CIP Security and IEC 62443-4-2

Jack Visoky
Security Architect and Sr. Project Engineer
Rockwell Automation

Joakim Wiberg
Manager Technology and Platforms
HMS Networks

Presented at the ODVA
2020 Industry Conference & 20th Annual Meeting
March 4, 2020
Palm Harbor, Florida, USA

Abstract

ISA/IEC 62443 is a standard focusing on cyber security in industrial control systems. It is comprised of a suite of specifications including policies, procedures, and requirements for system-level installations as well as industrial control systems and devices. One part of ISA/IEC 62443, specifically ISA/IEC 62443-4-2, contains detailed technical requirement for industrial control systems and devices. IEC 62443 utilizes the concept of Security Requirements as well as Security Levels to classify the security features and security functionality for industrial control systems and devices. Devices fulfilling those Security Requirements and Security Levels may achieve a security certificate if reviewed by an accredited auditor.

In this paper we will look at how the feature set of CIP Security™, both the existing CIP Security EtherNet/IP Confidentiality Profile as well as the in-development CIP Security User Authentication Profile, maps to and fulfills requirements defined in IEC 62443-4-2. The Security Requirements in IEC 62443-4-2 have been reviewed and the paper presents an investigation on which security requirements are fulfilled by CIP Security and which are out of scope and need to be fulfilled by other means.

A company developing products intended to be certified against a security level in IEC 62443-4-2 can leverage the information in this paper to facilitate their investigation and design. The investigation done in this paper can reduce the effort needed to achieve a certification. Beyond IEC 62443-4-2, this analysis can also aid in vendors seeking IEC 62443-3-3 certification, as that is a certified system rather than a single product. For IEC 62443-3-3, this analysis can show what capabilities a CIP Security enabled product can provide to the system, which can help in constructing an IEC 62443-3-3 argument. However, the focus of this paper is generally on IEC 62443-4-2 requirements.

Keywords

CIP Security, Cybersecurity, IEC 62443-4-2, OpenID Connect, OAuth 2.0, TLS, DTLS

Definition of terms

Acronym/term	Definition
AES	Advanced Encryption Standard: a symmetric encryption algorithm that is in wide use today and endorsed by several standards organizations. AES

	is a block cipher, and as such there are several modes of performing AES, which allow for various trade-offs.
Certificate	Also known as a “Digital Certificate”, this is a piece of data signed by a Certificate Authority that is associated with a public/private keypair. The certificate can be used to prove the identity of a given party and is often used for authentication within a secure connection, such as a TLS session. See also: TLS
Cipher Suite	A collection of algorithms for protection of data communication. Cipher suites for TLS and DTLS specify the endpoint authentication mechanism, key agreement mechanism, and subsequent data encryption and data authentication mechanisms. See also: TLS, DTLS
DTLS	Datagram Transport Layer Security: a version of TLS that does not rely on guaranteed message delivery. This protocol is very similar to TLS with a few exceptions to allow for out of order transmission and non-reliable packet delivery (such as a sliding window of acceptable sequence counts on packets). See also: TLS
ECC	Elliptic Curve Cryptography: an asymmetric cryptography algorithm that relies on the hardness of the Discrete Logarithm Problem. ECC is in wide use today for both digital signatures and key agreement.
EST	Enrollment over Secure Transport: A protocol that allows an entity to request a certificate securely over HTTPS
IANA	Internet Assigned Number Authority: an international organization that is responsible for assigning various numbers to items related to Internet standardization, including things like RFC number, port number assignments, and others. See also, RFC.
ICMP	A supporting protocol in the Internet protocol suite used for error handling, diagnostic and control.
IEC	International Electrotechnical Commission: a standards organization that publishes standards related to electronic technology.
IEC 62443	Standard published by the IEC focusing on cybersecurity within industrial automation systems. This standard has several parts and covers a wide variety of material, including product functional requirements, processes, systems, etc.
IETF	Internet Engineering Task Force: the most widely recognized, participated in, and used Internet standards body which develops open standards through open processes.
JWT	JSON Web Token: Standard used to create access tokens representing claims. Examples of claims including information on how a user is logged in or when the user information was updated, although claims are very general and can communicate a wide variety of information. The JWT is digitally signed using public/private keypairs.
OAuth 2.0	An open standard commonly used on the Internet to provide access delegation and authorization. OAuth 2.0 include three elements: a client, an authorization server, and a resource server. Access tokens are granted to the clients by the authorization server that uses the access token to access protected services hosted by the resource server. Using this method, the resource owner (server) authorize third parties (the client) to access services without sharing credentials.
OpenID Connect	An identification layer used on top of OAuth 2.0 in order to create interoperability between systems. OpenID Connect contains information about the end user within a JWT, which verifies the user’s identity and basic profile information. See also: JWT
PKI	Public Key Infrastructure: is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

	In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority.
RFC	Request For Comment: the de-facto Internet standards documents produced and managed by the IETF. Not all of these documents serve as normative standards, but many of the technologies that define how the Internet works are specified through IETF RFCs. See also: IETF.
RSA	Rivest Shamir and Adleman: an asymmetric cryptosystem that relies on the hardness of the factoring large numbers problem for its cryptographic properties. This cryptosystem is in wide use today and can be used for digital signatures, encryption/decryption, and key agreement.
SHA	Secure Hash Algorithm: a family of cryptographic hash functions that are widely used and endorsed by the US National Institute of Standards and Technology (NIST). Although use of the SHA-1 version of the SHA family has been deprecated due to insecurity, the SHA-2 family and SHA-3 family are still widely considered to be robust and secure cryptographic hash algorithms.
TCP	Transmission Control Protocol: Provides connection management and guaranteed end to end delivery of data between two network devices.
TLS	Transport Layer Security: the most ubiquitous secure communications protocol in use today. This protocol is defined by the IETF in a series of RFCs. Although TLS 1.2 is the most widely used, TLS 1.3 has recently been published and is beginning to gain traction and adoption. See also: IETF, RFC.
UDP	User Datagram Protocol: Connectionless data transmission protocol. DTLS uses UDP services.
Vendor Certificate	A certificate issued to a device by the device vendor. Within CIP Security, this certificate serves as the default certificate that can be used to bootstrap a secure connection for the purpose of provisioning the device with CIP Security configuration which includes either a new certificate or a Pre-Shared Key.

Table 1 Definitions of Terms and Acronyms

Introduction

IEC 62443 is an international standard around the security of industrial control systems. Over the last several years this standard has grown in prominence to become a highly recognized, ascendant standard for industrial control system security. The standard itself contains several parts, with part 4-2 focused specifically on the security requirements an individual product must satisfy in order to be certified. CIP Security is the ODVA standard for securing CIP and EtherNet/IP, with reliance on widespread and robust technologies such as TLS, DTLS, OpenID Connect, and OAuth 2.0. This paper analyses CIP Security and the IEC 62443 requirements to determine which requirements are satisfied, either partially or fully by CIP Security.

It is important to keep in mind that certification of a product to IEC 624434-2 is an intensive process that requires formal threat modeling and analysis of the product. Given this, it is not possible to make claims that CIP Security will satisfy IEC 62443 requirements in all possible cases and all possible implementations. This paper is intended to be a guide for those seeking IEC 62443-4-2 certification and leveraging CIP Security for meeting some of the requirements. Necessarily, some assumptions must be made for the analysis done in this paper, and those assumptions do not necessarily apply in all scenarios.

For the purpose of this paper, the product under consideration is assumed to be a simple device with one physical Ethernet port. That port allows for EtherNet/IP and CIP communications (other communication protocols are not considered). CIP Security has been implemented, which includes the EtherNet/IP Confidentiality Profile and the User Authentication Profile. Note that at the time this paper is published,

the CIP Security User Authentication Profile has not yet been published. However, work is nearing completion on this profile, and this paper reflects the current known thinking around what functionality this profile will cover. Further, it is assumed that no other communications protocols are implemented in the device beyond those necessary for EtherNet/IP, CIP, and CIP Security. In many cases, devices will have other protocols, although the evaluation of this is outside the scope of this paper.

For the sample CIP Security device under consideration in this paper, a trust boundary can be drawn as shown in Figure 1.

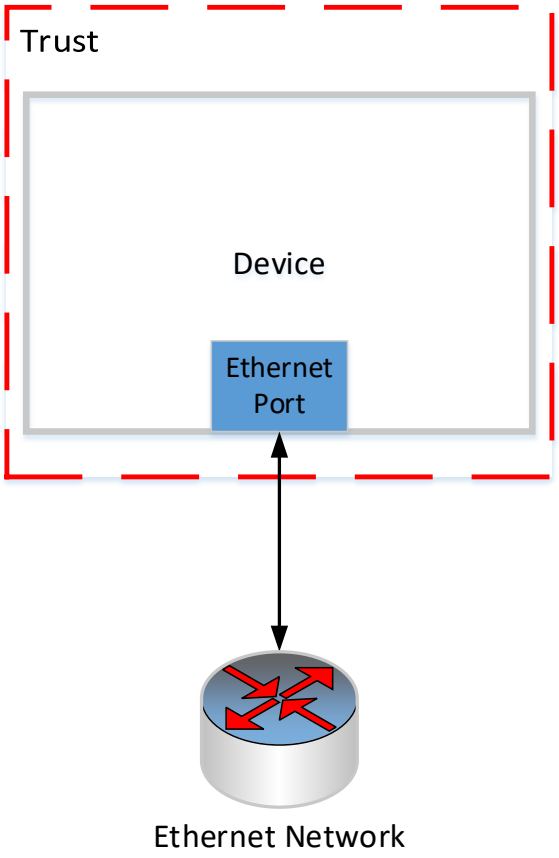

Figure 1 Trust Boundary

That is, the trust boundary is drawn around the device, with the data coming in from or going out to the Ethernet port crossing the trust boundary. Many devices that will be certified to IEC 62443-4-2 will have other ports and more complex trust boundaries, however for the purposes of this paper the device and trust is assumed to be this simple, illustrative case.

CIP Security

CIP Security has two main profiles: the EtherNet/IP Confidentiality Profile and the User Authentication Profile. The former is focused on transport level security for EtherNet/IP, and the latter is focused on providing user authentication and basic authorization. A brief description of these two profiles is given, for more information please see Volume 8 of the CIP networks specification.

The EtherNet/IP Confidentiality Profile makes use of the IETF-standard TLS (RFC 5246) and DTLS (RFC 6347) protocols in order to provide a secure transport for EtherNet/IP traffic. TLS is used for the TCP-based communications (including encapsulation layer, unconnected messaging, transport class 3), and DTLS for the UDP-based transport class 0/1 communications. This approach is analogous to the way that

HTTP uses TLS for HTTPS. Certificate management is also provided by this profile. Certificates can be managed over the standard EST protocol, or over CIP via defined attributes and services.

This profile provides the following security attributes:

- Authentication of the endpoints – ensuring that the target and originator are both trusted entities. End point authentication is accomplished using X.509 certificates or pre-shared keys.

- Message integrity and authentication – ensuring that the message was sent by the trusted endpoint and was not modified in transit. Message integrity and authentication is accomplished via TLS/DTLS hashed message authentication code (HMAC).

- Message encryption – optional capability to encrypt the communications, provided by the encryption algorithm that is negotiated via the TLS/DTLS handshake.

The CIP Security User Authentication Profile provides mechanisms to authenticate users and to limit access to the least privilege appropriate for a given role. The User Authentication Profile again takes advantage of IETF standard technology, such as JWTs, OAuth 2.0 and OpenID Connect to authenticate the user and grant the appropriate level of access to protected resources. This profile allows for a CIP target to act as an identity authority itself, containing a database of users and their associated claims (referred to as Local Authentication, see Figure 2), or allows devices to integrate into a third-party identity management system (referred to as Central Authentication, see Figure 3). This integration is achieved through the standard OpenID Connect technology, commonly leveraged throughout the Internet and in enterprise systems and IT systems. A basic level of authorization is also defined by the User Authentication Profile, although for most actions it is up to the vendor to determine what roles have appropriate privilege. Note that the User Authentication Profile is scheduled to be published by ODVA in the Fall of 2020.

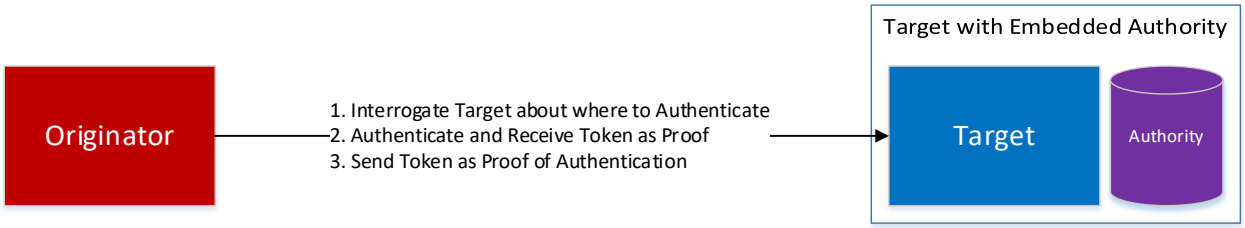

Figure 2 Local Authentication

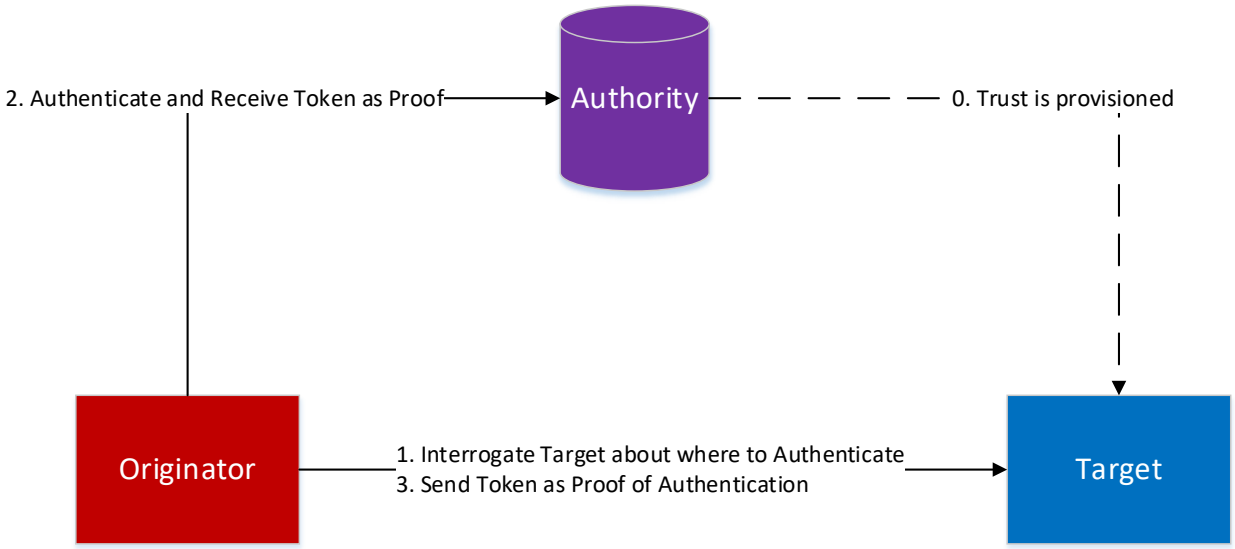

Figure 3 Central Authentication

IEC 62443

The IEC 62443 series have been developed to address the need for cyber security and robustness in industrial control systems. Some general background information will be given here on the IEC 62443 specification, and especially the IEC 62443-4-2 specification. However, the IEC documents remain the authoritative reference; understanding of the IEC documents is necessary for a full interpretation of the information presented in this paper.

The family of the IEC 62443 standards is divided into 4 parts, General, Policies & Procedures, System, and Components. Within each part there are several elements that address specific topics related to the specific part of the standard. The standard in the series have the name of IEC 62443-X-Y. Figure 4 shows the groups and the individual elements of IEC 62443.

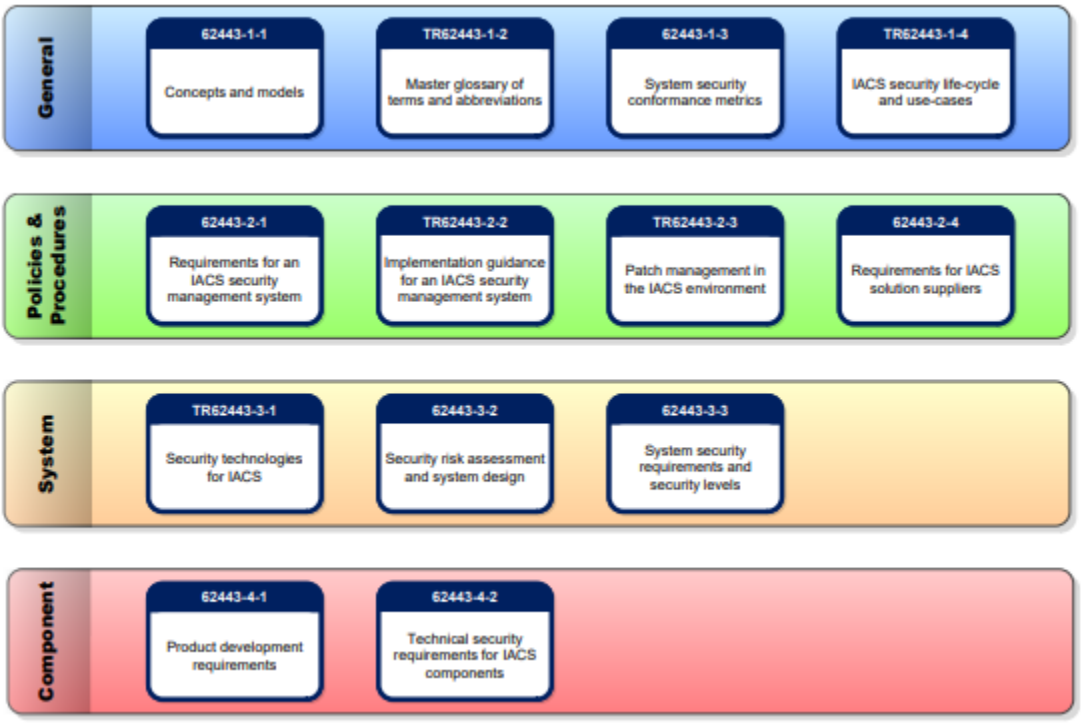

Figure 4 IEC 62443 Organization

Each part deals with information related to the focus of that part and its intended audience. The parts refer to the X in the naming of the standard and the four are:

1. **General**: this group provides elements that discuss items that are common and general for the whole series.
2. **Policies & Procedures**: items in this address policies and procedures used to implement a cybersecurity management system.
3. **System:** elements in this group describes requirements and management of systems.
4. **Components**: describes requirements for components used in industrial automation systems.

For the component there are two parts, IEC 62443-4-1 and IEC 62443-4-2.

IEC 62443-4-1

IEC 62443-4-1 introduces an established secure development process, and this is the basis for developing products that comply to IEC 62443-4-2. For the purposes of this paper, IEC 62443-4-1 and the associated processes are outside of scope.

IEC 62443-4-2

In IEC 62443-4-2 functional requirements for components that are to be used in industrial control systems are defined. Although the term component is quite general, it can naturally be applied to a singular product or device. The document defines requirements for different types of components: software applications, embedded devices, host devices, and network devices. Each component type has its individual set of requirements defined, however most of the requirements that are defined within IEC-62443-4-2 are generic for all types of components.

The cyber security requirements that are defined in the specification for the different components are derived from the industrial control system requirements defined within IEC 62443-3-3. This is derived from the intention of the IEC 62443 series to provide a flexible framework that assists in addressing existing and future cyber security vulnerabilities in industrial automation control systems by applying necessary

mitigations for defense. IEC 62443-3-3 defines the concept of system requirements which IEC 62443-4-2 then expands into a series of component-level requirements; these two portions of the IEC 62443 specification align with one another.

The component-level requirements are a technical description of the cyber security requirements in an industrial control system device. Those descriptions give the implementor an understanding about the requirements and what they are intended to protect against. It does not give any direct guidance on how to implement and apply the specific requirement in a product; this is left to the discretion of the implementer. The component-level requirements are derived from foundational requirements in IEC 62443-1-1; there are a total of seven foundational requirements. Within each foundational requirement group there are a set of component-level requirements. The foundational requirements are used for grouping the component-level requirements as follows:

1. Identification and authentication control
2. Use control
3. System integrity
4. Data confidentiality
5. Restricted data flow
6. Timely response to events
7. Resource availability

Each component-level requirement has a defined component security level, described with a value of 0 through 4. The value of 0 for a component-level requirement indicates that it is not defined as a requirement. A higher value denotes a higher and more stringent requirement. A brief description of the different security levels is:

- SL 1 – Focused on actors who unintentionally cause security events
- SL 2 – Focused on motivated attackers with basic skills and resources
- SL 3 – Focused on advanced attackers with moderate resources
- SL 4 – Focused on the highest level of attackers with significant skills and resources

The evaluation done in this paper are targeting an SL 3 level attacker; therefore SL 4 capabilities are outside the scope of this evaluation.

Table 1 shows an example of how a requirement might be structured at different security levels. For some requirements there is a base requirement with additional requirement enhancements that become mandatory only at a particular SL. Below two component requirements are shown, CR 1.1 and CR 1.2. BR stands for Base Requirement, RE stands for Requirement Enhancement.

SR	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control				
CR 1.1 – Human user identification and authentication	BR	BR, RE-1	BR, RE-1, RE-2	BR, RE-1, RE-2
CR 1.2 - Software process and device identification and authentication	None	BR	BR, RE-1	BR, RE-1

Table 2 Security Level requirements

CIP Security mapping to component requirements

This section discusses how CIP Security maps to and fulfills the individual component-level requirements. Each IEC 62443-4-2 component-level requirement is listed, along with the relevant CIP Security

functionality that covers the requirement. Any requirements that are out of scope are denoted as such with a justification given.

CR 1.1 Human user identification and authentication – Met by CIP Security

Devices that implement the CIP Security User Authentication Profile will be able to identify and authenticate human users requesting access to the device using CIP Security. CIP Security User Authentication Profile makes use of OpenID Connect when integrating with an external authority. Beyond OpenID Connect integration, the User Authentication Profile also provides the option for the device to store the user account information locally, in which case no authority external to the device is needed. In either case JWTs are used for identification of the users.

CR 1.1 RE-1 Unique identification and authentication – Met by CIP Security

The User Authentication Profile allows for unique identification and authentication through tokens (JWTs). Each JWT is unique and provides proof of authentication, either via a central mechanism like OpenID Connect, or locally to the device's database of users.

CR 1.1 RE-2 Multifactor authentication for all interfaces – Met by CIP Security

The User Authentication Profile supports integration into a third-party identity provider via OpenID Connect and OAuth 2.0, which can support multifactor authentication. CIP Security devices will not support multifactor authentication within the device itself, although they will fully integrate into third-party systems supporting OpenID Connect, which can support multifactor authentication. However, it is also possible for a vendor to extend the User Authentication Profile to support multifactor authentication locally within the device if they wish to do so.

CR 1.2 Software process and device identification and authentication – Met by CIP Security

Devices implementing CIP Security use either X.509 certificates or pre-shared keys as a proof of their identity. The X.509 certificates or pre-shared keys are also used when devices authenticate themselves within a system, via the CIP Security User Authentication Profile. In the User Authentication Profile, JWTs are used as proof of authentication and allow integration into central identity management solutions. JWTs can be utilized by software processes, devices, and human users.

CR 1.2 RE-1 Unique identification and authentication – Met by CIP Security

JWTs and X.509 certificates both provide unique identification for components. PSKs do not, and therefore should not be selected as the authentication mechanism for users wishing to meet this requirement.

CR 1.3 Account management – Met by CIP Security

CIP Security User Authentication profile defines the functionality for CIP Security devices to manage accounts either locally using username and password or certificates or integrate in an OAuth 2.0/OpenID Connect system for a centralized account management.

CR 1.4 Identifier management – Met by CIP Security

For locally stored users in the CIP Security Authentication profile the device must keep a list of all usernames and to be able to identify the account via a unique username. In the case where the CIP Security device integrates with an OAuth 2.0/OpenID Connect system, the system identity provider ensures that the user identifier is unique.

CR 1.5 Authenticator management – Met by CIP Security

The CIP Security User Authentication Profile allows for optional implementation of initial authenticators. This is meant to bootstrap the system for trust provisioning of the user's preferred authenticators; the user is prevented from using the default authenticator for any activity outside of provisioning user-controlled authenticators. The User Authentication Profile also allows for updates of the authenticators, whether stored locally or managed externally via OpenID Connect/OAuth 2.0. When used with EtherNet/IP the authenticators are required to be transmitted over TLS/DTLS with a confidentiality-based cipher suite, ensuring protection from

disclosure and modification. Storage of the authenticators internally is not specified by CIP Security, although the specification notes that best practices should be followed to prevent any vulnerabilities that may compromise the authenticator. Other than the internal storage of authenticators, which is outside of scope of the specification, this requirement is met by the User Authentication Profile.

CR 1.5 RE-1 Hardware security for authenticators – Out of Scope

The use of hardware security for authenticators is not required by CIP Security, however it is something that CIP Security enables through its integration with standard OpenID Connect/OAuth 2.0 authentication workflows. Furthermore, for local authenticators CIP Security specifies that best practices are followed for protection, which includes hardware protections.

CR 1.6 Wireless access management – Out of Scope

Wireless communications are not in scope for CIP Security. In any case where CIP is communicated over wireless, the protections specified would still apply. Therefore, the presence of wireless in and of itself does not impact the security case.

CR 1.7 Strength of password-based authentication – Met by CIP Security

For locally authenticated users, the CIP Security User Authentication Profile provides functionality to enforce the length and complexity of the password. In the case when integrating with an OAuth 2.0/OpenID Connect system it is up to the system to enforce this requirement; many OpenID Connect systems provide support for this functionality.

CR 1.7 RE-1 Lifetime Restrictions for Human Users – Met by CIP Security

For this requirement again OpenID Connect/OAuth 2.0 servers can be configured for this. For locally stored passwords the CIP Security User Authentication Profile provides the option to prevent previously used passwords for a configurable number of generations.

CR 1.7 RE-2 Password Lifetime Restrictions for all Users – Met by CIP Security

CIP does not differentiate between human users and non-human users; this requirement is met using the same rationale as CR 1.7 RE-1

CR 1.8 Public key infrastructure certificates – Met by CIP Security

The CIP Security public key infrastructure integration is based on EST (Enrolment over Secure Transport) which is an established standard from the IETF. EST relies on X.509 certificates which is the industry standard defining digital certificates. Using EST a number of workflows and processes can be used to deploy certificates; some of the most common are described in the Pull Model paper presented at the ODVA 2018 Industry Conference (see reference [2]). Certificates may also be managed over CIP, through which integration with a PKI can be achieved using CIP client software that can manage certificates on CIP endpoints and can be designed to interact with the PKI (through EST for example).

CR 1.9 Strength of public key-based authentication – Met by CIP Security

This requirement has a number of sub requirements:

a) Validate certificates by checking the validity of the signature of a given certificate
   - This is done via the TLS/DTLS handshake and the Verify_Certificate service of the Certificate Management Object.

b) Validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;
   - This is done via the TLS/DTLS handshake, and the Verify_Certificate service of the Certificate Management Object.

c) Validate certificates by checking a given certificate's revocation status;
   - This is done via the TLS/DTLS handshake, and the CRL, structured according to RFC 5280.

d) Establish user (human, software process or device) control of the corresponding private key;

- Private keys for a CIP endpoint are generated on that endpoint and never leave it, per the Create_CSR service of the Certificate Management Object. This ensures control is maintained by the CIP endpoint.

e) Map the authenticated identity to a user (human, software process or device)
   - This is done via user accounts in OAuth/OpenID Connect, or via the Username/Passwords or Certificates stored locally via the User Authentication Profile.

f) Ensure that the algorithms and keys used for the public key authentication conform to CR 4.3 Use of Cryptography
   - RSA and ECC are used via IETF standards for TLS and DTLS cipher suites, conforming to best practices for modern public key algorithms

CR 1.9 RE-1 Hardware security for public key-based authenticators – Out of Scope

CIP Security recommends, but does not mandate, hardware mechanisms are used to protect the private keys. It is up to the vendor to ensure that appropriate hardware-based mechanisms are used to satisfy this requirement.

CR 1.10 Authenticator feedback – Out of Scope

This requirement has to do with the user interface for authentication and is therefore outside of the scope of CIP Security and delegated to the user interface that interacts with the OpenID Connect or local authenticator.

CR 1.11 Unsuccessful login attempts – Met by CIP Security

When using the centralized authentication scheme of the CIP Security User Authentication Profile this is covered by using an OpenID Connect Authority which enforces limits on unsuccessful login attempts. When using local authentication this is achieved via setting an attribute in the Password Authenticator Object to enforce the number of allowed unsuccessful login attempts.

CR 1.12 System use notification – Out of Scope

This requirement has to do with the user interface for authentication and is therefore outside of the scope of CIP Security.

CR 1.13 Access via untrusted networks – Out of Scope

CIP is an application layer protocol and therefore requirements on underlying networking and routing are outside the scope of CIP Security.

CR 1.14 Strength of symmetric key-based authentication – Met by CIP Security

This requirement has a number of sub requirements:

a) Establish the mutual trust using the symmetric key
   - This is done via the TLS/DTLS handshake when Pre-Shared Keys (PSKs) are configured

b) Store securely the shared secret (the authentication is valid as long as the shared secret remains secret)
   - It is the responsibility of the vendor to ensure this, although hardware based secure key storage is recommended by the CIP Security specification

c) Restrict access to the shared secret
   - It is the responsibility of the vendor to ensure this.

d) Ensure that the algorithms and keys used for the symmetric key authentication conform to CR 4.3 – Use of Cryptography which requires internationally recognized and proven algorithms be used
   - TLS/DTLS cipher suites are used which conforms to best practices for symmetric keys (AES-128 and AES-256, SHA-2 family of algorithms)

CR 1.14 RE-1 Hardware security for symmetric key authentication – Out of Scope

CIP Security recommends, but does not mandate, hardware mechanisms are used to protect the private keys. It is up to the vendor to ensure that appropriate hardware-based mechanisms are used to satisfy this requirement.

CR 2.1 Authorization enforcement – Met by CIP Security

CIP Security User Authentication Profile mandates authorization enforcement based on roles. CIP Security specifies role assignments that are required to perform specific security-related operations. For other operations, general guidance is provided by the in the CIP Security Specification as to what is appropriate for a given role. Due to the wide variety of functions a product which implements CIP can perform it is ultimately up to the vendor to decide what roles can perform what operations on a given product, although CIP Security requires that these decisions be made and enforced via the product's access policy.

CR 2.1 RE-1 Authorization enforcement for all users – Met by CIP Security

CIP Security User Authentication Profile does not differentiate between humans, software processes, and devices. All of these types of users are subject to authorization controls.

CR 2.1 RE-2 Permission mapping to roles – Met by CIP Security

CIP Security User Authentication Profile provides well-defined roles, with the possibility for a vendor to add more roles. The roles are not strictly hierarchical and apply to humans as well as software processes and devices.

CR 2.1 RE-3 Supervisor Override – Met by CIP Security

CIP Security User Authentication Profile provides a service allowing for a temporary escalation of privilege. This escalation lasts for a configurable amount of time.

CR 2.1 RE-4 Dual Approval – Out of Scope

Dual Approval is not currently supported by CIP Security, and is a requirement that is only needed at the SL-4 level. As discussed, this evaluation is targeting SL-3, therefore SL-4 requirements are not within scope. However, this is something that could be added later to the CIP Security User Authentication Profile if deemed necessary by ODVA members. This functionality could also be supported external to CIP Security by an OpenID Connect provider that supported dual authentication to issues a security token.

CR 2.2 Wireless use control – Out of Scope

Wireless communications are not in scope for CIP Security. However, where CIP is communicated over wireless, CIP Security protections specified would still apply. Therefore, the presence of wireless in and of itself does not impact the security case.

CR 2.3 Use control for portable and mobile devices – Out of Scope

There is no requirement at the IEC 62443-4-2 level for portable and mobile devices.

CR 2.4 Mobile code – Met by CIP Security

Given the assumption that only CIP and EtherNet/IP is used for data communication, then mobile code is transmitted using CIP Security. Therefore, mobile code is protected in transit via TLS or DTLS, and only an authorized user via the User Authentication Profile can transmit Mobile Code (Engineer or Administrator). This requirement is met via CIP Security.

CR 2.5 Session lock – Out of Scope

This requirement has to do with the user interface for authentication and is therefore outside of the scope of CIP Security.

CR 2.6 Remote session termination – Met by CIP Security

Remote sessions are terminated automatically after inactivity time. This applies to TLS sessions, DTLS sessions, and User Authentication sessions, each having its own configurable inactivity time.

CR 2.7 Concurrent session control – Met by CIP Security

CIP Security devices support and Electronic Data Sheet (EDS) file which includes information on connection capacity. This defines limits on number of CIP sessions as well as I/O sessions.

CR 2.8 Auditable events – Out of Scope

Events are not within scope for CIP Security. However, note that ODVA members have discussed adding standardized Syslog support to CIP Security, with the intention of covering this requirement.

CR 2.9 Audit storage capacity – Out of Scope

Events are not within scope for CIP Security. However, note that ODVA members have discussed adding standardized Syslog support to CIP Security, with the intention of covering this requirement.

CR 2.10 Response to audit processing failures – Out of Scope

Events are not within scope for CIP Security. However, note that ODVA members have discussed adding standardized Syslog support to CIP Security, with the intention of covering this requirement.

CR 2.11 Timestamps – Out of Scope

Events are not within scope for CIP Security. However, note that ODVA members have discussed adding standardized Syslog support to CIP Security, with the intention of covering this requirement.

CR 2.12 Non-repudiation – Out of Scope

This is generally not within scope as it pertains to human interfaces, although using the User Authentication profile and TLS/DTLS a device has knowledge that a particular user took a particular action, providing the basis for non-repudiation

CR 2.13 Use of physical diagnostic and test interfaces – Out of Scope

The management and protection of these interfaces is not within scope of an application layer communication protocol.

CR 3.1 Communication integrity – Met by CIP Security

Integrity of communications is provided by HMAC on TLS/DTLS sessions, using SHA-2 family algorithms. This provides best-in-class integrity protections for data in transit via internationally recognized and well-vetted cryptography and security protocols.

CR 3.1 RE-1 Communication authentication – Met by CIP Security

Authenticity of communications is provided by HMAC on TLS/DTLS sessions, using SHA-2 family algorithms. This provides best-in-class integrity protections for data in transit via internationally recognized and well-vetted cryptography and security protocols.

CR 3.2 Protection from malicious code – Out of Scope

Specific malicious code protections are not within the scope of CIP Security. However, note that the TLS/DTLS protections, as well as authentication and authorization provided by the User Authentication Profile can be seen as a compensating countermeasure for some devices against malicious code, although this is subject to a specific device threat assessment.

CR 3.3 Security functionality verification – Out of Scope

This requirement is not within scope of CIP Security, as it relies on testing the security configuration of a component. However, CIP Security configuration can be tested using standard mechanisms for TLS/DTLS, and User Authentication.

CR 3.3 RE-1 Security functionality verification during normal operation – Out of Scope

Similar to CR 3.3 this is also out of scope for CIP Security.

CR 3.4 Software and information integrity – Out of Scope

Any form of checks related to the firmware integrity is out of the scope for CIP Security. CIP Security EtherNet/IP Confidentiality Protocol is based on TLS/DTLS, this provides integrity checks of the communication session and thus protects the configuration and information deployed via CIP Security, however the full integrity guarantee of software and information is out of scope.

CR 3.4 RE-1 Authenticity of software and information – Out of Scope

Similar to CR 3.4 this is out of scope for a communication protocol.

CR 3.4 RE-2 Automated notification of integrity violations – Out of Scope

Similar to CR 3.4 this is out of scope for a communication protocol.

CR 3.5 Input validation – Out of Scope

CIP Security as a protocol itself does not directly protect and implement countermeasures against input validation. Even if CIP Security and CIP itself in many cases defines valid values and ranges for application data, it is up to the vendor to implement those checks. Furthermore, implementing those checks are a requirement within IEC 62443-4-1 as part of a vendor's development process. The vendor developing products that are intended to be IEC 62443-4-2 shall have those processes in place making this indirectly covered.

CR 3.6 Deterministic output – Out of Scope

This is not within the scope of CIP Security, however, in the event that normal operations are disrupted, devices are required to set their outputs to a deterministic fault state. This ensures that the process goes to a safe state in case the normal operation cannot be maintained. The specific state and output a drive shall take are almost always application-specific and needs to be determined and configured by the end user commissioning the device and system. CIP provides means to configure devices which failsafe state it shall take for outputs, but this is not within scope of CIP Security specifically

CR 3.7 Error handling – Partially Met by CIP Security

Generally, CIP provides a rich set of error handling and feedback in order to allow integrators and users to commission a device within a system. However, this information is application related information. CIP Security has specifically been designed not to disclose or reveal any information that can be used to exploit the device or system; the error codes defined do not leak sensitive information.

CR 3.8 Session integrity – Met by CIP Security

This requirement has a number of sub requirements:

a) The capability to invalidate session identifiers upon user logout or other session termination (including browser sessions);
   - This is described in the CIP Security Specification for TLS, DTLS, and User Authentication IDs. Once a session is terminated the identifiers are closed and deallocated, the client is forced to create a new session to continue communication.

b) The capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and
   - This is described in the CIP Security Specification for TLS, DTLS, and User Authentication IDs. User Authentication creates a new Security Session ID mapped to the user. TLS and DTLS have their own identifiers that are part of the session.

c) The capability to generate unique session identifiers with commonly accepted sources of randomness.
   - This is described in the CIP Security Specification for TLS, DTLS, and User Authentication IDs. Session identifiers for each of these are unique and are generated randomly.

CR 3.9 Protection of audit information – Out of Scope

Events are not within scope for CIP Security. However, note that ODVA members have discussed adding standardized Syslog support to CIP Security, with the intention of covering this requirement.

CR 3.10 Support for updates – Out of Scope

Product updates are not within scope for CIP Security or communication protocols in general.

CR 3.11 Physical tamper resistance and detection – Out of Scope

Physical tamper resistance and detection is not within scope for CIP Security or communication protocols in general.

CR 3.12 Provisioning product supplier roots of trust – Partially Met by CIP Security

CIP Security defines the use of vendor certificates, which includes a root of trust managed by the vendor. Those certificates and associated root of trust can be used as the key to perform the integrity check and offer a way to prove it is a genuine device that has not been tampered with. However, it is up to the vendor to securely store the vendor certificate and provide means to use the vendor certificates.

CR 3.13 Provisioning asset owner roots of trust – Met by CIP Security

CIP Security provides interfaces to commission user-defined certificates used for secure communication between devices in a system. Besides this the User Authentication Profile adds interfaces and capabilities to authenticate users that have access to the device or system as a whole.

CR 3.14 Integrity of the boot process – Out of Scope

The boot process is not within scope of CIP Security or a communication protocol in general.

CR 4.1 Information confidentiality – Partially Met by CIP Security

Protecting the data at rest is out of the scope for CIP Security as this is not related to the communication protocol. However, for data in transit CIP Security fully covers this requirement via the CIP Security EtherNet/IP Confidentiality Profile. This profile is built on TLS and DTLS which has the capability to provide confidentiality to the data in transit. The protection of data is done via TLS and DTLS confidentiality-based cipher suites.

CR 4.2 Information persistence – Out of Scope

The persistence of information within a component is out of scope for CIP Security.

CR 4.3 Use of cryptography – Met by CIP Security

As noted before data at rest is out of scope for CIP Security. To protect data in transit CIP Security is built using standards such as TLS and DTLS, OpenID Connect, X.509, OAuth 2.0, RSA, ECC, AES, SHA-2, which represent widely accepted and widely used, well-vetted and well-tested algorithms and technologies.

CR 5.1 Network segmentation – Out of Scope

Network segmentation is not within scope for CIP Security, as it is an application layer protocol. However, CIP Security can work in segmented network architectures.

CR 5.2 Zone boundary protection – Out of Scope

This is not within scope for CIP Security or any application level communication protocol.

CR 5.3 General-purpose person-to-person communication restrictions – Out of Scope

This is not within scope for CIP Security as it does not allow for general person-to-person communication.

CR 5.4 Application partitioning – Out of Scope

There is no component level requirement within IEC 62443-4-2 for application partitioning.

CR 6.1 Audit log accessibility – Out of Scope

Events are not within scope for CIP Security. However, note that ODVA members have discussed adding standardized Syslog support to CIP Security, with the intention of covering this requirement.

CR 6.2 Continuous monitoring – Out of Scope

Events are not within scope for CIP Security. However, note that ODVA members have discussed adding standardized Syslog support to CIP Security, with the intention of covering this requirement.

CR 7.1 Denial of service protection – Out of Scope

In general, the ability to protect against a DoS attack is not within scope of a communication protocol. However, CIP Security does include functionality that will help to prevent possible DoS-style attacks such as closing TCP and UDP ports not in use. The same option is provided to close down IANA protocols such as ICMP. Another option provided by CIP Security to withstand a denial of service attack is that all interfaces can be configured to require authentication and authorization. Furthermore, EtherNet/IP and CIP Security by design uses separate ports for Messaging and I/O which reduces the attack surface via separation of these two types of communication.

CR 7.1 RE-1 Manage communication load from component – Out of Scope

This requirement is not within scope for an application layer communication protocol.

CR 7.2 Resource management – Out of Scope

The management of resources to prevent a DoS attack is not within scope of an application-layer communication protocol.

CR 7.3 Control system backup – Out of Scope

System level backup is not within scope for an application-layer communication protocol.

CR 7.3 RE-1 Backup integrity verification – Out of Scope

As with the base requirement, this is not within scope for an application-layer communication protocol.

CR 7.4 Control system recovery and reconstitution – Out of Scope

This requirement is not within scope for an application-layer communication protocol.

CR 7.5 Emergency Power – Out of Scope

IEC 62443-4-2 does not have a requirement for components for CR 7.5, this is only applied at the IEC 62443-3-3 level.

CR 7.6 Network and security configuration settings – Met by CIP Security

CIP Security provides the ability to configure a device according to recommendations provided by documents such as The Converged Plant-Wide Ethernet guide.

CR 7.6 RE-1 Machine-readable reporting of current security settings – Met by CIP Security

The Get Attributes service of the CIP Security Objects allow for security settings to be read out of a device in a machine-readable format.

CR 7.7 Least functionality – Met by CIP Security

CIP Security includes options to close TCP and UDP ports not in use, the same option is provided to close down IANA protocols such as ICMP.

CR 7.8 Control system component inventory – Out of Scope

This is not within scope for an application-layer communication protocol.

Summary

This paper has shown that CIP Security meets a significant number of IEC 62443-4-2 requirements. CIP Security utilizes robust and ubiquitous security technologies to achieve protection of the control system device. These technologies can be used as a major part of an IEC 62443-4-2 security certification, and also can apply to the system level through IEC 62443-3-3. A breakdown of the requirements met, not met, not in scope, and partially met is shown in Figure 5 and Table 3.

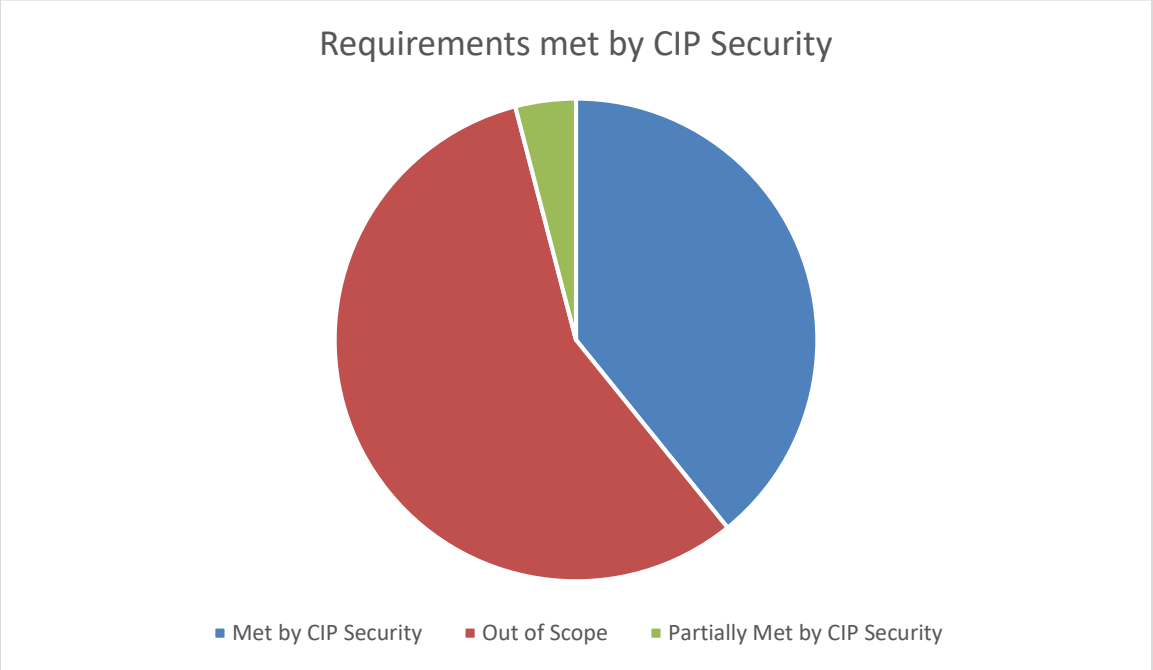

Figure 5 IEC 62443-4-2 requirements met by CIP Security

Component requirement	CIP Security mapping
CR 1.1 – Human user identification and authentication	Met by CIP Security
CR 1.1 RE-1 – Unique identification and authentication	Met by CIP Security
CR 1.1 RE-2 – Multifactor authentication for all interfaces	Met by CIP Security
CR 1.2 – Software process and device identification and authentication	Met by CIP Security
CR 1.2 RE-1 Unique identification and authentication	Met by CIP Security
CR 1.3 – Account management	Met by CIP Security
CR 1.4 – Identifier management	Met by CIP Security
CR 1.5 – Authenticator management	Met by CIP Security
CR 1.5 RE-1 – Hardware security for authenticators	Out of scope
CR 1.6 – Wireless access management	Out of scope

CR 1.7 – Strength of password-based authentication	Met by CIP Security
CR 1.7 RE-1 – Lifetime restrictions for human users	Met by CIP Security
CR 1.7 RE-2 – Password lifetime restriction for all users	Met by CIP Security
CR 1.8 – Public key infrastructure certificates	Met by CIP Security
CR 1.9 – Strength of public key-based authentication	Met by CIP Security
CR 1.9 RE-1 – Hardware security for public key-based authenticators	Out of scope
CR 1.10 – Authenticator feedback	Out of scope
CR 1.11 – Unsuccessful login attempts	Met by CIP Security
CR 1.12 – System use notification	Out of scope
CR 1.13 – Access via untrusted networks	Out of scope
CR 1.14 – Strength of symmetric key-based authentication	Met by CIP Security
CR 2.1 – Authorization enforcement	Met by CIP Security
CR 2.1 RE-1 – Authorization enforcement for all users	Met by CIP Security
CR 2.1 RE-2 – Permission mapping to roles	Met by CIP Security
CR 2.1 RE-3 Supervisor override	Met by CIP Security
CR 2.1 RE-4 Dual approval	Out of scope
CR 2.2 – Wireless use control	Out of scope
CR 2.3 – Use control for portable and mobile devices	Out of scope
CR 2.4 – Mobile code	Met by CIP Security
CR 2.5 – Session lock	Out of scope
CR 2.6 – Remote session termination	Met by CIP Security
CR 2.7 – Concurrent session control	Met by CIP Security
CR 2.8 – Auditable events	Out of scope
CR 2.9 – Audit storage capacity	Out of scope
CR 2.10 – Response to audit processing failures	Out of scope
CR 2.11 – Timestamps	Out of scope
CR 2.12 – Non-repudiation	Out of scope
CR 2.13 – Use of physical diagnostic and test interfaces	Out of scope
CR 3.1 – Communication integrity	Met by CIP Security
CR 3.1 RE-1 – Communication authentication	Met by CIP Security
CR 3.2 – Protection from malicious code	Out of scope
CR 3.3 – Security functionality verification	Out of scope
CR 3.4 – Software and information integrity	Out of scope
CR 3.4 RE-1 – Authenticity of software and information	Out of scope
CR 3.4 RE-2 – Automated notification of integrity violations	Out of scope
CR 3.5 – Input validation	Out of scope
CR 3.6 – Deterministic output	Out of scope
CR 3.7 – Error handling	Partially Met by CIP Security
CR 3.8 – Session integrity	Met by CIP Security
CR 3.9 – Protection of audit information	Out of scope
CR 3.10 – Support for updates	Out of scope

CR 3.11 – Physical tamper resistance and detection	Out of scope
CR 3.12 – Provisioning product supplier roots of trust	Partially Met by CIP Security
CR 3.13 – Provisioning asset owner roots of trust	Met by CIP Security
CR 3.14 – Integrity of the boot process	Out of scope
CR 4.1 – Information confidentiality	Partially Met by CIP Security
CR 4.2 – Information persistence	Out of scope
CR 4.3 – Use of cryptography	Met by CIP Security
CR 5.1 – Network segmentation	Out of scope
CR 5.2 – Zone boundary protection	Out of scope
CR 5.3 – General-purpose person-to-person communication restrictions	Out of scope
CR 5.4 – Application partitioning	Out of scope
CR 6.1 – Audit log accessibility	Out of scope
CR 6.2 – Continuous monitoring	Out of scope
CR 7.1 – Denial of service protection	Out of scope
CR 7.1 RE-1 – Manage communication load from component	Out of scope
CR 7.2 – Resource management	Out of scope
CR 7.3 – Control system backup	Out of scope
CR 7.3 RE-1 – Backup integrity verification	Out of scope
CR 7.4 – Control system recovery and reconstitution	Out of scope
CR 7.5 - Emergency Power	Out of scope
CR 7.6 – Network and security configuration settings	Met by CIP Security
CR 7.7 – Least functionality	Met by CIP Security
CR 7.8 – Control system component inventory	Out of scope

Table 3 IEC 62443-4-2 requirements met by CIP Security

Future Work

One major area of requirements that are currently out of scope for CIP Security are around secure event reporting and management. This is something that has been discussed before in the SIG, and there have been preliminary discussions about standardizing Syslog capabilities for CIP Security endpoints. Bringing this standardization would increase IEC 62443-4-2 coverage by CIP Security significantly, therefore this is a natural area of work for the SIG to pursue.

The only SL-4 requirement for a communication protocol was CR 2.2 RE-4 Dual Approval. Given that this is at SL-4, it was determined that this requirement is not necessary for a majority of the products implementing CIP Security. However, this requirement does represent a future area of work if one or more vendor wishes to produce an SL-4 product.

References

[1] RFC7030, Enrolment over Secure Transport, October 2013, IETF (https://tools.ietf.org/html/rfc7030)
[2] CIP Security Pull Model from the Implementation Standpoint, 2018, Visoky & Wiberg (https://www.odva.org/Portals/0/Library/Conference/Paper%204_2018-ODVA-Conference_Visoky%20Wiberg_Pull%20Model_FINAL.pdf)
[3] ODVA, Inc. The CIP Networks Library, Volume 8: CIP Security™, PUB00299
[4] TLS, RFC5246, Transport Layer Security (TLS) Protocol Version 1.2, Aug 2008 (https://tools.ietf.org/html/rfc5246)
[5] DTLS, RFC6347, Datagram Transport Layer Security Version 1.2 (https://tools.ietf.org/html/rfc6347)
[6] Open ID Connect, OpenID Authentication 2.0 – Final (https://openid.net/connect/)

[7] OAuth 2.0, RFC6749, The OAuth 2.0 Authorization Framework (https://tools.ietf.org/html/rfc6749)
[8] JWT, RFC7519, JSON Web Token (JWT) (https://tools.ietf.org/html/rfc7519)
[9] Syslog, RFC5424, The Syslog Protocol (https://tools.ietf.org/html/rfc5424)
[10] Converged Plantwide Ethernet Guide
(https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf)

****