

Investigation of Risk Assessment Methodology for Physical Layer Attacks to Prevent Vehicle Theft

Maki Shimokawa¹⁾ Takanori Miyoshi¹⁾ Kazuhiro Kakito¹⁾ Satoshi Horihata¹⁾ Isaac Mpidi Bita²⁾ Hugo Basabe²⁾ Ioannis Sokoros³⁾ Felix Möhrle³⁾ Reinhard Schwarz³⁾ Eric Wagner⁴⁾

1) Sumitomo Electric Industries, Ltd. (1-1-3, Shimaya, Konohana-ku, Osaka 554-0024, Japan)

2) Fraunhofer IEM (Zukunftsmühle 1 33102 Paderborn).

3) Fraunhofer IESE (Fraunhoferstraße 20 D-53343 Wachtberg-Werthhoven)

4) Fraunhofer FKIE (Fraunhofer-Platz 1 67663 Kaiserslautern)

KEY WORDS: software and its underlying technologies, security requirements analysis, ISO/SAE 21434

As automotive systems evolve into highly integrated Cyber-Physical Systems (CPS) through autonomous driving and connectivity, the threat of cyber-attacks targeting vehicle control functions has intensified. Securing in-vehicle networks, such as CAN and LIN, is a critical challenge directly linked to functional safety. Unlike conventional IT systems, automobiles possess unique physical characteristics; they are tangible assets accessible in various operational environments, such as public parking lots or shared mobility services. This accessibility allows attackers to bypass logical security boundaries by directly connecting unauthorized devices to in-vehicle networks via physical access, increasing the risk of physical crimes such as vehicle theft. However, current risk assessment standards, such as ISO/SAE 21434, tend to treat physical access uniformly, failing to reflect the actual difficulty and constraints of physical attacks.

This paper proposes a novel risk quantification methodology that integrates physical constraints into the ISO/SAE 21434 framework. Existing IT-centric approaches, such as CVSS 3.1, often underestimate physical threats. In CVSS 3.1, the Exploitability value is calculated as $E = 8.22 \times AV \times AC \times PR \times UI$. When the Attack Vector (AV) is categorized as "Physical," it is assigned a constant coefficient of 0.2. Consequently, even if all other parameters are at their maximum, the exploitability score remains extremely low, leading to an underestimation of risk in standard risk matrices shown in Table 1. To address this, we redefined the physical attack vector into three hierarchical levels based on the physical barriers and operational constraints: Surface-Accessible (SA), Restricted-Accessible (RA), and Isolated-Accessible (IA). The transition between these levels is determined by evaluating dimensions such as physical barrier strength, environmental constraints, operational complexity, and procedural requirements.

1. Surface-Accessible (SA): Targets located on the exterior or easily accessible areas requiring minimal intervention (e.g., exposed connectors).
2. Restricted-Accessible (RA): Targets protected by physical barriers or located within the interior, requiring moderate effort or specialized tools (e.g., accessing the OBD-II port after entering the cabin).
3. Isolated-Accessible (IA): Targets highly isolated in protected environments, requiring significant effort and invasive procedures (e.g., dismantling an ECU housing)

As detailed in Table 2, this revised mapping reassigns the AV coefficients to better reflect these physical realities. The validity of the proposed method was verified through two case studies. First, we applied the method to a known CAN injection vulnerability involving physical access via vehicle exterior damage. While the conventional CVSS 3.1 approach yielded an exploitability score of $E = 0.91$ (Very Low) and a risk value of 2, our proposed method, classifying the vector as SA, resulted in $E = 2.84$ (Medium) and a risk value of 4. This demonstrates the method's ability to appropriately escalate underestimated risks. Second, we conducted a large-scale assessment of approximately 30 threat scenarios using a virtual central zone architecture. The results confirmed that the proposed method effectively identifies risks related to physical contact with the TCU and in-vehicle networks, which were previously undervalued.

Furthermore, by mapping countermeasures to attack phases (initial, execution, and diagnosis), we found that existing security measures alone may not be sufficient to mitigate attacks during the initial phase. This highlights the need for a multi-layered defense strategy that considers multiple perspectives, such as the corresponding attack phases and the OSI layers of the countermeasures.

In conclusion, the proposed methodology enables more accurate risk quantification by incorporating physical constraints into the TARA process. This approach supports informed decision-making regarding security countermeasures during the design phase and contributes to the refinement of cybersecurity management in automotive development processes.

Table 1 Risk matrix example in ISO/SAE21434

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Table 2 Proposed Attack vector (AV)

AV Metric Value		Numerical Value
Network		0. 85
Adjacent		0. 62
Local		0. 55
Physical	Surface-Accessible (SA)	0. 62
	Restricted-Accessible (RA)	0. 40
	Isolated-Accessible (IA)	0. 20