PSP Framework: A novel risk assessment method in compliance with ISO/SAE-21434

PSP Framework: A novel risk assessment method in compliance with ISO/SAE-21434

Franco Oberti[1,2] , Ernesto Sanchez[1], Alessandro Savino[1], Filippo Parisi[2], and Stefano Di Carlo[1]
[1]*Control and Computer Eng. Dep., Politecnico di Torino* Torino, Italy
[2]*PUNCH Softrontix*, Torino, Italy

***Abstract*—As more cars connect to the internet and other devices, the automotive market has become a lucrative target for cyberattacks. This has made the industry more vulnerable to security threats. As a result, car manufacturers and governments are working together to reduce risks and prevent cyberattacks in the automotive sector. However, existing attack feasibility models derived from the information technology field may not always provide accurate assessments of the potential risks faced by Vehicle Electronic Control Units in different operating conditions and domains. This paper introduces the PUNCH Softronix and Politecnico di Torino (PSP) framework to address this issue. This framework is designed to provide accurate assessments compatible with the attack feasibility models defined by the automotive product security standards. The PSP framework utilizes social sentiment analysis to evaluate the real threat risk levels.**

***Index Terms*—Safety Critical Embedded system, Security Embedded System, Embedded System Security Threat, Threat Modeling, Road Vehicle, Natural Language Processing**

I. Introduction

Currently, the automotive industry is facing a number of intricate challenges. Automakers are experimenting with new technologies and advanced architectures to accommodate the new automotive frontiers driven by the green transition, with Zero-Emissions Vehicles (ZEVs) being part of the ”Fit for 55” package approved by the European Community [1]. In addition, since 2021, several ISO standards and European directives have inundated the road vehicle domain, with a focus on increasing resilience to cyberattacks. The most popular directives are UN Regulation No. 155 - Cybersecurity and Cybersecurity Management System [2] and UN Regulation No. 156 - Software Update and Software Update Management System [3]. These European directives require Type Approval (TA) for each vehicle or road application to gain European market access. Although certification bodies empower compliance with UNR-156 and UNR-155 for Original Equipment Manufacturers (OEMs) only, it is the OEM's responsibility to cascade the security requirements until the last company in the supply chain, thus ensuring that each vehicle component complies with European directives. To facilitate the deployment of security requirements, ISO has ratified a series of specific standards:

Authors contacts: {franco.oberti, alessandro.savino, ernesto.sanchez, stefano.dicarlo}@polito.it and filippo.parisi@punchtorino.com

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU

- The *ISO/SAE-21434:2021 Road vehicles - Cybersecurity Engineering Standard [4]* introduces precise and structured security requirements for road vehicles and their components to be resilient against hacks. The standard also supports implementing the UNR155 requirements in organizations across the supply chain.
- The *ISO 24089:2023 Road vehicles - Software Update Engineering Standard [5]* introduces requirements and recommendations for engineering the software update process across the supply chain to support the UNR156 EU directive.
- The *ISO/PAS 5112:2022 Road vehicles - Guidelines for Auditing Cybersecurity Engineering [6]* provide procedures for managing audit security programs, setting audit criteria based on ISO/SAE-21434 objectives.

In January 2022, the publication of the Radio Equipment Directive (RED) [7] delegated act triggered articles 3(3)(d), (e), and (f) for devices that can communicate over the internet directly or through a secondary device to improve the general level of security and the protection for personal data and privacy. With this new interpretation of radio devices, the RED impacts most of the onboard Electronic Control Units (ECU). The provision will be mandatory starting on the 1st of August 2024 through Notified Body certification that each automotive supplier shall fulfil for their devices. In 2026, the European Cyber Resilience Act (CRA) [8] shall substitute the RED directive for Automotive supplier companies with an upcoming cybersecurity certification. Eventually, the European Parliament is reviewing the Resilience of Critical Entities (CER) Directive [9] that proposes to expand the coverage of the Network and Information Security (NIS2) Directive [10], including transportation in the ten new sections. This foreshadows the automotive industry (OEMs and suppliers), seeing the automotive as an essential service provider actor, which is undoubtedly in scope for NIS2.

In this complex scenario [11], [12], this paper discusses potential inconsistencies generated using the Threat Analysis Risk Assessment (TARA) model proposed by automotive security standards during TA certification. Primarily focusing on ISO/SAE-21434:2021, the paper highlights the possible erroneous risk evaluation misled by the static model proposed by the standard and introduces preliminary ideas for making those models more tailored to evaluate the risk accurately.

The paper is organized as follows: Section II overviews the ISO/SAE-21434 standard highlighting its main limitations.

Section III describes the proposed solution named PSP framework from the name of the developers (PUNCH Softronix and Politecnico di Torino) and presents preliminary results obtained through a proof of concept implementation of the framework. Eventually, Section IV summarizes the paper's main contributions and outlines the next steps for the continuation of this work.

II. ISO/SAE-21434 STANDARD

In August 2021, the ISO/SAE-21434 was released, the first standard focused on cybersecurity for road vehicles. It was designed to support and ensure security throughout the ECU supply chain, specifically to help original equipment manufacturers (OEMs) comply with the UN R155 regulation. Figure 1 displays all the standards for developing the ISO/SAE-21434 standard. It is worth noting that many of the standards used in its creation are not solely related to the automotive industry, particularly those related to cybersecurity.

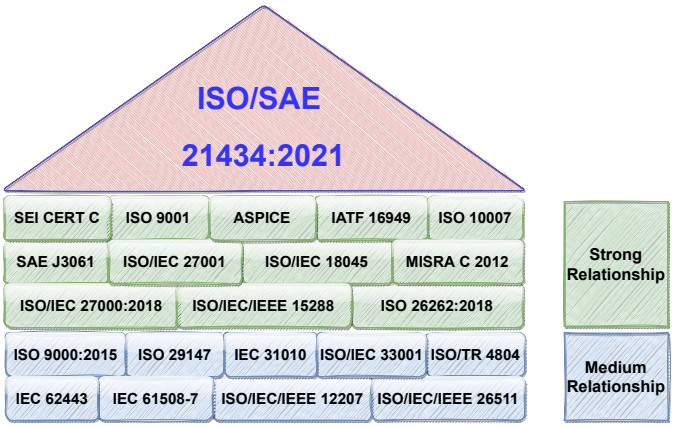

Fig. 1: Standards contribution list to ISO/SAE-21434

The ISO/SAE development process is rooted in the renowned V-model widely used in software development. The ISO-26262 [13] standard and Automotive SPICE framework [14] have also embraced it. The journey starts with creating a Threat Analysis and Risk Assessment (TARA) model, which comprises four TARA process activities: asset identification, threat scenario identification, impact rating, and attack path analysis. These activities are recursive at any point during the development cycle and are systematically applied as per Deliverable D2 in the HEAVENS project [15]. TARA is typically called upon during production phases when a vulnerability is detected in the field. Figure 2 depicts the occurrence of TARA throughout the various development phases.

Unlike other standards like ISO-26262, the ISO/SAE-21434 provides predefined models with fixed weights defined in Clause 15 of the standard (see Figure 3) that prevent tuning the model to fit the automotive network domain. This lack of flexibility in the model is a limitation in the TARA development that can lead to misleading results.

The inaccurate analysis outcomes can be clarified by the influence of other security standards emphasizing IT security

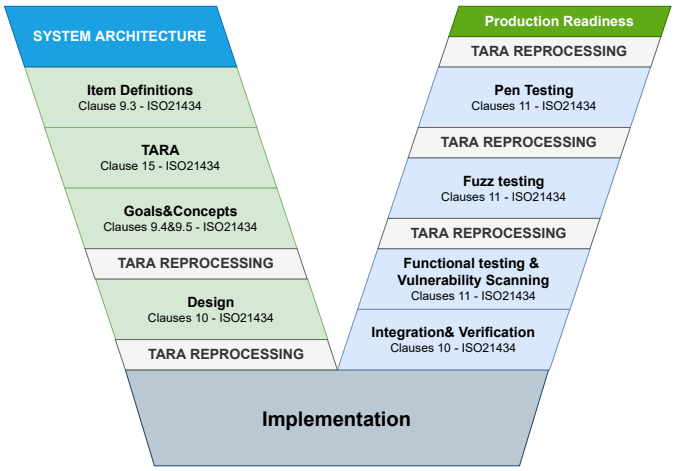

Fig. 2: ISO/SAE-21434 Development Life Cycle

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Fig. 3: Attack Potential weights model extracted by ISO/SAE-21434

rather than product security. The TARA model of ISO/SAE-21434 performs well in the domains closely related to the IT Infrastructure perimeter but requires improvement in other areas. Vehicles are becoming increasingly complex, and their architecture is highly diverse, making it challenging for static modeling to function in all domains. Figure 4 displays a simple vehicle architecture with various functional domains and ECUs. However, not all domains are suitable for the same types of attacks. In its reports, Upstream [16] identifies three types of attacks: long-range, short-range, and physical access. At the same time, potential attackers may have different profiles, targets, resources, and motivations [17].

The ISO/SAE-21434 standard introduces threat feasibility models that aim to standardize threat modeling techniques across users, projects, applications, and companies. These models are significant because they promote harmonization in threat modeling. The standard defines three attack feasibility models: attack potential-based, CVSS-based, and attack vector-based. Attackers are generally classified into several categories, including Insider (such as service or maintenance personnel), Outsider (such as black hats), Rational (such as car owners), Malicious (such as criminals), Active (such as standard thieves), Passive (such as a rival/competitor), Local (such as the vehicle's owner), and so on [18].

However, using a static Enterprise IT TARA model in a complex and heterogeneous environment like the automotive industry can lead to counterproductive results. This is particularly true when developing TARA for an Engine ECU

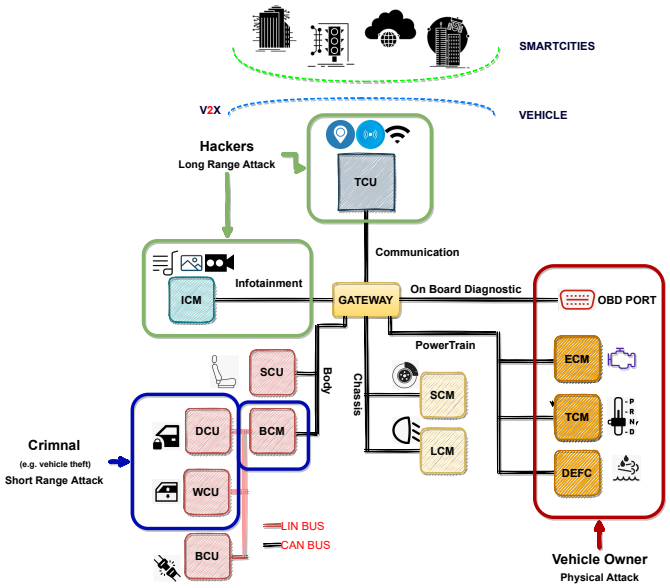

Fig. 4: The figure highlights in green the ECUs with a suitable rate for Long-range Attack, in blue the Short-range Attack while the red confines the Physical Attack ECUs

compliant with ISO-21434, as it highlights the inaccuracies in all three models when determining the attack feasibility rates.

Attack feasibility rating	Criteria
High	**Network:** Potential attack path is bound to network stack without any limitation. EXAMPLE 1 Cellular network connection making the ECU directly connected and accessible on the internet.
Medium	**Adjacent:** Potential attack path is bound to network stack; however, the connection is limited physically or logically. EXAMPLE 2 Bluetooth interface, virtual private network connection.
Low	**Local:** Potential attack path is not bound to network stack and threat agents require direct access to the item for realizing the attack path. EXAMPLE 3 Universal serial bus mass storage device, memory card.
Very low	**Physical:** Threat agents require physical access to realize the attack path.

Fig. 5: Attack vector-based approach extracted by ISO/SAE-21434

In this particular situation, when the suggested models from the standard were applied, the result was a very high score for a remote attack and a low score for a physical attack (see an example in Figure 5). However, this approach may not be suitable for automotive safety-critical hard real-time powertrain devices, where physical attacks are not rare or complex. In these systems, the primary communication occurs on the CAN bus, and external access is available through the OBD port, easily accessible in the cabin. Possible attacks on the CAN bus, particularly on the powertrain subnet domain, are physical in nature [19]. Implementing a remote attack against the ECU without Firmware On The Air (FOTA) support is uncommon and challenging. Powertrain attackers usually fall into the Insider or Rational Local profile categories, which means they have unlimited time and free device access. Therefore, the ISO-21434 score produced by the ISO-21434 attack feasibility model for the powertrain scenario is misleading. Many papers report weaknesses or inaccuracies in the TARA results produced following the ISO-21434 model [20], [21].

Additionally, the Cybersecurity Assurance Level (CAL) is determined by attack vectors such as Physical, Local, Adjacent, and Network (Figure 6). ISO-21434 defines four target security levels, with the highest being CAL4 and the lowest being CAL1. These levels correspond to the ASIL levels used in ISO-26262.

The powertrain domain oversees real-time functions that carry critical safety implications and are at risk of being targeted by Denial of Service (DoS) attacks [22] triggered by physical attacks. It is worth noting that such attacks do not pose a significant threat beyond CAL2 security status, which indicates a medium-low level of security emphasis. This limitation is due to the ISO-21434 standard's range of physical attack levels extending to CAL2, as illustrated in Figure 6.

		Attack vector[b]			
		Physical	**Local**	**Adjacent**	**Network**
Impact	Severe	CAL2	CAL3	CAL4	CAL4
	Major	CAL1	CAL2	CAL3	CAL4
	Moderate	CAL1	CAL1	CAL2	CAL3
	Negligible	---[a]	---[a]	---[a]	---[a]

[a] See [PM-06-08].
[b] Attack vector is a static parameter of attack feasibility.

Fig. 6: CAL determination based on impact and attack vector parameters table extracted by ISO/SAE-21434

Therefore, many industrial technical forums require revising the TARA model applied by ISO-21434. Those papers provide solutions or improvements. However, since the system is so complex, heterogeneous, and exposed to the Man At The End (MATE) attack [23], only some solutions can cover the entire attack surface and attacker profiles with sufficient accuracy.

III. PSP Dynamic TARA Model for Road Vehicle Purpose

As mentioned in Section II, the Road Vehicle sector has a lot of diversity in terms of domains, sub-domains, attack surfaces, attack vectors, and attacker profiles. Therefore, relying on fixed-weight models to evaluate security may lead to inaccurate results in certain circumstances. This situation can be detrimental to the automotive industry, as companies invest a lot of resources to make their products secure to meet legal requirements and enhance the value of their products. However, if the models used to assess security are unreliable, it can result in inefficient allocation of resources, with companies focusing on the wrong areas. We aim to prevent such a situation by providing a non-intrusive and dynamic framework called PSP, named after its developers. This framework can assist analysts during the assessment of attack feasibility.

The PSP framework works in two distinct ways. Firstly, it utilizes active models based on ISO-21434 standard guidelines

and consistently incorporates dynamic weights to evaluate all conditions. Secondly, it enables the creation of a specialized runtime model that assesses the feasibility of attacks based on financial exposure.

The PSP framework utilizes Natural Language Processing (NLP) methods to enhance the attack feasibility model. Although Machine Learning and Deep Machine Learning [24] have already been implemented in various automotive applications such as Intrusion Detection Systems (IDS) [25] and Manufacturing [26], the use of NLP in the road vehicle field is still limited [27], [28]. The proposed solution uses NLP to compute sentiment classification using social media information for a subset of attacks, namely Insider, Rationale, and Local attacks described in Section II. By exploiting NLP, the PSP framework can auto-generate updated weight tables that comply with ISO-21434, providing better analysis accuracy in all scenarios. This allows product security teams to provide a more precise rating on MATE attacks, which existing literature has reported as difficult to assess [29].

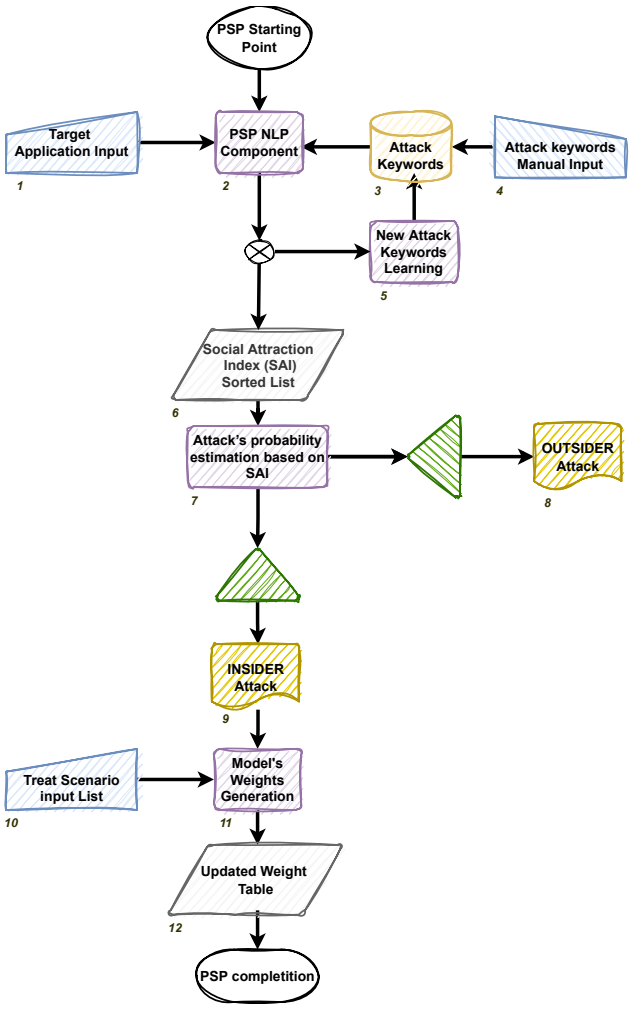

Fig. 7: PSP Work-Flow Scheme

The diagram in Figure 7 illustrates the PSP workflow. The initial implementation of the PSP framework uses Twitter APIs [30]. The framework takes in the target application (e.g., cars, trucks, agriculture machines), region (e.g., Europe, NA, etc.), and application category (e.g., sports cars, vans, industrial, domestic, etc.) as inputs (Figure 7, block 1). At the first interaction, a list of standard hashtags (e.g., #dpfdelete, #egrremoval, #egrdelete, #egroff, #dieselpower, #chiptuning) manually populates the keyword attack database (Figure 7, blocks 3 and 4).

These inputs are then processed by the PSP NLP component (Figure 7, block 2), which produces a sorted Social Attraction Index (SAI) list. The SAI items are calculated by querying Twitter posts based on the target application and attack keywords and elaborating on the number of views, interactions, and popularity of the identified posts. Each entry in the SAI has its attack probability estimation (Figure 7, blocks 6 and 7).

While computing the SAI list, the NLP triggers a component that facilitates an auto-learning strategy to incorporate new keywords into the database for future runs. This ensures no hashtag deficiencies, which may cause partial and incomplete findings, as depicted in Figure 7 at block 5.

Afterward, the entries in the SAI list are separated into insider or outsider categories. Here, we define insiders as all attacks that the owner is aware of and approves, even if the attack comes from third parties (e.g., an untrusted service, a racing workshop, etc.). Outsider attacks are all attacks conducted by a third party only, where the owner is oblivious (e.g., criminal attacks, thefts, black hat attacks, etc.). Typically, most threat scenarios on social media are insider, so re-tuning the standard model weight values on the outsider entries does not make sense.

The main contribution provided by the PSP framework is for all threat scenarios that belong to the insider category. These attacks are product-specific, particularly in road vehicles and IoT domains. They are new and different from the standard attacks that IT domains have experienced, requiring more experience.

At this stage, the PSP framework utilizes the insider attack list and a manually identified threat scenario list created by the product security team to generate new ISO-21434 attack feasibility tables with updated weight values (as seen in block 12 of Figure 7).

The ISO-21434 standard outlines constant weights for the attack vector-based approach model (as seen in Figure 5). The PSP framework uses the same weight value for outsider threats, as shown in Figure 8-A. However, for insider threats, the platform adjusts the weights by tuning them with corrective factors derived from SAI (seen in block 7 of Figure 7), which can change the priority of the attack vectors (as shown in Figure 8-B).

To demonstrate the capabilities of the PSP framework, we will examine a potential threat scenario involving Engine Control Module (ECM) reprogramming. While this type of attack has a low feasibility rating according to ISO-21434 weights due to its physical attack vector (Figure 5) [31], according to [16], it has a high occurrence rate preferably

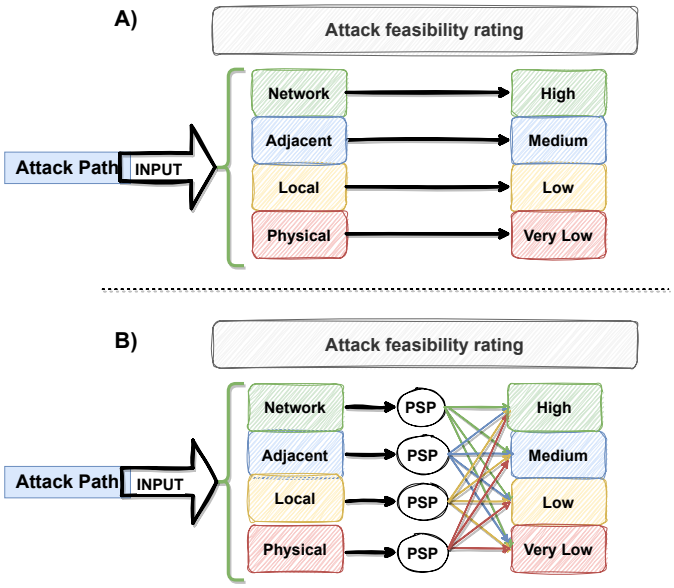

Fig. 8: The figure **A)** shows the attack feasibility weights, defined by ISO-21434, for outsider threats **B)** On the contrary, the insider threats get attack feasibility weights tuned by PSP framwork

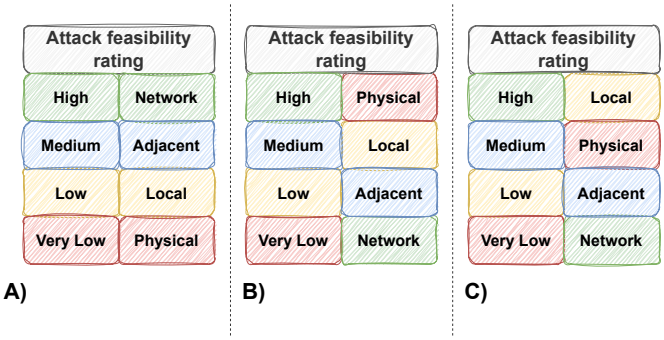

Fig. 9: The figure **A)** show the original G.9 table titled Attack vector-based approach provided in ISO-21434 document. Figure **B)** revised the G.9 table applying the PSP model corrections for ECM reprogramming as a Threat Scenario. The final figure, **C)**, always shows a revised G.9 table by PSP model built on the same database but limiting the data since 2022.

based on physical attacks. By utilizing the PSP framework, we were able to update the standard attack feasibility value table, resulting in a more accurate assessment of the threat (Figure 9-B).

It's worth noting that the social sentiment analysis time window plays a crucial role in the PSP framework's analysis. For instance, Figures 8-B and 8-C show different attack feasibility ratings for the same threat scenario in the insider attack domain. This is because the PSP platform considers all Twitter posts in the former, while it only focuses on recent posts from 2021 onwards in the latter. The trend inversion highlighted by PSP began last year and is confirmed by the Upstream global automotive cybersecurity report. As a result, reprogramming via a physical attack is no longer mainstream, and attackers are more likely to opt for a local attack via OBD. While this demonstrates PSP's ability to detect current threats, it also highlights the attackers' improved techniques for bypassing secure mechanisms using local attacks.

Improving attack feasibility models, as defined by ISO-21434, is just one aspect of the PSP framework. This framework also introduces a unique strategy for creating an attack feasibility model based on a financial index. The underlying assumption is that vehicle owners initiate all internal breaches of tampering or reprogramming, even though they are illegal, to gain an advantage.

Insider attacks have established themselves as a profitable market. The significant market penetration in aftermarket tuning, such as ECU reprogramming, external control boxes, and emission defeat devices, provides access to a very lucrative market. These actions are driven either by reducing operational costs or increasing performance. Industrial vehicles fall into the first category, while standard passenger cars and light trucks belong to the second. The owner or another person must bear the cost of executing an insider attack. If the costs are reasonable for the market demand, the feasibility of that insider attack is much higher. Conversely, the attack does not match the market demand if the occurrences are infrequent.

The PSP framework provides a way to map, classify, and rank all insider attacks, leveraging the high visibility offered by the market. This approach is effective, especially in assessing critical aspects with a high level of unpredictable and volatile statements led by MATE. Social tags make it easy to gather new data and instantly capture current trends quickly. Figure 10 illustrates the PSP action flow.

The PSP framework is used to determine the market value (MV) of a potential insider attack by computing each threat scenario through equation Equation 1. MV is the initial measure of the size and profitability of an attack. The equation takes into account two factors: PAE (Figure 10, block 1) estimates the number of potential attackers, while $PPIA$ (Figure 10, block 2) represents the maximum purchase price a vehicle owner would be willing to pay for an insider attack. To estimate $PPIA$, the framework utilizes NLP and text mining techniques to cluster adversary devices or services found online based on their prices. The PAE value is determined by Equation 2, which relies on past year's vehicle sales (VS) trend reports. In non-monopolistic markets, VS is replaced with market share (MS). The framework also considers the percentage of potential attackers (PEA), which is determined by analyzing vehicle cybersecurity annual reports. The search parameters can be customized based on vehicle, application, years, period, historical trend, and region.

$$MV = PAE \cdot PPIA \tag{1}$$

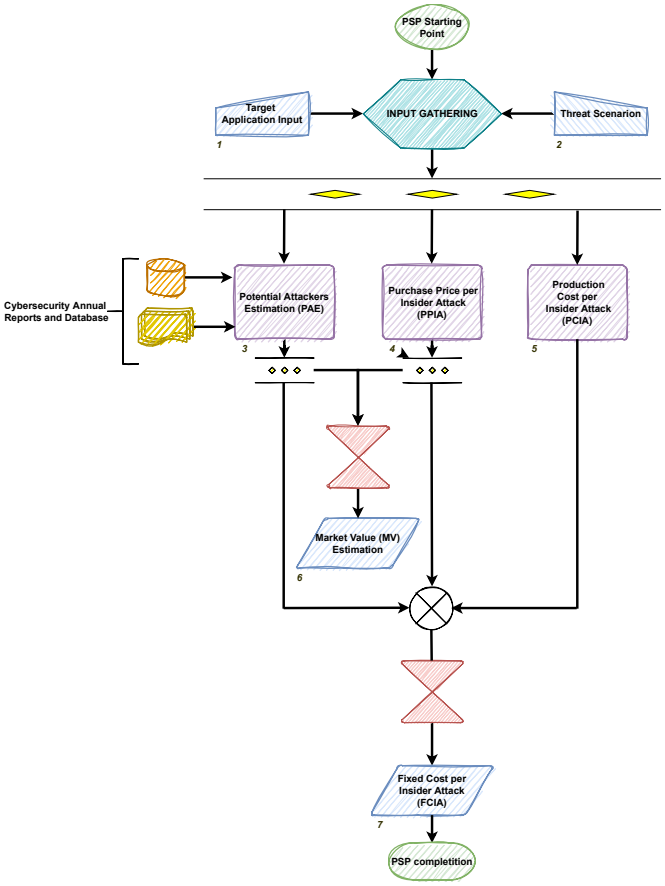

Fig. 10: Financial attack feasibility PSP Work-Flow Scheme

$$PAE = \begin{cases} VS \cdot PEA, & \text{for monopolistic markets} \\ MS \cdot PEA, & \text{for non-monopolistic markets} \end{cases} \quad (2)$$

The MV index helps us determine whether an attack falls within the intended scope. To increase our confidence level in estimating the feasibility of an attack, it is crucial to calculate the break-even point (BEP) using mathematical methods [32]. The BEP is the point at which the cost of producing an asset, in this case, an insider attack, is equal to its purchase price. Insider attacks are profitable in the blue area (shown in Figure 11), where their feasibility rate ranges from medium to high. Conversely, attacks in the red zone are not profitable, as their revenue is lower than their costs.

In Equation 3, a formula is presented for calculating the BEP. This formula uses a numerator that represents the fixed cost (FC) and a denominator that represents the difference between the purchase price per unit (PPU) and the variable cost per unit (VCU). The VCU considers the manufacturing cost, such as the cost of installing a defeat device in the case of an insider attack. In the scenario discussed in this paper, the PPU is defined as $PPIA$ in Equation 1, which is the highest price that an attacker would be willing to pay.

Since it is unlikely that a single attacker would be able to conduct a global physical attack, the revenue per unit

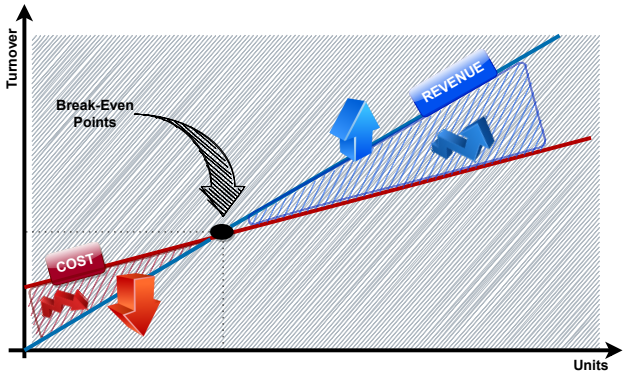

Fig. 11: The figure shows a standard BEP diagram. In our study, that is important to understand where the zone is profitable for the attackers.

expressed in the denominator is divided by the number of attackers (n), which is equivalent to multiplying the fixed cost (FC) by n.

$$BEP = \frac{FC}{\frac{(PPIA - VCU)}{n}} = \frac{FC \cdot n}{(PPIA - VCU)} \quad (3)$$

As demonstrated in Equation 4, the value of FC is determined by considering the total number of hours required to organize the research and development activities for the adversary ($FTEH$). The hourly cost (ch) is based on a standard salary for black hat hackers. The final factor involves calculating the depreciation of Capital Expenditures (CAPEX) items on a straight-line basis (SLD), which includes various development tools, electronic instruments, and specialized hardware and software, primarily laboratory instrumentation such as Analyzers, Tracers, Debuggers, and Oscilloscopes.

$$FC = (FTEH \cdot ch) + SLD \quad (4)$$

The information provided by the break-even point is useful for enhancing product security. The PSP framework utilizes the inverse function (Equation 5) where FC is an unknown term, and the BEP value is equivalent to the PAE. In this way, the framework allows for calculating the total investment required to develop an insider attack.

$$FC = \frac{BEP \cdot (PPIA - VCU)}{n} \quad (5)$$

For example, suppose we consider the query ”excavator, Europe” in the PSP framework. In that case, the platform will return a picture of insider attacks concerning excavators. The SAI graph, displayed in figure 12, reveals that disabling the Diesel Particular Filter (DPF) is the insider attack with the highest score. The PSP calculates these scores by processing and matching SAI data with the post outline, including views, occurrences, and interactions.

The estimated market value (MV) for the DPF tampering attack in Europe is 506,160 EUR per year (as referenced

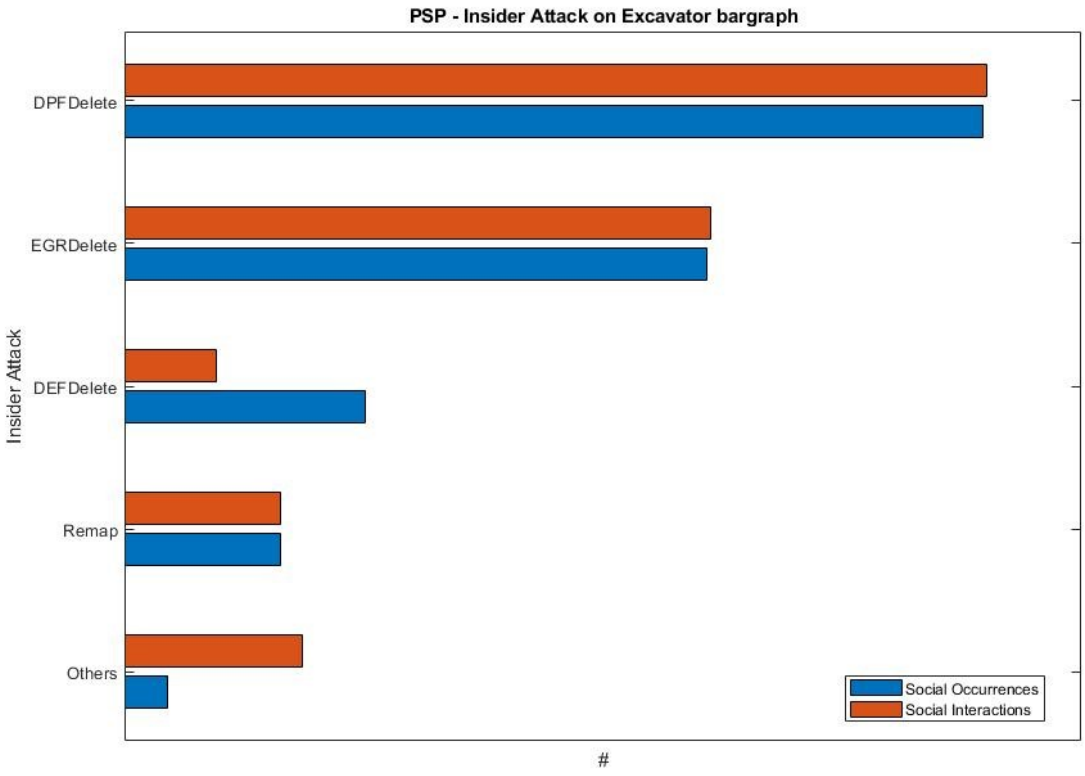

Fig. 12: PSP draft result about Excavator Insider Attack gotten by SAI

in Equation 6). This figure is based on sales data from the previous year and refers to DPF tampering incidents on European soil excavators. The NLP method determines that a defeat device's average cost is 360 EUR after network screening. Text mining on cybersecurity reports provides the number of potential attackers, which is 1,406 for a major company based on the Upstream annual report.

$$\begin{aligned} MV &= PAE \cdot PPIA \\ &= 1,406 \cdot 360\ EUR \approx 506,160\ EUR \end{aligned} \tag{6}$$

Simultaneously, the PSP platform returned an approximate value of 145,286 EUR for FC as indicated in Equation 7. This calculation considers the difference of 310 EUR between $PPIA$ and VCU, provided by the PSP platform's NLP search. It assumes three potential competitors for the attack (as estimated by the same NLP search).

$$\begin{aligned} FC &= \frac{BEP \cdot (PPIA - VCU)}{n} \\ &= \frac{1,406 \cdot 310}{3} \approx 145,286 \text{ EUR} \end{aligned} \tag{7}$$

The value of FC reflects the investment required for an attacker to execute an insider attack successfully. The higher the FC, the less feasible the attack becomes, significantly when the cost outweighs the potential revenue. In light of this example, the development team should create a secure anti-tampering DPF architecture to ensure product security that can withstand an adversary's investment of up to 145,286 EUR without being compromised.

This illustrates how the FC index computed by the PSP platform can serve as a new attack feasibility index integrated into the general ISO-21434 models discussed earlier, fine-tuning market demand to better reflect the attack trend.

IV. Conclusion

This paper presented an analysis of improving current models for assessing the feasibility of attacks in the automotive industry and introducing a new financial-based model. The main aim of the PSP platform is to move from static risk assessment models, as outlined in ISO-21434, to a runtime model environment. This approach allows for monitoring internal risks while avoiding uncertainty in all areas of the automotive sector. This flexibility ensures the models are adaptable and suitable for all vehicle domains.

The preliminary PSP framework concept presented in this paper was developed using Twitter APIs and has shown satisfactory results in terms of model quality. However, significant work must be done to operationalize the framework and automate the validation process. Additionally, enhancing

features are needed to improve the automation of new keyword updates and to make attacker keyword strategies more resilient to poisoning.

Our next improvement plan is implementing a filtering strategy for messages to ensure we process only authentic posts and prevent attackers from poisoning the data. Additionally, we plan to expand the support of our framework to other social media platforms like Instagram. Our roadmap also includes a feature allowing us to access the deep web level to improve outsider attack analysis potentially.

REFERENCES

[1] European Counsil. Fit for 55, 2023.

[2] UN Economic Commission for Europe. Un regulation no. 155 - cyber security and cyber security management system, 2021.

[3] UN Economic Commission for Europe. Un regulation no. 156 - software update and software update management system, 2021.

[4] International Organization for Standardization. Iso/sae 21434:2021 road vehicles — cybersecurity engineering, 2021.

[5] International Organization for Standardization. So 24089:2023 road vehicles — software update engineering, 2023.

[6] International Organization for Standardization. Iso/pas 5112:2022 road vehicles — guidelines for auditing cybersecurity engineering, 2022.

[7] European Counsil. Radio equipment directive (red), 2022.

[8] European Counsil. Cyber resilience act (cra), 2022.

[9] European Counsil. Resilience of critical entities (cer), 2022.

[10] European Counsil. Network and information security (nis), 2023.

[11] Franco Oberti, Ernesto Sanchez, Alessandro Savino, Filippo Parisi, and Stefano Di Carlo. Mitigation of automotive control modules hardware replacement-based attacks through hardware signature. In *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, pages 13–14, 2021.

[12] Franco Oberti, Alessandro Savino, Ernesto Sanchez, Filippo Parisi, and Stefano Di Carlo. Ext-taurum p2t: An extended secure can-fd architecture for road vehicles. *IEEE Transactions on Device and Materials Reliability*, 22(2):98–110, 2022.

[13] International Organization for Standardization. So 26262-1:2018road vehicles — functional safety, 2018.

[14] Quality Management in the Automotive Industry. Automotive spice, 2015.

[15] Aljoscha Lautenbach, Magnus Almgren, and Tomas Olovsson. Proposing heavens 2.0 – an automotive risk assessment model. In *Proceedings of the 5th ACM Computer Science in Cars Symposium*, CSCS '21, New York, NY, USA, 2021. Association for Computing Machinery.

[16] Upstream. Global automotive cybersecurity report, 2023.

[17] Marko Wolf. *Attackers and Attacks in the Automotive Domain*, pages 77–89. Vieweg+Teubner, Wiesbaden, 2009.

[18] Vinh LA. Security attacks and solutions in vehicular ad hoc networks: A survey. *International Journal on AdHoc Networking Systems (IJANS)*, Volume 4:1–20, 04 2014.

[19] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and I.K. Jennions. Evaluation of can bus security challenges. *Sensors*, 20:16–17, 04 2020.

[20] Simon Greiner, Maike Massierer, Claudia Loderhose, Bernd Lutz, Frederic Stumpf, and Franziska Wiemer. A supplier's perspective on threat analysis and risk assessment according to iso/sae 21434. In *20th escar Europe - The World's Leading Automotive Cyber Security Conference (15. - 16.11.2022)*. 2022.

[21] Sergej Japs, Frank Kargl, Harald Anacker, and Roman Dumitrescu. Why make it hard? - usage of aggregated statistical data for risk assessment of damage scenarios in the context of iso/sae 21434. *Procedia CIRP*, 109:293–298, 01 2022.

[22] Yousik Lee and Samuel Woo. Can signal extinction-based dos attack on in-vehicle network. *Security and Communication Networks*, 2022:1–10, 09 2022.

[23] Adnan Akhunzada, Mehdi Sookhak, Nor Badrul Anuar, Abdullah Gani, Ejaz Ahmed, Muhammad Shiraz, Steven Furnell, Amir Hayat, and Muhammad Khurram Khan. Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, 48:44–57, 2015.

[24] Nevrus Kaja. *Artificial intelligence and cybersecurity: Building an automotive cybersecurity framework using machine learning algorithms*. PhD thesis, 2019.

[25] Elies Gherbi. *Machine learning for intrusion detection systems in autonomous transportation*. PhD thesis, 07 2021.

[26] Andre Luckow, Ken Kennedy, Marcin Ziolkowski, Emil Djerekarov, Matthew Cook, Edward Duffy, Michael Schleiss, Bennie Vorster, Edwin Weill, Ankit Kulshrestha, and Melissa C Smith. Artificial intelligence and deep learning applications for automotive manufacturing. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 3144–3152, 2018.

[27] Luca Bertoglio, Valentina Penso, and Cosimo Senni Guidotti Magnani. Machine learning and artificial intelligence boosting automotive threat intelligence. 2022.

[28] Jun Zhao, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, and Bo Li. Timiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Computers & Security*, 95:101867, 2020.

[29] Adnan Akhunzada, Mehdi Sookhak, Nor Anuar, Abdullah Gani, Ejaz Ahmed, Muhammad Shiraz, Steven Furnell, Amir Hayat, and Khurram Khan. Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, 48, 11 2014.

[30] Twitter, Inc. Twitter API, 2023.

[31] Shiho Kim. *Automotive cyber security : introduction, challenges, and standardization*. Springer, Cham, Switzerland, 1st ed. 2020. edition, 2020.

[32] Naning Fatmawatie. Implementation of break event point analysis and margin of safety in profit planning. *Idarotuna : Journal of Administrative Science*, 2:132–146, 12 2021.

[33] Jesús García, José Luis Guerrero, Alvaro Luis, and José M. Molina. Robust sensor fusion in real maritime surveillance scenarios. In *2010 13th International Conference on Information Fusion*, pages 1–8, 2010.

[34] Junfeng Huang, Jianbing Gao, Yufeng Wang, Haibo Chen, Juhani Laurikko, A.-P Pellikka, Ce Yang, and Chaochen Ma. Insight into the penalty of exhaust emissions and fuel consumption by dpf regeneration of a diesel passenger car. *Chemosphere*, 309:136629, 09 2022.