

Wie die Endian Secure Digital Platform zur Einhaltung der IEC 62443 beiträgt



Die digitale Transformation hält Einzug in die industriellen Märkte und mit ihrer raschen Ausbreitung steigt auch der Anspruch an die IT-Sicherheit. Dieser Trend wurde frühzeitig erkannt und führte zu der Entwicklung des Sicherheitsstandards IEC 62443 (früher bekannt als ISA 99). Damit entstand ein Standard für Cybersicherheit, der für alle industriellen Anwendungen gültig ist.

Die IEC 62443-Standards ermöglichen Industrieunternehmen, Cybersecurity-Risiken in ihren industriellen Prozessen, Netzwerken und Geräten zu bewerten und zu minimieren. Der Standard ist in vier Hauptkategorien unterteilt, deren relevante Komponenten in Abbildung 1 aufgeführt sind.

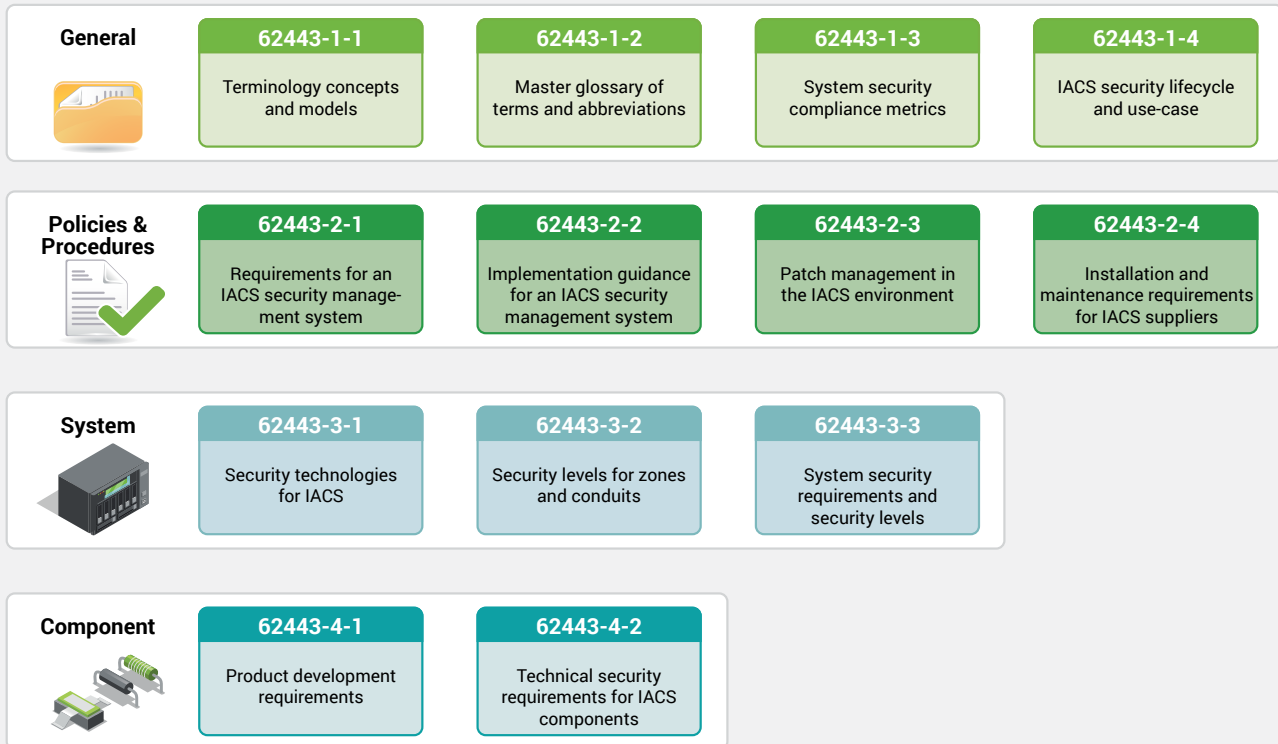


Abbildung 1: IEC 62443

Rollen und Zuständigkeiten

Die Norm IEC 62443 definiert drei zentrale Rollen, die für den Aufbau, die Implementierung und die Verwaltung von industriellen Automatisierungs- und Steuerungssystemen verantwortlich sind.

- **Asset-Eigentümer:** Verantwortlich für den Betrieb und die Wartung des IACS
- **Systemintegrator:** Verantwortlich für die Integration und Inbetriebnahme von IACS-Produkten und -Komponenten
- **Produktlieferant (Vendor):** Verantwortlich für die Entwicklung und das Testen von IACS-Produkten

Endian als Produktlieferant ist verantwortlich für die Entwicklung und das Testen der Secure Digital Platform. Diese besteht aus zwei Komponenten: Dem Switchboard als zentrales Managementtool und den Geräten der 4i Edge X Produktserie, die an den verteilten Standorten zum Einsatz kommen. Das bedeutet, dass die Endian Secure Digital Platform nur ein Teil eines größeren, komplexeren Systems aus Menschen, Prozessen und Produkten ist, das jedes Unternehmen einsetzen muss, um den Anforderungen der IEC 62443 zu entsprechen. Mit anderen Worten: Die Endian-Lösung ist ein Werkzeug, das, wenn es richtig konfiguriert und eingesetzt wird, ein Unternehmen dabei unterstützen kann, die Anforderungen der IEC 62443 in Bezug auf die von ihm angebotenen Dienste zu erfüllen.

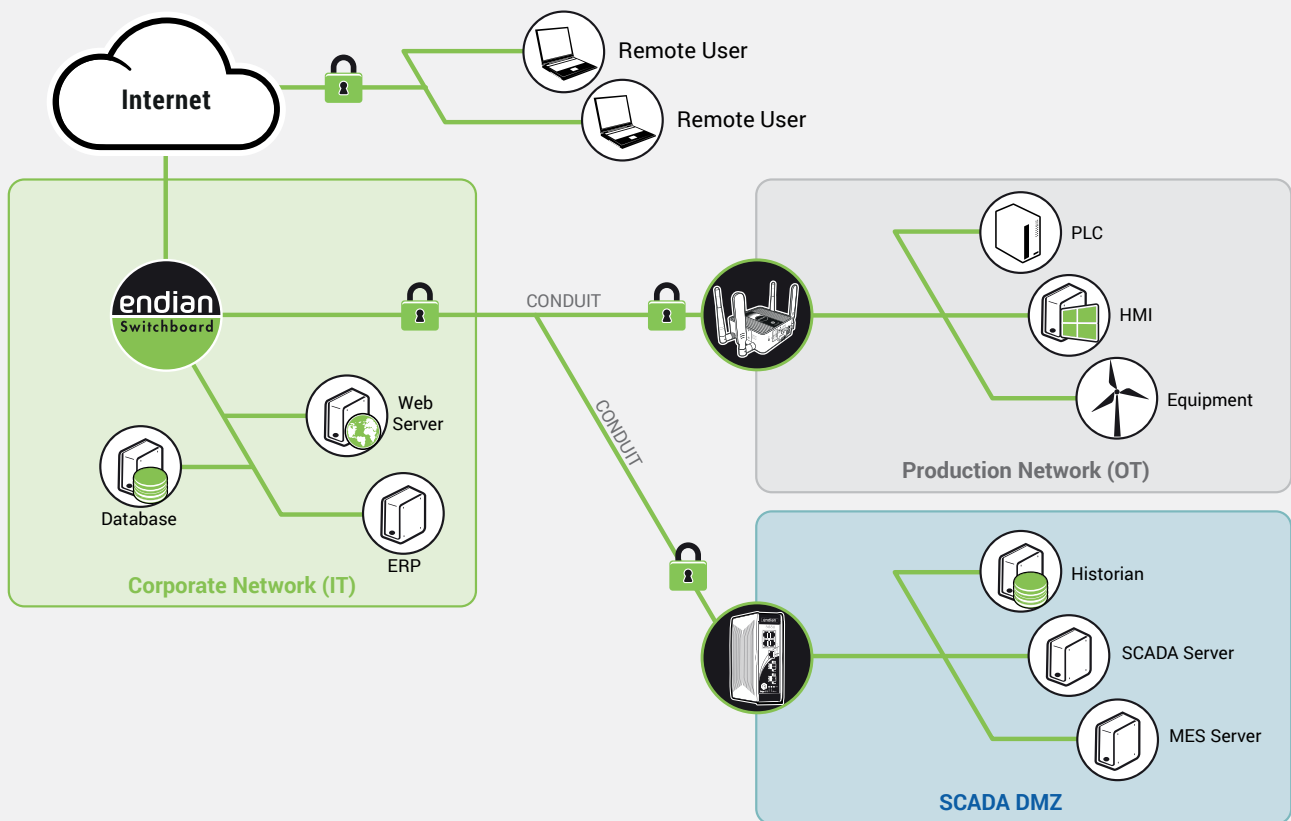


Abbildung 2: Zones & Conduits

Zonen und Übergänge (Zones and Conduits)

Die IEC 62443 sieht eine Methode zur Unterteilung von Netzwerken vor, die als „Zones and Conduits“ bekannt ist. Dabei werden die industriellen Anlagen in logische Gruppen aufgeteilt, die ähnliche Kommunikationsprotokolle oder -muster haben. Diese fasst man dann in Zonen zusammen, die anschließend über sichere Übergänge, sogenannte Conduits, per Firewall miteinander verbunden werden. Der Datenverkehr zwischen den Zonen wird streng kontrolliert und überwacht (siehe Abbildung 2).

Mit dieser Methode ist ein Unternehmen in der Lage, Anlagen nach Typ zu isolieren und die Ausbreitung potenzieller Schäden auf alle Anlagen zu begrenzen. Darüber hinaus lässt sich das Risiko eines versehentlichen oder nicht autorisierten Zugriffs zwischen den Zonen minimieren. Die Endian 4i Produktserie hilft dabei, die Secure Conduits mit fortschrittlicher Netzwerksegmentierung und -sicherheit auszustatten, einschließlich leistungsstarker und dennoch einfach zu bedienender Firewall-Kontrollen (in alle Richtungen) und Deep-Packet-Inspection-Technologie mit Intrusion Detection/Prevention.

Sicherheitsnormen

Die Sicherheitsstandards der IEC 62443, Teile 3-3 und 4-2, enthalten jeweils eine Liste von Anforderungen, die in mehrere logische Kategorien unterteilt sind. Diese Anforderungen beschreiben die spezifischen Prozesse und Technologien, die ein Produkt und System enthalten sollte, um die in den Standards festgelegten Sicherheitsstufen zu erreichen. Im Folgenden werden die wichtigsten Funktionen der Endian Secure Digital Platform genannt, die dazu beitragen können, die Anforderungen der Teile 3-3 und 4-2 der Norm 62443 zu erfüllen. Es handelt sich hierbei um keine komplette Liste und einige der 62443-Anforderungen treffen aus verschiedenen Gründen nicht zu.

FR 1 / CR 1: Identifikations- und Authentifizierungskontrolle

☒ Konten- und Rechteverwaltung für Benutzer/Gruppen

☒ Active Directory / LDAP-Unterstützung

☒ Unterstützung von Zwei-Faktor-Authentifizierung

☒ PKI-Unterstützung mit X.509-Zertifikat

☒ Option für Benutzer, das Passwort selbständig zurückzusetzen

☒ Benutzer zum Ändern des Kennworts auffordern oder E-Mail zum Festlegen des ursprünglichen Kennworts senden

☒ Brute-Force-Kontosperrung

☒ Zeitüberschreitungen für inaktive Konten

FR 2 / CR 2: Identifikations- und Authentifizierungssteuerung

☒ Konten- und Rechteverwaltung für Benutzer/Gruppen

☒ Active Directory / LDAP-Unterstützung

☒ Klar definierte Berechtigungen zu Benutzerkonten hinzufügen/entfernen

☒ Timeouts für das Beenden von Sitzungen

☒ Brute-Force-Kontosperrung

☒ Zeitüberschreitungen bei Inaktivität des Kontos

☒ Vollständiges Audit-Log standardmäßig aktiviert

☒ Alle Benutzerereignisse werden im Audit-Protokoll aufgezeichnet

FR 3 / CR 3: Systemintegrität

☒ Verwendung starker VPN-Verschlüsselung für die gesamte Kommunikation

☒ Standardprotokolle erzwingen einheitliche Integritätschecks

☒ Sichere Aufbewahrung aller Audit-Protokolle

☒ Das Produkt erhält regelmäßig Software-Updates und -Upgrades

☒ Endian stellt Versionshinweise mit Änderungsprotokoll für jedes Update/Upgrade zur Verfügung

FR 4 / CR 4: Vertraulichkeit der Daten

☒ Verwendung starker VPN-Verschlüsselung für die gesamte Kommunikation

☒ Die Plattform unterstützt nur starke kryptographische Algorithmen und Schlüssel

☒ Reset auf Werkseinstellungen löscht alle sensiblen Informationen

☒ Das Produkt bietet eine hohe Vertraulichkeit der Informationen

FR 5 / CR 5: Eingeschränkter Datenfluss

- ✓ Alle Produkte unterstützen Netzwerksegmentierung mit mehreren Zonen
- ✓ Vollständige Stateful-Firewall schützt und überwacht den Datenverkehr in alle Richtungen
- ✓ Firewall-Sicherheit schützt standardmäßig interne Zonen
- ✓ Deep-Packet-Inspection-Technologie überwacht und stoppt hochentwickelte Angriffe
- ✓ Content-Filtering-Technologie zur Einhaltung von Sicherheitsrichtlinien

FR 6 / CR 6: Zeitnahe Reaktion auf Ereignisse

- ✓ Schreibgeschützter Zugriff auf Audit-Protokolle
- ✓ Sicherheitsmechanismen sorgen für kontinuierliche Überwachung

FR 7 / CR 7: Ressourcenverfügbarkeit

- ✓ Plattform nutzt starke DoS-Mechanismen (Denial of Service)
- ✓ Einmalige oder geplante Backups, um eine schnelle Disaster Recovery zu gewährleisten
- ✓ Hochgradig skalierbare Lösung verhindert Engpässe bei Anwendern oder Geräten
- ✓ Die Produkte verwenden eine sichere Standardkonfiguration

Fazit

Mit all diesen Funktionen kann die Endian Secure Digital Platform einen entscheidenden Beitrag zu den Konformitätsbemühungen einer Organisation in Bezug auf die IEC 62443 leisten, insbesondere in den Bereichen Fernzugriff, Netzwerksicherheit (Conduits und Zonen) und Netzwerküberwachung.

Wollen Sie mehr darüber erfahren, wie Ihre Organisation von Endian und seiner Lösung profitieren kann, oder möchten Sie sich mit einem Vertriebsmitarbeiter in Verbindung setzen, dann besuchen Sie unsere Website unter www.endian.com

