Defense-in-Depth Security for Industrial Control Systems

Jess Smith, Nathan Kipp, Dennis Gammel, and Tim Watkins
Schweitzer Engineering Laboratories, Inc.

Revised edition released August 2022

Published in
Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions, 2018

Originally presented at the
EEA Conference, June 2016

Defense-in-Depth Security for Industrial Control Systems

Jess Smith, Nathan Kipp, Dennis Gammel, and Tim Watkins
Schweitzer Engineering Laboratories, Inc.

Nathan Kipp, Presenting Author

EEA Conference & Exhibition 2016, 22 - 24 June, Wellington

Abstract

There are three core goals of cybersecurity: confidentiality, integrity, and availability. They are commonly known as the security triad, or CIA. Confidentiality is the idea that information can be kept secret and known only to those people or systems who need that information to perform their duties. Integrity is the idea the information is valid and verifiably correct. Availability is the idea that a system or data is running or available when it is needed. To obtain true security, all three of these core concepts are required.

Grouping an industrial control system (ICS) into zones of security is a logical way to begin planning for availability, integrity, and confidentiality in the system. First, we break the system into three regions: 1) the analog data and devices region, 2) the region encompassing devices with machine-to-machine communications, and 3) a region where humans interact with the system.

The second of these, the machines-only region, we further separate into three zones based on the application and function of the devices therein. The first or lowest zone is analog and includes devices that directly interact with the analog region and perform real-time monitoring and issue corrective instructions. The second machine-only zone performs non-real-time automated functions such as event collection and upstream reporting. The third machine-only zone is the barrier that deters humans from directly interacting with the first two zones. Each of these regions and zones has specific considerations for the operations and security of that zone and, therefore, the entire system.

By logically breaking up the network in this fashion, we are able to apply security tools, techniques, and procedures to ensure the confidentiality, integrity, and availability required at each of the individual devices or levels. We are also able to take advantage of the network itself to support our security. Finally, this system allows us to consider methods for implementing security, not only in newly commissioned ICSs but also in existing ICSs, by identifying and prioritizing critical regions.

Defense-in-Depth Security for Industrial Control Systems

Jess Smith, Nathan Kipp, Dennis Gammel, and Tim Watkins
Schweitzer Engineering Laboratories, Inc.

I. Introduction

Cybersecurity is traditionally considered to be composed of three competing goals: confidentiality, integrity, and availability (CIA). Confidentiality prevents users from accessing unauthorized information or objects. Integrity is assurance that a device is correctly functioning and that the information it communicates is complete and without fault. Availability requires that a resource be available in a reasonable amount of time to an authorized user. [1] [2]

Access to remote industrial control system (ICS) components, such as substations, was (and still often is) managed primarily through physical access control measures such as locks, fences, and guards. The focus in the design and development of an ICS was availability, with secondary attention and resources given to integrity. Confidentiality was considered and planned for last. Increased communication and connectivity, when implemented safely and securely, provides opportunities for the automation and integration of systems, which can increase reliability and efficiency.

Modern substation designs provide enhanced functionality through increased connectivity, communication, and advanced computing devices. Advanced computing devices provide the opportunity for additional data analysis and can provide better situational awareness. An advanced computing device also often has more storage for alarms and logs, increasing the confidentiality and integrity security positions. [3]

ICSs are engineered for specific applications. Communications and functionality are designed into the system as needed rather than being required in every single device. This reduces the complexity and cost of ownership.

A defense-in-depth method has been proposed by the United States Department of Homeland Security [4] and many other researchers [5] as being secure and flexible as an end-to-end cybersecurity solution. In this paper, we describe a defense-in-depth scheme that applies specifically to the ICS realm, with implementation details and an example system.

Section II discusses defense in depth as it applies to an ICS at a high level. Section III dives into the security at each level of the diagram. We explore the security challenges found at the edges of the ICS in Section IV. Section V provides an example system in which we have implemented defense in depth from the ground up.

II. Proposed Levels

ICSs differ from enterprise networks in many ways, but one of the primary ones is the computing capabilities of the end devices. In an enterprise network, the end devices are desktop PCs, laptops, smart phones, and other general purpose devices that can perform a range of duties. They are designed to ensure both their own security as well as the security of their communications. In an ICS, devices have a wide range of capabilities, from old mechanical relays to modern, microprocessor-based relays, all of which are focused on ensuring continued operations of the ICS.

There are also a wide range of security goals, performance requirements, and access needs throughout the ICS network. By applying the proposed defense-in-depth model, it is possible to more easily focus on the security goal that is most critical at part of the network. At the lowest regions of the

network, where the devices that directly control the physical switches, actuators, etc. are located, availability is critical. At higher regions, the confidentiality and integrity of the data presented to the human user are more important.

With these many factors in play, it makes sense to adopt a layer-based security model, where each layer builds more security into the network to ensure that mission-critical resources and tasks are handled.

A. A Holistic View of the Levels

The proposed defense-in-depth model of an ICS network has seven levels, each with its own considerations for security and monitoring (see Figure 1). These levels are delineated by their functional tasks and the focus of their goals. Levels 3 and below are machine-based and communications are largely machine-to-machine, with a focus on ensuring continued operation of the ICS. Level 4 and above are human-to-machine, with a focus on providing high-level services like data aggregation and logging. At lower levels of the ICS, availability and integrity remain the goals, while in the human-interfacing regions confidentiality and integrity become more important.

Different aspects of security are considered at each of these layers. In the human-to-machine communications region (Level 4 and above), confidentiality and integrity are of higher importance. In the machine-to-machine communications region (Level 3 and below), the need for availability increases, while the integrity requirement remains. In the enterprise world, if email or web traffic is delayed 200 to 400 milliseconds, there isn't an issue. However, in an ICS, a GOOSE message must get from relay to relay and be processed in 4 milliseconds. Similarly, it is possible and suggested to allowlist communications in the machine-to-machine region of an ICS, but a denylist approach is required in the human-to-machine and enterprise regions because the constantly changing range of communications.

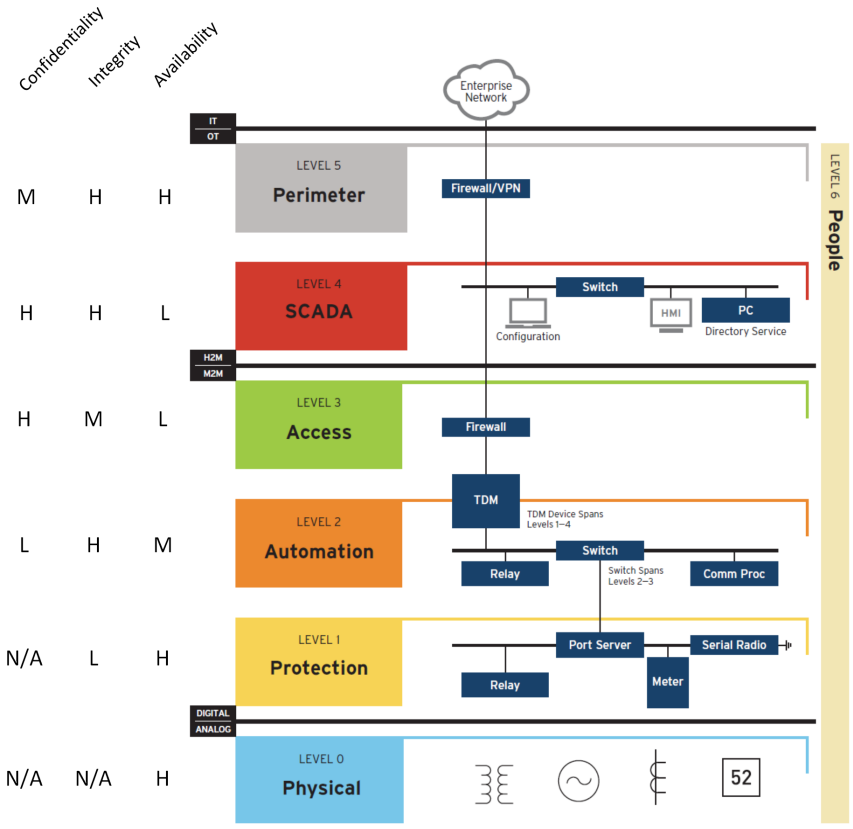

Figure 1 Defense-in-Depth Levels Diagram

The complexity in the network and devices increases in Level 4 and above, reaching into the enterprise network. This can include more-traditional operating systems that must be maintained on a regular basis. The complexity of Level 4 offers a malicious actor a different and much wider attack surface than the lower levels. Alternatively, it may be much easier for a malicious actor to gain access to Level 0 sensors placed outside of the physical security perimeter.

B. Security at Each Level

The strength of a defense-in-depth model is that it allows a specific security focus at each layer and a comprehensive security solution for the overall ICS.

1) Level 0 – Physical

Included: Analog data collection and direction devices, such as relays, sensors, meters, motor control units, valves, and solenoids.

Focus: Availability is the focus at this level because the raw data are transferred here before any processing has taken place.

Implementation: Security at this level is primarily physical in nature. Substation physical security to enable the availability of Level 0 should be focused on keeping intruders away through deterance: obstacles, borders, visible signs, visible cameras, etc. Secondarily, detective and defensive measures in the form of alerts and armed responses should be implemented in the cases where deterance isn't sufficient. Detective measures include motion detectors, occupancy sensors, and cameras.

2) Level 1 – Protection

Included: Devices that process the sampled data produced by the sensors and convert it into digital data for internal processing and decision making. Devices at this level rely on data in real time to actuate substation yard assets (switchgear, breakers, capacitor banks, etc.) for electricity reliability and safety.

Focus: Availability is paramount at this level, both that of the intelligent electronic devices (IEDs) and their processing capabilities and that of the communications because of their real-time nature. The integrity of the IEDs is also of concern. If the IEDs are not set correctly, they cannot perform correctly.

Implementation: One technique to ensure the integrity of IED configurations is baselining and baseline verification. When an IED is first configured and placed in service, take a baseline of all settings on the device. Periodically return to the device and compare existing settings to the baselined settings. If anything doesn't match, it means the device is no longer set correctly.

The nature of the seven-level architecture helps maintain the availability at Level 1. Limiting unnecessary incursions by legitimate users, malicious users, automation processes, and other unnecessary processes keeps communications channels open for the time-critical communications that occur at Level 1. Level 1 devices and communications should be carefully defined and separated from the rest of the system with port servers and gateways.

There is increasing desire to add more capabilities to Level 1 devices, such as LDAP/RADIUS and other centralized management-oriented protocols. While these protocols may make sense in enterprise systems, the result is increased complexity and attack surface for Level 1 devices. The increased attack surface provides opportunities for malicious actors to compromise the devices while the increased complexity results in a greater likelihood of misconfiguration by the end user and improper implementation by the manufacturer. Complex devices must be actively maintained.

3) Level 2 – Automation

Included: Devices that take in the analog data produced by sensors, digitize it, and process it at a non-life-safety priority. These devices can also take digital input from Level 1 and provide non-protection related processing, such as for SCADA, metering, event retrieval/recording, synchrophasor collection, etc.

Focus: A focus on integrity should take precedence at this level. Integrity is important to ensure that the system state and events are correctly reported to operators.

Implementation: Integrity can be achieved through baselining and baseline verification. The architecture Level 2 is built with can also help achieve availability and integrity goals at Levels 0 and 1. Requiring all communications from higher levels to Level 1 to go through Level 2 devices means that Level 2 devices can filter and process those communications and prevent certain activities, such as denial of service (DoS), remote firmware updates, etc. While this potentially compromises the availability of devices at Level 2, it increases the availability of devices at Level 1.

4) Level 3 – Access

Included: Devices that separate, restrict, and filter the human-to-machine levels from the machine-to-machine levels. One function is to proxy only authenticated access from the approved SCADA devices for those users with the correct access privileges to machines in the lower levels.

Focus: Integrity and confidentiality increase in importance. Levels 3 and above interact with external networks and cannot always be thought of as truly private. This is especially true when higher levels start including general purpose computers, which are easier to compromise and use as pivots to access control system devices.

Availability begins to fall off in importance at this level because the primary purpose of this level is to act as the last barrier before the machine-to-machine communications region. As a barrier, it is intended to pass through only authorized communications; it is also designed to take the brunt of any DoS attacks, preventing those types of attacks from reaching downstream layers. Level 3 availability is not expected to be 100 percent. In a situation where the availability of Level 3 is lost, Levels 0–2 will not be negatively affected, and they will continue to perform as though no attack were in progress.

Implementation: To secure communications from the human-to-machine region, commonly used technologies include encryption techniques such as IPsec, TLS, SSH, and others. Integrity and confidentiality become more important because there are attack methods that can manipulate even encrypted data. Fortunately, many of the techniques used to encrypt data can also be used to cryptographically ensure the integrity of communications. IPsec and TLS both provide cryptographic integrity verification in addition to encryption.

5) Level 4 – SCADA

Included: Devices in this layer provide the human-machine interface (HMI) view of the system. This is where humans can influence the system. This level can also be thought of as a demilitarized zone (DMZ), where humans can safely interact with the system without potentially compromising the protection and automation tasks occuring at lower levels. Centralized management protocols are used here because this is where the humans who require these data reside. Alarms, logs, and events are collected from all of the lower-layer sites to build a strategic picture of the ICS; machines with traditional operating systems and other advanced computing devices often operate in Level 4.

Focus: Both confidentiality and integrity are of critical importance at Level 4 because of the prevalence of general purpose computers, while availability takes a back seat.

Implementation: General purpose computers have more attack surfaces that malicious actors can compromise and then utilize as pivots to propogate their attacks throughout the system. From a network/system perspective, the risk that general purpose machines introduce can be reduced with encryption, which prevents compromised computers from sniffing network traffic and collecting sensitive information such as usernames and passwords. Encryption can also be used to

protect data at rest, such as those found in information archives, data historians, credential storage, etc. (all Level 4 devices).

Integrity becomes very important at Level 4 to mitigate the kinds of techniques seen in Stuxnet and the recent Ukraine attack. In these attacks, the HMIs and system data were compromised to present false information to system operators. This allowed malicious actors to tamper with the control system IEDs without the operators being aware. Cryptographically authenticated communications protocols help ensure integrity, while peer authentication and redundant/backup HMIs can detect these types of attacks.

6) Level 5 – Perimeter

Included: The perimeter level is both a physical perimeter and an electronic perimeter.

Focus: Integrity and availability of the perimeter are paramount.

Implementation: A good physical perimeter includes mulitple layers, such as a barrier (fence), access control (lock), and monitoring (cameras). From an electronic perspective, confidentiality and integrity of communications leaving or entering are also important. The perimeter gateway is the front door of the system. Any external attacks will hit the gateway first, potentially rendering it unavailable, but preserving the integrity, confidiality, and availability of lower levels.

Virtual private networks (VPNs) provide confidentiality and integrity. A VPN simultaneously validates peer networks, encrypts communications, and performs packet integrity verification. Popular VPN technologies include IPsec and TLS.

7) Level 6 – People

The people that interact with the system deserve special consideration because they are typically the wild card of any security program. People are irrational beings that, even if honest, can make mistakes. Unlike devices, people can be compromised through blackmail, threats, or social engineering.

The concepts of CIA apply to processes and procedures that users are expected to follow. These include the concepts of “least privilege” and “need to know.” These concepts state that a user should only be given the information and access privileges needed to perform their day-to-day duties. This mitigates the risk of people disclosing information or abusing their access rights. Additionally, if a user’s credentials are stolen, the malicious actor using the credentials will have limited access to the system.

Training is one of the most important steps to protecting users of the system. Constantly repeated training on procedures, policies, best practices, etc. will educate and reinforce good security awareness within an organization. Training doesn’t have to be in depth. Frequent small reminders, such as “use strong passwords” and “be careful of email attachments,” can go a long way toward protecting users and organizations.

C. Borders

When considering risk, one of the first thoughts any defender must have is, where are all the places an intruder can get into the network? Internet connections and physical access are two of the most obvious external borders, but USB drives, microwave and other wireless communications, and power supplies also need to be considered and protected. In a modern ICS network, it is possible to have access points even at Level 1 via USB, so be sure to consider the whole network, not just the desktop PCs.

III. Example System

Traditionally, the United States Department of Defense (DoD) has focused on security only in their enterprise IT systems. The DoD has recently realized how vulnerable their control systems are. The control systems were not originally included in the security accreditations process because they were on their own “closed” network, and most had little to no cybersecurity.

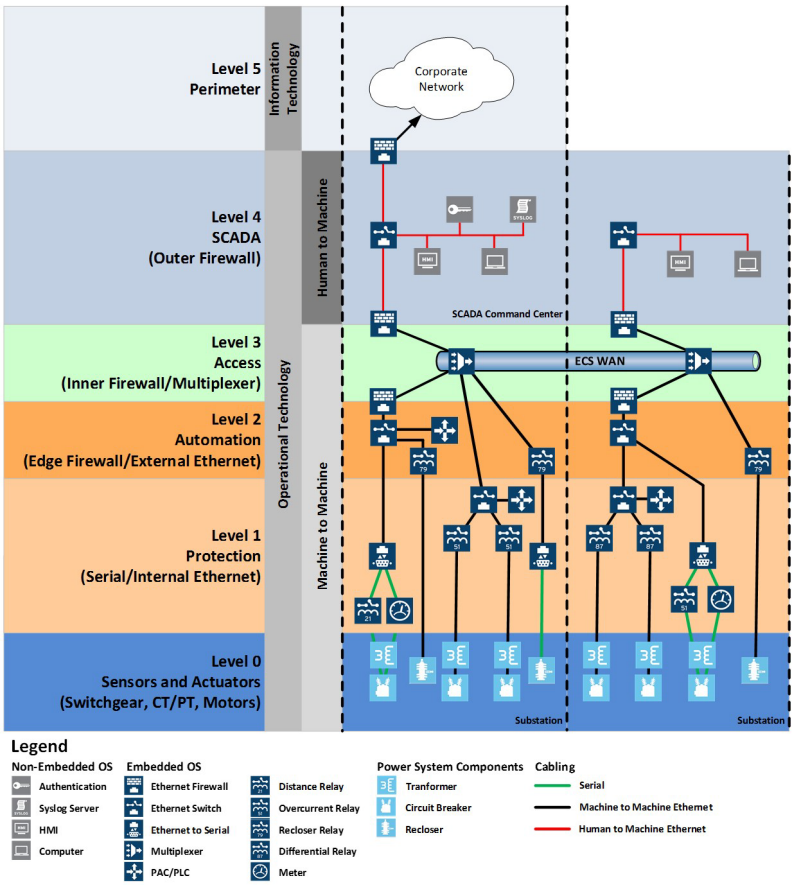

Figure 2 Example System

DoD has implemented what are termed "type systems," meant to represent an engineered reference architecture of best practice design and configuration. The type system assessment augments the numerous site system assessments, which use the type system as a best practice template. This makes site assessments more efficient and less costly. The Energy Control System Security Reference Architecture (ECSSRA) has been stood up for the DoD as a working type system for assessment by United States military services. A one-line diagram of this system is shown in Figure 2.

The ECSSRA highlights the benefits of implementing a defense-in-depth security scheme from the ground up. For a site authorization, the Army Corps of Engineers has estimated there to be a 75 percent cost savings and an 80 percent time savings from using the Risk Management Framework (RMF) structure that ECSSRA highlights. The ECSSRA will also provide the real-time continuous monitoring required by RMF and NERC CIP.

IV. Conclusions

Security is critical at all levels of a control system, but each level may have a different focus for its security (see Figure 3). By dividing up a control system into levels, defenders can take advantage of the resources available to accomplish the requirements of each level.

Level 0 (physical) measures and operates inputs and outputs to ensure system safety and stability, while Level 1 (protection) handles the logical tasks that ensure safety and availability. These two levels are the foundation of an ICS, and availability is critical.

Continuous monitoring and baselining are the focus of Level 2 (automation). Level 3 (access) is internal segmentation that divides the ICS into machine-to-machine levels and human-to-machine levels.

Moving up in the levels, confidentiality and integrity become more important.

Level 4 (SCADA) is the level most users interface with most often. It handles tasks like user authorization and data aggregation for analysis and visualization, and the integrity and availability of those data is critical. Level 5 (perimeter) is similar to Level 3 in that it provides separation and segmentation; in this case, it separates the control system from the enterprise network, both physically and electronically.

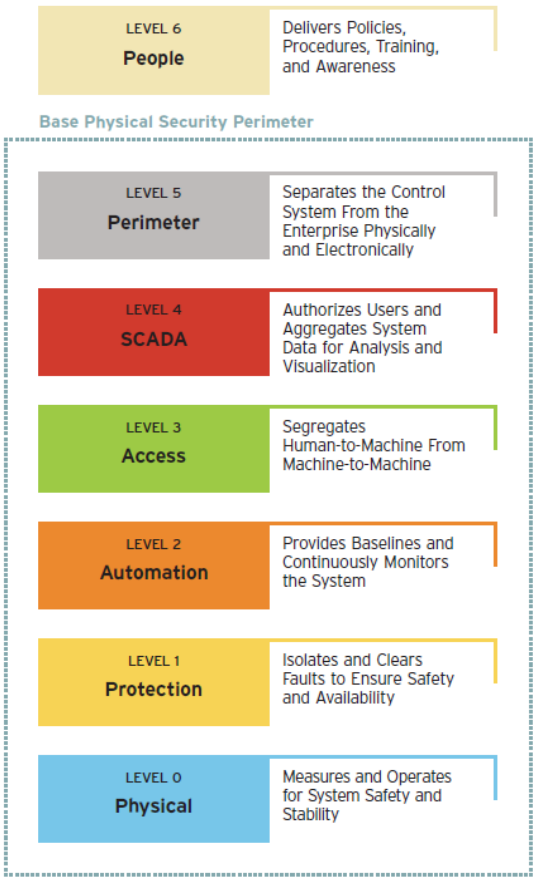

Figure 3 Defense-in-Depth Levels

People are the foundation for Level 6, which does not fit into the physical model of the control system. The policies, procedures, training, risk analyses, and other human-based tools and techniques that are used to ensure the security of the system are included in this level. Level 6 spans all of the other levels because of the impact of things like policies and procedures at all levels of the control system.

Security is an ongoing process. Continuous monitoring of the network is critical to catch intruders or infections, and monitoring should be performed at all levels of the network. Different levels provide different data, and sometimes it is possible to see problems that are not obvious at a single level by combining data from multiple levels.

References

[1] M. Bishop, "What Is Computer Security?," *IEEE Security & Privacy Magazine*, January 2003, pp. 67–69.

[2] J. M. Stewart, M. Chapple, and D. Gibson, *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 7th Edition*, John Wiley & Sons, Inc., Indianapolis, Indiana, 2015.

[3] J. Smith, J. Pereyda, and D. Gammel, "Cybersecurity Best Practices for Creating Resilient Control Systems," submitted to the 9th International Symposium on Resilient Control Systems, Chicago, IL, August 2016.

[4] K. Barnes and B. Johnson. "Introduction to SCADA Protection and Vulnerabilities," Idaho National Engineering and Environmental Laboratory, March 2004.

[5] P. Oman, E. O. Schweitzer, III, and D. Frincke, "Concerns About Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems," proceedings of the 27th Annual Western Protective Relay Conference, Spokane, WA, October 2000.

20220727 • TP6762-01