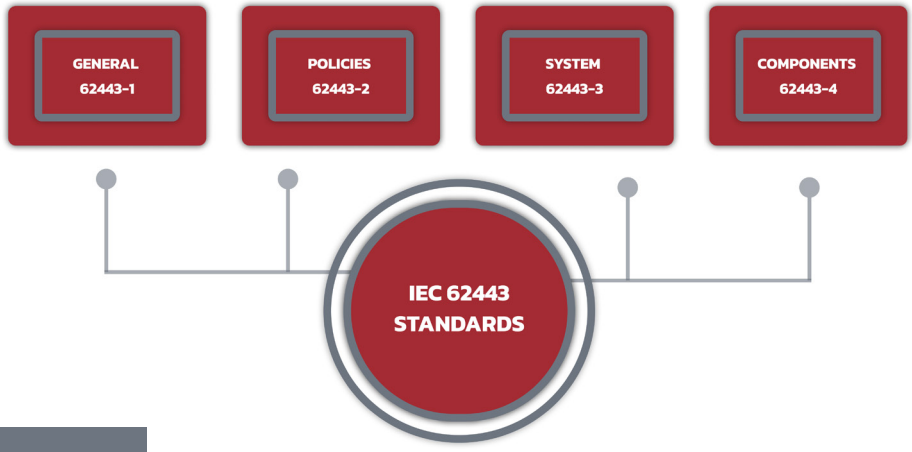
Ipari vezérlőrendszerek

– ISA/IEC 62443-4-1

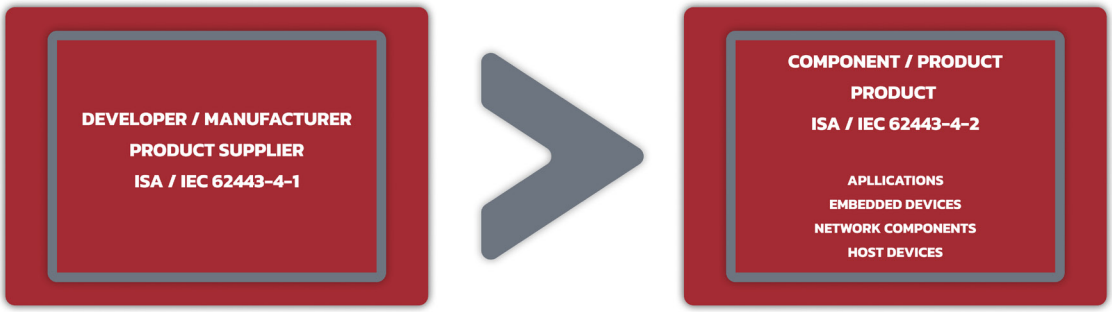
Az ipari vezérlőrendszerek kibertámadások elleni védelme fontosabbá vált, mint valaha. Az ISA/IEC 62443 szabványsorozat azért jött létre, hogy könnyen használható, megvalósítható modellt nyújtson a kockázatok kezelésére és a kiberbiztonsági fenyegetések mérséklésére.

Az IEC 62443 az ipari vezérlőrendszerek védelmére vonatkozó szabvány és a leghatékonyabb kiberbiztonsági megoldás az ipar 4.0 számára. A termelési eszközök fokozott összekapcsolhatóságával (IIoT) új veszélyek jelennek meg, amelyeket be kell vonni a hagyományos kockázatkezelési folyamatokba. Az ipari automatizálási vezérlőrendszer-alkatrészek gyártójának (beszállítójának) a termékfejlesztési folyamatokba be kell építenie az IEC 62443 4-1 szerinti biztonsági követelmények figyelembevételét. Az IEC 62443 szabvány 4-1. része biztonságos fejlesztési életciklust határoz meg az ipari automatizálási és vezérlőrendszerekben (IACS) használt biztonságos termékek kifejlesztése és karbantartása céljából. Az IEC 62443-4-1 tanúsítás azt igazolja, hogy a fejlesztő a termékfejlesztési folyamatok első napjától kezdve a tervezési biztonság módszertanát alkalmazza, amely magában foglalja a teljes biztonsági életciklust és a javítások kezelését.



TAM CERT Magyarország Kft
www.tamcert.hu

Annak érdekében, hogy az ügyfelekre vonatkozó biztonsági követelmények teljesüljenek, ezeket az ipari alkatrészeket az IEC 62443-4-2 szabvány szerint kell tanúsítani. Ha az alkatrészszállítók követik az IEC 62443-4-2 alfejezetben meghatározott irányelveket, akkor a legjobb eséllyel ruházzák fel ügyfeleiket a kibertámadások elleni védelemre. Bár az alkatrészszállítóknak bizonyos funkciókat és képességeket kell hozzáadniuk az eszközeikhez ahhoz, hogy az eszközök alkalmasak legyenek az ipari IoT-hálózatokban való telepítésre, az IEC 62443-4-2-ben meghatározott követelményeknek való megfelelés garantálja a biztonságos és ellenálló alkatrészeket, amelyeket a 62443 tanúsított és biztonságos IACS-szervezeteknek kell beszerezniük.



Biztonsági szint	Visszaélés	Eszköz	Forrás	Ismeret	Motiváció
1	véletlen	-	-	-	-
2	szándékos	egyszerű	kevés	általános	alacsony
3	szándékos	magas szintű	mérsékelt	automatizált vezérlő rendszer	átlagos
4	szándékos	magas szintű	kiterjedt	automatizált vezérlő rendszer	átlagos

Tanúsítás:

Az IEC 62443 szabvány 4 szintű biztonsági funkciót ír le a komponensek biztonságára (62443-4-2).

SL1: Védelem az ok-okozati vagy véletlenszerű megsértés ellen.
SL3: Védelem a szándékos jogsértés ellen kifinomult eszközökkel, mérsékelt forrásokkal, IACS-specifikus készségekkel és mérsékelt motivációval.
SL3: Védelem a szándékos jogsértés ellen egyszerű eszközökkel, alacsony forrásokkal, általános készségekkel és alacsony motivációval
SL4: Védelem a szándékos jogsértés ellen kifinomult eszközökkel, kiterjedt forrásokkal, IIER-specifikus készségek és magas motiváció

Az auditálás fontossága:

Az auditálás kritikus szerepet játszik az ipari vezérlőrendszerek rugalmasságának és biztonságának fenntartásában. A rendszeres ellenőrzések elvégzésével a szervezetek értékes betekintést nyerhetnek kiberbiztonsági gyakorlataik, irányelveik és eljárásaik erősségeibe és gyengeségeibe. Az ICS-ben végzett auditálás előnyei a következők:

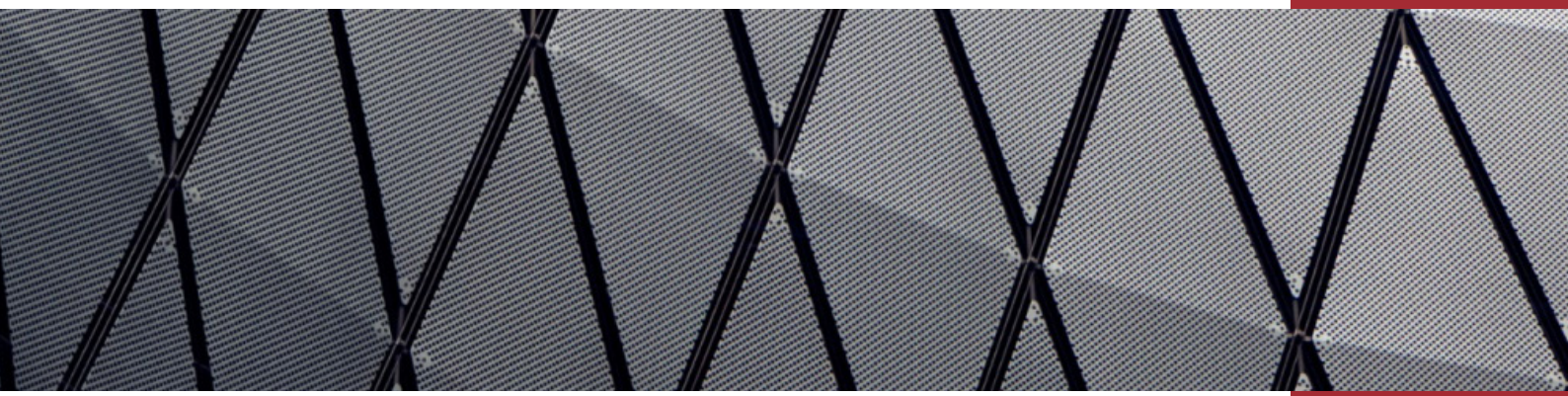
A sebezhetőségek azonosítása: Az IEC 62443-4-1 szabványnak megfelelően elvégzett auditok segítenek a szervezet irányítási rendszerének potenciális sebezhető pontjainak feltárásában. E gyenge pontok proaktív azonosításával a vállalatok megfelelő intézkedéseket hozhatnak a kockázatok mérséklésére, mielőtt azokat rosszindulatú szereplők kihasználhatnák.

A megfelelőség biztosítása: Számos iparágban, például az energiaiparban, a gyártásban és a kritikus infrastruktúrákban szigorú szabályozási követelmények vonatkoznak a kiberbiztonságra. Az IEC 62443-4-1 megfelelőség strukturált megközelítést biztosít a szervezetek számára e követelmények teljesítéséhez és a szükséges tanúsítványok fenntartásához.

A rugalmasság növelése: Az auditok hozzájárulnak a robusztus kiberbiztonsági stratégia kialakításához. A szervezetek az audit megállapításait felhasználhatják az incidensekre való reagálási képességeik, üzletmenet-folytonossági terveik és a kiberfenyegetésekkel szembeni általános ellenálló képességük javítására.

Kockázatkezelés: A hatékony kockázatkezeléshez elengedhetetlen az ICS-t fenyegető kockázatok megértése. Az IEC 62443-4-1 szabványnak megfelelő auditok segítenek a szervezeteknek felmérni a különböző kiberfenyegetések potenciális hatását, és ennek megfelelően rangsorolni a biztonsági erőfeszítéseiket.

Az érdekelt felek bizalmának elnyerése: Az ügyfelek, a partnerek és a szabályozó szervek gyakran megkövetelik a hatékony kiberbiztonsági gyakorlatok bizonyítását. Az IEC 62443-4-1 szabványnak való megfelelés bizonyítja a szervezet elkötelezettségét az ICS védelme iránt, és ezzel bizalmat épít az érdekeltek körében.



Az IEC 62443-4-1 szerinti audit elvégzése:

A hatókör meghatározása: Az audit hatályának egyértelmű meghatározása, beleértve az értékelendő rendszereket, eszközöket és folyamatokat, alapvető fontosságú az értékelés összpontosítása és a szervezet célkitűzései szempontjából való relevanciájának biztosítása szempontjából.

Kockázatértékelés: Az egyes ellenőrzött területekhez kapcsolódó kockázatok értékelése lehetővé teszi a szervezet számára, hogy rangsorolja erőfeszítéseit és hatékonyan ossza el az erőforrásokat.

A biztonsági ellenőrzések értékelése: Az auditorok megvizsgálják a meglévő biztonsági ellenőrzéseket és intézkedéseket, összehasonlítva azokat az IEC 62443-4-1 szabvány követelményeivel.

Dokumentáció és jelentéstétel: Az audit megállapításainak és ajánlásainak részletes dokumentálása alapvető fontosságú ahhoz, hogy a szervezetek megértsék a kiberbiztonsági felkészültségük jelenlegi állapotát, és fejlesztési terveket dolgozzanak ki.

Folyamatos fejlesztés: Az ideális esetben előre meghatározott időközönként végzett rendszeres auditok lehetővé teszik a szervezetek számára, hogy nyomon kövessék fejlődésüket és folyamatosan javítsák kiberbiztonsági helyzetüket.

Konklúzió:

Az IEC 62443-4-1 értékes keretet biztosít az ipari vezérlőrendszerek auditjainak elvégzéséhez, strukturált megközelítést kínálva a szervezeteknek a kiberbiztonság értékeléséhez és a kockázatkezeléshez. E szabvány betartásával a vállalkozások azonosíthatják a sebezhetőségeket, fenntarthatják a megfelelőséget, fokozhatják az ellenálló képességet, és bizalmat építhetnek az érdekelt felekkel. Az IEC 62443-4-1 alapján végzett rendszeres auditok végrehajtása proaktív lépés a kritikus infrastruktúrák védelme és az ipari ágazatban a kiberbiztonsági fenyegetések folyamatosan változó környezetében való előretörés felé.

Vegye fel a kapcsolatot egy olyan tanúsító szervezettel, amelyben megbízik. Az akkreditáció mindig garanciát jelent a felkészültségre. A TAM CERT akkreditált kiberbiztonsági tanúsító szervezet, az akkreditációról szóló kijelölést innen éri el:

https://nah.gov.hu/admin/staticmedia/Reszletezo_okiratok/RO4-NAH-6-0070-2023-B1-IG-11756640_a.pdf

Vegye fel velünk a kapcsolatot!

Kiss Tibor

Kiberbiztonsági Tanúsítóhely vezető

+36 30 5150840

kiss.tibor@tamcert.hu

www.tamcert.hu