

A JÁRMŰVEK KIBERBIZTONSÁGI MEGFELELŐSÉGE

MEGBÍZHATÓSÁG A DIGITÁLIS KORSZAKBAN



DR. PETHŐ ZSOMBOR

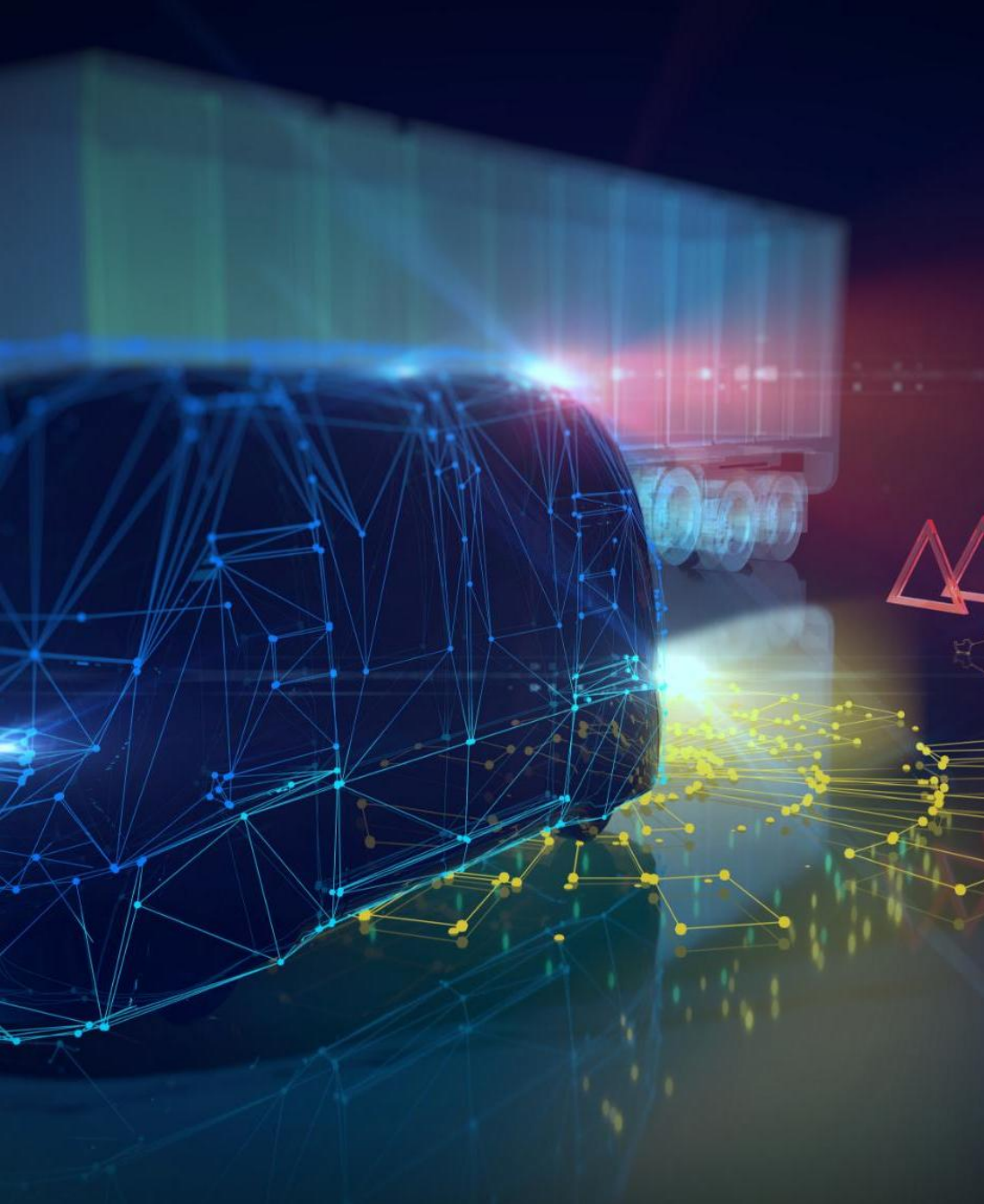
BME KJK - GÉPJÁRMŰTECHNOLÓGIA TANSZÉK



BME
Gépjárműtechnológia
Tanszék



BEVEZETÉS



Miért fontos a kiberbiztonság az autóiparban?

A modern járművek belső rendszere

A mai járművek négy keréken futó **számítógépes hálózatokat** tartalmaznak, **komplex belső információcserével** és folyamatokkal.

A hálózatba kapcsolt járművek térnyerése

Az intelligens járművek és az IoT-eszközök új lehetőségeket és kiberbiztonsági fenyegetéseket hoznak az autóiparban.

A távoli hozzáférés kockázatai

A hackerek távolról is hozzáférhetnek a járművek rendszereihez, ami adatlopás és közlekedésbiztonsági kockázatokat jelent.

Biztonsági és jogi kihívások

A kiberbiztonság hatással van a járművek megbízhatóságára és a közlekedés biztonságára, ami jogi és biztonsági aggályokat vet fel.

JOGI ÉS SZABÁLYOZÁSI HÁTTÉR



Nemzetközi és európai szabályozások

UNECE WP.29 R155 (ENSZ EGB előírás)

Bevezeti az autógyártók számára kötelező **kiberbiztonsági irányítási rendszert (CSMS)** a kiberkockázatok kezelésére.

ISO/SAE 21434 szabvány

Részletes iránymutatásokat tartalmaz a kiberbiztonsági mérnöki munkához, beleértve a kockázatelemzést és az életciklus-kezelést a járművekben

Kapcsolódó biztonsági és védelmi szabványok

Az **ISO 26262** és **ISO 27001** szabványok kiegészítik a kiberbiztonsági előírásokat, és a **funkcionális és információbiztonságra** összpontosítanak.

EU-megfelelési követelmények

2022 és 2024 óta az EU előírja az új járműmodellek megfelelőségének igazolását a kiberbiztonsági szabványok biztosítása érdekében.

A KIBERBIZTONSÁGI MEGFELELÉS FOGALMA

Megfelelőségi és tanúsítási folyamat

Megfelelőségi igazolás

A gyártóknak és beszállítóknak igazolniuk kell, hogy rendszereik megfelelnek a vonatkozó kiberbiztonsági szabványoknak és előírásoknak.

Tanúsítási értékelés

A tanúsítási folyamat során egy független harmadik fél értékeli a kiberbiztonsági intézkedéseket, hogy biztosítsa a pártatlan értékelést.

Életciklus-megfelelőségi menedzsment

A megfelelőség a rendszer teljes életciklusára kiterjed, beleértve a frissítéseket, az incidensek kezelését és a folyamatos figyelemmel kísérést.

CSMS keretrendszer szerepe

A kiberbiztonsági menedzsment rendszer keretrendszere támogatja az autóiipari kiberbiztonság folyamatos karbantartását és fenntarthatóságát.



KOCKÁZATELEMZÉS ÉS BIZTONSÁGI INTÉZKEDÉSEK

Kockázatelemzés és biztonsági intézkedések

Kockázatelemzés

A potenciális fenyegetések azonosítása és hatásuk értékelése a hatékony kiberbiztonsági megfelelés biztosítása érdekében.

Security by Design

A fejlesztés során integrálni kell a biztonsági intézkedéseket, hogy eredendően ellenálló rendszereket hozzunk létre.

Incidenskezelés és -figyelés

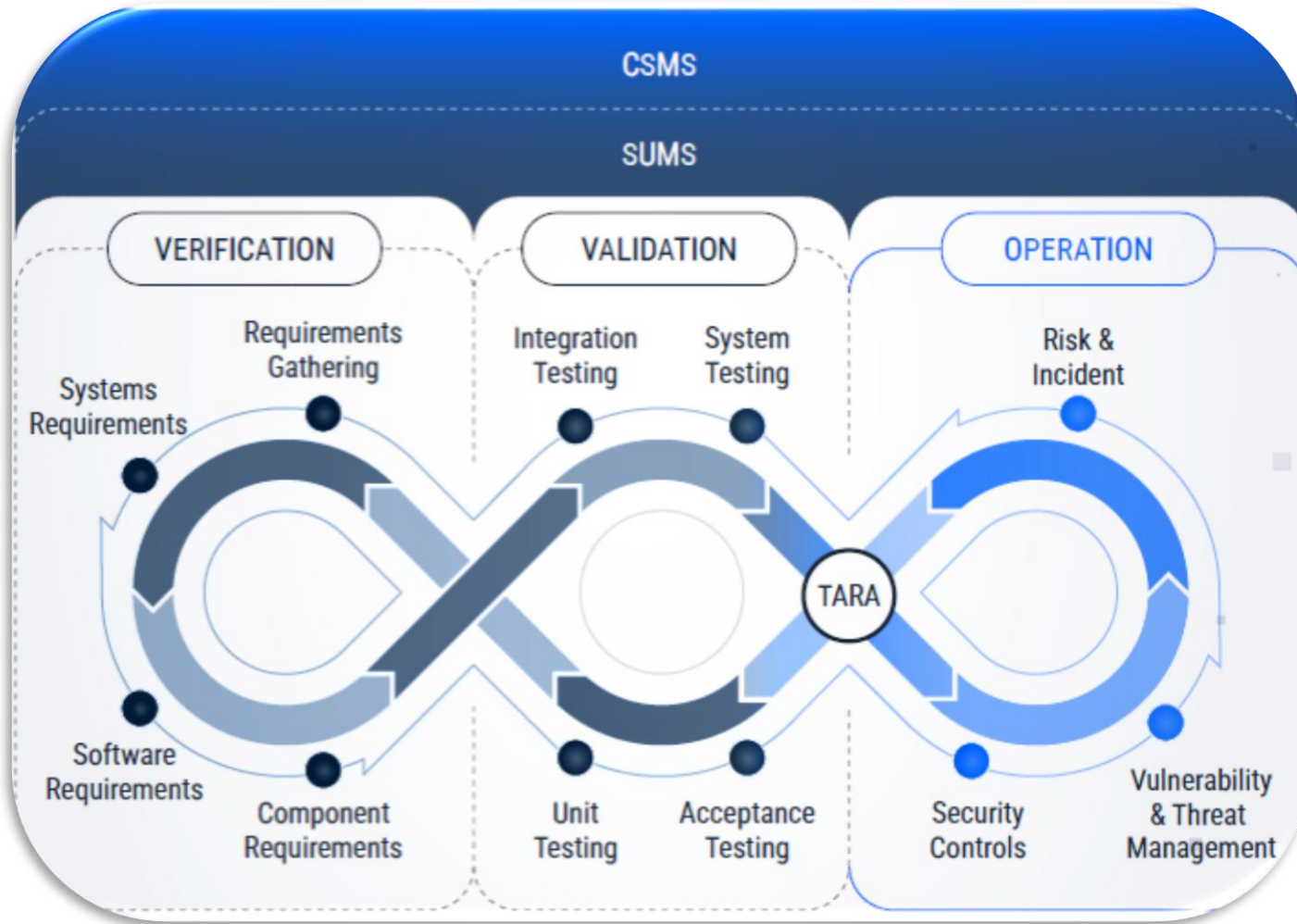
Incidenskezelés megvalósítása, folyamatos monitorozás és OTA-frissítések kezelése a gyors reagálás és a tartós biztonság érdekében.

Ellátási lánc biztonsága

Alkalmazni kell kiberbiztonsági kontrollokat az ellátási láncban a járműrendszer teljes biztonságának védelme érdekében.



Kiberbiztonsági menedzsment rendszer (CSMS)



Verifikáció: A követelmények gyűjtésétől a szoftver- és komponenskövetelményekig tartó szakasz.

Validáció: A szoftver tesztelését és a rendszer validálását foglalja magában, beleértve az egység-, integrációs, rendszer- és elfogadási teszteket.

Működés: A biztonsági ellenőrzéseket, a sebezhetőségi és fenyegetéskezelést, valamint a kockázatok és incidensek kezelését tartalmazza (TARA).

CSMS: Cybersecurity Management System (**R155**)

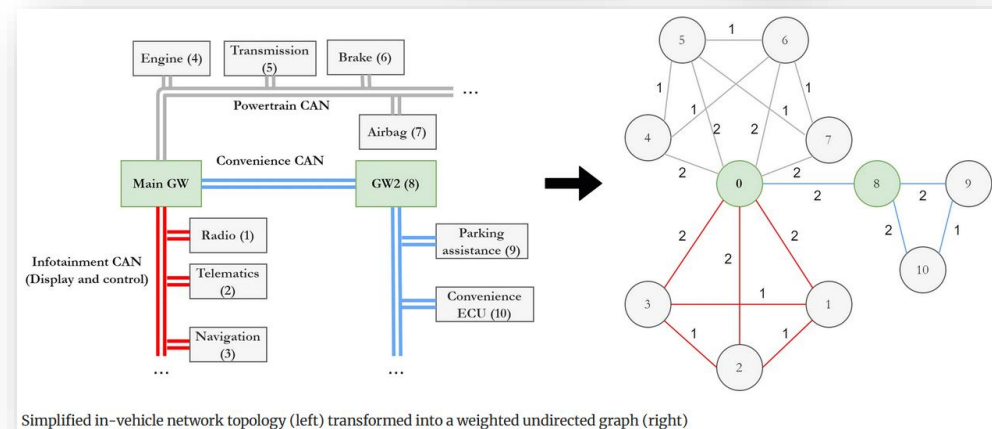
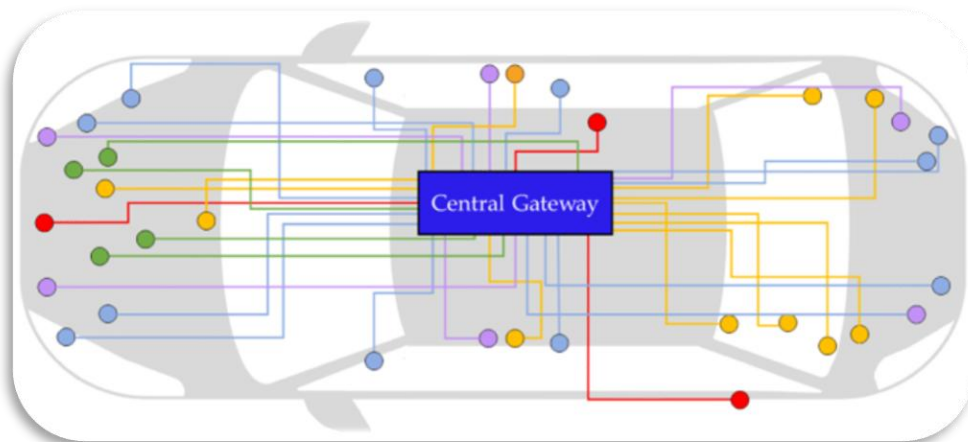
SUMS: SW Update Management System (**R156**)

Kutatás és innováció szerepe az autóiipari kiberbiztonságban

A járművek belső rendszerei ma már összetett, hálózatba kötött szoftverek. Ezért, hogy biztonságosak maradjanak, **folyamatos kutatásra és innovatív tesztelési módszerekre** van szükség.

Az olyan megoldások, mint a „**smart fuzzing**”, lehetővé teszik, hogy

- ✓ **automatikusan felismerjük a sérülékenységeket,**
- ✓ **valós támadási mintákat szimuláljunk,**
- ✓ **és megelőzzük a biztonsági incidenseket** már a fejlesztés korai szakaszában.



Simplified in-vehicle network topology (left) transformed into a weighted undirected graph (right)

TANÚSÍTÁS ÉS AUDITÁLÁS

Auditfolyamat és dokumentáció

Tanúsítás és megfelelőség-ellenőrzés

A tanúsító szervezetek részletes auditokkal ellenőrzik, hogy a gyártók megfelelnek-e a kiberbiztonsági követelményeknek.

Audit folyamat lépései

Az audit magában foglalja az előzetes értékelést, a helyszíni vizsgálatot, a dokumentáció felülvizsgálatát és a tanúsítvány kiadását.

Dokumentációs követelmények

A **CSMS** és **TARA*** dokumentumok benyújtása elengedhetetlen az alapos kockázatértékeléshez és az audithoz.

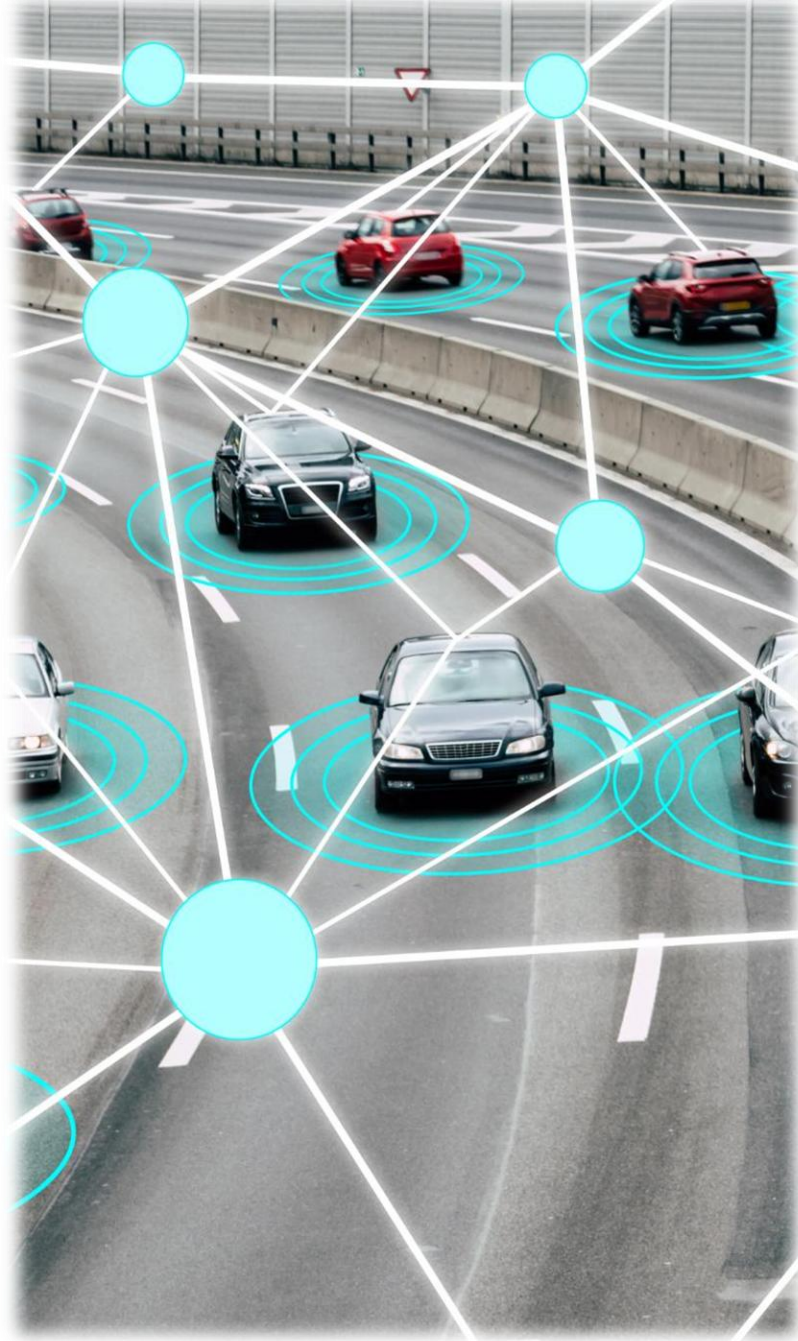
Tanúsítási szintek és bizalom

A tanúsítási szintek a megfelelés mélységét tükrözik, és a jogi kötelezettségeken túl a piaci bizalom megalapozását is szolgálják.

***TARA** – Threat **A**nalysis and **R**isk **A**ssessment



KIHÍVÁSOK ÉS TRENDEK



Technológiai és szervezeti kihívások

Fenyegetési környezet változása

Az új támadási módszerek gyors megjelenése alkalmazkodó és rugalmas kiberbiztonsági védekezést igényel.

Jármű-életciklus vs. szoftverfrissítések

A hosszú jármű-életciklus és a gyors szoftverfrissítési ciklusok ütközése megnehezíti a folyamatos biztonságmenedzsmentet.

Ellátási lánc komplexitása

A több beszállító biztonsági szintje kritikus hatással van a teljes rendszer kiberbiztonsági ellenállóképességére.

Új kockázatok hálózatba kapcsolt és autonóm járművek esetén

Az autonóm járművek az 5G/V2X valós idejű adatcserét és távoli hozzáférést tesznek lehetővé, új kiberbiztonsági kockázatokat jelentve.

Jövőbeli kihívások

A jogi megfelelés fontossága

Az **EU-s** és **nemzetközi kiberbiztonsági előírásoknak való megfelelés kötelező**, és piaci előnyt is biztosít.

Jövőbeli biztonsági technológiák

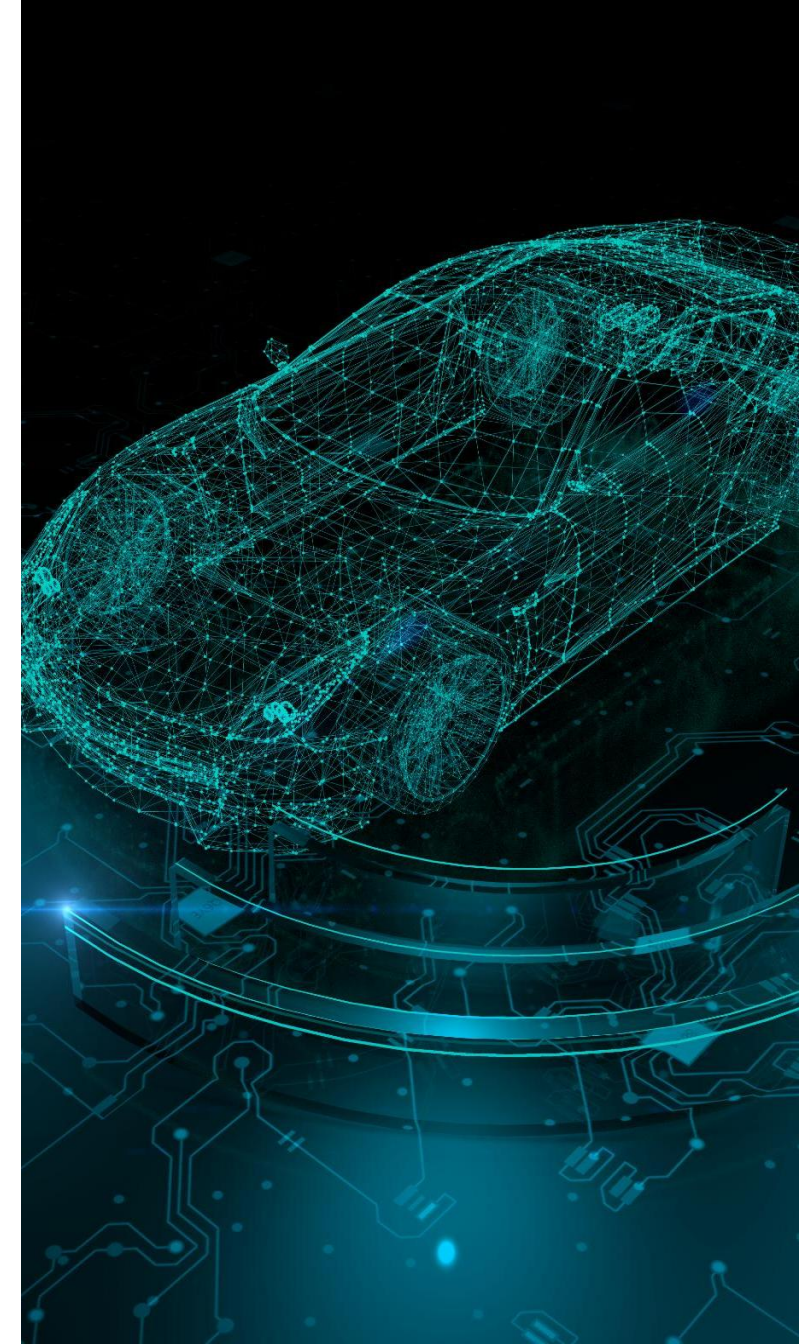
A folyamatos frissítések, az automatizált védelem és a mesterséges intelligencián alapuló biztonsági rendszerek formálják a járműipari kiberbiztonságot.

Folyamatos életciklus-folyamat

A kiberbiztonsági megfelelés biztosítása a jármű teljes életciklusa során folyamatos feladat.

A K+F+I szerepe

A **kutatás-fejlesztés és innováció létfontosságú** a járművek biztonságának megőrzéséhez a digitális korszakban.





**KÖSZÖNÖM A
FIGYELMET!**