

Industrial Cybersecurity for Automotive Components: Risk Assessment and Defense Mechanisms

Conf.dr.ing. Muguraș Mocofan

muguras.mocofan@upt.ro

Universitatea Politehnica Timișoara

Piața Victoriei no. 2
RO 300006 - Timisoara
Tel: +40 256 403000
Fax: +40 256 403021
rector@upt.ro
www.upt.ro

ETcTI

Centrul MULTIMEDIA

Centrul ID/IFR și e-Learning

Major differences between TISAX and ISO 27001

	TISAX	ISO 27001
Scope	Automotive industry-specific	Applies to any industry or business type
Requirements	Requirements include 3 closed criteria catalogs for information security, prototype protection, and data protection	Requirements cover a broad range of security issues in an open, adaptable catalog
Certification levels	3 levels based on process maturity and level of security required	1 certification level, either compliant or non-compliant
Frequency of changes	Standard reviewed annually by the governing body	Standard reviewed every five years by the governing body

Universitatea Politehnica Timişoara



Zero Trust Architecture / Zero Trust Security

VULNERABILITIES



THREAT ACTORS AND MOTIVATIONS




PHISHING SCAM
MALWARE DISTRIBUTION
MALWARE DISTRIBUTION
DATA THEFT

Universitatea Politehnica Timișoara





“How the CEO thinks the Cybersecurity department is!”



Who do we really rely on?
Generally, there is a **smart guy** in every factory!



AUTOMOTIVE DATA ECOYSTEM



LOGGING



TELEMETRY



FORENSICS

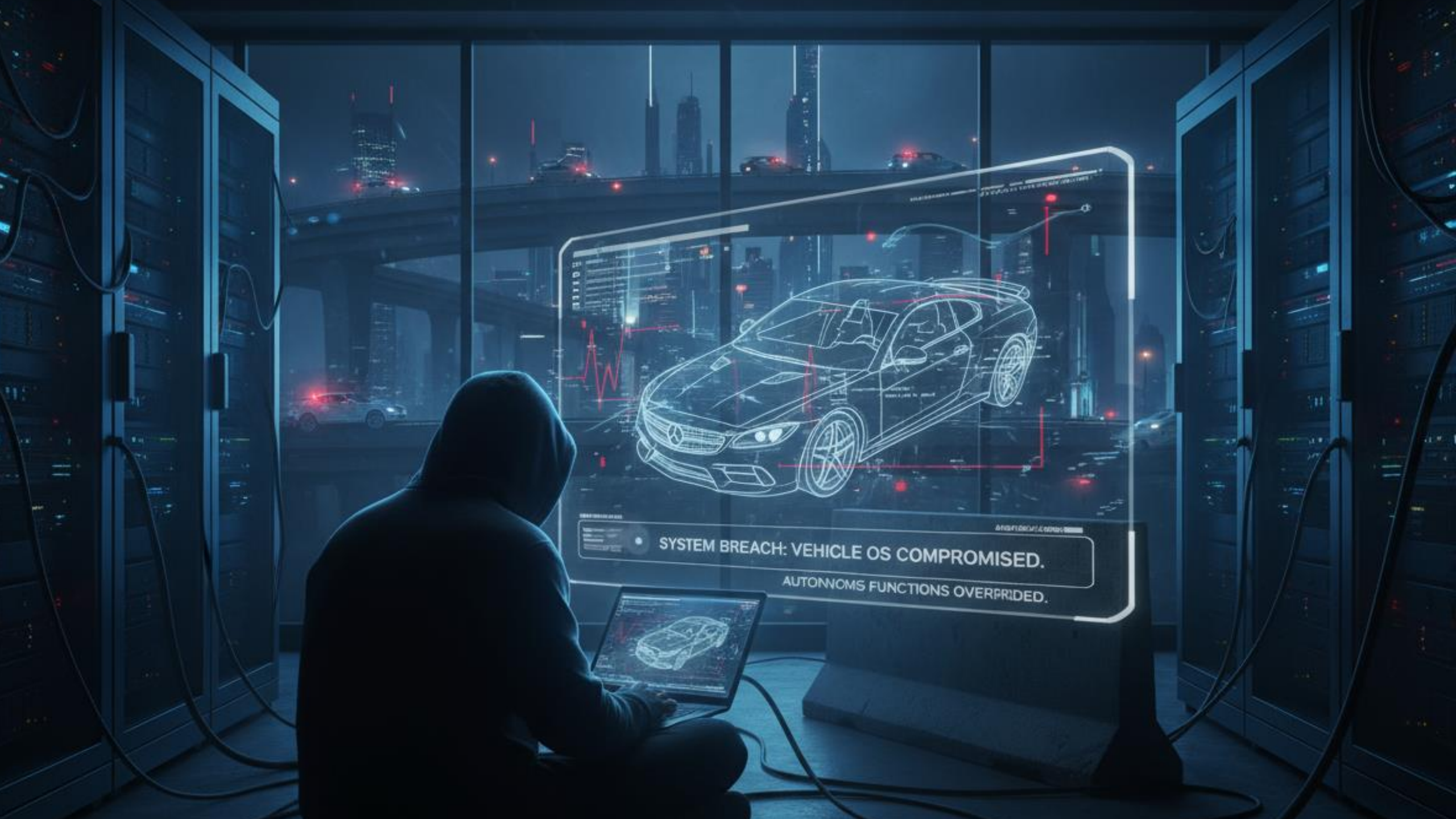


Automotive Cybersecurity Attacks

(2010–2025)

notable incidents that shaped the industry

Generated 2025-10-28


SYSTEM BREACH: VEHICLE OS COMPROMISED.
AUTONOMS FUNCTIONS OVERRIDED.

Part I — Vehicle & Service Security Incidents



Real-world attacks and research demos impacting vehicle functions, data, or connected services.

Generated 2025-10-28

2010 — Experimental Security Analysis of a Modern Automobile

- Brands: **Academic research -** University of Washington (UW) and University of California, San Diego (UCSD)
  - *Scope/scale*: Two late-model vehicles (same make/model)
  - *Attack vector*: In-vehicle networks; remote & physical vectors
  - *Effect*: Demonstrated remote/physical control pathways
  - *Financial/operational impact*: N/A (research demo)
  - *Response & fixes*: Foundational study; **influenced industry standards**

2011 — Comprehensive Experimental Analyses of Automotive Attack Surfaces

- Brands: **Academic research -** University of California, San Diego (UCSD) and University of Washington (UW)
  - *Scope/scale*: Systematic mapping of external attack surface
  - *Attack vector*: Cellular, Bluetooth, CD player, tire sensors, OBD-II
  - *Effect*: Showed feasibility of long-range control & tracking
  - *Financial/operational impact*: N/A (research demo)
  - *Response & fixes*: Underpinned later OEM cybersecurity programs

2015 — BMW ConnectedDrive Remote Unlock Vulnerability

- Brands: **BMW/MINI/Rolls-Royce** (~**2.2M vehicles**)
  - *Scope/scale*: Affected ConnectedDrive telematics; OTA fix deployed
  - *Attack vector*: Fake GSM base station impersonated backend; missing HTTPS in specific paths
  - *Effect*: Potential remote door unlock; no engine start
  - *Financial/operational impact*: No public cost; reputational impact; OTA infra investment
  - *Response & fixes*: ADAC disclosure; patch closed HTTP endpoints and enforced TLS

2015 — Jeep Cherokee Uconnect Remote Takeover

- Brands: **FCA (Jeep/Dodge/Chrysler/Ram)**
  - *Scope/scale*: **~1.4 million** vehicles recalled
  - *Attack vector*: Cellular-connected Uconnect head unit RCE → pivot to CAN bus
  - *Effect*: Remote control of steering, brakes, transmission; tracking via GPS
  - *Financial/operational impact*: Recall service costs undisclosed; class action filed; significant remediation + network filtering with carrier
  - *Response & fixes*: Patched via mailed USB & dealer updates; NHTSA pressure accelerated recall

Jeep®

2015 — Corvette Brakes via OBD-II Dongle (SMS)

- Brands: **Aftermarket** (Mobile Devices/Metromile), 2013 **Corvette** demo
  - *Scope/scale*: OBD-II insurance/fleet dongles widely deployed
  - *Attack vector*: SMS commands to telematics dongle w/ insecure config
  - *Effect*: Remote wipers; low-speed brake control; DoS potential
  - *Financial/operational impact*: Vendors issued patches; potential liability for fleets/insurers
  - *Response & fixes*: Highlights risk from third-party dongles attached to CAN



2015 — **GM OnStar** / Mobile Apps MITM

- Brands: **GM OnStar**; similar patterns in other OEM apps
  - *Scope/scale*: Millions of app users at risk pre-patch
  - *Attack vector*: Rogue Wi-Fi AP → app MITM (Man-in-the-Middle) token capture
  - *Effect*: Locate/unlock/start; account takeover
  - *Financial/operational impact*: Unstated; app and backend updates deployed
  - *Response & fixes*: Catalyzed broader app security hardening across OEMs

2016 — **Nissan** LEAF App/API Exposure

LOGO: Nissan LEAF

- Brands: **Nissan LEAF** (gen-1)
  - *Scope/scale*: Global app temporarily disabled; VIN-based unauth calls
  - *Attack vector*: Unauthenticated telematics APIs tied to visible VIN
  - *Effect*: Remote climate control; access trip/energy history
  - *Financial/operational impact*: Unstated; customer data exposure concerns
  - *Response & fixes*: Service disabled then re-launched with auth fixes



2016 — Tesla Model S Remote Hack
(Keen Security Lab)

- Brands: **Tesla**
  - *Scope/scale*: Multiple chained vulns; patched OTA rapidly
  - *Attack vector*: Browser/Wi-Fi/cellular → ECU CAN injection
  - *Effect*: Remote control incl. brakes; demo under controlled conditions
  - *Financial/operational impact*: No reported financial loss; strengthened code signing/SDLC
  - *Response & fixes*: Tesla's OTA agility showcased; coordinated disclosure



TESLA

2016 — Keyless Entry Crypto Weaknesses

- Brands: **VW Group** & others (~100M vehicles impacted historically)
  - *Scope/scale*: Keyfob crypto & HiTag2 weaknesses demonstrated (48 b)
  - *Attack vector*: Capture rolling codes & shared keys; crack to clone fobs
  - *Effect*: Unlock vehicle; some immobilizer bypass scenarios
  - *Financial/operational impact*: Theft risk increase; retrofit/recall not feasible at scale
  - *Response & fixes*: Spurred migration to stronger crypto and UWB distance-bounding



2019 — Tesla Model 3 Pwn2Own

- Brands: **Tesla Model 3** (Pwn2Own target)
  - *Scope/scale*: Browser exploit chain; car awarded to winners
  - *Attack vector*: Infotainment browser exploit; sandbox escape
  - *Effect*: Control of infotainment; patched quickly
  - *Financial/operational impact*: **Prize $35k + Model 3 awarded**; no fleet risk post-patch
  - *Response & fixes*: Automotive category debut raised bar for coordinated research



2019 — Toyota Data Breaches in APAC & Japan

- Brands: **Toyota & Lexus** sales subsidiaries (Japan/APAC)
  - *Scope/scale*: Up to 3.1M customers affected (Japan)
  - *Attack vector*: Network intrusions at subsidiaries/dealers
  - *Effect*: Personal data exposure; no payment data confirmed
  - *Financial/operational impact*: Notification & monitoring costs; reputational impact
  - *Response & fixes*: Multiple incidents within weeks triggered broader review

2021 — VW/Audi Vendor Breach (3.3M)

- Brands: **Volkswagen/Audi** (North America)
  - *Scope/scale*: 3.3M current/prospective customers impacted
  - *Attack vector*: Unsecured vendor marketing datastore
  - *Effect*: Driver license numbers in 95% of cases; some SSNs
  - *Financial/operational impact*: Free credit monitoring; legal exposure/class actions
  - *Response & fixes*: Vendor oversight & data minimization reinforced





2022 — SiriusXM Connected Vehicle Flaw

- Brands: **Honda/Nissan/Infiniti/Acura** et al.
  - *Scope/scale*: VIN-based API auth logic enabled remote commands
  - *Attack vector*: Telematics API flaws
  - *Effect*: Unlock/start/locate potential until patched
  - *Financial/operational impact*: Unstated; rapid patch and monitoring
  - *Response & fixes*: Reinforced API security testing and least-privilege design

2022 — Spireon Telematics Platform Vulns

- Brands: **Spireon** (fleet/consumer telematics) ~15M vehicles
  - *Attack vector*: Platform/API issues enabling remote commands
  - *Impact*: Potential fleet-wide remote actions; fixed
  - *Source*: https://www.securityweek.com/vulnerabilities-spireon-telematics-system-allow-remote-commands-vehicles/

2023 — Toyota T-Connect Cloud Misconfiguration

- Brands: **Toyota** (Japan)
  - *Scope/scale*: 2.15M users' vehicle/location data exposed for ~10 years
  - *Attack vector*: Cloud storage misconfigured (public access)
  - *Effect*: Potential exposure of vehicle IDs & location data
  - *Financial/operational impact*: Regulatory notifications; trust impact
  - *Response & fixes*: Triggered global cloud review at Toyota Connected



2023 — Nissan Oceania — Akira Ransomware

- Brands: **Nissan** (Australia/New Zealand)
  - *Scope/scale*: ~100,000 people affected; some IDs compromised
  - *Attack vector*: Ransomware intrusion; data exfiltration
  - *Effect*: Customer/employee/dealer data exposure
  - *Financial/operational impact*: Notification & support costs; regulatory scrutiny
  - *Response & fixes*: Public advisories issued by authorities; hardening underway

2024 — Kia Web Portal Takeover via License Plate

- Brands: **Kia** (global)
  - *Scope/scale*: Millions of vehicles potentially reachable pre-patch
  - *Attack vector*: Dealer web portal API flaws; license-plate → VIN → control
  - *Effect*: Remote unlock/start/track until patched
  - *Financial/operational impact*: Unstated; rapid patch; potential liability avoided
  - *Response & fixes*: Highlights excessive dealer portal privileges

Part I — Key Takeaways

- **Common root causes impacting vehicles/services**:
  - Weak API/auth in telematics/portals; excessive dealer privileges
  - Legacy protocols/crypto (keyless entry, immobilizers, unauth CAN)
  - Third-party dongles and mobile apps with insecure defaults
  - Cloud/storage misconfigurations exposing telemetry & personal data
- **Controls that help**:
  - ISO/SAE 21434 + UN R155 processes; TARA-driven requirements
  - mTLS/OAuth2, least-privilege RBAC, rate limiting, telemetry (VSOC)
  - ECU hardening: secure boot, HSM, message auth/segmentation
  - SBOM + vuln management; CVD/bug bounty; OTA patching

GLOBAL AUTOMOTIVE SUPPLY CHAIN COMPLEXITY




CYBERSECURITY ALERT:

Part II — Production & Supply-Chain Impacts

(2010–2025)



Incidents that disrupted manufacturing, logistics, or supplier operations.

Generated 2025-10-28

2020 — Honda EKANS/Snake Ransomware

- Brands: **Honda** (global ops)
  - *Scope/scale*: Plant shutdowns in multiple regions
  - *Attack vector*: Ransomware impacting IT/OT processes
  - *Effect*: Production halted; logistics/service disruption
  - *Financial/operational impact*: Undisclosed; downtime & recovery costs significant
  - *Response & fixes*: Highlighted ICS-aware ransomware risk to auto manufacturing

2022 — Toyota Supplier Kojima Attack Halts Production

- Brands: **Toyota** (Japan)
  - *Scope/scale*: All 14 plants halted for one day (≈13,000 vehicles output loss est.)
  - *Attack vector*: Supplier compromise → JIT supply disruption
  - *Effect*: Nationwide production stop for a day
  - *Financial/operational impact*: Lost output + recovery; underscores supply-chain risk
  - *Response & fixes*: Rapid resumption; supplier hardening program expanded



2022 — Continental AG — LockBit Ransomware

- Brands: **Continental** (Tier-1)
  - *Scope/scale*: Data exfiltration; $50M ransom demand reported
  - *Attack vector*: LockBit intrusion; data for sale after refusal
  - *Effect*: Sensitive plans & customer data posted
  - *Financial/operational impact*: Undisclosed; potential legal & competitive risk
  - *Response & fixes*: FBI involvement; elevated supplier due-diligence by OEMs

2025 — Jaguar Land Rover Cyberattack & Production Halt

- Brands: **Jaguar Land Rover** (JLR) — UK's largest automaker
  - *Timeline/scope*: Intrusion detected Aug 31–Sep 1, 2025 → production paused for **3–5 weeks**; phased restart in October
  - *Operational impact*: Global manufacturing + sales/registration systems disrupted; key UK sites (Solihull, Halewood, Castle Bromwich, Wolverhampton) restarted in phases; Nitra (Slovakia) later
  - ***Supply-chain effect***: Thousands of suppliers impacted; UK gov. announced a £1.5B loan guarantee to support the network
  - *By-the-numbers*: Estimated losses up to **£50M/week**; ~1,000 vehicles/day typical output; quarter ending Sep 30 saw −17% retail and −24% wholesale deliveries
  - *Macro impact*: Estimates put UK economic cost near **$2.5B**; investigations ongoing; attackers' claims under review

Part II — Key Takeaways

- **Production/supply-chain patterns**:
  - Ransomware and supplier compromises halting JIT manufacturing
  - Flat OT/IT networks and weak workstation hardening at plants
  - Insufficient vendor due diligence and incident contracts
- **Controls that help**:
  - Network segmentation (IT/OT), allow-listed tooling, station attestation
  - Supplier security requirements, audits, and joint incident playbooks
  - Offline recovery procedures; immutable backups; tabletop exercises


ALERT

THE 7 LAYERS OF CYBERSECURITY – Generally used

Universitatea Politehnica Timişoara

1. **Human Layer** – Security awareness training to prevent phishing & social engineering.
2. **Perimeter Security** – Firewalls & VPNs protect against unauthorized access.
3. **Network Security** – Segmentation & monitoring prevent internal threats.
4. **Endpoint Security** – Antivirus & encryption safeguard devices.
5. **Application Security** – Secure coding & updates prevent software exploits.
6. **Data Security** – Encryption & access controls protect sensitive information.
7. **Operations Security** – Incident response & backups ensure quick recovery.

Cybersecurity Complete Suite

Universitatea Politehnica Timişoara

Security Management

Information Security

Network Security

Cloud Security

Application Security

Security Management

Universitatea Politehnica Timişoara

Information classification	Backup and Recovery	Password Policy	**Bring Your Own Device**
Information Transfer policy	Disposal & Destruction	**Compliance Management**	Acceptable use of assets

Information Security

Universitatea Politehnica Timişoara

1. Access Rights & Permissions Matrix
2. Document Retention & Disposal
3. **Security KPI Dashboard**
4. Information Security Compliance
5. Incident Reporting & Tracking Sheet
6. Encryption Key Management Sheet
7. Data Loss Prevention (DLP) Incident
8. **Data Classification Register**
9. Data Breach Notification Log

Network Security

Universitatea Politehnica Timişoara

What is a Security Risk?

Threat, vulnerability, impact
Business vs. technical risk

Common Network Threats
Unauthorized access
Malware/ransomware entry points
Man-in-the-middle / sniffing
DoS/DDoS
Misconfigurations

Risk Assessment Basics
Asset inventory
Likelihood × impact
Prioritizing critical services

Mitigation Strategies
Network segmentation/VLANs
Firewalls & NGFW rules hardening
IDS/IPS deployment
Secure remote access (VPN, MFA)

Identity & Access Controls
Least privilege
MFA
Centralized auth (RADIUS/LDAP/AD)
Key/secret rotation

Monitoring & Logging
Syslog/SIEM
Alerts on anomalous traffic
NetFlow analysis

Policies & Response
Incident response plan
Backup & recovery
Regular security audits/pen tests
User awareness

Ongoing Improvement
Continuous vulnerability scanning
Change management
Metrics (MTTD/MTTR)

Network Device Inventory
Network Access Control Log
IP Whitelist-Blacklist Tracker
VPN Usage Log
Patch and config management

File servers / Portals / Cloud Security



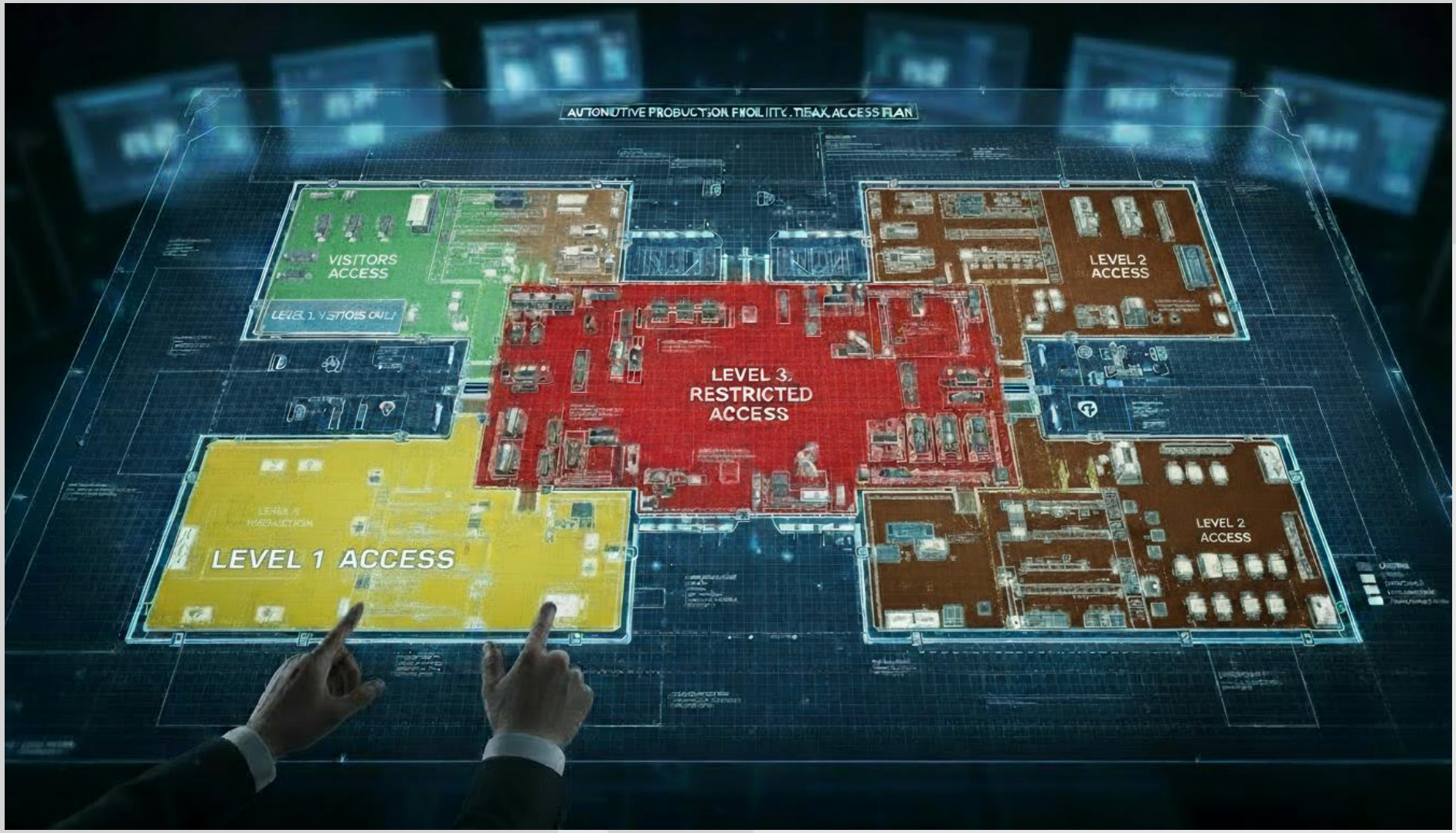

SCM

Cybersecurity Complete Suite

Universitatea Politehnica Timişoara

- Application Risk Assessment Matrix
- Web Application Vulnerability
- Static Code Analysis Log
- Security Misconfiguration Log
- Secure Mobile App Testing Tracker
- Application Threat Modeling and Test
- Secure Coding Checklist
- Patch & Update Tracker
- Authentication & Authorization Control
- Application Data Encryption Checklist

Physical Access Levels



What is wrong from a cybersecurity perspective?




Automotive Business Continuity Plan
• Risk Assessment & BIA
• Supply Chain Resilliance
• IT Operational Resilience
• IT Disaster Recovery
• HR & Management
• Testing & Improvement



Thank you!

Industrial Cybersecurity for Automotive Components: Risk Assessment and Defense Mechanisms

Conf.dr.ing. Muguraș Mocofan

muguras.mocofan@upt.ro

Universitatea Politehnica Timișoara

Piața Victoriei no. 2
RO 300006 - Timisoara
Tel: +40 256 403000
Fax: +40 256 403021
rector@upt.ro
www.upt.ro

ETcTI

Centrul MULTIMEDIA

Centrul ID/IFR și e-Learning