TMC Drive - Autonomous EV Concept

Threat Modeling Report

Team 7

13.04.2025 - TMC Threat Modeling Hackathon 2025

Executive Summary

Team 7 conducted a focused threat modeling exercise on the TMC Drive autonomous electric vehicle concept to identify high impact threats, evaluate their business impact and recommend actionable and cost effective mitigations. Our results are limited with multiple factors such as lack of experience in the field of EV design, missing technical and security relevant information, and without deeper knowledge of financial risks simulations including safety and compliance standards that apply. Therefore we made multiple assumptions under which we identified and analyzed critical components and key risk areas such as Autonomous Driving Systems, Backend Cloud Infrastructure, and partially customer data privacy.

Following are details about the key findings identified:

- Identified **8 critical threats** with a total potential **risk exposure of €20M–€60 M EUR**.
- The highest-risk threats include:
  - **T25: Ransomware Deployment** (€2.79M exposure).
  - **T19: Supply Chain Attack** (€2.4M exposure).
- Privacy violations pose regulatory risks with potential fines reaching up to €50M.

Our Key recommendations for immediate risk response measures are:

- **Prioritize High-Risk Areas**: Allocate immediate resources to address ransomware deployment, supply chain attacks, and privacy violations.
- **Implement Layered Security Measures**:
  - **Short-Term**: Focus on firmware security and AI/ML integrity.
  - **Mid-Term**: Strengthen API and DDoS protections.
  - **Long-Term**: Complete network zero-trust implementations and regulatory compliance audits.
- **Additional Measures to Consider on Long Term**:
  - Establish continuous security monitoring and incident response (e.g. MSS SOC Service)
  - Perform regular technical and process audits, penetration tests, and monitoring systems to stay ahead of evolving threats.

By integrating the proposed measures, the organization can achieve over **75% risk exposure reduction**, with an emphasis on securing critical systems, ensuring operational continuity, and protecting customer data. We strongly believe this proactive approach will strengthen both **cyber-resilience** and **regulatory alignment**, ensuring long-term business sustainability of the TMC Drive autonomous EV Concept .

Table of Contents

Introduction

Objective

The goal was to identify the threats and corresponding risk scenarios with the most critical ratio of business impact and likelihood and suggest appropriate cost-effective risk responses for them aligned with overall business strategy.

Scope

Based on our analysis of the overall concept, the user stories , and mission critical functions and features provided by different subsystems, our team decided to focus threat modeling on

- Autonomous Driving Stack
- Cloud Backend Infrastructure
- Data Privacy Assessment

In addition mobile application and 3rd party risks were discussed, rather on a high level and hence partially covered.

Out Of Scope

Due to time and resource constraints, the following subsystems were out of the scope of our analysis: IoT devices embedded in EV, EV Road Infrastructure, Battery Charging Infrastructure and traditional mechanical elements of the cars.

Assumptions

Following were our main assumptions:

- The TMC Drive is fully Self Autonomous to level 6
- Waymo Like Software Architecture
- AWS IaaS is used for TMC Cloud Backend
- Multiple assumptions used for risk scoring, business impact assessment and financial risk exposure (explained in the corresponding section)

Approach

The reported threats were identified and structured using STRIDE and LINDDUN threat modeling methodologies. Then the threats were then assessed and prioritized according to their business impact and likelihood estimated according to available evidence. Finally, we made assumptions of financial damages based on industry benchmark reports, which helped us to estimate exposure to financial risks for the corresponding risks of highly prioritized threats.
Based on that we identified and recommended efficient and cost-effective risk response measures and security controls for each risk scenario and its corresponding threats by using the simplified OpenFAIR Framework.
Independently from our research oriented threats identification effort, an additional threat list was generated by using the community version of the IriusRisk with intention to explore it and used the results for validating our approach, although obviously facing the time limitations as the diagram used as an input was rather high level compared to our more detailed one we used.

1.TMC Drive Concept Breakdown - What are we working on?

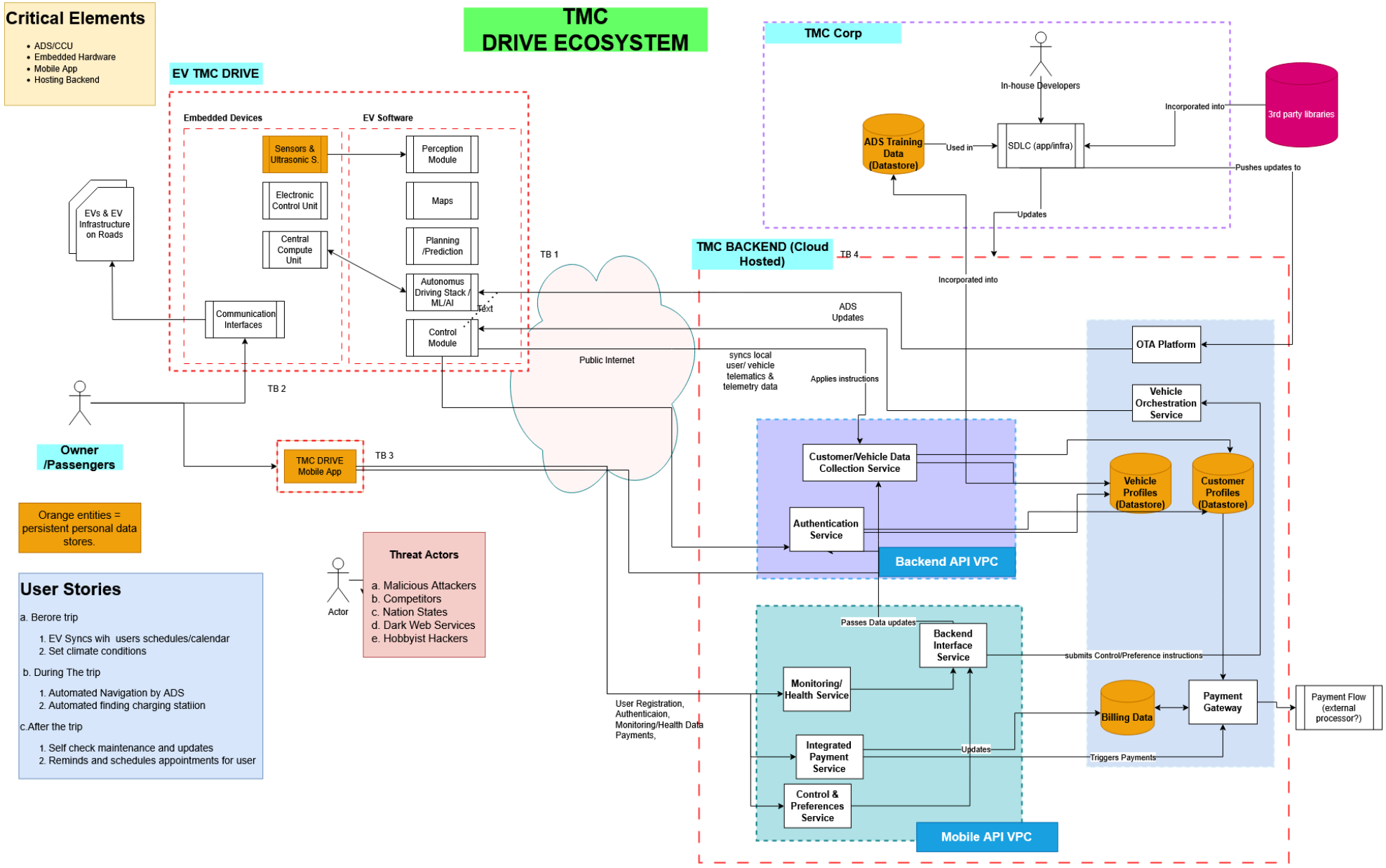

Figure 1: TMC Drive Architecture Diagram

1.1 User Stories

This threat modeling was based on identified roles, user stories and functions provided by subsystems and components identified within the provided system description

Role	User Story	Functions /Features	Components
Owner /Passenger	As an EV owner I want to control my vehicle using a mobile app so that I can manage its health and performance remotely.	Remote Management and Monitoring	Mob App
Owner /Passenger	As a payment service customer I want to make secured payments for EV upgrades and services so that I can enhance its capabilities without risks.	Payment Service	Mobile App
Owner /Passenger	As a passenger I want the TMC Drive to autonomously while following traffic regulations, avoid obstacles, navigate roads and bring me to the selected destination at the best possible time without my manual intervention	Autonomous Driving, Navigation and Control	ADS, EV Hardware (Sensors,ECU, CCU)
Owner /Passenger	As a passenger I want the ADS to monitor road conditions in real time and to handle emergencies like sudden stops,unexpected maneuvers so that it prevents accidents an protects passengers.	Real Time Monitoring and Emergency Response	ADS, EV Hardware (Sensors, CCU)
Owner /Passenger	As an owner or driver I want the ADS to monitor battery status, automatically take decisions about the charging and drive to the available charging station, to recharge the batter with automated payment of the service.	Autonomous Charging Station and Service Payment	ADS, EV Hardware (Sensors, CCU)
AI Developer	As a developer I want to continuously improve AI algorithms, so that the vehicle can learn from the past experience and continuously improve its decision making capabilities	ADS Continuous Improvement	ADS (AI Algorithms, LLM)
AI Developer	As a developer I want to collect real time telematics and AI/M data, to be used for ML feedback loop in order to optimise ar retrain ADS so that my EV has better performances	Telematics Data Collection and Optimisation	ADS (AI Algorithms, LLM)
Developer /Sys. Admin	As a developer I want to remotely update ADS to improve its AI algorithms, fix vulnerabilities and ensure EV safe operatior	Remote ADS Updates deployment	OTA; ADS, Cloud Backend,

Safety Engineer	As a safety analyst I want to ensure that the ADS adheres to the safety standards so that it ensures passengers safety and prevention of accidents	ADS operates according to safety standard	ADS (AI Algorithms, LLM)
Safety Engineer	As a safety analyst I want to ensure that the ADS validates inputs from radar sensors, communication interfaces and GP signals so that any tampering that misleads the EV is prevented.	Sensors and Signal Validation Mechanism	ADS; EV Hardware
Regulators/ Auditors	As a regulator I want to ensure that EV adheres to complianc and data privacy requirements, securely store or anonymize sensitive and PII data so that legal and privacy standards are followed	Compliance and Data Privacy Protection	EV Software and Hardware System, Mobile App, Hosting Cloud Backend
Threat Actor/ Maliciou Attacker	As an attacker I want to reveal EV systems vulnerabilities, design and configuration flaws, compromise the EV system, manipulate it or steal the sensitive data	Exposed insecure EV features and interfaces	EV Software and Hardware System, Mobile App, Hosting Cloud Backend

Table 1: User Stories, Functions & Subsystems

After breaking down the architecture diagram and analysing the subsystems we identified as mission critical following elements of the TMC Drive Concept: IaaS Cloud Backend, EVs Autonomous ML/AI Driving Stack and its elements, Embedded Devices, 3rd party software libraries, OTA Platform, TMC Drive Mobile Application.

Following are the important trust boundaries identified on the concept diagram:

- TB1 - between EV and the Cloud Backend
- TB2 - between EV and Mobile App
- TB3 - between Mob App and the Cloud Backend
- TB4 - between the Cloud Backend and 3rd party providers

Moreover, we have identified the following sensitive data assets: Customer Personal Data (PII), Financial Transaction, Sensors Data, Telematics and EV diagnostic data, ML Training Data.

As main attack surface areas we have identified the cloud IaaS due to significant likelihood of inherited attack surface such as IaaS misconfiguration, public Internet facing interfaces such as web admin interfaces, service APIs used by mobile app or EV software, customers/vehicle portal, cloud object storage services (AWS S3 Bucket), OTA Platform combined with potentially insecure data transport links etc. On the side of EV itself, we consider as significant attack surfaces Sensors (LIDAR; RADAR; Cameras, Ultrasonic radars), communication interfaces (Bluetooth, WiFi), CAN Bus, OBD II, AI Models Algorithms and Training Data.

2.Key Findings - What can go wrong ?

This section and the subsections below highlight only the top 3 threats vectors per subsystems with the highest total risk score assessed as well as a data privacy assessment, while a detailed threat matrix with all the threats listed and corresponding DFDs are attached at the end in the Appendix section.

2.1. ADS - Autonomous Driving Stack

According to the user stories, functions and features, we consider ADS as one of mission critical elements. It is a kind of “brain” for an self driven electric vehicle, playing the role of an artificial driver, hence it’s safety, security and reliability are of the key importance. We assumed our ADS is designed according to the Waymo architecture which is for the purpose of this analysis simplified accordingly (Figure 2).

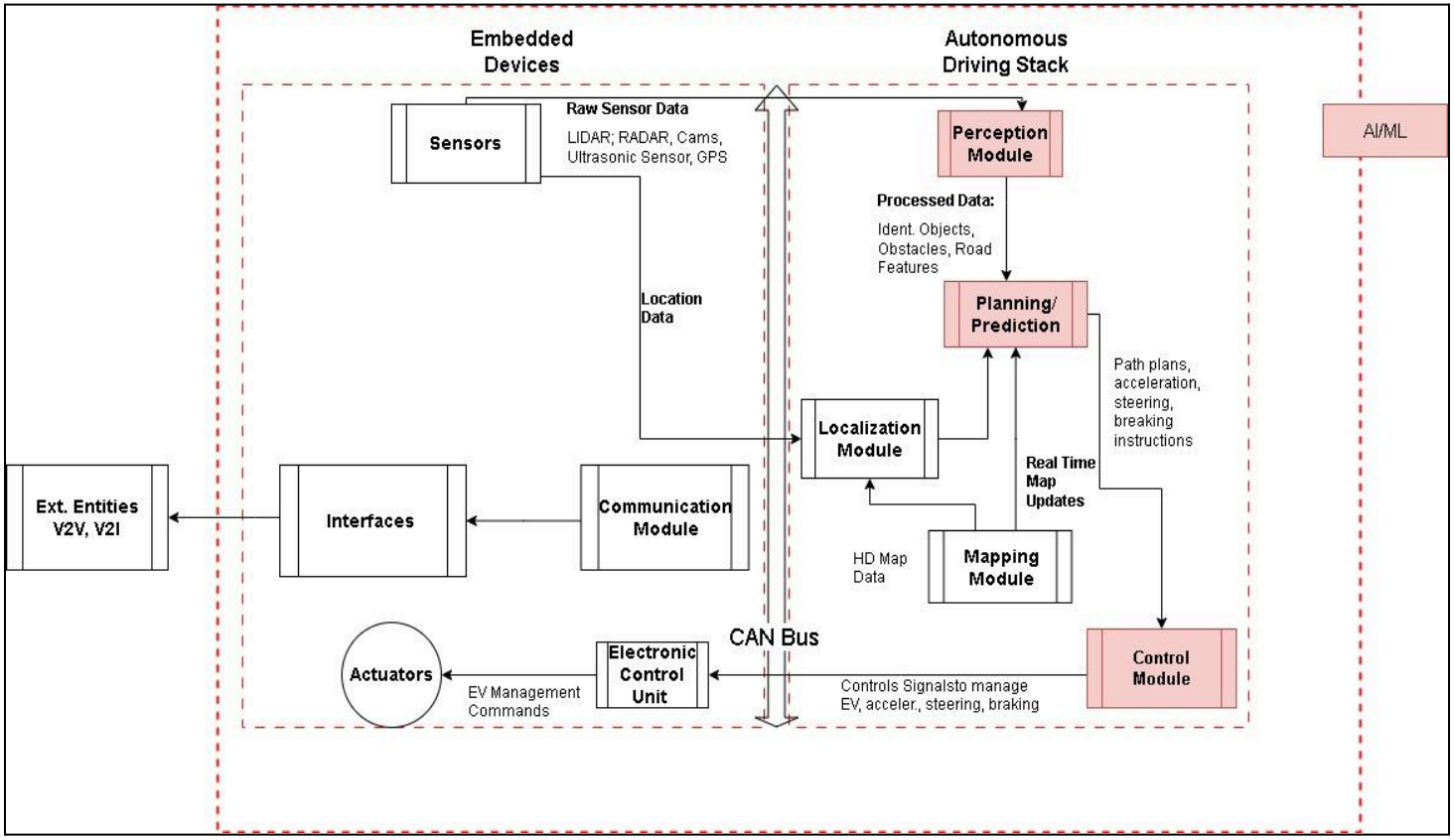

Figure 2: Simplified ADS Architecture

For the purpose of this report, in the Table 2 below we highlighted 3 interesting examples of ADS threat vectors that have potential to significantly impact

all areas of the business risks (not limited to them only, though), for a full list which includes detailed assessment and the total risk score as well as the references to the real life cases please refer to the Appendix 2, the Threat Matrix sheet.

2.1. Autonomous Driving Stack - ADS High Risk Threats

To demonstrate our approach we highlighted a few of the threats with high risk scores, while a full list of those that are identified is available in the attached Threat Matrix file. For each of the threats we assessed their Risk Score based on impact on Business Impact score and estimated Likelihood based on available evidence of their occurrence i.e. likelihood -1 no available information, likelihood 2 - academic research reports and PoC, likelihood -3 reported real life incidents.

ID	Threat Name	Threat Description	Potential Impact	Risk Score = Bus. Impact * Likelihood
T13	**Compromise Embedded Device / Rogue Firmware Update**	a.A third-party manufacturer delivers a device with pre-installed malicious firmware or hardware-based vulnerabilities which due to lack of proper inspection/testing allows tampered components to enter production unnoticed. or b. an attacker with local physical access to EV interfaces, flashes embedded device (e.g.ECU) firmware with maliciously crafted binary code due to weaknesses in the firmware update procedure. The motivation can be different like causing direct damage of the targeted vehicle (e..g triggering battery explosion) or damaging/disabling some EV functions (e.g. brake) or tracing location of high profile passengers/owners.	*Stealthy EVs control via unauthorized persistent presence and control over the EV's systems. * Reduced passenger's safety - threat to vehicle reliability and passengers' safety. * Physical harm - potential crash accidents and operational disruptions. * Privacy violation - compromise owner's/ passenger privacy through hidden activities tracking and personal data collection	32*2=64
T16	**AI/ML Models Poisoning**	Adversarials tamper or "poison" ADS AI/ML algorithms or data (e.g. via training dataset) in order to modify ADS's components ability for processing received sensors data (Perception Module), route planning and making driving decisions (Planning, Controlling Modules) affecting ADS's	* Passengers safety risk due to improper ADS decisions (due to wrong perception of road situation, traffic signs or obstacles) * Operational disruptions and fleet downtime - fleet downtime due to EV failures, down time due to revoked/damaged EVs and the need for	36*1=36

		operating "logic" causing erratic driving.	interventions to fix ADS * Financial losses due to damage compensations to customers and costs of retraining/redeploying fixed ADS * Non compliance issues due to violation of safety standards * Brand reputation/ loss of the market position due to reduced customer trust * Privacy violation as poisoned models data can extract or expose private passengers data	
T17	**Malicious OTA Updates**	Deploying maliciously crafted software update or tampered firmware binaries pushed remotely via compromised OTA/CDN.	* Reduced passengers safety due to mislead and insecure EV driving behaviour on the road * Compromised brand reputation, customers trust and loyalty as result of affected EVs reliability and safety * Financial losses due to legal processes and regulatory fines	36*2=72

Table 2: High Risk Threats to ADS

2.2. Cloud Backend High Risk Threats

The TMC Drive mission critical services and data are hosted in the cloud backend which can have a number of security issues as results of misunderstanding of shared responsibility model for implementing security in the public cloud, missing IaaS security configuration, missing data protection, insecure public APIs or weak authentication on web interfaces and customer portals, lack of business continuity, data backup and restore procedures and plans etc. All of these can impact the overall business strategy and passengers safety and privacy.

ID	Threat Name	Threat Description	Potential Impact	Risk Score = Bus. Impact * Likelihood
T19	**Software Supply Chain Attack**	Internal development teams rely on third party libraries / frameworks that can pose a significant security risk. Internal development team might not have enough insights into the secure software development process that 3rd party follows nor the potential backdoors or vulnerabilities that may exist inside the libraries.. This can lead to control over a vulnerable 3rd party library being assumed by a malicious actor. They introduce malicious code into the packages, which are subsequently integrated into TMC applications and infrastructure.	Due to possible backdoors installation, data exfiltration, system compromise may lead to: a. Non compliance with privacy regulation b. Unauthorized remote access to ADS or EV SW elements c. Remote access and manipulating EV	**32*3=96**
T20	**Misuse Compromised API /Unauthorized Access**	A malicious actor can exploit vulnerability or misconfigurations such as weak API key protection to compromise a public API Interface that connects autonomous EVs to the cloud backend services. If the API gets compromised, attackers can manipulate EVs functions, extract sensitive intellectual property or customers data, and disrupt fleet operations. Possible APIs that could be targeted by this attack are APIs used for fleet management, navigation, and OTA updates, APIs for telematic handling EVs diagnostics, location tracking, and user preferences data,	* Unauthorized EVs control - attackers could send malicious commands to manipulate EVs with its acceleration, braking, or steering. * Customer data breach/privacy violations - exposure of owners PII data, location history. * Manipulate and disrupt EV fleet orchestration - manipulation of EVs fleet, leading to operational interruptions. * Financial loss - costs associated with data leaks, system recovery, and regulatory fines. * Non-compliance risks - violations of safety standards (ISO/SAE 21434, UNECE WP.29).and privacy regulations (GDPR) * Loss of brand reputation - loss of customer trust and loyalty due to compromised data and EVs security.	**28*3=84**

T25	R**ansomware Deployment**	A threat actor exploits a vulnerability in the cloud infrastructure (e.g., exposed API, misconfigured object storage, or unpatched server instance/container) to gain access to the cloud backend system managing EVs data, OTA (Over-the-Air) updates, or EVs telemetry, and user accounts. After that threat actor deploys ransomware that encrypts critical data and resources and demands a ransom for decryption keys.	* Fleet management and orchestration services are non accessible. * Telemetry and OTA updates are interrupted i.e. can not be sent/received. * Remote EV control features (lock/unlock, diagnostics) fail. * Potentially compromised customer private data. * Brand reputational damage due to interrupted operations and attention in media * FInancial losses due to paid ransom or service, costs of incident investigation/response, recovery costs	**31*3=93**

T29	**Dos/DDoS on Cloud Backend**	The DDoS/DoS attack vector can be conducted on different layers of the stack such as: * HTTP Flooding to APIs or OTA endpoints * DNS Amplification - exploit misconfigured DNS servers to flood backend with amplified traffic * TCP Syn Flood - target load balancers with half open connections * IoT Botnet - hijack vulnerable EVs to launch DDoS	*Safety risks if EVs can not receive critical security patches and functional updates (ADS upgrades, braking or planning logic etc) *Disrupted Navigation Services - traffic route updates in real time gets interrupted *Telemetry Data Flow - Loss or interrupted vehicle health status monitoring, delaying maintenance notifications * Disrupted EV Monitoring and management - Owners can not receive mobile app notifications in their EV requires some attention or action (e.g. physical safety or maintenance notifications) and can not remotely control the EVs	**27*3=81**

Table 3: High Risk Threats to Cloud Backend

2.3. Data Privacy Risks Assessment

During this threat modeling, we've identified several privacy risks related to the EV with autonomous driving, especially when it comes to collecting, storing, and processing sensitive personal data like owners location, sensors collected, visual, vehicle diagnostics, and passenger data. We've used the LINDDUN Privacy Framework to identify these privacy risks, to the best of our ability. Below listed are top risks that are most common and relevant, based on real-world incidents we've studied, as part of this exercise. We have also mapped the identified risks to the LINDDUN framework, including details such as impact, entry points, and attack scenarios, which are documented in the Threat Matrix spreadsheet provided in the deliverable folder.

Personal Data	Privacy Risks	Description	LINDDUN Category	References
Location Data (GPS, Network)	Risk of re-identification & behavioral profiling, surveillance, stalking	Collection of location data (like GPS) and vehicle telemetry can reveal sensitive information (addresses, daily routes).	Linkability, Detectability	https://www.edps.europa.eu data-protection/our-work/pu lications/techdispatch/techdi patch-3-connected-cars_en
Sensors Data (LIDAR,RADAR, Audio)	EV Sensors perform privacy surveillance, without the owner's consent.	Captured environmental, biometrics, and audio data inside the EV without consent of the owner/passenger	Disclosure of Information, Unawareness	https://www.abc.net.au/new /science/2024-10-09/car-bra ds-are-tracking-and-sharing-y our-data-with-third-parties/1 4440742
Visual Data (Camera)	Privacy violation, systematic surveillance	Identifies the moments of time while recording passengers, pedestrians, vehicles, and surrounding environment of the EV, violating their privacy	Non-Repudiation, Disclosure of Information	https://link.springer.com/cha ter/10.1007/978-3-031-7332 -5_20 https://www.theguardian.co /technology/2023/apr/07/te a-intimate-car-camera-image -shared
Passenger Data	Profiling,, unauthorized sharing, systematic surveillance	Collecting sensitive passenger data and sharing it with 3rd parties e.g. advertisers without proper anonymization or consent. Affected registration data, connected devices, contacts, and personal interactions within the car	Identifiability, Non-Compliance	https://blog.barracuda.com/ 024/01/22/data-privacy-con rns-in-ridesharing-what-you- eed-to-know
EV's Diagnostic Data	Data collection and retention, without transparency and owner's consent	Using vehicle diagnostic data to monitor owner's behavior without their consent, breaching privacy regulations	Detectability, Non-Compliance	https://www.dataprotection. e/en/dpc-guidance/employe vehicle-tracking https://www.washingtontime .com/news/2016/feb/25/nis n-disables-app-after-hackers- how-how-remotel/
Passengers Data	Third-Party Sharing	Passenger and vehicle data can be shared with 3rd parties without being anonymized leading to targeted ads, risks of profiling while lack of transparency about data sharing can	Linkability, Non-Compliance	https://cyberinsider.com/vw- uffers-major-breach-exposing location-of-800000-electric-v hicles/

		impact customers loyalty and lead to privacy violations.		
Non-Compliance	Privacy violations impact customers trust and cause costs of regulatory fines and legal processes	An EV manufacturer fails to demonstrate transparency in handling personal data access requests, leading to privacy non compliance and penalties.	Non-Compliance	https://incountry.com/blog/key-data-sovereignty-regulation-in-the-automotive-industry/

Table 4: Personal Data Privacy Risks

Note: More detailed privacy assessment based on the LINDDUN framework is available in the Appendix 2 Threat Matrix.

2.4. Privacy Enhancement Recommendations

Although the overall impact scope includes Privacy Violation as one of the key strategic risks, the table below contains recommendations on how to manage the privacy risks and those are also taken in consideration later in the dedicated section of the Recommended Risk Management strategy.

Recommendation	Objective	Timeline
1. Establish Privacy Governance Framework	Integration of privacy into engineering, operations, security and product teams.	Short-term
2. Creation of Personal Data Inventory	Data collected must reside in a centralized inventory	Short-term
3. Robust consent management	Ensuring passengers have transparency on collected personal data and mechanism of control over its storage and processing	Mid-term
4. Anonymize/Minimize collected data	Reduce privacy burden by only collecting data that's absolutely necessary	Mid-term
5. Enforcement of strong technical controls	Prevent unauthorized access to privacy sensitive data by implementing access controls and audit trails	Short-term
6. Implement Data Retention & Deletion Policie	Reduce data exposure over extended period of time and handle in accordance with privacy laws	Mid-term
7. Strengthen AI/ML practices	Protect visual and sensor data used in the ecosystem by using strong privacy techniques like differential privacy.	Long-term
8. Improve Third-Party Data Sharing Practices	Make sure data processors handle passenger data properly and securely	Long-term

Although impact on privacy was considered as one of the key business risks, due to time constraints we did not manage to evaluate separately each of the privacy threats, instead of that we added a generic Privacy Violation Risk which has assumed high likelihood and high business impact in terms of

the financial risks and simulation in section 3.1. Afterwards. The consequences are normally Regulators imposed fines, lawsuits and compensations, loss of customer trust, For concrete cases please check references to reported cases earlier in Table 4.

3. Risk Assessment

As mentioned earlier, In order to quantify the overall risk to TMC of each identified threat, a risk assessment was undertaken . This process incorporates two aspects of each threat - the **Likelihood** (the probability of the threat occuring) and the **Business Impac**t (the resulting effect from the threat). # The Likelihood was determined by categorising each threat by type, and matching these against the *Upstream's 2024* attack vector report as well as any publicly available evidence of research or 'in the wild' attacks or exploits existing relating to those threats.

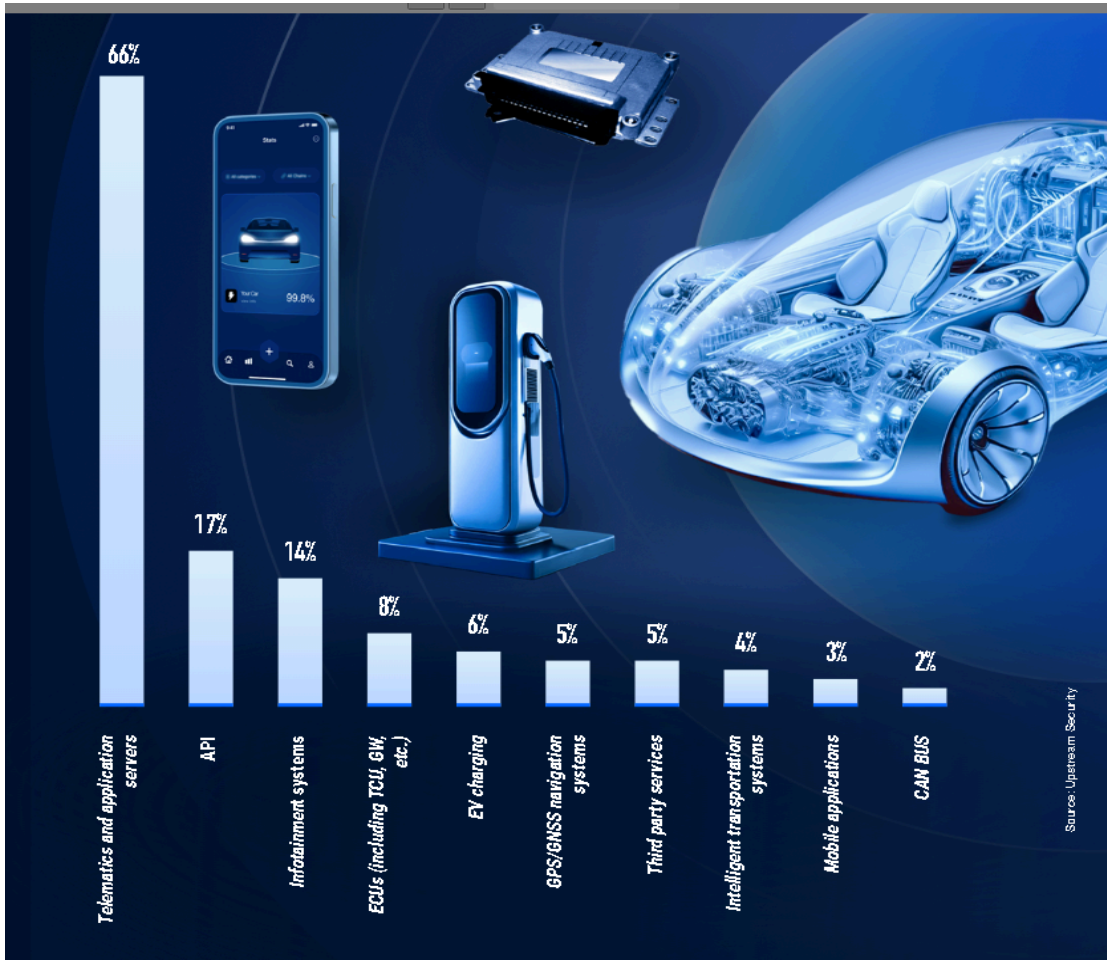

Figure 3: Different Cyber Attacks in EV IIndustry in 2024 (Source: Upstream Benchmark Report)

The **Business Impact** was estimated by assessing each threat on the following strategic risk areas, each assigned specific weight:

- Passenger safety Weight - 5
- Direct Financial Loss >1M$ Weight - 4
- Privacy Violation Weight -3,5
- Brand Reputation/Market Position Damage Weight -3
- Fleet Operations Downtime >1h Weight -2,5

After assigning estimated values to Likelihood, for each of the threats a **Total Risk Severity** score was determined. The next step is to prioritize risks for all the mentioned threats by using a risk heating map.

Likelihood **Business Impact**	**Low** (Likelihood value 1)	**Medium** (Likelihood value 2)	**High** (Likelihood value 3)
Low (Weighted score <=12)	Low	Medium	Medium
Medium (Weighted score 13>= & <=24)	Medium	Medium	High
High (Weighted score 25>=)	Medium	High	High

Table 6: Qualitative Risk Score (Prioritization)

Due to time and resource constraints, we selected the above-mentioned 7 threats with high business impact, however due to time limits we missed to expand the heating map so that it includes all of the threats available in the Threat Matrix:

ID	Threat Name	Description	Business Impact	Likelihood	Total Risk
T16	AI/ML Models Poisoning	Adversarials tamper or "poison" ADS AI/ML algorithms or data (e.g. via training dataset) in order to modify vehicle behaviour.	36	1	/36/ Medium
T17	Malicious OTA Updates	Deploying maliciously crafted software or firmware updates pushed remotely via compromised OTA/CDN.	36	2	/72/ High
T13	Compromised Embedded Device /Rogue Firmware Update	Weaknesses in vehicle firmware is exploited to influence or force vehicle behaviour	32	2	/64/ Medium
T19	Software Supply Chain Attack	Third party libraries used in the creation vehicle systems or supporting infrastructure are compromised, introducing vulnerabilities or malicious functionality into affected systems.	32	3	/96/ High
T20	Misuse Compromised API /Unauthorized Access	A malicious actor can exploit vulnerability or misconfigurations such as weak API key protection to compromise a public API Interface that connects autonomous EVs to the cloud backend services. If the API gets compromised, attackers can manipulate EVs functions, extract sensitive intellectual property or customers data, and disrupt fleet operations. Possible APIs that could be targeted by this attack are APIs used for fleet management, navigation, and OTA updates, APIs for telematic handling EVs diagnostics, location tracking, and user preferences data,	28	3	/84/ High
T25	Ransomware Deployment	A threat actor exploits a vulnerability in the cloud infrastructure to deploy malware that encrypts critical data and resources, preventing their usage until a ransom is paid. Customer data is exfiltrated and threatened with wider release.	31	3	/93/ High
T29	DDoS/DoS on Cloud Backend	The DDoS/DoS attack vector can be conducted on different layers of the stack such as: * HTTP Flooding to APIs or OTA endpoints * DNS Amplification - exploit misconfigured DNS servers to flood backend with amplified traffic * TCP Syn Flood - target load balancers with half open connections * IoT Botnet - hijack vulnerable EVs to launch DDoS	27	3	/81/ High

Table 7: Total Risk Score Heating Map

3.1. Financial Impact - Simulation

In order to prioritize risks and therefore the necessary investments in mitigation of the risks, we estimated potential financial impact if any of the threats above get materialized. For that we used sources such as industry benchmark cybersecurity reports and publicly available incidents loss information and based on them we assumed total financial losses for each of the threats mentioned earlier as follows: According to the simplified Open FAIR methodology agreed we then categorized the risks of the threat events as per the assumed FInancial Risk from High Priority >2 M $, 1M $ < Medium < 2M$ and Low < 1M$ and the threats with assigned priority levels are available in the Table 8 below.

Threat Event	Total Risk Score	Assumed Loss Magnitude (€)	Estimated FInancial Risk Exposure (€)	Priority as per Estimated
T13: Rogue Firmware Update	64	20M Eur	**1.28M Eur**	**Medium**
T16: AI/ML Models Poisoning	36	15M Eur	**540K Eur**	**Low**
T17: Malicious OTA Updates	72	17M Eur	**1.22M Eur**	**Medium**
T19: Software Supply Chain Attack	96	25M Eur	**2.4M Eur**	**High**
T20: Misuse of API	84	20M Eur	**1.68M Eur**	**Medium**
T29: DDoS on Cloud Backend	81	10M Eur	**810K Eur**	**Low**
T25: Ransomware Deployment	93	30M Eur	**2.79M Eur**	**High**
TPV: Privacy Violation Risk * (Customer Data Breach, Spying and Tracking, Misuse of Private Data)	90	40M Eur	**1.6 M Eur**	**High**

Table 8: High Risk and FinancialRisk Exposure

3.2. Risk Response Recommendations

In order to neutralize attack surfaces identified and reduce risk exposure, we suggested following risk response measures, grouped according to the technical domains and prioritized according to the urgency as per above mentioned level of financial risk exposure. Basically an absolutely secured environment or subsystem with 100% risk reduction is impossible, however once applied, suggested mitigations according to the simulation are capable of significantly reducing the risks to the acceptable levels. Moreover, having in mind that initial risk exposure is often lower than the investment, recommendation is to consider, expected Return of Investment is in expected due to reduced probability of the risks occurrence within next 3-5 years

A. Very High Urgency (High Financial Risk > 2M)

Anti-Ransomware Measures **T25: Ransomware Deployment**	**- Enforce MFA on backend access** **-Hardening APIs and object storage (S3 buckets)** **- Zero-trust networks architecture design** **- EDR systems and honeypots** **- Patch management Plan** **- IAM audits**	**Long-Term** **(1–2 years)**	**Investment :5M EUR** **Initial Risk Exposure: 2,79 M EUR** **Expected Risk Reduction: 90%** **Residual Risk Exposure: 279 K EUR**
Supply Chain Security **T19: Software Supply Chain Attack**	**- SBOM tracking** **- Automated SAST/OWASP scans/code vuln. mitigations** **- Regular third-party audits** **- Secure dependency management** **- Sandbox test environment for new libraries**	**Mid-Term** **(3–6 months)**	**IInvestment: 3M EUR** **Initial Risk Exposure: 2,4 M EUR** **Expected RIsk Reduction: 75%** **Residual Risk Exposure: 600 K EUR**

B. High Urgency (Medium Financial Risk 1-2 M EUR)

Firmware/Embedded Systems Security **T13: Rogue Firmware Update**	**- Secure Boot (trusted firmware)** **- Digital Signatures** **- Firmware Encryption** **- ECU Hardening** **- Secure OTA Updates** **- Intrusion Detection for CAN traffic**	**Short-Term** **(up to 3 months)**	**Investment: 2 M EUR** **Initial Risk Exposure: 1,28 M EUR** **Expected RIsk Reduction: 85%** **Reduced RIsk Exposure: 300 K EUR**
Cloud Backend/API Security **T20: API Misuse/Unauthorized Access**	**- API Gateway with rate limiting** **- OAuth 2.0 and TLS 1.3** **- Zero Trust API access** **- Continuous audits and pentesting**	**Mid-Term (3–6 months)**	**Investment 1.8 M EUR** **Initial RIsk Exposure:1,68 M EUR** **Expected Risk Reduction:80%** **Reduced Risk Exposure: 336 K**
Privacy Protection Measures	**- Data at rest encryption** **- Compliance Audits (GDPR, UNECE WP.29)** **- Privacy dashboards for customers** **- Hardened data storage**	**Long-Term (1–2 years)**	**Investment: 4 M** **Initial Risk Exposure: 1,22 M EUR** **Expected Risk Reduction:80%** **Residual Risk Exposure: 244 K Eur**
Secure OTA Update Process	**- Digitally signed and encrypted updates (TLS 1.3)** **- Firmware validation tests** **- Zero trust architecture at CDN level**	**Mid-Term (3–6 months)**	**2 M** **Expected Risk Reduction**

C. Medium Urgency (Lower Financial Risk < 1 M EUR)

AI/ML Model Integrity **T16: AI/ML Models Poisoning**	**- Secure OTA Updates** **- Data validation for ML training** **- Drift detection and continuous monitoring**	**Short-Term (up to 3 months)**	**Investment: 1.5 M EUR** **Initial RIsk Exposure: 540 M EUR** **Expected RIsk Reduction: 75%** **Residual Risk Exposure: 162 K Eur**
Anti-DDoS Measures **T29: Cloud Backend Dos/DDoS**	**- Anti-DDoS tools (e.g., AWS Shield)** **- Failover systems** **- API rate limiting** **- Traffic monitoring (CloudWatch)** **- Auto Scaling**	**Mid-Term (3–6 months)**	**Investment: 2 M EUR** **Initial RIsk Exposure: 810 K** **Expected Risk Reduction: 75%** **Residual Risk Exposure: 202 K EUR**

Conclusion

By integrating the proposed measures, the organization can achieve over 75% risk reduction, with an emphasis on securing critical systems, ensuring operational continuity, and protecting customer data. This proactive approach strengthens both cyber-resilience and regulatory alignment, ensuring long-term business sustainability.

Appendix

Team 7: TM Presentation Slidedeck
TMC Drive Threat Matrix Team 7

REFERENCES

1. Upstream Global Automotive Cyber Security Report 2025
2. VicOne 2025 Automotive Cybersecurity Report
3. LINDDUN Framework Overview https://cif-seminars.github.io/slides/20200929-kwuyts-linddun-go.pdf
4. Anonymize data technique: https://cloud.google.com/bigquery/docs/differential-privacy
5. Real-world privacy concerns

a. https://www.eff.org/deeplinks/2023/08/impending-privacy-threat-self-driving-cars

b. https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/

6. Emerging Privacy Issues in AV https://ieeexplore.ieee.org/document/9687196
7. Waymo's Privacy Concern: Data Collection Malpractice & Targeted Ads

https://www.ainvest.com/news/waymo-data-dilemma-privacy-profit-2504/