How the Endian Secure Digital Platform helps to Achieve IEC 62443 Compliance

As the digital transformation takes hold in the industrial markets and starts to spread rapidly the need for cybersecurity gets more and more amplified. Fortunately this was recognized early on and the IEC 62443 (formerly known as ISA 99) security standards were created in order to provide a cybersecurity standard that applies in all industrial applications. The IEC 62443 standards allow industrial operators to assess and mitigate cybersecurity risks across their industrial processes, networks and devices. The standard is broken into four major categories each with relevant components listed in Figure 1.

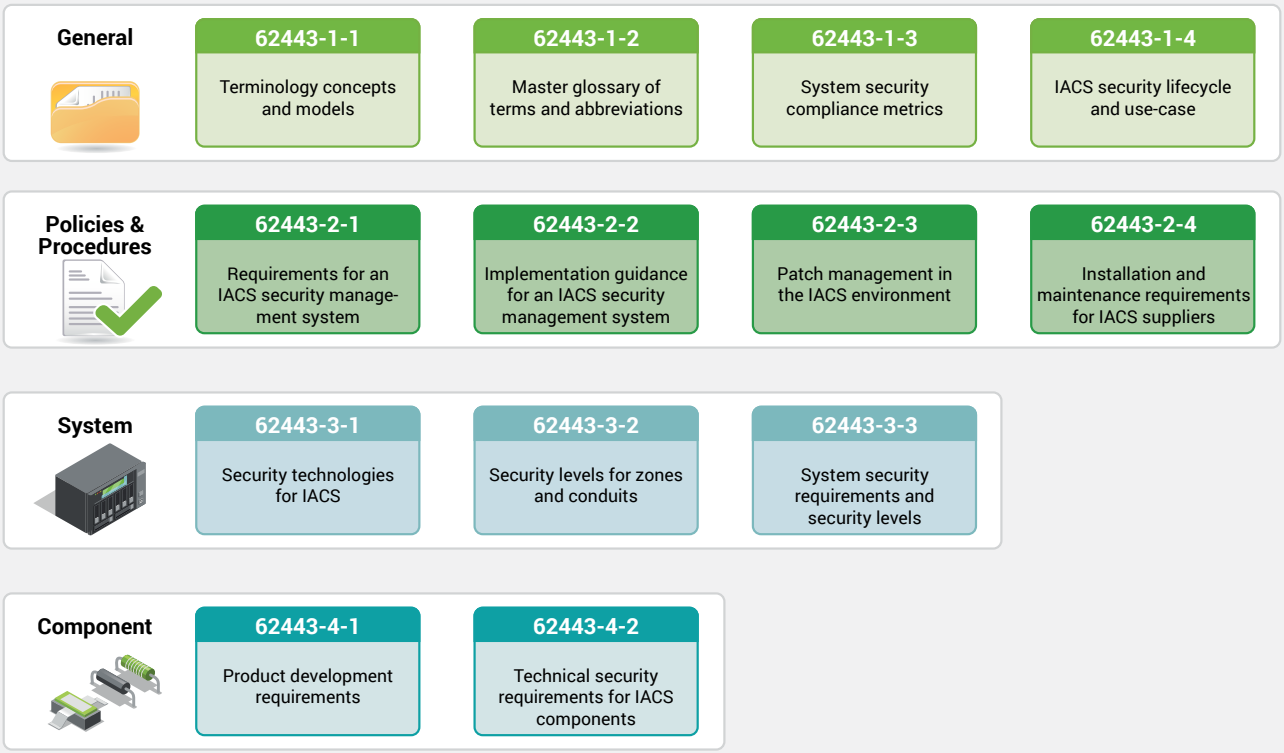

Figure 1: IEC 62443

Roles and Responsibilities

The IEC 62443 standard defines three primary roles that are responsible for designing, implementing and managing industrial automation and control systems (IACS).

- **Asset Owner:** Responsible for operating and maintaining the IACS
- **System Integrator:** Responsible for the integration and commissioning of IACS products and components
- **Product Supplier (Vendor):** Responsible for development and testing of IACS products

Endian as the product supplier is responsible for developing and testing the Secure Digital Platform which comprises the Switchboard, acting as the central component and 4i Edge product series devices deployed at the remote sites. This means that the Endian Secure Digital Platform is only one part of a larger more complex system of people, processes and products that each business must employ in order to satisfy the requirements of IEC 62443. In other words, the Endian solution is a tool that when configured and utilized properly can help assist an organization in meeting compliance with IEC 62443 in regards to the services it provides.

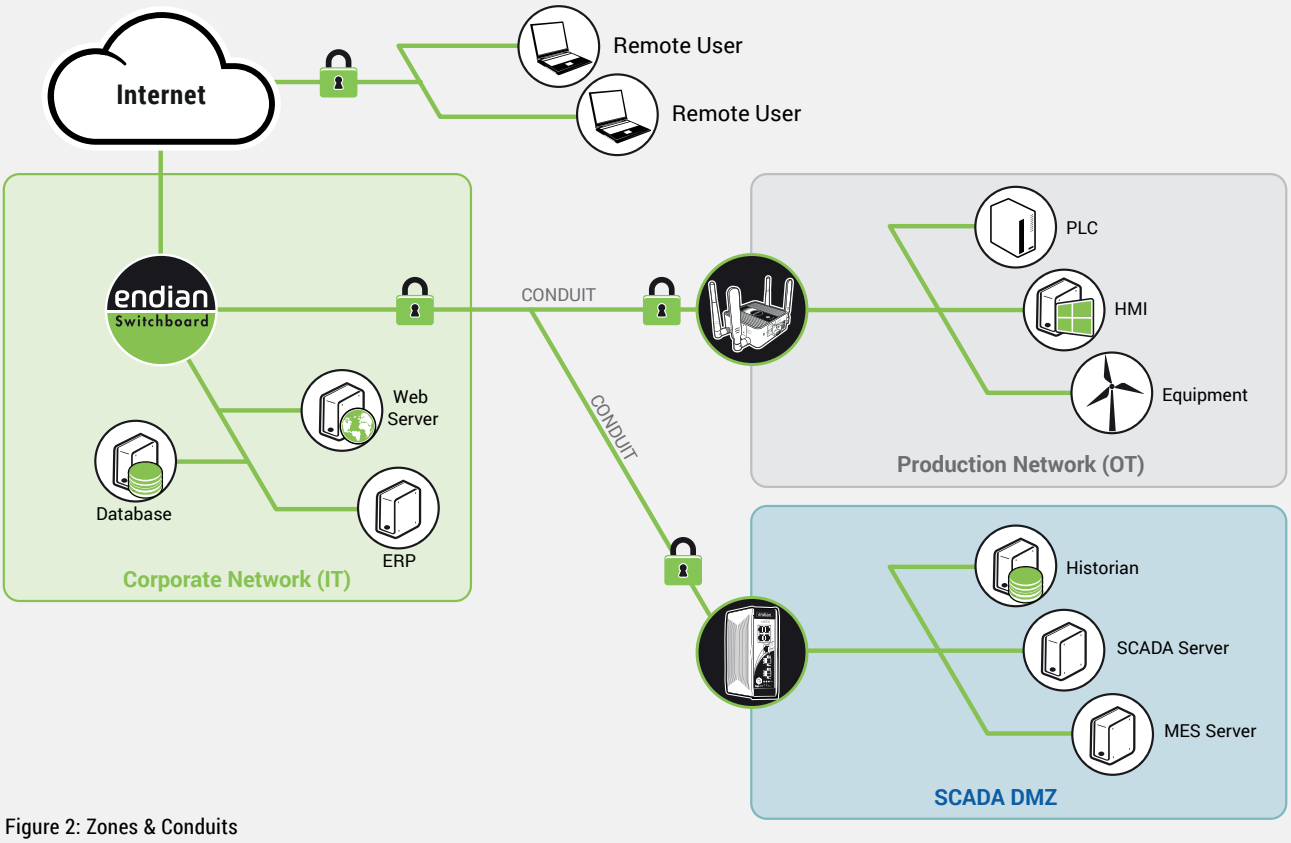

Figure 2: Zones & Conduits

Zones and Conduits

The IEC 62443 standard outlines a network separation technique known as zones and conduits. Essentially, using this technique you separate your industrial assets in logical groups that have similar communication protocols or patterns into zones which are then interconnected to each other using secure conduits utilizing firewalls whereby the traffic between the zones are strictly controlled and monitored (see Figure 2). Using this method, a business can isolate assets by type and limit potential damage from spreading to all assets. In addition, they can minimize the risk of accidental or unauthorized access between zones. The Endian 4i product series can be used to provide the secure conduits with advanced network segmentation and security including powerful yet easy to use firewall controls (in all directions) and deep-packet inspection technology with intrusion detection/prevention.

Security Standards

The IEC 62443 security standards parts 3-3 and 4-2 both specify a list of requirements grouped into logical categories. These requirements enumerate the specific processes and technology a product and system should contain in order to meet the specified security levels within the standards. Below we'll identify the primary features in the Endian Secure Digital Platform that can help to address the 62443 requirements of parts 3-3 and 4-2. It's important to note this is not an exhaustive list and that some of the 62443 requirements don't apply for various reasons.

FR 1/ CR 1: Identification and Authentication Control

- ☑ User/Group account and permission management
- ☑ User self-service options for password resets
- ☑ Active Directory / LDAP support
- ☑ Require user to change password or send email to set initial password
- ☑ Two-factor authentication support
- ☑ Brute force account lockout
- ☑ PKI support with X.509 certificate
- ☑ Inactivity account timeouts

FR 2 / CR 2: Identification and Authentication Control

- ☑ User/Group account and permission management
- ☑ Brute force account lockout
- ☑ Active Directory / LDAP support
- ☑ Inactivity account timeouts
- ☑ Clearly defined permissions can be added/removed from user accounts
- ☑ Complete audit log enabled by default
- ☑ Session termination timeouts
- ☑ All user events logged to audit log

FR 3 / CR 3: System Integrity

- ☑ Strong VPN encryption used for all communications
- ☑ Endian provides release notes with change log for each update/upgrade
- ☑ Product receives regular software updates and upgrades
- ☑ Audit logs kept in a secure fashion
- ☑ Standard protocols enforce common integrity checks

FR 4 / CR 4: Data Confidentiality

- ☑ Strong VPN encryption used for all communications
- ☑ Platform only supports strong cryptographic algorithms and keys
- ☑ Factory reset purges all sensitive information
- ☑ Product provides strong confidentiality of information

FR 5 / CR 5: Restricted Data Flow

- All products support network segmentation with multiple zones
- Complete stateful firewall protects and monitors traffic in all directions
- Content-filtering technology to enforce security policies
- Firewall security protects internal zones by default
- Deep-packet inspection technology monitors and stops advanced attacks

FR 6 / CR 6: Timely Response to Events

- Read-only access to audit logs
- Security mechanisms provide for continuous monitoring

FR 7 / CR 7: Resource Availability

- Platform utilizes strong DoS (Denial of Service) mechanisms
- Highly scalable solution prevents user or device bottlenecks
- Create one-time or schedule backups to ensure quick disaster recovery
- Products utilize a secure-by-default configuration

Conclusion

Given all of this, the Endian Secure Digital Platform can be a crucial contributor to an organization's compliance effort in regards to IEC 62443 especially in the areas of remote access, network security (conduits and zones) and network monitoring. To find out more how Endian and our solution can benefit your organization or to get in touch with a sales representative, visit our website at www.endian.com.