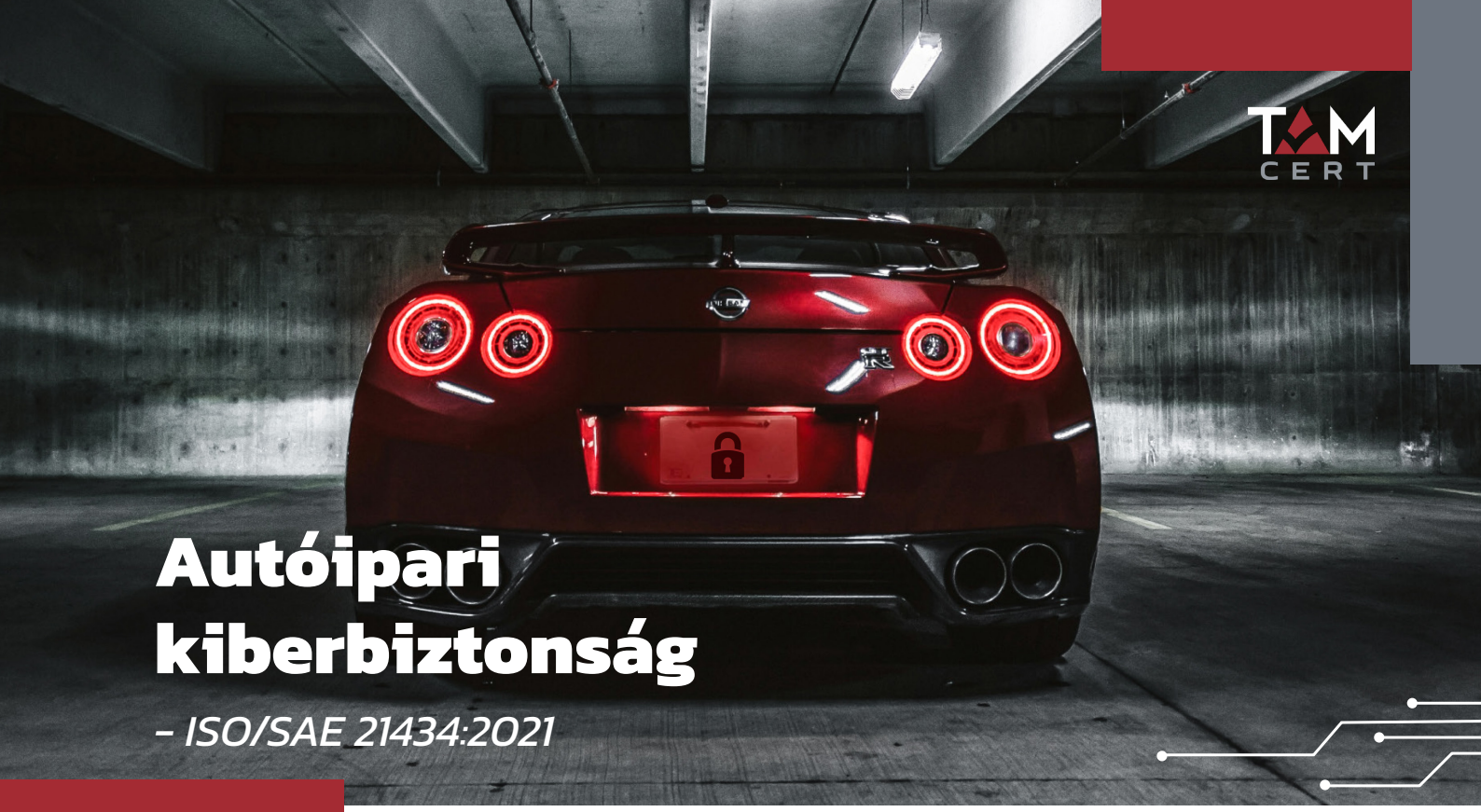

Autóipari kiberbiztonság

– ISO/SAE 21434:2021

A kiberbiztonsági törvény

A kiberbiztonsági törvény (pontosabban az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról) létrehozza a termékek és szolgáltatások kiberbiztonsági tanúsítási keretrendszerét. A törvény az egész EU-ra kiterjedő kiberbiztonsági tanúsítási keretrendszert vezet be az ICT-termékek (information and communitacions technologies), -szolgáltatások és -folyamatok számára. A tanúsítás kulcsfontosságú szerepet játszik a digitális világ számára fontos termékekbe és szolgáltatásokba vetett bizalom és biztonság növelésében.

Jelenleg az EU-ban és világviszonylatban számos különböző biztonsági tanúsítási rendszer létezik az ICT-termékekre vonatkozóan. A vonatkozó tanúsítási keretrendszer az egész EU-ra kiterjedő tanúsítási rendszereket fog biztosítani, mint átfogó szabályrendszert, műszaki követelményeket, szabványokat és eljárásokat. A keret egy adott ICT-alapú termék vagy szolgáltatás biztonsági tulajdonságainak értékeléséről szóló, nemzetközi megállapodáson fog alapulni, és tanúsítja, hogy az ilyen rendszerrel összhangban tanúsított ICT-termékek és -szolgáltatások megfelelnek a meghatározott követelményeknek.

Autóipar

A kiberbiztonsági törvény önmagában nem fogalmaz meg semmilyen közvetlen piaci követelményt. Az autóipar számára jelentős kiberbiztonsági kihívást jelent az UNECE WP29 rendelete. Ez egy megelőző intézkedés a jelentős kiberbiztonsági kockázatokra. A hackerek igyekeznek hozzáférni az elektronikus rendszerekhez és adatokhoz, veszélyeztetve a járműbiztonságot és a fogyasztók magánéletét.

A WP29 két új ENSZ-rendeletet vezet be a kiberbiztonságról és a 2021 januárjában hatályba lépett szoftverfrissítésről, amely négy különböző szakterület végrehajtását írja elő:

- A járművekkel kapcsolatos kiberkockázatok kezelése
- A járművek tervezési biztonsága a kockázatok csökkentése érdekében az értéklánc mentén.
- A biztonsági incidensek felderítése és az azokra való reagálás a járműparkban
- Biztonságos és biztonságos szoftverfrissítések biztosítása és annak biztosítása, hogy a járművek biztonsága ne sérüljön, jogalapot teremtve a fedélzeti szoftverek úgynevezett „Over – the – Air" (O.T.A.) frissítésére.

Az UN R155. és 156. számú rendeletek célja, hogy szabályozzák az autóipari szereplők kiberbiztonságát.

- UN R155: Kiberbiztonsági irányítási rendszer (CSMS) kialakítása és működtetése szervezeti szinten.
- UN R156: Szervezeti szintű Szoftverfrissítési irányítási rendszer (SUMS) kialakítása és működtetése.

Az autógyártók felelőssége, hogy megfeleljenek a jogi követelményeknek és biztosítsák a teljes ellátási láncuk kiberbiztonságát. Hatályos az EU-ban 2022. július 6-tól az új típusokra és 2024 júliusától minden újonnan gyártott járműre. (Japán és Dél-Korea hasonló ütemezést követ.)

Autóipari kiberbiztonság

Az autóipari kiberbiztonság kihívást jelent az autógyártók számára. Minden további kommunikációs interfész és alkatrész potenciális sebezhetőséget jelenthet a kiberbűnözők számára. A manipulációs lehetőségek gyorsan növekednek, különösen az önvezető járművek vagy az elektronikusan vezérelt vezetési és fékezési funkciók tekintetében.

Az ENSZ két új rendeletet hozott létre a gépjárművek kiberbiztonságának alapvető kereteinek meghatározására. Ezek közé tartozik az UNECE kiberbiztonsági (UN R 155) rendelet, amely közvetlenül hivatkozik az új ISO/SAE 21434 szabványra, valamint az UNECE szoftverfrissítési (UN R 156) rendelet. Az új járműtípusokra vonatkozó előírások az EU-ban 2022 júliusában léptek hatályba. Az autóiparnak tehát komoly kihívásokkal kell szembenéznie.

Az autóipari kiberbiztonság jelentősége

Míg az ISO/IEC 27001 nemzetközi szabvány az információbiztonság általános megközelítését jelenti, az autóipari kiberbiztonság fogalma az autóiparban a digitális rendszerek biztonságára utal. Járműveink egyre inkább támaszkodnak a hálózatba kapcsolt elektronikus rendszerekre és szoftveralkalmazásokra. Ennek eredményeként ezeknek a komponenseknek a védelme és biztonsága egyre nagyobb hangsúlyt kap – az egész iparágban. Ez a folyamat a járműgyártóknál kezdődik, majd a beszállítók és a mérnöki szolgáltatók is bekapcsolódnak, és magában foglalja a szoftver- és ICT-infrastruktúra-szolgáltatókat is.

Áttekintés: ISO 21434

Az ISO/SAE 21434 a WP29 jogi követelményeinek való megfelelés érdekében szabványba épített követelmények részletes listája. Ez a CSMS és a SUMS kialakítására és működtetésére vonatkozó specifikus műszaki követelmények, feladatok, termék-tervezési előírások leírása. Az ISO/SAE 21434 egy egyedi megfelelőségértékelési követelményeket rögzítő szabvány, amely megköveteli egy minőségirányítási rendszer működtetését, ezért átfedések vannak az IATF 16949 és az ISO 9001 megfeleléssel. Az ISO/SAE 21434 szabvány a kiberbiztonsági irányítás következő szempontjairól rendelkezik:

- Általános | A kiberbiztonsági tevékenységek irányítása
- Projektfüggő | A kiberbiztonsági tevékenységek tervezése és végrehajtása a felelősségi körökkel együtt.
- Folyamatos | Állandó kiberbiztonsági tevékenységek (monitoring, sebezhetőségi elemzés stb.)
- Kockázatértékelési módszerek | Kockázatértékelés
- Biztonság a tervezés során | Kiberbiztonsági tevékenységek a tervezés, fejlesztés, gyártás és üzemeltetés során
- Elosztva | A kiberbiztonság biztosítása az ellátási láncban (a beszállítók ellenőrzése).

Az autógyártók felelőssége, hogy biztosítsák a WP 29 jogi követelményeinek való megfelelést. Az UN R 155 rendelet közvetlen hivatkozása az ISO/SAE 21434 szabványra, mint az ezen előírás szerinti megfelelőségértékelés lehetőségére azt jelenti, hogy az ISO/SAE 21434 tanúsítvánnyal rendelkező szállítók/alkatrészgyártók a vonatkozó jogszerű működés igazolásában előnyben részesülnek. Ha egy alkatrészgyártó/szállító rendelkezik tanúsítvánnyal, a gépjárműgyártó elfogadhatja a beszállító és a szállított termék megfelelőségét, ami ösztönző szempont a beszállítói lánc számára, hogy a kiberbiztonsági követelményeket saját maga is teljesítse.

Tanúsítás az ISO 21434 szerint:

Az ISO/SAE 21434:2021 „Road vehicles – Cybersecurity engineering" az autóiparban alkalmazandó követelményeket és iránymutatásokat tartalmazza a járművek kiberbiztonságának terén.
A szabvány célja az autóipari vállalatoknak iránymutatást nyújtani a járművek kiberbiztonságának **értékeléséhez, tervezéséhez, fejlesztéséhez és teszteléséhez.**

Az ISO/SAE 21434 szerinti tanúsítás folyamata egy vállalatnál általában a következő lépéseket tartalmazza:

Gap elemzés:
A vállalat azonosítja jelenlegi kiberbiztonsági gyakorlatait és folyamatait, majd összehasonlítja azokat az ISO/SAE 21434 előírásaival. Ez segít azonosítani azokat az esetleges hiányosságokat, amelyeket meg kell oldani a tanúsítás előtt.

Képzés és tájékoztatás:
A dolgozók képzést és tájékoztató programokat kapnak annak érdekében, hogy megértsék az ISO/SAE 21434 fontosságát és követelményeit. Ez biztosítja, hogy mindenki a vállalatnál tisztában legyen a kiberbiztonsági intézkedésekkel.

Implementáció:
A vállalat megkezdi a szükséges kiberbiztonsági intézkedések és gyakorlatok bevezetését az ISO/SAE 21434 irányelvei alapján. Ez lehetővé teszi a kiberbiztonsági eszközök telepítését, a szoftverek frissítését és az incidenskezelési tervek kialakítását.

Dokumentáció:
Készül egy részletes dokumentáció az összes kiberbiztonsági folyamatról és intézkedésről, amit a tanúsítási audit során felülvizsgálnak.

Belső audit:
A vállalat belső auditot végez annak érdekében, hogy értékelje a kiberbiztonsági intézkedések hatékonyságát és az ISO/SAE 21434-re való megfelelést.

Előzetes értékelés:
Az előzetes értékelés célja az, hogy felmérje a szervezet felkészültségét a hivatalos tanúsítási auditra. Az előzetes értékelés során azonosított problémákat megoldják.

Tanúsítási audit:
Az akkreditált Tanúsító szervezet végzi el a hivatalos tanúsítási auditot. Az auditor felülvizsgálja a vállalat dokumentációját, folyamatait és gyakorlatait annak érdekében, hogy ellenőrizze az ISO/SAE 21434-el való megfelelést.

Korrekciós intézkedések:
Ha az audit során nem megfelelőségek merülnek fel, a vállalatnak korrekciós intézkedéseket kell tennie azok kezelésére.

Akkreditált Tanúsítvány:
Ha a vállalat teljesíti az ISO/SAE 21434 követelményeit, akkor megkapja az Akkreditált Tanúsítványt. A Tanúsítvány érvényessége 3 éves időtartamra szól, és rendszeres (éves) felügyeleti auditok kerülnek végrehajtásra annak érdekében, hogy a folyamatos megfelelést az Akkreditált Tanúsítóhely ellenőrizze és igazolja.

Milyen előnyökhöz jut az így tanúsított vállalat?

Fokozott kiberbiztonság:
A tanúsított vállalat magasabb szintű kiberbiztonsági intézkedéseket valósít meg, csökkentve ezzel a kibertámadások és adatvédelmi incidencek kockázatát.

Megfelelés az iparági szabványoknak:
A vállalat az ISO/SAE 21434 előírásainak való megfeleléssel azt mutatja, hogy elkötelezett a járműiparra vonatkozó nemzetközi kiberbiztonsági szabványok betartása mellett.

Növelt ügyfélbizalom:
Az ISO/SAE 21434 tanúsítvány megerősíti az ügyfelekben a bizalmat a vállalat termékeivel és szolgáltatásaival szemben, mivel tudják, hogy adataik és biztonságuk védelme érvényesül.

Versenyelőny:
Az ISO 21434 tanúsítás révén a vállalat előnyt szerez a versenytársakkal szemben, ami a piaci versenyben kiemelt helyzetet biztosít.

Új üzleti lehetőségek:
Számos ügyfél és partner követeli az ISO 21434 tanúsítást az együttműködés feltételeként, így új üzleti lehetőségek nyílnak meg a vállalat számára.

Jobb kockázatkezelés:
A tanúsított vállalat jobban képes azonosítani és kezelni a kiberbiztonsági kockázatokat, ezáltal erősebb kockázatkezelési keretet alakít ki.

Fejlettebb incidenskezelés:
Az ISO/SAE 21434 megfelelés révén a vállalat hatékony incidenskezelési terveket fejleszt ki, csökkentve a kiberincidensek potenciális hatásait.

Költségmegtakarítás:
Egy erős kiberbiztonsági alap lehetőséget teremt költségmegtakarításra, mivel megakadályozza a drága kiberincidenseket és károkat.

Iparágbeli elismerés:
Az ISO/SAE 21434 szabvány szerinti tanúsítás egyetemlegesen ismert az iparág szereplői között, és annak akkreditált tanúsítása nemzetközileg elfogadott és elismert nívót jelent, tovább erősítve a vállalat hírnevét a járműiparban.

Folyamatos fejlesztés:
A tanúsítási folyamat ösztönzi a kiberbiztonsági gyakorlatok folyamatos értékelését és fejlesztését, biztosítva, hogy a vállalat mindig naprakész legyen a kiberbiztonsági előrelépések terén.

Az ISO/SAE 21434 szabvány (ISO/SAE 21434:2021) nem kötelező érvényű szabvány, hanem egy ajánlás és iránymutatás az autóipari vállalatok számára a járművek kiberbiztonságával kapcsolatban. Az autóipari beszállítók és partnerek is egyre inkább elvárják a kiberbiztonsági szabványok betartását a vállalatoktól, mivel ezek bizonyítják az adott vállalat komoly elkötelezettségét a kiberbiztonság terén. Az autóiparban a kiberbiztonság egyre nagyobb jelentőséggel bír, mivel a járművek egyre összetettebbek és összekapcsoltabbak lesznek, és a kibertámadások kockázata növekszik. A szabvány betartása előnyöket nyújthat a biztonság, a megbízhatóság, a versenyképesség és a piaci pozíció szempontjából.

Kapcsolódó szolgáltatások:

A GDPR (General Data Protection Regulation) az Európai Unió által bevezetett adatvédelmi rendelet, amely szabályozza a személyes adatok kezelését és védelmét. Az ISO/IEC 27001 egy nemzetközi szabvány, amely az információvédelmi rendszerek követelményeit tartalmazza. Az ISO/SAE 21434 pedig az autóiparban alkalmazott biztonsági és adatvédelmi szabvány, amely a járművek kiberbiztonságára és adatvédelmére vonatkozik.

Az összefüggés ezek között a szabványok között az adatvédelem és a kiberbiztonság területén található. A GDPR és az ISO/IEC 27001 célja az adatok védelmének biztosítása, míg az ISO/SAE 21434 kifejezetten az autóiparban alkalmazott kiberbiztonsági és adatvédelmi intézkedésekre fókuszál. Az autóiparban a járművekben tárolt és feldolgozott adatokra vonatkozóan mind a GDPR, mind az ISO/IEC 27001 irányelvei alkalmazhatóak. Az ISO/SAE 21434-es szabvány segít a járműgyártóknak és a szállítóknak biztosítani, hogy a járművek megfeleljenek az adatvédelem és a kiberbiztonság szigorú követelményeinek.

https://nah.gov.hu/admin/staticmedia/Reszletezo_okiratok/RO1-230601-6-0070-IG-11756640_a.pdf

Vegye fel a kapcsolatot egy olyan akkreditált tanúsító szervezettel, amelyben megbízik. Az akkreditáció mindig garanciát jelent a megfelelőségértékelő szervezet felkészültségre, függetlenségére és nemzetközi elismertségére.
A TAM CERT Kiberbiztonsági Tanúsítóhelye a NAH által NAH-6-0070/2023 számon akkreditált terméktanúsító szervezet, továbbá – a tárgyi akkreditáció területére tekintettel – a NAH az EA MLA aláírója a vizsgálat, kalibrálás, jártasságvizsgálat, ellenőrzés, terméktanúsítás, irányítási rendszer tanúsítás, személytanúsítás és hitelesítés területén.

TAM CERT

A TAM CERT Kiberbiztonsági Tanúsítóhely tárgyi Akkreditálási Okiratának érvényességi területét rögzítő Részletező Okirata a következő hivatalos címen érhető el:

https://nah.gov.hu/admin/staticmedia/Reszletezo_okiratok/RO1-230601-6-0070-IG-11756640_a.pdf.

Vegye fel velünk a kapcsolatot!

Kiss Tibor

Kiberbiztonsági Tanúsítóhely vezető

mobil: +36 30 5150840

Email: kiss.tibor@tamcert.hu

Egyéb kapcsolódó szolgáltatások:

Adatvédelmi (GDPR) audit és megfelelőség az Europrivacy séma alapján

Ipari vezérlőrendszerek biztonsága – IEC 62443-4-1