Veracity OT Network Controller Supports and Exceeds 62443 Compliance

Implementing IEC 62443 can mitigate the effects and often prevent successful cyber-attacks. IEC 62443 addresses not only the technology that comprises a control system, but also the work processes, countermeasures, and employees. Veracity Industrial Networks' OT Network Management Platform both simplifies implementing and maintaining IEC-62443, but also exceeds the zones and conduits model layout using micro segmentation to further isolate all end points on a network than traditional network segmentation is capable of accomplishing.

The Veracity solution is typically at least 50% faster to implement the networking component of IEC 62443 and 75% less time consuming to manage over the lifecycle of the system. This speed is gained by having a single location to manage the entire network that is presented in a way familiar to OT professionals. System changes and updates can be made quickly and safely without compromising the security of the network.

From the 62443 specification "Organizations deploying business information technology (IT) cyber security solutions to address IACS security may not fully comprehend the results of this decision. While many business IT applications and security solutions can be applied to IACS, they need to be applied in an appropriate way to eliminate inadvertent consequences. For this reason, the approach used to define system requirements needs to be based on a combination of functional requirements and risk assessment, often including an awareness of operational issues as well. IACS security measures should not have the potential to cause loss of essential services and functions, including emergency procedures. (IT security measures, as often deployed, do have this potential.)"

The Veracity OT Network controller is the only network management tool that uses software defined networking and is designed specifically for the industrial or OT environment.

The Veracity OT Network Controller supports the following 62443 requirements:

IEC 62443-3-2

ZCR 1.1 The organization shall clearly identify the SuC (System under Consideration), including clear definition of the security perimeter and identification of all access points to the SuC.

ZCR 3.1 The organization shall establish zones and conduits by grouping IACS and related assets. Grouping shall be used upon the results of the high-level cybersecurity risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access or responsible organization.

ZCR 3.2 IACS shall be grouped into zones that are logically or physically separated from business or enterprise system assets.

ZCR 3.3 Safety related assets shall be grouped into zones that are logically or physically separated from zones with non-safety related assets.

ZCR 3.4 Devices that are permitted to make temporary connections to the SuC should be grouped into a separate zone or zones from assets that are intended to be permanently connected to the IACS.

ZCR 3.5 Wireless signals are not controlled by fences or cabinets and are therefore more accessible than normal wired networks. Because of this increased access potential, they are more likely exposed to a different and wider variety of threats than devices that are wired.

veracity.io
888.383.2397

ZCR 3.6 Devices that are permitted to make connections to the SuC via networks external to the SuC should be grouped into a separate zone or zones

ZCR 6.4 The following items shall be identified and documented for each defined zone and conduit:

1. Name and/or unique identifier;
2. Accountable organization(s);
3. Definition of logical boundary;
4. Definition of physical boundary, if applicable;
5. Safety designation;
6. List of all logical access points;
7. List of all physical access points;
8. List of data flows associated with each access point;
9. Connected zones or conduits;
10. List of assets and their classification, criticality and business value;
11. SL-T;
12. Applicable security requirements;
13. Applicable security policies; and
14. Assumptions and external dependencies."

IEC 62443-3-3

SR 1.1 The control system shall provide the capability to identify and authenticate all human users on all interfaces that provide human user access to the control system.

SR 1.7 For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. Additionally, control systems shall prevent password reuse for a configurable number of generations and enforce minimum and maximum password lifetime restrictions.

SR 1.8 Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

SR 1.10 The control system shall provide the capability to obscure feedback of authentication information during the authentication process.

SR 1.13 The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted network.

SR 2.1 On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.

SR 2.8 The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events.

SR 2.9 The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

SR 2.11 The control system shall provide timestamps for use in audit record generation.

veracity.io
888.383.2397

SR 2.12 The control system shall provide the capability to determine whether a given human user took a particular action.

SR 3.1 The control system shall provide the capability to protect the integrity of transmitted information. SR 3.2 The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software transported by electronic mail, Internet access, removable media, network connections, infected laptops or other common means.

SR 3.9 The control system shall protect audit information and audit tools (if present) from unauthorized access, modification, and deletion.

SR 5.1 The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

SR 5.2 The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zone and conduits model.

SR 5.3 The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system. These include e-mails, social media, or other message systems that permit the transmission of any type of executable file.

SR 5.4 The control system shall support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.

SR 6.1 The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

SR 6.2 The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. Monitoring can be achieved through a variety of tools and techniques such as IDS, IPS, network monitoring mechanisms, etc.

SR 7.1 The control system shall remain operative in a degraded mode during a DoS event.

SR 7.2 The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

SR 7.6 The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.

SR 7.7 The control system shall restrict the use of unnecessary functions, ports, protocols and/or services.

SR 7.8 The control system shall provide the capability to report the current list of installed components and their associated properties.

To learn more about how Veracity Industrial Networks can help make 62443 compliance easier, please visit our website at www.veracity.io