience in electric utility Transmission and Distribution protection, control and telecommunication engineering, operations and management. Leading a team of global subject matter experts, he is responsible for the development of Protection, Asset Management, Monitoring and Security solutions. Bryan received his BEng (Hons) Electrical and Electronic Engineering degree and his PhD at City University, London, UK. He is a Chartered Engineer and Senior Member of IEEE.

Sagar S. Singam is a Senior Cybersecurity Engineer at Doble with over 8 years of experience in industrial and IT cybersecurity architecture. He obtained his Master's in Information Assurance and Cybersecurity from Regis University. He is a member of IEEE PES.

Operational Technology (OT) is a broad category of programmable systems or devices that interface with or manage equipment that interacts with the physical environment.

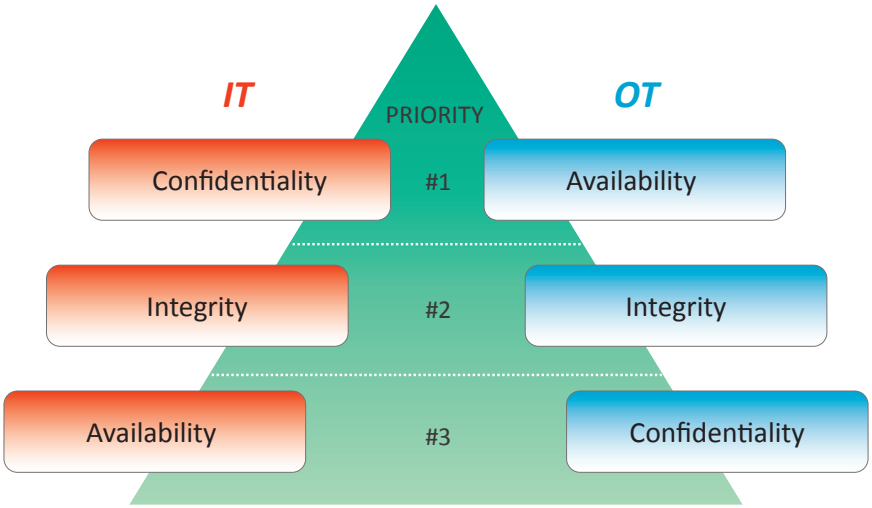

Figure 1. CIA Triad

Confidentiality-Integrity-Availability (CIA) Triad

The CIA Triad is a data security concept. It directs a company's data security efforts. In fact, including these ideas in any security program is ideal. The three pillars of security architecture are as follows.

Confidentiality

In today's world, it is critical for people to protect their sensitive private information from unauthorized access. Protecting confidentiality necessitates the ability to define and enforce specific levels of access to information. In some cases, this entails categorizing information into different collections based on who needs access to the information and how sensitive the data is—the amount of damage suffered if confidentiality is breached. Access control lists, volume and file encryption, and Unix file permissions are some of the most used methods for managing confidentiality.

Integrity

The "I" in the CIA triad represents data integrity. This critical component of the CIA Triad is intended to prevent data from being deleted or modified by unauthorized parties. For example, online buyers demand accurate product and pricing information and assurances that the quantity, cost, availability, and other information will not change after they make their order. Data integrity safeguards include encryption, hashing, digital signatures, and digital certificates.

> Confidentiality, Integrity and Availability make the CIA Triad, and they are the three pillars of security architecture.

Availability

The availability of your data is the focus of this stage—the third in the CIA Triad. High availability systems are computing resources with architectures specifically designed to increase availability. The most well-known attack that jeopardizes availability is called a "denial-of-service" attack, in which a system, website, or web-based application has its performance purposely and maliciously compromised, or the system is rendered inaccessible. The breakdown of hardware or software, power outages, natural catastrophes, and human error are other possible risks to availability. The information must be protected and made available when needed, which requires that authentication procedures, access routes, and systems all function effectively.

The CIA Triad is all about information and data security. But the first thing to note in Figure 1 is that, in general, IT and OT risk management priorities differ. **IT prioritizes confidentiality, while OT prioritizes availability, followed by integrity and confidentiality (A-I-C).**

IT and OT Security Management in Substations

Attacks on critical infrastructure have caused power outages and compromised sensitive data, as well as evoking nightmare scenarios involving environments such as water supply systems, petrochemical installations, nuclear power plants, and transportation infrastructure systems, all of which rely on operational technology (OT) and, to varying degrees, information technology (IT) [2]. The primary focus of IT is data and its free and secure flow. It is fluid and has many moving parts and gateways, which makes it more vulnerable and provides a larger surface for a broader range of constantly evolving attacks. Defending against attacks entails protecting every layer and constantly identifying and correcting flaws to keep data flowing.

> While IT prioritizes confidentiality, OT prioritizes availability, followed by integrity and confidentiality (A-I-C).

Traditionally, IT and OT had distinct roles. OT teams were accustomed to working with closed systems that relied heavily on physical security mechanisms to ensure integrity. The industrial Internet of Things (IIoT) and the integration of physical machines with networked sensors and software are blurring the lines between the two. As the Internet of Things (IoT) connects, communicates, and interacts with more objects, the number of endpoints and potential ways for cybercriminals to gain access to networks and infrastructure systems grows. Interaction between operational

and information technology systems is essential for the Digital Substation. Control systems, SCADA, and industrial networks connect to IT components like processors, storage, and systems management. **Data collected by physical and Industrial Internet of Things (IIOT) devices can be used to identify problems and improve efficiency with IT-OT integration.**

Understanding the difference between IT and OT is crucial because the two are frequently confused. While operational technology controls equipment, information technology (IT) controls data. IT mainly ensures systems and data confidentiality, integrity, and availability.

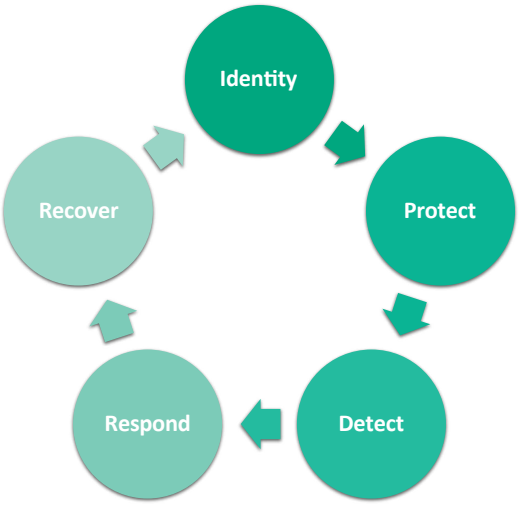

Figure 2. NIST Cybersecurity Framework (CSF)

> Data collected by physical and Industrial Internet of Things (IIOT) devices can be used to identify problems and improve efficiency with IT-OT integration.

OT Security Governance

The Federal government has issued many executive orders in the past to strengthen the cybersecurity posture of vital infrastructure [3]. President Biden most recently signed Executive Order 14028 "Improving the Nation's Cybersecurity" in May 2021 to protect critical infrastructure [4]. This directive focuses on modernizing cybersecurity requirements such as data encryption at rest and in transit, a zero-trust architecture, and the deployment of multifactor authentication and data encryption within a certain time frame. This demonstrates that even today, having a basic security foundation, such as the NIST Cybersecurity Framework (CSF), which went into force nearly a decade ago, is vital for critical infrastructure organizations. The NIST CSF consists of the framework core, profiles, and implementation tiers. While the core functions of the NIST CSF include categories, subcategories, and informative references, **we will focus on the first two core components shown in Figure 2 of this framework from a 1000-foot perspective.**

Asset Management, a comprehensive inventory of all OT assets, is one of the essential core components of an OT asset database. Not only hardware but also a comprehensive view of the data, personnel, devices, systems, and facilities that enable the organization to meet its objectives. They must be identified, and their importance in business objectives and risk management must be clearly established.

Database management software can bridge the divide between competing IT and OT priorities. Look for a relational database architecture that will support a central data warehouse structured for universal interfacing to external systems. Bringing such a system online will integrate OT data into a hub where asset management and work management will intersect.

Connecting dataflows emanating from different sources enables OT teams to have the data integrity, availability and confidentiality they prioritize while critical elements related to human performance and network security remain intact for IT intents and purposes. The ideal OT database management system will accept user authentications developed in the IT domain which complements the corporate cyber security measures put in place for user (and device) password management, which assures data security and integrity as well.

> The ideal OT database management system will accept user authentications developed in the IT domain which complements the corporate cyber security measures put in place for user (and device) password management, which assures data security and integrity as well.

After identifying and categorizing your assets, you should take proactive measures to safeguard them from internal and external cyber threats. Security maintenance rules and practices, including **software patch management** and whitelisting, must be created and implemented for the NIST CSF's Protect component.

Figure 3. Integrated OT and Security Management Platform

These two methods are most often used in vulnerability management and protection.

In practice, maintaining approved software is a labor-intensive obligation with tremendous implications on IT resources. For instance, some electrical equipment requires software that could be many years older than software used with newer equipment. Monitoring the wide variety of software applications used in OT, not to mention the sheer quantity of laptop computers and electrical device firmware versions, is a major effort that directly impacts IT teams. Regardless, it is critical that the software and computers used in OT do not pose any cyber security vulnerabilities that could risk cyberattacks successfully entering critical infrastructures.

Regulatory standards, like NERC CIP-10 for example, spell out baseline requirements IT must abide by in regard to cyber security that affects OT. According to NERC, any computerized device that is connected temporarily to any component of a cyber system is classified as a Transient Cyber Asset (TCA) and must not only be hardened, but also receive software and security patch updates regularly. Failure to provide evidence that NERC requires during audits can incur financial penalties.

Facing heavy responsibilities and internal costs, IT can look to a managed program from a vendor that can augment in-house resources with proactive software and security patch monitoring. Look for a program that offers a comprehensive and secure portal that both centralizes management functions and automates approving and deploying patches and updates to TCAs.

> The CIA Triad, like the NIST CSF or any other successful security practices like asset management and software patch management cycle, ensures resistance against attackers.

The solution should accommodate all whitelisted software regardless of the operating systems older applications might require, and it should offer tracking and reporting tools that promote NERC compliance audit readiness. Additionally, the solution should scale to your requirements and offer flexible commercial terms.

Summary

Finally, because every business has various security concerns, the CIA Triad and NIST CSF are not a one-size-fits-all solution for handling OT Security challenges in Substation environments. This is where a solid security foundation comes into play, allowing organizations to assess which solutions are necessary to safeguard their vital infrastructure. Many high-profile cyberattacks on industrial companies in recent times have influenced how corporations approach security. The CIA Triad, like the NIST CSF or any other successful security practices like asset management and software patch management cycle, ensures resistance against attackers.

To sustainably contribute value to and seize the benefits of the future digital economy, every company must withstand cyber disruption.

References

[1] Operational Technology Security, *NIST*, 2021, accessed at https://csrc.nist.gov/projects/operational-technology-security

[2] Cyber Security, *IEC*, 2021, accessed at https://storage-iecwebsite-prd-iec-ch.s3.eu-west-1.amazonaws.com/2021-08/content/media/files/iec_2021_cyber_security_a4_en_lr_0.pdf

[3] G. Meghan, *What is the NIST Cybersecurity Framework?, Verve*, 2022, accessed at https://verveindustrial.com/resources/blog/what-is-the-nist-cybersecurity-framework/

[4] Executive Order on Improving the Nation's Cybersecurity, 2021, accessed at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Photo: Shutterstock