Do IT Cryptographic Security Controls Work for Energy Systems?

Josh Carlson
Dragos, Inc.

Dan Gunter
Formerly of Dragos, Inc.

Casey Roberts
Duke Energy Corp.

Colin Gordon and George Masters
Schweitzer Engineering Laboratories, Inc.

Revised edition released August 2022

Previous revised edition released May 2021

Original edition released April 2021

Do IT Cryptographic Security Controls Work for Energy Systems?

Josh Carlson, *Dragos, Inc.*
Dan Gunter, *Formerly of Dragos, Inc.*
Casey Roberts, *Duke Energy Corp.*
Colin Gordon and George Masters, *Schweitzer Engineering Laboratories, Inc.*

Abstract—**The threats of unauthorized access to or manipulation of commands and data drive the incorporation of cryptographic security controls into critical energy system communication infrastructure. However, cryptographic security controls that are inappropriately or poorly applied can lead to a decline in reliability and availability and an inadvertent expansion of the attack surface available to attackers. Furthermore, most modern information technology (IT)-originating cryptographic security controls include encryption (a minimal-priority security control in energy systems), which brings the side effect of crippling the operators' ability to monitor their systems for intrusions.**

This paper discusses reasons why many security techniques commonly applied in IT systems and based on cryptography may be unsuitable for application in critical portions of energy systems. We propose for system owners an approach to designing energy systems that separates system elements into those that are dynamic (designed to serve human users, reconfigurable, plug-and-play) and static (fixed-task, fixed-configuration, and machine-oriented, e.g., high-speed protection and telemetry). Lastly, we build on that approach with recommendations for operational technology (OT) cryptographic security controls in energy system networks.

I. Introduction

Industrialized societies require infrastructure to support the most critical and basic needs of their citizens. Electric energy systems are uniquely critical infrastructure elements since the availability of reliable electric power enables most other areas of critical infrastructure and is also directly used by citizens [1]. Well-functioning energy systems themselves require highly available and reliable components.

Cybersecurity in energy systems should serve the mission for which those system components are built or designed and "help more than hurt" the energy system over the life of the components. This principle applies to cybersecurity applications such as cryptography (the discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity [2]) for commands and data. If cryptography in general can affect the reliability and availability of an energy system (as we will show) then much care and planning must be used when considering *where* or (more importantly) *whether* to integrate cryptographic security controls into energy systems.

A current trend in operational technology (OT) is the integration of commercial-off-the-shelf (COTS) cryptographic protocols and implementations, borrowed from business information systems and integrated directly into critical energy systems or their components. Even though many cryptography advocates' goals are laudable (the integrity, availability, and confidentiality of digital signals in power systems), there has been minimal critical analysis by the industry of the possible downsides of this recent trend. Discussion of whether a general application of cryptographic security controls actually "does more harm than it does good" is overdue.

One example of an element critical to the energy system is the protective relay. To perform their protective functions, relays must operate within times on the order of milliseconds. This is necessary to prevent electrical fault currents from endangering human beings, destroying valuable power system equipment, causing fires, or resulting in blackouts that could cause property damage or the loss of electricity for hundreds or thousands of people. The protective relay performs a vital role for energy systems, and yet there has been little interest by the security community in exploring if and how cryptography in general or perhaps certain kinds of cryptographic security controls can negatively affect the applications of protective relays.

This paper is an attempt to provide that missing discussion. In aggregate, the authors have several decades of experience with cryptography (both theoretical and applied) in various environments, from information technology (IT) to OT, the latter term being used in this paper synonymously with energy systems. The authors are not arguing against implementing all elements of cryptographic functions into energy systems *per se*. Instead, their goal is to suggest an approach that demands a detailed understanding of the many downsides of cryptographic functions when incorporated into critical intelligent embedded devices (IEDs) in power systems. For even when cryptography-based security is implemented securely and maintained correctly, its impact on performance as well as its adverse effects on other security functions like intrusion detection must be assessed to see if it provides a net benefit that justifies its costs and impacts.

Before going into more depth on the potential downsides of cryptographic security controls for data-in-motion in operational environments, this paper begins with a basic overview of energy system lifespan and constraints compared to their IT counterparts and provides a brief exposition of typical IT cryptographic protocol implementation in energy systems.

II. Energy System Lifespan and Constraints

Fig. 1 shows how a typical supervisory control and data acquisition (SCADA) communication channel for a digital secondary system is organized. SCADA communications generally travel from a SCADA master or front-end processor across a wide-area network (WAN) link owned by a third-party organization, and for that reason is not trusted. Substations provide a reasonable amount of physical security, protecting the system from equipment and connection tampering. As a bare minimum for basic security practices, the firewall provides points for controlling data ingress and egress through the electronic security perimeter. The remote terminal unit (RTU) provides some processing and simplifies security by reducing the number of devices communicating outside the electronic perimeter, which is considered to be at the facility boundary in Fig. 1. Below this layer is where the primary energy system processes occur and power protection and control equipment communicate to the RTU via simple industry protocols.

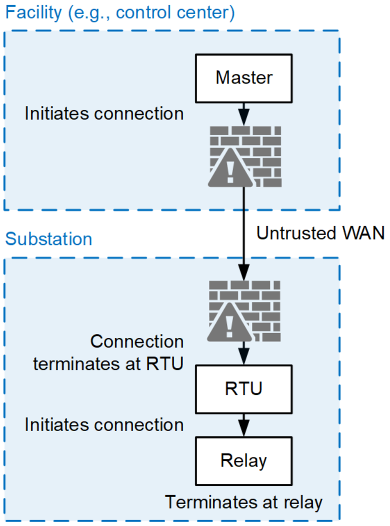


Fig. 1. Discussion Model of Digital Communications in an Energy System

Modeling the system in this way can clarify where cryptographically secured communications are required and where they should be avoided in the interests of system simplicity and reliability. Fig. 1 will be expanded upon later.

There are some fundamental differences between the less-critical applications traditionally served by IT solutions and those typically found in energy systems and devices in those environments. The assets that comprise an energy system need to be more tolerant of harsher environmental elements than consumer products or IT-specified equipment operating in an environmentally controlled building. Unlike most server room failures where exchanging a failed drive or a network switch is a routine task with minimal personal safety concerns or negative effects on essential services, equipment changes in an OT environment may require costly interruption of critical industrial or electrical processes and may require maintenance technicians to enter hazardous areas. Even in situations where a critical IT datacenter presents hazards to its staff or difficulties for maintenance tasks, there remains a fundamental difference: IT services are generally entirely digital, whereas energy system infrastructure is a combination of digital and physical elements. IEDs in energy system infrastructure ultimately require direct interaction with physical elements (e.g., breakers, switches, and electric lines) that are geographically fixed and thus cannot simply be duplicated or migrated while providing continuous uninterrupted energy supply, and thus require greater care when undergoing maintenance operations.

Because of maintenance and replacement costs and risks, OT devices (controllers, switches, relays, and more) are expected to have a lifecycle of decades. Per the North American Energy Reliability Corporation's (NERC) Protection and Control (PRC) standard requirements, many OT owners and operators generally do not plan to physically touch IEDs until 12 years into their useful lifespan [3]. Maintenance costs can determine whether a project (which may include implementing cryptographic security controls) is a success or failure based on whether there was a positive return on investment. For the sake of reliability and cost, some technology in OT systems may be decades behind current IT technology. Manufacturers of OT system elements are cognizant of the demanding nature of this lifespan requirement and therefore purpose-build those elements to perform a specific minimal and rigidly defined set of functions consistently and reliably with the same equipment for decades. The technology (including cryptographic security controls) that goes into the IED needs to be suitable for this service lifespan, or risk more frequent maintenance cycles to update or replace that technology. In contrast to OT, IT systems are built on general-purpose platforms, where extensibility and plug-and-play are desirable features for their ability to balance myriads of different types of products and functions, and to take advantage of new applications and technologies. For this reason, IT devices are often "over built" with additional hardware and software capacity to handle a wide range of contingencies.

An illustration of these differences between technologies as applied in IT and OT systems is useful. Software-defined networking (SDN) provides a fundamental separation of the data plane from the control plane, to allow Ethernet connectivity implemented by simpler network switches to be "orchestrated" by a central controller. IT systems use SDN for load and bandwidth management, including maximizing bandwidth usage on expensive overseas fiber connections, load-balancing server requests, and the integration of highly complex functions such as machine-learning or network function virtualization (NFV) with connections being managed dynamically by the controller. OT systems use SDN in the same fundamental architecture (by separation of data and control planes). However, SDN as applied in OT systems is used to maximize the determinism of network performance, provide the fastest possible failover, and use allowlisting to detect or prevent unauthorized communications with minimal participation by the controller once the network is configured. The unique advantages that SDN brings when applied to OT systems are made possible by their purpose-built nature. The purpose-built nature of OT systems can also provide some advantages when operators augment these systems with robust defense-in-depth layered controls, as will be discussed later.

III. The Challenges of IT Cryptographic Security Controls in Energy Systems

A. Principal Challenges Enumerated

The following is a list of some considerations and challenges related to applying IT cryptographic security controls in energy systems. These weigh against the security benefits of employing cryptography in energy systems. Note that some of these might not apply for every system.

1) Frequent Changes to Standards and Best Practices

Cybersecurity and cryptographic standards frequently change based on external factors such as the availability of new cryptanalysis tools, the increase in computational power available to threat actors, and the introduction of novel attack techniques, among others. These frequent cryptographic standard changes, by both private industry groups and government entities, are problematic for energy system environments. The lag time between a standard's ratification and its implementation by OT manufacturers, and subsequently by system owners, can be considerable due in part to the constraints of cyber-physical systems outlined in Section 2. As a result, firmware upgrades may already be out-of-date according to current cryptographic standards when upgrades are deployed within the energy system environment.

Best practices for implementations can change with, or be independent of, standards. Security practitioners are always refining guidance for cryptographic system implementations for evolving threats or advances in research. In either case, the effect is the same: a requirement to update IEDs in the field. One example is a recent change from the National Institute of Standards and Technology (NIST) on secure password management, specifically shifting from a focus on password complexity with stringent password rotation schedules to longer "passphrases" [4].

Because changes to standards and best practices require security updates in the same way as implementation flaws, they also contribute to higher operating costs and reduced availability of protection.

The framework that we propose in Section 4 strategically simplifies designs to minimize complexity, risk, and maintenance requirements. It helps to use standards that are not subject to frequent changes or that are designed for infrastructure with different mission requirements.

2) Firmware Maintenance Burden

Protective relays have evolved from purely electromechanical devices to devices with adjustable analog electronics, and to microprocessor-based relays with adjustments and protection schemes in code. As communications networks have grown to include them, design choices made to provide security for this new communications functionality can require additional maintenance and introduce higher chances of firmware flaws that are unrelated to their critical functionality. Consequently, the number of lines of code (LoC) has progressed from a minuscule 40,000 [5] in early protection relays to over 600,000 today, with only 7 percent of that count involved directly with protective relay functions. OpenSSL (the popular open-source package for transport layer security [TLS] implementations) currently contains over 500,000 LoC [6]. Finally, there has been a positive correlation with increasing firmware LoC and critical system protection unavailability (the fraction of time the protection system is not available as measured by the average downtime per failure divided by mean time between failures [MTBF]) [7] at a rate commensurate with that shown in Table 1.

Table 1
Software-Caused Unavailability [5]

LoC (in 1000s)	Unavailability • 10^{-6}
100	100
500	223
800	282
1,000	316
1,500	387
2,000	447
2,500	500
3,000	547
3,500	591
4,000	632

OT manufacturers design, build and optimize each device for a specific mission. Those OT devices are optimized to provide the minimum complexity and hardware capabilities necessary to accomplish their designed mission. OT end-users take those devices and use them in a way that maximizes reliability and availability. General-purpose (IT-oriented) devices are typically designed with substantial excess technical-hardware capacity to be applicable to a wide variety of missions. A substantial amount of complexity and capability in IT-oriented devices goes unused in a particular application. General-purpose cryptographic security controls are often resource-intensive. This is acceptable for general-purpose platforms because that type of cryptography takes general-purpose IT-oriented devices into account (many missions) and not the OT single-mission focus. Therefore, IT devices are best served by general-purpose cryptography.

Judiciously implemented cryptography may indeed enhance the reliability, safety, and economical nature of power systems and associated components over their lifetimes by mitigating certain threats to data-in-motion, but these features come at the cost of additional complexity within the communications system. In the cybersecurity industry, it is undeniable that additional complexity creates opportunities for threat actors to exploit [8] [9]. Researchers have discovered and cataloged thousands of vulnerabilities in cryptographic implementations and standards in the MITRE database [10]. Probably the most well-known example of an implementation mistake is the Heartbleed vulnerability, which affected most installations of the popular OpenSSL library and allowed attackers to remotely read data from memory on millions of vulnerable systems [11]. When the fix for the Heartbleed flaw was publicly released, it generated world-wide patch activity within minutes. The Heartbleed flaw turned out to be more serious than initial reports made it appear because the flaw not only affected server implementations but client implementations as well.

3) Loss of Situational Awareness

IT-oriented cryptographic protocols (such as TLS, SSH, and IPsec) focus on providing end-to-end confidentiality first and foremost, as well as integrity and authenticity controls for communication links to keep out intruders and ensure that authorized users who are trusted to be on the system can work securely. The protocols ensure that the information traversing the connection cannot easily be read or captured by anyone (or any *thing)* on the network. Confidentiality is such a critical requirement of TLS 1.3 that the standard does not allow the use of "null-cipher" suites that remove confidentiality while keeping integrity and authenticity controls [12].

Confidentiality prevalent in IT-oriented cryptographic protocols prevents a passive listener from gaining access to communications. However, the use of cryptographic protocols that mandate confidentiality impacts passive network monitoring because they prevent inspection of the traffic content. Lower visibility into OT data-in-motion also makes it easier for malicious actors to pivot through a network. For example, OT protocols (e.g., DNP3) often contain file-transfer functionality [13]. A malicious actor might leverage this type of protocol with file-transfer functionality to execute lateral movements within the environment. In this case, an organization with visibility into DNP3 communications would observe the function codes related to file transfer if the malicious actor leveraged DNP3 to move attack tools. However, if all the DNP3 traffic is encrypted, this type of malicious file-transfer activity would be hidden from the network-monitoring solutions. Network threat detection would only observe the existence of the session, and it could not identify malicious activity with high confidence.

A typical solution in IT environments for this lack of visibility is the implementation of decrypting techniques. However, the time-sensitive nature of OT process-bus communication networks eliminates the suitability of interception-then-decryption techniques requiring TLS-decrypting proxies and web gateways that are often used in IT networks unsuitable for many OT networks, especially those that operate at low bandwidth which is common in OT. Interception-then-decryption (which is more suitable for engineering access in OT systems) also increases the time needed to respond to an observed threat. Note, however, that the use of cryptographic protocols that enforce integrity controls still allows passive network monitoring.

The framework we propose in Section 4 focuses on integrity and authenticity controls that accommodate the time-sensitivity of OT processes and allows confidentiality protection to be optional.

4) Required End-User Expertise

The IT departments at many organizations already have security and cryptographic expertise for managing and securing large numbers of users, which is due to the variety of ecosystems based on public-key infrastructure (PKI). OT units within smaller energy organizations (such as public utilities or distribution companies) without embedded IT experience can find it challenging to know how to configure cryptographic systems in OT environments. OT system owners may prefer to avoid patch mandates and vulnerability findings coming from the IT department by not enabling security features, but IT-oriented cryptography can often force the hands of OT system owners. At the end of the day OT systems need to minimize patches. Allowing IT control over OT assets also may impose IT helpdesk processes on critical energy systems and devices. This IT-OT divide is often handled by dividing IT and OT equipment into separate physical zones, with IT security governance falling on the communications gateway equipment at the perimeter location, and OT owning the critical devices within the energy system.

The imposition of additional security functions can lead to compliance issues. Cryptographic security may require business processes and auditing to protect the secrecy of data such as keys, as well as processes for items which require regular maintenance, such as X.509 cryptographic certificates. One way to mitigate the introduction of stringent new security features are to simplify the new controls as much as possible and keep the complexity minimized.

The authors are personally familiar with systems where technical personnel avoided security devices and systems due to ease-of-use concerns. It requires expertise, and errors are more probable if users are forced to make arcane choices in a user interface (UI) that technicians do not understand. The more complex or the greater the overall number of system or device settings there are, the greater the chance technicians will apply them incorrectly. Table 2 shows the calculated unavailability of electric protection correlated to increased LoC, which assumes that the number of settings increases linearly with device code size.

TABLE 2
FIRMWARE LOC CORRELATED TO HUMAN-CAUSED UNAVAILABILITY

LoC (in 1000s)	**Unavailability • 10^{-6}**
100	100
500	500
800	800
1,000	1,000
1,500	1,500
2,000	2,000
2,500	2,500
3,000	3,000
3,500	3,500
4,000	4,000

Improper configuration can diminish, or even eliminate, the effectiveness of cryptographic implementations. For these reasons, we propose that a key goal in energy system design is to minimize the expertise needed to apply and maintain the technology securely.

5) *The Difficulty of Key Management*

Security key management in OT is notoriously tricky because manual key management has the same issues as patching, and the other choice, automated key management, increases complexity and attack surface. The outcome of this is that, typically, cryptographic keys will not change after system commissioning for the lifetime of the device. There are NIST standards (such as NIST SP800-57 [14]) that contain recommendations for key management timelines and lifecycles. However, due to the management lifecycles of competing standards or difficulties associated with key management, these recommendations are rarely followed [15].

Rekeying operations for bump-in-the-wire (BITW) encrypting communication gateways are often difficult to execute even by trained operations personnel and often require coordination across geographical regions, including notifications to upstream SCADA control operators of expected downtime. The hazards of rekeying operations are the same for bump-in-the-stack (BITS) embedded cryptographic protocol solutions, or even application-layer protocols with security extensions as in the case of DNP3 Secure Authentication (DNP3-SA). The use of temporary session keys and perfect-forward secrecy (PFS) are often recommended as methods to minimize the number of key management operations that require operator intervention. But those cryptographic implementation techniques can only reduce and not eliminate the key management problem, which is exacerbated by the device lifespan of decades for medium or long-term keys that provide root key infrastructures.

We propose that design criteria include the need to avoid any key management that requires periodic downtime or work in hazardous locations unless an in-depth evaluation demonstrates a security improvement that justifies the costs and difficulty associated with cryptographic key management.

6) *Performance Degradation*

Cryptographic methods can add overhead to communications links. In energy systems infrastructure, high-latency (300+ milliseconds) and low-bandwidth (25 kbps) connections are still common. Cryptographic systems requiring multiple round trips for negotiation or challenge-response exchanges (e.g., DNP3-SA) to establish a valid cryptographic session can perform poorly and burden shared-medium links [16].

With high-speed protection schemes, multiple protective relays may need to send high-speed signals over dedicated serial links. These signals are required to operate within a 2 to 4 millisecond window to meet protection design objectives. If these signals are delayed or blocked for any reason then protection response to fault currents is slowed, resulting in increased risk of physical damage to equipment or lines and further outages [17]. Integrity checking by cryptographic means of messages may lead to substantial delays since the entire digital signal frame must be "held back" for the integrity check process to be completed before the protective device can act on the frame [18] [19].

As a result, the framework that we propose in Section 4 recommends cryptography that ensures performance is acceptable for protection-class environments under worst-case conditions, and to maintain this goal even if cryptography is implemented.

7) *Hardware Requirements*

Modern cryptographic protocols often rely on special hardware, including cryptographic accelerators, to meet performance goals. Embedded devices, particularly legacy IEDs, were built without cryptographic accelerators, so many modern cryptographic methods may prove infeasible or may quickly become so as standards evolve. For devices such as protective relays, their primary designed functions do not evolve in this way, and they will be capable of reliably performing those functions (e.g., fault protection) for much longer [20].

Many legacy systems also lack the required entropy (randomness) sources to produce strong cryptographic keys. A common approach to this challenge from the IT manufacturer community is adding specialized cryptographic hardware to devices and systems for these kinds of functions [21] [22] [23].

Adding specialized hardware is an excellent strategy for typical IT hardware with a lifespan of 3 to 7 years. However, this expected cryptographic platform obsolescence does not suit critical protection devices with service lifetimes of over a decade or more. Implementing off-the-shelf cryptography seems efficient and cost-effective, but it often costs more in the long-term. When the device platform falls behind enough that it cannot be upgraded to use up-to-date cryptographic functions, it remains what can be called "forever-day vulnerable" until it is replaced.

B. *Summary of Objectives*

Critical infrastructure manufacturers wanting to implement cryptography into energy system components should be aware of the following considerations to help avoid the downsides:

- Use standards that are not subject to frequent changes or that are designed for infrastructure with different mission requirements that still meet necessary cybersecurity objectives.
- Simplify designs to minimize the effects of expanded LoC and maintenance requirements associated with additional features.
- Minimize the impact of cryptographic security controls on critical time-sensitive protection protocols.
- Use cryptographic implementations for data-in-motion that support network visibility requirements and maximize situational awareness.
- Choose technologies with lifespans suited to application in devices with long service life spans.

Having discussed energy systems in general, cryptographic protocols, and the challenges of their being "bolted-on" to OT environments, the next section discusses recommended approaches to cryptography moving forward.

IV. Framework Proposal for OT Cryptographic Security Controls for Energy Systems

This section proposes a framework for sensibly applying cryptography in OT systems by categorizing energy system elements into static, dynamic, or mediator types. Before further discussing this framework, we must explore what we mean by a layered-defense model.

A. A Layered-Defense Model

Cybersecurity practitioners often approach cybersecurity controls by first understanding communication flows and access controls between categories of assets. A common approach to identifying suitable categories is the Purdue Model [24]. Developed originally by Theodore J. Williams and the Purdue University Consortium for Computer Integrated Manufacturing in the 1990s, the Purdue Model divides systems and assets into levels based on purpose. From a cybersecurity perspective, the model helps by formalizing the separation of devices into groups that have similar purpose, security requirements, and communications.

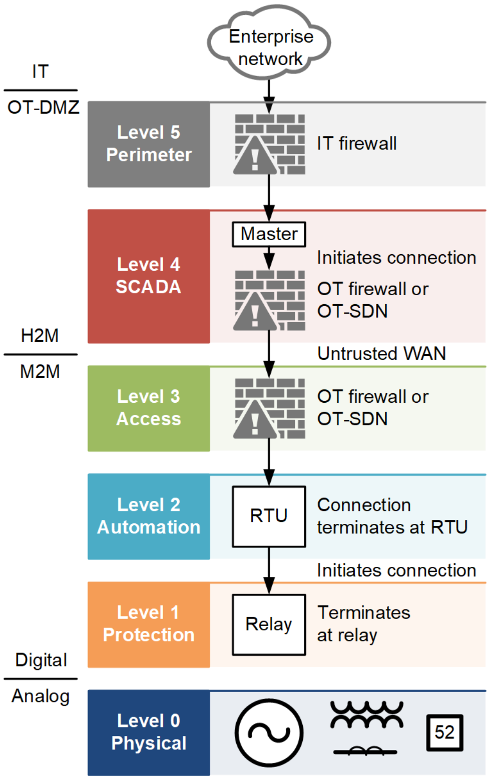


Fig. 2. Layered Cybersecurity for a Utility OT Network

The following is a brief description of the security layers shown in Fig. 2:

- L5, Perimeter: contains IT-OT segmentation devices that terminate connections from any necessary corporate communications. Generally, practitioners recommend using advanced IT-oriented firewalls or one-way data diodes, read-only human-machine interfaces (HMIs), or both to prevent direct communication from IT to OT environments. Devices at this level interact with a wide variety of network hosts from the enterprise network, including some that process email or other data originating from outside the organization. This traffic is the least trusted and may or may not be encrypted using IT cryptographic security controls.
- L4, SCADA: contains HMI and SCADA master controllers, centralized authentication systems, historians, and intrusion detection and monitoring devices. Devices at this level are predominantly computer-based, receive frequent software updates, and operate on a network that includes transient devices like technician laptops. Removable media are sometimes used on this layer. Although similar to IT environments, Level 4 differs by its purpose-built nature, making its network suitable for OT-SDN.
- L3, Access: contains devices which separate humans from machines on local-area networks (LANs) and may include encrypted WAN communication devices. Devices on this layer communicate with secure encrypted channels using IT cryptographic security controls on the upper edge and use simple and/or cleartext communications with devices in Layer 2.
- L2, Automation: contains RTUs, data concentrators, event collectors, and logic controllers. Devices on this layer communicate with peers on a tightly controlled network segment.
- L1, Protection: contains protection and control devices such as protective relays.
- L0, Physical: contains sensors, actuators, and other devices that physically control electric power flow.

Generally speaking, the hosts and traffic are less trusted and have less stringent availability requirements at higher layers. At lower layers, the hosts are more trusted and the need for availability is greatest.

The security objective is to group devices into levels with similar security requirements and capabilities to assist owners and operators in understanding the trust boundaries and select appropriate security controls to protect the system. The goal of the devices at each level, shown in Fig. 2, is to enable and facilitate best-in-class energy system operational functionality on highly specialized layers to promote energy system safety, reliability, and economy. Energy system owners and operators add appropriate cybersecurity controls to devices in the levels, or between the levels, to establish different trust boundaries.

As previously discussed, the use of cybersecurity approaches that force the requirements of upper-level devices (which require more and different types of security) down to low-level device models can negatively affect the performance and reliability of those devices. Assessing the appropriateness of cryptographic security controls must include a holistic evaluation that considers cryptography as just one part of a layered approach to security composed of complementary security controls (personnel, procedural, physical, detective, and more).

The best balance of security overhead and functionality is different on different layers. Due to the concerns of reliability, lifespan, and longevity, implementations stressing reliability of functionality are most critical at the physical layer (L0) and the protection layer (L1), which directly controls and protects the physical elements. Devices in these layers are highly specialized, with implementations that are simple and highly optimized. As discussed in Section 3, this approach is largely antithetical to the approach of IT that generally seeks to overbuild devices and components to fit general use cases.

Here, an example is useful to illustrate why specialization is critical at these levels. Public-key infrastructure common in IT infrastructure has undergone significant revisions in two decades. Where 1024-bit, or even 768-bit, RSA keys were considered secure before the 2000s, subsequent revisions to NIST SP800-57 have resulted in 2048-bit being considered the secure standard, soon to be followed by 3072-bit keys in 2023 [25]. X.509 certificates relying on RSA for public/private-key pairs have gone through significant standards revisions. Even if specialized devices in L1 or L0 were able to keep up with the number of revisions necessary to remove vulnerabilities from PKI implementations, it is doubtful that embedded hardware built in the late 1990s could continue to support significantly expanding asymmetric key sizes required by those newer standards.

The next section will evaluate what criteria we should use to integrate OT cryptographic security controls into energy system infrastructure.

B. A Proposal for Cryptographic Security Controls for Communications in Energy Systems

In general, energy system elements can be sorted into two distinct types that the authors call *static* and *dynamic*. Static elements prioritize reliability by providing automated telemetry and high-speed protection functions or other automated controls and operating routinely and automatically for lengthy periods of time without human interaction. Static system elements are physically protected and isolated, and all communications are as-designed, making allowlisting an attractive cybersecurity approach.

Dynamic elements support business requirements for the control and supervisory functions used to manage the system. They are dynamic in that applications, communications, and configurations change more frequently to serve changing business needs. Dynamic system elements are more exposed to other hosts, unauthorized personnel, and novel threats, increasing the need for up-to-date cybersecurity support. Because of their ad-hoc nature, allowlisting is difficult to apply to dynamic elements.

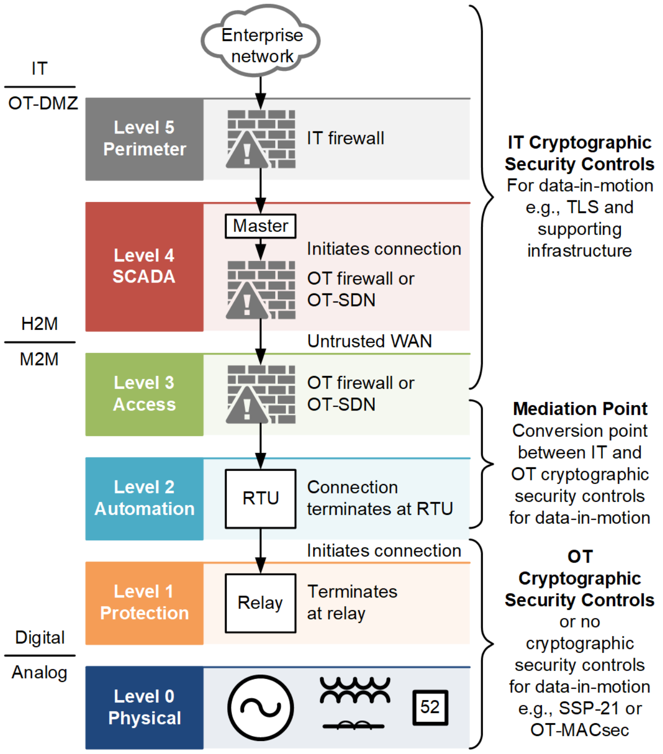
The difference in the kinds of attacks associated with dynamic and static elements also point to the need to consider different threat models during the selection and service life of static and dynamic elements. Since the threat environments in which those devices operate are different, the corresponding choices for appropriate security controls are also different. We propose that if owners and operators choose to integrate cryptographic security controls into energy systems, they should specify very differently implemented controls for the first type (dynamic elements) than for the second type (static elements).

The result is a partitioning of IT cryptographic security controls and their associated downsides into those more dynamic areas of energy systems with IT device lifecycles and less stringent reliability and availability requirements to support the more frequent maintenance that comes with their additional features and complexity.

The usual cryptographic choices for dynamic elements include protocols that are subject to frequent standard changes and implementation updates. They are complex to develop and require considerable management functionality. These kinds of cryptographic protocols require substantial configuration and operational expertise, and complicate application monitoring efforts. When applied in OT environments, their complexity tends to negatively affect the overall safety, reliability, and availability of critical energy system elements, as previously discussed. Our framework advises against IT cryptographic security controls to data and commands exchanged with other dynamic system elements only (not for static system elements). Examples of these kinds of protocols include TLS, IPsec, Secure Shell (SSH), and associated PKI types of protocols (e.g., Online Certificate Status Protocol [OCSP] for certificate revocation) and supporting protocols and infrastructure (e.g., Domain Name System [DNS]).

The best cryptographic choices for static elements are protocols and algorithms that are not subject to frequent changes, are simple to develop and apply, do not block modest monitoring efforts, and also do not negatively affect the overall safety, reliability, and availability of critical energy system elements. Our framework also recommends either abstaining altogether from cryptographic protocols for static elements, or, if justified by threat analysis, using static-oriented cryptographic protocols. An example of a cryptographic security control that is suitable for static environments due to its simplicity and longevity is a form of IEEE 802.1AE Media Access Control Security (MACsec) tailored for this type of application. MACsec, when implemented in the IT domain, includes IEEE 802.1AR (Secure Device Identities) and IEEE 802.1X (Network Access Control) Supplicant and Authenticator functionality, along with additional Extensible Authentication Protocol with TLS (EAP-TLS) controls. An optimized variant of MACsec purpose-built for static environments would remove additional complexity (Supplicant, Authenticator, and EAP-TLS functions) and focuses on providing authentication and optional encryption for commands and data, with an eye towards minimizing firmware churn and maximizing reliability and simplicity. Other examples of similar OT cryptographic security controls include IEEE 1711.1 SSCP for serial, or a hybrid protocol, SSP-21 [26], which can be used for either communication medium. Suitable cryptographic protocols for static elements are simple and designed for long-term usage (10 to 15 years minimum) without requiring upgrades to continue supporting the availability and reliability of energy system devices and assets.

As Fig. 3 shows, in our model, any digital signals that must flow between dynamic and static elements are handled by a third element type—a device type we call *mediators*. A mediator incorporates both IT and OT security controls and communicates with both dynamic and static infrastructure elements. A mediator already exists in most OT systems, since advanced RTUs, jump boxes, protocol converters, proxies, gateways, and embedded terminal servers often take on the role of a mediator. Mediators are candidates for additional security controls, such as secure allowlist-based operating systems, and the focus of stringent monitoring. The mediator also effectively acts as a cryptographic protocol break, if not as an application-layer protocol break and inspection chokepoint (as is often used for NERC CIP applications [27]).



Enterprise network
IT
OT-DMZ
Level 5 Perimeter
IT firewall
Level 4 SCADA
Master
Initiates connection
OT firewall or OT-SDN
H2M
M2M
Untrusted WAN
Level 3 Access
OT firewall or OT-SDN
Level 2 Automation
RTU
Connection terminates at RTU
Initiates connection
Level 1 Protection
Relay
Terminates at relay
Digital
Analog
Level 0 Physical
52
IT Cryptographic Security Controls
For data-in-motion e.g., TLS and supporting infrastructure
Mediation Point
Conversion point between IT and OT cryptographic security controls for data-in-motion
OT Cryptographic Security Controls
or no cryptographic security controls for data-in-motion e.g., SSP-21 or OT-MACsec

Fig. 3. Adding Recommendations for Security Controls to the Model

The idea of a mediator should be already quite familiar to those system operators subject to NERC CIP standards: where an intermediate system (i.e., a jump box) is a mandatory part of any system using interactive remote access.

For a machine-to-machine data transfer that routinely crosses trust boundaries (e.g., SCADA), the recommendation is to terminate any cryptographic protocols used by dynamic elements (e.g., TLS) at the mediator. The mediator would regenerate the communication flow (or even the underlying communications protocol itself) using either no cryptographic protocol or protection by a static-oriented cryptographic protocol. System owners and operators may choose to forego the use of cryptography for protection-based protocols (such as IEC 61850 GOOSE) that ordinarily do not cross trust boundaries. This architecture does not rule out end-to-end "lateral" connections between discrete static elements traversing dynamic energy system infrastructure types. For instance, critical devices may use OT cryptographic security controls or protocols oriented for static elements through less trusted channels with added security controls to maintain the same level of trust.

V. Conclusion

Before the concept "operational technology" existed, the energy system staffs of an electric utility rarely encountered the IT department. The need to deliver electricity, to know when and why a fault occurred, along with the capability to control the equipment to restore electricity to customers, was their priority, and the electric grid operated in a stable and reliable manner. The IT department supported the needs on the corporate side for services like email, end-user information, accounting, web presence, and more. However, as the energy system industry has matured over time, the need for these two groups to interact has grown. One such area of interaction focuses on how systems and devices within the energy system infrastructure communicate securely.

It is not uncommon for utilities to implement separate OT cybersecurity groups or merge with the corporate IT cybersecurity groups to oversee how the utility energy system operates. The real concern is introducing cryptography into the mix. Just because a utility has an IT or OT department experienced in networking and cybersecurity does not guarantee that they have the tools to make the utilities secure. The development of standard best practices that ensure constant visibility and control of the energy system is the first step. Unfortunately, this is not as easy as plugging in a new application, system, or device and expecting everything to work perfectly together.

The key objective of any energy system is always maintaining availability. Most cybersecurity personnel who have experience working in OT environments see the typical CIA triad as more the AIC (availability, integrity, and confidentiality) triad. Again, this reflects that availability is the topmost concern for an energy system owner/operator. Any downtime has the potential for operators to lose the viability or control of their systems. Therefore, when considering software, hardware, or network architectural type changes within the energy system environment, it is critical to understand the potential risks. If the energy system processes are jeopardized, the resulting cause is likely to be a monetary loss for the utility. More importantly, the risks to the health and safety of their customers and employees could be impacted. While that may be a challenge, providing solid security should be considerably less problematic if a solid plan is created and followed by the teams.

VI. References

[1] U. S. President, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," Presidential Policy Directive (PPD-21), February 2013. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[2] K. Greene, J. Kelsey, and J. Franklin, "Measuring the Usability and Security of Permuted Passwords on Mobile Platforms, NISTIR 8040, National Institute of Standards and Technology (NIST), April 2016. Available: https://doi.org/10.6028/NIST.IR.8040.

[3] U. S. Federal Energy Regulatory Commission, “Mandatory Reliability Standards for Critical Infrastructure Protection,” 18 CFR Part 40, Docket No. RM06-22-000; Order No. 706, January 2008. Available: https://www.ferc.gov/sites/default/files/2020-05/E-2_52.pdf.

[4] National Institute of Standards and Technology, “NIST Special Publication 800-63B Digital Identity Guidelines,” June 2017. Available: https://pages.nist.gov/800-63-3/sp800-63b.html.

[5] E. O. Schweitzer, III and D. E. Whitehead, “Resetting Protection System Complexity,” proceedings of the 46th Annual Western Protective Relay Conference, Spokane, WA, October 2019. Available: https://selinc.com/api/download/129019/?lang=en.

[6] “OpenSSL,” Synopsys, October 2020. Available: https://www.openhub.net/p/openssl/analyses/latest/languages_summary.

[7] E. O. Schweitzer, III, B. Fleming, and T. J. Lee, “Reliability Analysis of Transmission Protection Using Fault Tree Methods,” proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997. Available: https://selinc.com/api/download/2465/?lang=en.

[8] C. Perrin, “The Danger of Complexity: More Code, More Bugs,” Tech Republic, February 2010. Available: https://www.techrepublic.com/blog/it-security/the-danger-of-complexity-more-code-more-bugs.

[9] A. Bessey, K. Block, B. Chelf, A. Chou, B. Fulton, S. Hallem, C. Henri-Gros, et al., “A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World,” Communications of the ACM, Vol. 53 No. 2, pp. 66–75, February 2010. Available: https://cacm.acm.org/magazines/2010/2/69354-a-few-billion-lines-ofcode-later/fulltext.

[10] “Common Vulnerabilities and Exposures,” Mitre, December 2020. Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SSL.

[11] “The Heartbleed Bug,” Synopsys, June 2020. Available: https://heartbleed.com/.

[12] “The Transport Layer Security (TLS) Protocol Version 1.3,” Internet Engineering Task Force (IETF), August 2018. Available: https://tools.ietf.org/html/rfc8446 Section B.4.

[13] “Features of DNP3,” DNP, December 2020. Available: https://www.dnp.org/About/Features-of-DNP3.

[14] National Institute of Standards and Technology, “NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management,” January 2016. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.

[15] North American Energy Reliability Corporation, “Cyber Security – Systems Security Management,” CIP-007-6, June 2014. Available: https://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/CIP-007-6_CLEAN_06022014.pdf.

[16] C. Rosborough, C. Gordon, and B. Waldron, “All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2019. Available: https://selinc.com/api/download/125641/?lang=en.

[17] E. O. Schweitzer, III, B. Kasztenny, A. Guzmán, V. Skendzic, and M. V. Mynam, “Speed of Line Protection – Can We Break Free of Phasor Limitations?” proceedings of the 41st Annual Western Protective Relay Conference, Spokane, WA, October 2014. Available: http://dx.doi.org/10.1109/CPRE.2015.7102184.

[18] R. Smith, “Cryptography Concepts and Effects on Control System Communications,” proceedings of the 11th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2019. Available: https://selinc.com/api/download/5200/?lang=en.

[19] “Tier Classification System,” UptimeInstitute, December 2020. Available: https://uptimeinstitute.com/tiers.

[20] D. Haas, M. Leoni, K. Zimmerman, A. Genz, and T. Mooney, “The Useful Life of Microprocessor-Based Relays: A Data-Driven Approach,” proceedings of the 72nd Annual Conference for Protective Relay Engineers, College Station, TX, March 2019. Available: https://selinc.com/api/download/125782/?lang=en.

[21] C. Robinson, “Mellanox ConnectX-6 Dx SmartNIC Better RoCE,” Serve the Home, August 2019. Available: https://www.servethehome.com/mellanox-connectx-6-dx-smartnic-better-roce/.

[22] “Intel Data Protection Technology with AES-NI and Secure Key,” Intel, October 2020. Available: https://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard-aes/data-protection-aes-general-technology.html.

[23] P. Kennedy, “AMD PSB Vendor Locks EPYC CPUs for Enhanced Security at a Cost,” Serve The Home, September 2020. Available: https://www.servethehome.com/amd-psb-vendor-locks-epyc-cpus-for-enhanced-security-at-a-cost/.

[24] D. Dolezilek, D. Gammel, and W. Fernandes, “Cybersecurity Based on IEC 62351 and IEC 62443 for IEC 61850 Systems,” proceedings of the 15th International Conference on Developments in Power System Protection, Liverpool, UK, March 2020. Available: https://selinc.com/api/download/130122/?lang=en.

[25] E. Barker, “Recommendation for Key Management: Part 1 – General,” NIST Special Publication 800-57 Part 1 Revision 5, National Institute of Standards and Technology (NIST), May 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

[26] U. S. Department of Energy, “Secure SCADA Protocol (SSP-21) Characterization and Standardization,” November 2018. Available: https://www.energy.gov/sites/prod/files/2018/12/f58/LLNL - Secure SCADA Protocol %28SSP-21%29.pdf.

[27] North American Energy Reliability Corporation, “Cyber Security – Security Management Protocols,” CIP-003-6, January 2016. Available: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-003-6.pdf.

VII. Biographies

Josh Carlson is a Senior Business Development Manager at Dragos, Inc., where he primarily focuses on identifying, establishing, and nurturing meaningful relationships and strategic alliances with other organizations that improve the overall value of Dragos offerings. He possesses 20 years of diverse cybersecurity experience in engineering and business development roles within high-tech companies supporting governments, global financial institutions, and customers in the various critical infrastructure sectors. Josh also participates in different working groups within nonprofit and for-profit organizations seeking to improve Industrial Control Systems safety and security through multiple guidelines/standards adoption and implementation.

Dan Gunter is the former Director of Research and Development at the industrial cybersecurity company Dragos, Inc., where he leads teams conducting industrial control system research and detection engineering in support of development of the Dragos Platform. Previously, Dan worked as a Principal Threat Analyst within the Dragos Threat Operation Center. Dan is a graduate of the U. S. Department of Defense’s elite Computer Network Operations Development Program (CNODP) and the Air Force Research Lab’s Advanced Course in Engineering Cybersecurity Boot Camp (ACE). He has spoken at S4, numerous EnergySec events, Blackhat, Shmoocon, and local information security events.

Casey Roberts is a Senior Cybersecurity Architect in Operational Technology at Duke Energy Corps. He has 12 years of industry experience including power, automation, control, and cybersecurity. He holds a Bachelor of Science degree in Electrical Engineering from the University of North Carolina, Charlotte.

Colin Gordon is a Senior Research Engineer with the Schweitzer Engineering Laboratories, Inc. (SEL), Infrastructure Defense division, specializing in communications, cybersecurity, and cryptographic solutions and services for critical infrastructure. His work experience includes secure network design, implementation, testing, and regulatory compliance consultation for utilities and asset owners in North America and abroad. Colin joined SEL in January 2008 and holds a Bachelor of Science degree in Computer Engineering from the University of Idaho.

George Masters is a Lead Application Engineer in the Security group, Research & Development division, at Schweitzer Engineering Laboratories, Inc. (SEL). He is a security architect and developer of cross-platform standards for security features built into SEL products. He has developed processes and testing procedures to ensure robust designs and is familiar with NERC CIP compliance programs. He has over 26 years of experience in security architecture and cryptography, software development, and hardware interface devices. He is a graduate of the University of Southern California with a Bachelor of Science degree in Electrical Engineering. He holds a CISSP certification and is a participant in the NERC RSTC Supply Chain Working Group.

20220802 • TP6997-01