Addressing ISA99/ IEC62443 Controls with Tripwire Industrial Visibility

Customer Survey

92% of surveyed energy & utilities customers consider Tripwire's capabilities to be critical to their cybersecurity program.

— TechValidate survey

TVID: E34-5AD-201

The ISA99/IEC62443 cyber security framework for OT networks, is widely recognized as an industry standard. Complying with ISA99/IEC62443 best practices, is a safe path to enhance the cybersecurity posture of any given OT environment. Tripwire® Industrial Visibility is purpose-built to secure the safety and reliability of OT networks. As such, it addresses the main ISA99/IEC62443 guidelines. Deploying Tripwire Industrial Visibility aids the OT network's stakeholders to comply with external regulations and internal policies that acknowledge ISA99/IEC62443 as a cybersecurity best practice.

Tripwire Industrial Visibility passively connects to the network and utilizes proprietary Deep Packet Inspection (DPI) capabilities to parse the network traffic and retrieve critical asset data, providing the following:

OT Network Topology and Asset Data

Tripwire Industrial Visibility delivers full data of the entire OT network, including explicit IP assets, as well as remote I/O, PLC DLR and serial devices. For each asset, it retrieves full set of unique descriptors such as IP and MAC addresses, firmware version, serial number, etc.

Activity Monitoring

Tripwire Industrial Visibility establishes a high-fidelity baseline for each asset's behavior, alerting when a non-baseline communication takes place. The baseline, coupled with the deviations, if those occur, provide full documentation of the asset's activities.

Alerts

Tripwire Industrial Visibility raises an alert upon occurrence of either anomalous activity (baseline deviations) and critical change (configuration download\

Controls Addressed

Tripwire Industrial Visibility's real time continuous network monitoring enables it to address the following ISA99/IEC62443 controls:

- **FR 1 – IDENTIFICATION AND AUTHENTICATION CONTROL**
  - **SR 1.3** – Account Management
  - **SR 1.5** – Authenticator Management
  - **SR 1.11** – Unsuccessful login attempts
  - **SR 1.13** – Access via untrusted networks
- **FR 2 – USE CONTROL**
  - **SR 2.8** – Auditable events, ANSI/ISA-62443-3-3 (99.03.03)-2013, Section 6.10
  - **SR 2.9** – Auditable Storage Capacity
  - **SR 2.10** – Response to audit processing failures
- **FR 3 – SYSTEM INTEGRITY**
  - **SR 3.1** – Communication Integrity SR 3.2 – Malicious Code Protection
  - **SR 3.4** – Software and Information Integrity
  - **SR 3.7** – Error Handling
  - **SR 3.8** – Session Integrity
  - **SR 3.9** – Protection of Audit Information
- **FR 5 – RESTRICTED DATA FLOW**
  - **SR 5.1** – Network Segmentation
  - **SR 5.2** – Zone Boundary Protection
  - **SR 5.3** – General Purpose Person-to-Person Communication Restrictions
- **FR 6 – TIMELY RESPONSE TO EVENTS**
  - **SR 6.1** – Audit Log Accessibility
- **FR 7 – RESOURCE AVAILABILITY**
  - **SR 7.8** – Control System Component Inventory

upload, firmware upgrade, etc.). These alerts correspond to all scenarios in which a running code impacts a production process.

Tripwire Industrial Visibility is the leading product for cyber security within the confinements of the OT network, i.e. Levels 0–2 of the Purdue Model. The visibility the solution introduces to OT networks enables security and control teams to combine their knowledge for rapid and efficient incident response and drive forward overall network resiliency.

ISA99/IEC62443 Use Cases

FR 1 – Identification and Authentication Control

This use case begins with the requirements for identification and authentication controls on the control system. Organizations must implement controls to limit unsuccessful authentication attempts, change/refresh all authenticators, and monitor access to the control systems as well as implement controls for account management. Many control systems may not support the ability to deny access based on the number of unsuccessful login attempts or to enforce authenticator refresh. By leveraging deep packet inspection (DPI), Tripwire Industrial Visibility can detect unsuccessful login attempts passively throughout the ICS network and detect known default passwords used during logins occurring over the network. It also provides alerting when the number of defined consecutive invalid access attempts is exceeded or when a default password is detected, and encrypts data that is collected and has the ability obfuscate sensitive data.

Tripwire Industrial Visibility creates baselines with approved configurations. If accounts or authenticators deviate from the approved baselines configurable alerts are generated.

FR 2 – Use Control

This use case begins with the requirement to implement multiple audit and accountability security controls to control systems. Tripwire Industrial Visibility provides auditable events by inspection of ICS network traffic. Even if a control system is not capable of creating the audit event, it is able to determine the event through DPI. Control system communication connections, user login/logouts, baseline network configuration, firmware changes, types of commands and registers used, and the values of the responses are captured by the solution and stored in the database. The auditable events for assets can be placed into a report for management review for a determined periodicity. Auditable events are configured to capture packets to support after-the-fact investigations of security incidents. The events are adjusted and configured based on current threat information.

Tripwire Industrial Visibility captures the event and provides details on what event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, allowing authorized users to select which events are audited. It provides a centralized architecture to manage audit records and prevent the alteration or destruction of the captured events.

Since the solution is capable of running in a virtual or physical environment, storage capacity for audit events can be modified to meet organizational requirements.

Tripwire Industrial Visibility seamlessly integrates OT alerts into an organization's existing security incident and event management (SIEM)—including Tripwire Log Center™—or security operations center (SOC) platforms to provide a holistic view of an organization's risks and security stance. It can provide a timestamp for events or leverage an existing centralized timeserver.

Tripwire Industrial Visibility provides audit records and reports for indications of inappropriate or unusual activity. The events and alerts may be configurable based on current threat information and requirements. It integrates audit review, analysis, and reporting processes for investigation and response to suspicious activities.

Tripwire Industrial Visibility protects audit information from unauthorized access, modification, and deletion. It also provides different layers of access based on the user's need to know.

FR 3 – System Integrity

This use case begins with the requirement to apply multiple system integrity controls to different aspects of the control system. These controls include the integrity of communications, software and information as well as controls for malicious code and the protection of audit information.

Tripwire Industrial Visibility security fabric monitors all network traffic using DPI capabilities, built specifically for ICS networks and protocols. Using advanced machine-learning algorithms, built with the machine-to-machine character of these networks in mind, the solution automatically allowlists legitimate, baseline activities and alerts on any changes or anomalies. The solution detects the effects of malicious code or unauthorized software and generates alerts. The situational awareness engine takes into consideration spoofing, poisoning, and man-in-the-middle attacks.

Tripwire Industrial Visibility monitors the OT network, leveraging a unique combination of signatures, purpose-built OT behavioral models and proprietary anomaly detection capabilities to immediately detect and provide actionable information on any human errors, network failures or malicious activities. By correlating information across the network, the solution gives organizations the situational awareness they need, out of the box, to identify the root cause of incidents and changes, so risks are mitigated.

Tripwire Industrial Visibility monitors the OT network to detect for known suspected malicious communications, leveraging a unique combination of signatures, purpose-built OT behavioral models and proprietary anomaly detection capabilities to immediately detect and provide actionable information on any human errors, network failures, communication integrity deterioration, or malicious activities.

Tripwire Industrial Visibility creates a configuration baseline of assets on the ICS network. Communication information, software, OS, firmware, serial numbers, and card rack slots are captured for baseline configuration. For example, such baselines are used to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).

It is also able to obfuscate data to protect sensitive information. The solution protects audit information from unauthorized access, modification, and deletion, and provides tiered access to ensure error messages are only revealed to authorized personnel.

FR 5 – Restricted Data Flow

This use case begins with the requirement to segment the control system via zones and conduits to limit the unnecessary flow of data. Tripwire Industrial Visibility identifies the specific assets on the network, the lines of asset communication, the type of commands and registers used, and even the values of valid responses. This decoded information provides visibility for open/insecure protocols, proprietary protocols, account information on CDAs, information flow, network access control, and even unsuccessful login attempts. Tripwire constructs network/communication maps with the ICS communications that are decoded. This robust information assists organizations by identifying control system zones and all data flow conduits. The solution provides a map of all assets communicating on an ICS network (Field Bus/Serial & IP Networks).

Tripwire Industrial Visibility delivers analysis of information flow throughout the ICS network (Field Bus/Serial & IP Networks). Baselines of control systems communication are created to detect any deviation in real-time.

FR 6 – Timely Response to Events

This use case begins with the requirement to respond to security violations by notifying the proper authority, reporting needed evidence of the violation, and taking timely corrective action when incidents are discovered. Tripwire Industrial Visibility provides auditable events by inspection of ICS network traffic. Even if a control system is not capable of creating the audit event, the solution is able to determine the event through DPI. Examples of these events include control system communication connections, user login/logouts, baseline network configuration, firmware changes, types of commands and registers used, and the values of the responses. The auditable events for assets are placed into a report for management review for a determined periodicity. Auditable events are configured to capture packets to support after-the-fact investigations of security incidents. Data is preserved in the asset's history in the solution's database. These robust features support an organization's ability to respond to events on the control system.

Tripwire Industrial Visibility security fabric monitors all network traffic using DPI capabilities, built specifically for ICS networks and protocols. Using advanced machine- learning algorithms, built with the machine-to-machine character of these networks in mind, the solution automatically whitelists legitimate, baseline activities and alerts on any changes or anomalies.

The solution protects audit information from unauthorized access, modification, and deletion. It also provides different layers of access based on the user's need to know.

FR 7 – Resource Availability

This use case begins with the requirement to apply configuration and asset management controls to control systems. Tripwire Industrial Visibility assists organizations by identifying baseline communication patterns on an ICS network (Field Bus/Serial & IP Networks). It decodes the embedded identity information in digital messages to detect the communication protocols used and displays the entire network of assets and asset architecture. Communication information, software,

operating system, firmware, serial numbers, and the card rack slots are captured for baseline configuration.

Tripwire Industrial Visibility passively collects all ICS network traffic. This traffic can be sent to a test or simulated environment. Within the test environment, production traffic can be utilized to determine the effects of equipment changes.

Historical data is stored for each individual asset, allowing organizations to review and report on changes that deviate from the authorized baseline. Reports can be executed on the assets to verify accepted changes. These reports can be routed to designated approval authorities and the documentation then placed in the organization's change control database.

Tripwire Industrial Visibility reflects the current system configuration of assets on the ICS network. If unauthorized components are connected to the ICS network, unauthorized changes to the ICS network, unauthorized changes to cyber assets occur, or unauthorized communications take place on the ICS network, it creates alerts for designated officials.

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit **tripwire.com/contact/request-demo**

ISA99/IEC62443 Compliance Matrix

FR 1 - Identification and Authentication Control			
Control	**Control**	**Control**	**Control**
SR 1.3 - Account Management	SL-C(IAC, control system) 1: SR 1.3 SL-C(IAC, control system) 2: SR 1.3 SL-C(IAC, control system) 3: SR 1.3 (1) SL-C(IAC, control system) 4: SR 1.3 (1)	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.	**Tripwire** creates a baseline for the asset and provides alerts when the asset deviates from the baseline.
SR 1.5 - Authenticator Management	SL-C(IAC, control system) 1: SR 1.5 SL-C(IAC, control system) 2: SR 1.5 SL-C(IAC, control system) 3: SR 1.5 (1) SL-C(IAC, control system) 4: SR 1.5 (1)	The control system shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon control system installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	By leveraging Deep Packet Inspection, **Tripwire** can detect known default passwords used during logins occurring over the network. **Tripwire** encrypts data that is collected and has the ability obfuscate sensitive data.
SR 1.11 – Unsuccessful login attempts	SL-C(IAC, control system) 1: SR 1.11SL-C(IAC, control system) 2: SR 1.11SL-C(IAC, control system) 3: SR 1.11SL-C(IAC, control system) 4: SR 1.11	The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.	Using DPI, **Tripwire** can detect unsuccessful login attempts passively throughout the ICS network. **Tripwire** provides alerting when the number of defined consecutive invalid access attempts is exceeded.

FR 1 - Identification and Authentication Control			
Security Levels	**Security Levels**	**Security Levels**	**Security Levels**
SR 1.13 – Access via untrusted networks	SL-C(IAC, control system) 1: SR 1.13 SL-C(IAC, control system) 2: SR 1.13 (1) SL-C(IAC, control system) 3: SR 1.13 (1) SL-C(IAC, control system) 4: SR 1.13 (1)	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.	**Tripwire** assists organizations by identifying Cyber Assets connected to a network with the ability to identify and map all assets communicating on an ICS network (Field Bus/Serial & IP Networks). **Tripwire** decodes the embedded identity information in digital messages to detect the communication protocols used and displays the entire network of assets and asset architecture. This information is used to construct network diagrams demonstrating all external routable communication paths and the identified electronic security perimeter.
FR2 - Use Control	**FR2 - Use Control**	**FR2 - Use Control**	**FR2 - Use Control**
Control	**Control**	**Control**	**Control**
SR 2.8 – Auditable events, ANSI/ISA-62443-3-3 (99.03.03)-2013, Section 6.10	SL-C(UC, control system) 1: SR 2.8 SL-C(UC, control system) 2: SR 2.8 SL-C(UC, control system) 3: SR 2.8 (1) SL-C(UC, control system) 4: SR 2.8 (1)	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. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	**Tripwire** provides auditable events by inspection of ICS network traffic. Even if an asset is not capable of creating the audit event, **Tripwire** is able to determine the event through DPI. Examples include the following; asset communication connections, user login/logouts, baseline network configuration, firmware changes, types of commands and registers used, and the values of the responses. The auditable events for assets are placed into a report for management review for a determined periodicity. Auditable events are configured to capture packets to support after-the-fact investigations of security incidents.
FR2 - Use Control			
Control	**Control**	**Control**	**Control**
SR 2.9 - Auditable Storage Capacity	SL-C(UC, control system) 1: SR 2.9 SL-C(UC, control system) 2: SR 2.9 SL-C(UC, control system) 3: SR 2.9 (1) SL-C(UC, control system) 4: SR 2.9 (1)	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.	**Tripwire** provides a centralized architecture to manage audit records and prevents the alteration or destruction of the captured events. **Tripwire** storage capacity is configurable to meet organizational needs. Records can also be integrated to a SIEM or other storage devices.
SR 2.10 – Response to audit processing failures	SL-C(UC, control system) 1: SR 2.10 SL-C(UC, control system) 2: SR 2.10 SL-C(UC, control system) 3: SR 2.10 SL-C(UC, control system) 4: SR 2.10	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	**Tripwire** acts as an external system to provide auditing capabilities for the ICS network despite the fact many ICS assets do not generate audits. The solution provides alerts for audit processing failures.
SR 2.11 – Timestamps	SL-C(UC, control system) 1: Not selected SL-C(UC, control system) 2: SR 2.11 SL-C(UC, control system) 3: SR 2.11 (1) SL-C(UC, control system) 4: SR 2.11 (1) (2)	The control system shall provide timestamps for use in audit record generation.	**Tripwire** has the capability of providing time stamps for all events monitored and collected as well as synchronize with a centralized timeserver.

FR 3 - System Integrity			
Control	**Control**	**Control**	**Control**
SR 3.1 – Communication Integrity	SL-C(SI, control system) 1: SR 3.1 SL-C(SI, control system) 2: SR 3.1 SL-C(SI, control system) 3: SR 3.1 (1) SL-C(SI, control system) 4: SR 3.1 (1)	The control system shall provide the capability to protect the integrity of transmitted information.	**Tripwire** monitors the OT network, leveraging a unique combination of signatures, purpose-built OT behavioral models and proprietary anomaly detection capabilities to immediately detect and provide actionable information on any human errors, network failures, communication integrity deterioration, or malicious activities.
SR 3.2 – Malicious Code Protection	SL-C(SI, control system) 1: SR 3.2 SL-C(SI, control system) 2: SR 3.2 (1) SL-C(SI, control system) 3: SR 3.2 (1) (2) SL-C(SI, control system) 4: SR 3.2 (1) (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. The control system shall provide the capability to update the protection mechanisms.	**Tripwire** security fabric monitors all network traffic using deep packet inspection (DPI) capabilities, built specifically for ICS networks and protocols. Using advanced machine-learning algorithms, built with the machine-to-machine character of these networks in mind, the solution automatically whitelists legitimate, baseline activities and alerts on any changes or anomalies.
SR 3.4 – Software and Information Integrity	SL-C(SI, control system) 1: Not Selected SL-C(SI, control system) 2: SR 3.4 SL-C(SI, control system) 3: SR 3.4 (1) SL-C(SI, control system) 4: SR 3.4 (1)	The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.	**Tripwire** creates a configuration baseline of assets on the ICS network. Communication information, software, OS, firmware, serial numbers, and card rack slots are captured for baseline configuration. For example, such baselines are used to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).
FR 3 - System Integrity			
Control	**Control**	**Control**	**Control**
SR 3.7 - Error Handling	SL-C(SI, control system) 1: Not Selected SL-C(SI, control system) 2: SR 3.7 SL-C(SI, control system) 3: SR 3.7 SL-C(SI, control system) 4: SR 3.7	The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	**Tripwire** creates alerts based on communications on the ICS network. **Tripwire** is able to obfuscate data to protect sensitive information. **Tripwire** provides tiered access to ensure error messages are only revealed to authorized personnel.
SR 3.8 - Session Integrity	SL-C(SI, control system) 1: Not Selected SL-C(SI, control system) 2: SR 3.8 SL-C(SI, control system) 3: SR 3.8 (1) (2) SL-C(SI, control system) 4: SR 3.8 (1) (2) (3)	The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.	**Tripwire** security fabric monitors all network traffic using deep packet inspection (DPI) capabilities, built specifically for ICS networks and protocols. Using advanced machine-learning algorithms, built with the machine-to-machine character of these networks in mind, the solution automatically whitelists legitimate, baseline activities and alerts on any changes or anomalies. The situational awareness engine takes into consideration spoofing, poisoning, and man-in-the-middle attacks.
SR 3.9 - Protection of Audit Information	SL-C(SI, control system) 1: Not selected SL-C(SI, control system) 2: SR 3.9 SL-C(SI, control system) 3: SR 3.9 SL-C(SI, control system) 4: SR 3.9 (1)	The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.	**Tripwire** protects audit information from unauthorized access, modifi-cation, and deletion. **Tripwire** provides different layers of access based on the user's need to know.

FR 5 - Restricted Data Flow			
Control	**Control**	**Control**	**Control**
SR 5.1 - Network Segmentation	SL-C(RDF, control system) 1: SR 5.1 SL-C(RDF, control system) 2: SR 5.1 (1) SL-C(RDF, control system) 3: SR 5.1 (1) (2) SL-C(RDF, control system) 4: SR 5.1 (1) (2) (3)	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.	**Tripwire** provides analysis of information flow throughout the ICS network (Field Bus/Serial & IP Networks). Baselines of control system communication are created to detect any deviation in real-time.
SR 5.2 - Zone Boundary Protection	SL-C(RDF, control system) 1: SR 5.2 SL-C(RDF, control system) 2: SR 5.2 (1) SL-C(RDF, control system) 3: SR 5.2 (1) (2) (3) SL-C(RDF, control system) 4: SR 5.2 (1) (2) (3)	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	**Tripwire** provides analysis of information flow throughout the ICS network (Field Bus/Serial & IP Networks). Baselines of control system communication are created to detect any deviation in real time.
SR 5.3 - General Purpose Person-to-Person Communication Restrictions	SL-C(RDF, control system) 1: SR 5.3 SL-C(RDF, control system) 2: SR 5.3 SL-C(RDF, control system) 3: SR 5.3 (1) SL-C(RDF, control system) 4: SR 5.3 (1)	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. 9.5.2	
FR 6 - Timely Response to Events	**FR 6 - Timely Response to Events**	**FR 6 - Timely Response to Events**	**FR 6 - Timely Response to Events**
Control	**Control**	**Control**	**Control**
SR 6.1 - Audit Log Accessibility	SL-C(TRE, control system) 1: SR 6.1 SL-C(TRE, control system) 2: SR 6.1 SL-C(TRE, control system) 3: SR 6.1 (1) SL-C(TRE, control system) 4: SR 6.1 (1)	The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	**Tripwire** protects audit information from unauthorized access, modification, and deletion. **Tripwire** provides different layers of access based on the user's need to know.
FR 6 - Timely Response to Events			
Control	**Control**	**Control**	**Control**
SR 6.2 - Continuous Monitoring	SL-C(TRE, control system) 1: Not Selected SL-C(TRE, control system) 2: SR 6.2 SL-C(TRE, control system) 3: SR 6.2 SL-C(TRE, control system) 4: 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.	**Tripwire** security fabric monitors all network traffic using deep packet inspection (DPI) capabilities, built specifically for ICS networks and protocols. Using advanced machine-learning algorithms, built with the machine-to-machine character of these networks in mind, the solution automatically whitelists legitimate, baseline activities and alerts on any changes or anomalies.
FR 7 - Resource Availability			
Control	**Control**	**Control**	**Control**
SR 7.8 – Control System Component Inventory	SL-C(RA, control system) 1: Not Selected SL-C(RA, control system) 2: SR 7.8 SL-C(RA, control system) 3: SR 7.8 SL-C(RA, control system) 4: SR 7.8	The control system shall provide the capability to report the current list of installed components and their associated properties.	**Tripwire** creates a configuration baseline of assets on the ICS network. Communication information, software, OS, firmware, serial numbers, and card rack slots are captured for baseline configuration. For example, such baselines are used to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at** tripwire.com

***The State of Security*: News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, Twitter **and** Facebook

SBISAIEC1a 2101