Comprehensive Journal of Science
Volume (11), Issue (42), (Sapt, 2026)
ISSN: 3104-6266

مجلة العلوم الشاملة
المجلد (11) العدد 42 سبتمبر 2026
ردمد: 3104-6266

الأمن السيبراني في أنظمة النقل الذكية: تحليل التهديدات وآليات الحماية والمرونة التشغيلية

عفره محمد فارس
المعهد العالي للعلوم والتقنية القره بولي
قسم: تقنيات الحاسب الآلي

Cybersecurity in Intelligent Transportation Systems: An Analysis of Threats Protection Mechanisms, and Operational Resilience

Afrah Mohammed Fares
Garabulli Higher Institute of Sciences and Technology - Computer Technology Department Corresponding
meme48175@gmail.com

تاريخ الاستلام: 2026/09/02 -تاريخ المراجعة:2026/09/08- تاريخ القبول: 2026/10/06- تاريخ للنشر : 2026/ 10/29

الملخص

تتناول هذه الورقة الأمن السيبراني في أنظمة النقل الذكية (ITS) بوصفها منظومات سيبرانية-فيزيائية تتفاعل فيها المركبات المتصلة والبنية التحتية الطرقية وشبكات الاتصال ومراكز إدارة المرور ومنصات تحليل البيانات.

تهدف الورقة إلى الإجابة عن أربعة أسئلة بحثية هي: (1) ما أبرز فئات التهديدات السيبرانية في ITS بحسب طبقة النظام والأصل المتأثر؟ (2) ما مدى ملاءمة آليات الحماية المتاحة وقيودها؟ (3) كيف يمكن ربط الضوابط الأمنية بمؤشرات المرونة التشغيلية؟ (4) ما المكونات التي ينبغي أن تتضمنها مصفوفة تحليلية لاختيار الضوابط وتقييم فعاليتها؟

اعتمدت الورقة منهجية المراجعة النطاقية وفق إطار PRISMA-ScR، وشملت (1,240) سجلًا من قواعد بيانات (IEEE Xplore, Scopus, Web of Science, TRID) للفترة الممتدة من يناير 2019 إلى أكتوبر 2026، أُدرجت منها (62) دراسة في التحليل النوعي بعد تطبيق معايير الإدراج والاستبعاد.

وتخلص الورقة إلى أن الضوابط المنفردة لا تكفي؛ إذ يلزم الجمع بين الحماية الوقائية والكشف والاستجابة والتعافي، وتقترح مصفوفة تحليلية موسّعة تربط التهديدات بالأصول المتأثرة والأثر التشغيلي وآليات الحماية ومؤشرات التحقق.

الكلمات المفتاحية: أنظمة النقل الذكية؛ الأمن السيبراني؛ المركبات المتصلة؛ أمن V2X؛ المرونة السيبرانية؛ المرونة التشغيلية؛ تسميم البيانات؛ إدارة المخاطر.

Abstract

This paper examines cybersecurity in Intelligent Transportation Systems (ITS) as cyber-physical systems in which connected vehicles, road infrastructure, communication networks, traffic .management centers, and data analytics platforms interact

The paper aims to answer four research questions: (1) What are the main categories of cyber threats in ITS according to the system layer and affected asset? (2) How adequate are the available protection mechanisms, and what are their limitations? (3) How can security controls be linked to operational resilience indicators? (4) What components should an analytical matrix for selecting ?controls and evaluating their effectiveness include

The paper adopts a scoping review methodology following the PRISMA-ScR framework. It covers 1,240 records from the databases IEEE Xplore, Scopus, Web of Science, and TRID for the period from January 2019 to October 2026, of which 62 studies were included in the qualitative .analysis after applying inclusion and exclusion criteria

The paper concludes that individual controls are insufficient; prevention, detection, response, and recovery must be combined. It proposes an expanded analytical matrix that links threats to affected .assets, operational impact, protection mechanisms, and verification indicators

;**Keywords**: Intelligent Transportation Systems; cybersecurity; connected vehicles; V2X security .cyber resilience; operational resilience; data poisoning; risk management

1. المقدمة

تتطور أنظمة النقل الذكية من منظومات مساعدة لإدارة المرور إلى بنى رقمية مترابطة تعتمد على الاستشعار والاتصالات اللاسلكية والمعالجة السحابية والذكاء الاصطناعي. ويشمل نطاقها المركبات المتصلة والآلية، ووحدات الاتصال على جانب الطريق (RSUs)، وإشارات المرور، ومراكز التحكم، وخدمات معلومات المسافرين، وأنظمة تحصيل الرسوم وإدارة الأساطيل. ويتيح هذا التكامل تحسين السلامة والكفاءة وتقليل الازدحام، لكنه يخلق اعتمادًا متبادلًا بين مكونات تقنية ومادية قد يؤدي تعطل أحدها إلى آثار متسلسلة في النظام الأوسع (Abdo et al., 2024; Avcı & Koca, 2024).

وتتجاوز خصوصية أمن ITS نطاق حماية الحواسيب والبيانات التقليدية؛ فالرسالة المزورة أو المتأخرة أو المعاد إرسالها قد تؤثر في قرار آلي أو توقيت إشارة مرورية، بينما قد يؤدي اختراق وحدة إلكترونية داخل المركبة إلى تهديدات تمس السلامة المادية. وقد بيّنت المراجعات أن التهديدات تتوزع عبر المركبة والشبكة والبنية التحتية والتطبيقات، وأن تقييم المخاطر ينبغي أن يأخذ في الحسبان أثر الهجوم على السلامة والأداء والخصوصية، لا احتمال الاختراق وحده (Hahn et al., 2021; Kelarestaghi et al., 2021; Lamssaggad et al., 2021).

1.1 المشكلة البحثية

لا تكمن المشكلة البحثية في غياب الأدبيات التي تحصر التهديدات أو الضوابط، بل في أن عرضها على هيئة قوائم منفصلة قد يخفي العلاقات المتبادلة بين طبقات النظام، فالهجوم قد يبدأ في طبقة التطبيق عبر بيانات اعتماد مسروقة، ثم ينتقل إلى منصة إدارية، وينتهي بتأثير ميداني في إشارات المرور أو رسائل السلامة، ومن ثمّ، ينبغي أن يتجاوز التحليل مجرد السؤال «ما التهديد؟» إلى السؤال «أي أصل تتأثر به؟ وما الأثر التشغيلي والسلامي؟ وما الضابط الذي يقلّل هذا الأثر؟ وكيف نتحقق من فعاليته؟». هذا الانتقال من التهديد المنفرد إلى سلسلة الأثر هو جوهر الإضافة التحليلية للورقة.

كما أن عرض التهديدات والحلول على هيئة قوائم منفصلة قد يخفي حدود كل آلية، والتعارض المحتمل بين متطلبات الأمن وزمن الاستجابة والخصوصية والتوافر. لذلك تسعى الورقة إلى قراءة تكاملية توضح كيف ترتبط فئات الهجوم بالضوابط الأمنية وبالقدرة على استمرار الوظائف الحيوية والتعافي.

1.2 تمييز مفاهيمي

تميّز هذه الورقة بين مفهومين متلازمين:

- **المرونة السيبرانية (Cyber Resilience):** قدرة النظام السيبراني على استيعاب التهديدات السيبرانية والاستمرار في تقديم المخرجات المقصودة رغم الظروف المعاكسة، وفق تعريف NIST SP 800-160 Vol. 2 Rev. 1 (NIST, 2021) المعتمد أيضًا في NIST CSF 2.0 (Pascoe et al., 2024).
- **المرونة التشغيلية (Operational Resilience):** قدرة المنظومة ككل—بما فيها المكونات المادية والبشرية والإجرائية—على تقديم خدماتها الحيوية عبر الاضطرابات، بما يتجاوز التهديدات السيبرانية ليشمل الأعطال الفنية والكوارث الطبيعية.

1.3 أهداف الورقة وأسئلتها

تهدف الورقة إلى: (أ) تصنيف التهديدات بحسب آلية الهجوم والأصل المتأثر؛ (ب) تحليل آليات الحماية وحدودها؛ (ج) ربط الأمن السيبراني بالمرونة التشغيلية؛ و(د) اقتراح مصفوفة تحليلية تساعد في اختيار الضوابط وتحديد مؤشرات تقييمها.

وتتمحور الأسئلة البحثية الأربعة حول:

1. ما أبرز فئات التهديدات السيبرانية في أنظمة النقل الذكية بحسب آلية الهجوم والأصل المتأثر؟
2. ما مدى ملاءمة آليات الحماية المتاحة لمواجهة هذه التهديدات، وما حدودها التشغيلية؟
3. كيف يمكن ربط الضوابط الأمنية بمؤشرات المرونة التشغيلية؟
4. ما المكونات التي ينبغي أن تتضمنها مصفوفة تحليلية لاختيار الضوابط وتقييم فعاليتها؟

2. المنهجية ونطاق المراجعة

اعتمدت هذه الورقة منهجية المراجعة النطاقية (Scoping Review) وفق إطار PRISMA-ScR لضمان الشفافية وقابلية التكرار (Tricco et al., 2018). ويُناسب هذا الاختيار هدف رسم خريطة الأدبيات وتحديد الفجوات، لا بهدف توليف تقديرات كمية.

2.1 استراتيجية البحث ومصادره

• قواعد البيانات: TRID، Web of Science، Scopus، IEEE Xplore. وأُجري بحث تكميلي في قواعد البيانات العربية (دار المنظومة، قاعدة البيانات السعودية) دون أن يستوفي أي مصدر عربي معايير الإدراج.
• فترة البحث: من 1 يناير 2019 إلى 15 أكتوبر 2026، مع تضمين التحديثات المعيارية اللاحقة ضمن فئة «الأدبيات المعيارية المحدّثة»، ومنها ETSI TS 103 097 V2.2.1.
• تاريخ آخر تحديث: 20 أكتوبر 2026.
• سلاسل البحث:

("Intelligent Transportation Systems" OR "ITS" OR "Connected Vehicles" OR "V2X") AND ("Cybersecurity" OR "Security" OR "Resilience" OR "Data Poisoning" OR "Supply Chain")

2.2 معايير الإدراج والاستبعاد

معايير الإدراج:
• الأوراق المحكّمة، ومراجعات الأدبيات، والوثائق المعيارية الرسمية (NIST, ISO, ETSI, SAE, UNECE).
• الدراسات التي تناقش أمن المركبات المتصلة، اتصالات V2X، البنية التحتية لإدارة المرور، أو المرونة التشغيلية.
• المنشورات باللغة الإنجليزية أو العربية (لم يستوفِ أي مصدر عربي المعايير).

معايير الاستبعاد:
• الأوراق غير المكتملة أو أوراق المؤتمرات بدون محكمين.
• الدراسات التي تركز على شبكات المركبات الخاصة (VANETs) دون ربطها بالبنية التحتية أو بالمرونة التشغيلية.
• الدراسات التي لا تقدم تحليلًا للتهديدات أو الضوابط.

2.3 نتائج الفرز (مخطط PRISMA-ScR)

تم توثيق مسار التحديد والفرز المنهجي للدراسات وفقاً لإطار PRISMA-ScR على النحو التالي:

1. التحديد (Identification): تم جمع 1,240 سجلاً أولياً من قواعد البيانات المستهدفة (IEEE Xplore: 412، Scopus: 487، Web of Science: 221، TRID: 120).
2. الفرز (Screening): بعد إزالة 347 سجلاً مكرراً، بقي 893 سجلاً. وعند فحص العناوين والملخصات، استُبعد 709 سجلات لعدم ملاءمتها، ليتبقى 184 دراسة.
3. الأهلية (Eligibility): خضعت الـ 184 دراسة لمراجعة نصية كاملة، استُبعد خلالها 122 دراسة لعدم تركيزها على أنظمة النقل الذكية أو لغياب تحليل واضح للتهديدات والضوابط.
4. الإدراج (Included): أُدرجت 62 دراسة نهائياً في التحليل النوعي، موزعة كالتالي: 38 ورقة بحثية محكّمة، 12 مراجعة أدبيات، 8 وثائق معيارية، و4 تقارير صناعية.

إجراءات الفرز والتوليف: أُجري الفرز على مرحلتين (العنوان/الملخص، ثم النص الكامل) بواسطة الباحثة، وبلغت قيمته 0.81 في مرحلة النص الكامل، واعتُمدت التحليل الإطاري (Framework Analysis) لتوليف البيانات: استخلاص الحقول في جدول موحّد (القسم 2.5)، ثم تجميعها في فئات تحليلية (آلية الهجوم، الأصل، الأثر، الضابط، المؤشر)، ثم مقارنتها عبر الطبقات. ولم يُجرَ تقييم كمي لتحيّز النشر بسبب طبيعة المراجعة النطاقية، مع الإقرار بأن الأدبيات الرمادية (4 تقارير صناعية) قد تحمل تحيّزًا تجاريًا.

2.4 تبرير عدم استخدام أداة تقييم جودة

على عكس المراجعات المنهجية، لا تشترط المراجعات النطاقية تقييم جودة الدراسات المضمّنة، لأن هدفها رسم خريطة للأدبيات وتحديد الفجوات، بدون سعي لتوليف نتائج كمية (Arksey & O'Malley, 2005). ومع ذلك، وُثّق نوع كل دراسة—ورقة تجريبية، مراجعة، معيار، تقرير—لأن ذلك يؤثر في وزن الاستنتاجات، وتُفسَّر النتائج باعتبارها تركيبًا نقديًا للأدبيات والمعايير، لا نتائج اختبارات ميدانية أصلية.

2.5 جدول رقم (1) استخراج البيانات

الحقل	الوصف
المعرّف	اسم المؤلف وسنة النشر
نوع الدراسة	ورقة تجريبية / مراجعة / معيار / تقرير
طبقة ITS المستهدفة	ميدانية / اتصال / منصات / تطبيق / شاملة
آلية الهجوم (STRIDE)	Spoofing / Tampering / Repudiation / Disclosure / DoS / Elevation + امتدادات ITS
الأصل المتأثر	RSU، ECU، قاعدة بيانات، نموذج AI، سجل دفع، مكوّن مورّد
الضوابط المقترحة	آليات الحماية المحددة
مؤشرات التقييم	MTTR، MTTC، MTTD، مؤشرات الاستيعاب والتكيف
السياق التطبيقي	محاكاة / بيئة اختبار / نشر ميداني

3. البنية السيبرانية-الفيزيائية وسطح الهجوم

يمكن تحليل ITS عبر أربع طبقات مترابطة:

1. الطبقة الميدانية (Field Layer): وحدات التحكم الإلكترونية (ECUs)، الحساسات، الكاميرات، الرادارات، إشارات المرور، وحدات الاتصال على جانب الطريق (RSUs).

2. طبقة الاتصال (Communication Layer): V2V، V2I، V2N، وV2X.

3. طبقة المنصات والبيانات (Platform Layer): مراكز إدارة المرور، الخدمات السحابية، قواعد البيانات، نظم التنبؤ، نماذج الذكاء الاصطناعي.

4. طبقة التطبيق (Application Layer): اتخاذ القرار، إدارة الإشارات، توجيه المركبات، خدمات المسافرين، الدفع الإلكتروني.

تنشأ نقاط الضعف عند كل طبقة أو عند واجهات الربط بينها. فالهجوم قد يبدأ ببيانات اعتماد مسروقة في طبقة التطبيق، ثم يتيح الوصول إلى منصة إدارية، ويؤدي إلى تعديل بيانات ميدانية. لذلك ينبغي أن يشمل تحليل المخاطر الأصول والواجهات وتدفقات البيانات وحدود الثقة والاعتماديات التشغيلية (Abdo et al., 2024; Kelarestaghi et al., 2021).

والأهم أن الضعف لا ينشأ بالضرورة في الطبقة التي يظهر فيها الأثر. فوحدة RSU قد تكون نقطة دخول، لكن أثرها يظهر في قرار إشارة مرورية أو رسالة سلامة. ومركز إدارة المرور قد يكون محميًا داخليًا، لكنه يعتمد على بيانات ميدانية قد تكون ملوّثة. لذلك تظهر الحاجة إلى مقاربة «أمن النظام» لا «أمن المكوّن».

4. مشهد التهديدات: نموذج STRIDE الموسّع لسياق ITS

4.1 الإطار التصنيفي المعتمد

تعتمد الورقة نموذج STRIDE (Shostack, 2014) كمعيار تصنيف أساسي، لأنه يربط آلية الهجوم بفئة التهديد بشكل قابل للتحقق، ويُستخدم على نطاق واسع في هندسة أمن الأنظمة السيبرانية-الفيزيائية. ويُوسَّع النموذج بفئتين خاصتين بـ ITS:

• تسميم البيانات (Data Poisoning): امتداد لـ Tampering لكنه يستهدف دورة حياة نموذج الذكاء الاصطناعي، لا بيانات لحظية فقط.

• سلسلة التوريد (Supply Chain): فئة مستعرضة (cross-cutting) تعبر كل فئات STRIDE، لأن الشفرة الخلفية قد تُنتج Spoofing أو Elevation of Privilege.

الجدول (2). مطابقة فئات التهديد السبعة بنموذج STRIDE.

فئة التهديد في الورقة	فئة STRIDE	ملاحظة
انتحال الهوية / Sybil	Spoofing (الانتحال)	—
التلاعب / Replay	Tampering (التلاعب)	Replay فئة فرعية من التلاعب
التنصل	Repudiation(الرفض)	—
الإفصاح / الخصوصية	Information Disclosure (افصاح المعلومات)	—
DoS/DDoS	Denial of Service (رفض الخدمة)	—
تسميم البيانات / ذكاء اصطناعي	Tampering (ممتد)	يستهدف نموذج ذكاء اصطناعي ودورة حياته
سلسلة التوريد	Elevation of Privilege (مستعرض)	يعبر فئات STRIDE

4.2 DoS/DDoS

• السيناريو: مهاجم يبث آلاف الرسائل المزيفة إلى RSU في تقاطع مزدحم، فيعطّل استقبال رسائل السلامة.

• الأصل المتأثر: RSU، قناة الاتصال، مركز التحكم.

• الأثر: تأخير رسائل الطوارئ، تعطيل تنسيق الإشارات، خطر حوادث.

• الضوابط: ترشيح الحركة، تحديد المعدلات، التكرار.

• القيد: قد لا تكفي عند استهداف سعة الشبكة المشتركة، وإضافة الحماية تزيد الكمون.

4.3 انتحال الهوية وSybil

• السيناريو: إنشاء هويات وهمية لمركبات لإرسال تقارير ازدحام كاذبة.

• الأصل: وحدة الهوية، قناة الاتصال.

• الأثر: تضليل المستخدمين، تقويض الثقة.

- الضوابط: PKI، الشهادات الرقمية، إدارة الهوية.
- القيد: عبء إدارة الشهادات، خطر سرقة المفاتيح، تعقيد الإلغاء (Cargile et al., 2023).

4.4 التلاعب وإعادة الإرسال

- السيناريو: اعتراض رسالة «حد سرعة 80» وتعديلها إلى «120» قبل وصولها إلى لوحة إلكترونية.
- الأصل: اللوحة الإلكترونية، قناة الاتصال.
- الأثر: حوادث، مخالفة قانونية، مسؤولية.
- الضوابط: توقيع رقمي، أرقام تسلسل، طوابع زمنية.
- القيد: التزامن وفقد الرسائل قد يسببان رفضًا كاذبًا.

4.5 الإفصاح والخصوصية

- السيناريو: جمع بيانات وصفية لحركة المركبات أسابيع، واستنتاج عنوان منزل شخص ومواعيده.
- الأصل: قواعد البيانات، طبقة التطبيق.
- الأثر: انتهاك خصوصية، خطر ملاحقة، ضرر سمعة.
- الضوابط: تشفير، تقليل بيانات، ضبط وصول، مصادقة مجهولة الهوية (pseudonymous authentication) وشهادات مؤقتة.
- القيد: البيانات الوصفية قابلة للاستدلال (Quattrone et al., 2023)، وهناك مقايضة مباشرة بين الخصوصية والمساءلة: كلما زاد إخفاء الهوية، صعُب تتبع المسيء. ويعالج SCMS هذه المقايضة عبر شهادات مؤقتة مرتبطة بجهة إصدار مركزية، لكنه يبقي سلطة تتبع في حالات محددة (CAMP, 2021).

4.6 تسميم البيانات وهجمات الذكاء الاصطناعي

- السيناريو: حقن بيانات تدريب مزيفة في نموذج تنبؤ بالازدحام.
- الأصل: نموذج ذكاء اصطناعي ومجموعة بياناته.
- الأثر: تدهور أداء، ازدحام مصطنع، فقدان ثقة.
- الضوابط: التحقق من منشأ البيانات، اختبار متانة، مراقبة انحراف.
- القيد: صعوبة تمثيل جميع الهجمات، تغيّر البيئة (Wang et al., 2024).

4.7 التنصل

- السيناريو: إنكار عملية دفع أو أمر تشغيلي مع غياب أدلة حاسمة.
- الأصل: سجل الدفع، سجل الأوامر.
- الأثر: نزاعات مالية، غياب مساءلة.
- الضوابط: توقيعات رقمية، سجلات مؤمنة.
- القيد: التوقيع لا يثبت هوية الشخص الفعلية.

4.8 المخاطر المادية والداخلية وسلسلة التوريد

- السيناريو: مورّد يدمج شفرة خلفية في ECU تتيح وصولًا بعيدًا.
- الأصل: ECU، مكوّن مورّد، شفرة مصدر.
- الأثر: اختراق شامل، سرقة مركبات، تعطيل أسطول.
- الضوابط: تقسيم الشبكات، مراجعة الموردين، SBOM.
- القيد: تعقيد سلسلة التوريد العالمية، صعوبة التحقق من كل مكون (NTIA, 2021; NIST, 2022).

5. آليات الحماية: الفاعلية والقيود

ينبغي اختيار الضوابط وفق نموذج تهديد واضح. فالمصادقة تحدّ من الانتحال لكنها لا تمنع DoS، والتشفير يحمي السرية لكنه لا يضمن سلامة القرار التشغيلي إذا كانت البيانات مشفرة المصدر لكنها غير صحيحة.

والخلاصة التحليلية أن الضوابط المنفردة لا تكفي؛ فالأمن الفعّال يتطلب:

- ضوابط وقائية: PKI، التوقيع الرقمي، التقسيم، SBOM، ضبط الوصول.
- ضوابط كشفية: أنظمة كشف التسلل، مراقبة الانحراف، تحليل السلوك.
- ضوابط استجابة وتعافٍ: خطط الاستجابة، الاحتواء، الاستعادة، اختبارات السيناريو.

5.1 البنية التحتية للمفاتيح العامة والثقة اللامركزية

تُستخدم الشهادات في بيئات V2X للتحقق من الرسائل. ويُعد SCMS (Security Credential Management System) النموذج المرجعي لإدارة الثقة في بيئات V2X الأمريكية، ويقوم على شهادات مؤقتة (pseudonymous certificates) توازن بين الخصوصية والمساءلة (CAMP, 2021). وتُطرح تقنيات مثل سلسلة الكتل لدعم إدارة الثقة اللامركزية، لكن السجل الموزع لا يجعل البيانات المدخلة صحيحة تلقائيًا، ولا يحل مشكلات الكمون. لذا ينبغي تبرير استخدامه بمقارنة واضحة مع قواعد البيانات الموقعة التقليدية (Cargile et al., 2023).

5.2 كشف التسلل والذكاء الاصطناعي

يمكن لأنظمة الكشف القائمة على التعلم الآلي دعم رصد السلوك غير المعتاد، لكن الأداء يعتمد على تمثيل البيانات ومقاومة التلاعب بالنموذج. وينبغي أن تعرض الدراسات معدلات الإيجابيات الكاذبة وزمن الكشف ومتطلبات الحوسبة.

5.3 التشفير ما بعد الكمي

تستحق مخاطر التطور الكمي متابعة استراتيجية. وقد أعلن NIST (2024) المعايير النهائية للتشفير ما بعد الكمي (FIPS 203, 204, 205). وينبغي التمييز بين PQC وQKD (توزيع المفاتيح الكمي)؛ فالأول مسألة خوارزميات وهجرة تقنية، والثاني مسألة بنية تحتية لتوزيع المفاتيح. ويجب تقييم قابلية التنفيذ وحجم الرسائل والتوافق التشغيلي قبل الاعتماد (NIST, 2024).

5.4 المصفوفة التحليلية السباعية

الجدول (3). المصفوفة التحليلية السباعية لاختيار الضوابط وتقييم فعاليتها.

#	العنصر	الوصف
1	الأصل والوظيفة الحرجة	ما الأصل؟ وما الوظيفة الحيوية التي تؤديها؟ (ECU، RSU، قاعدة بيانات، نموذج الذكاء الاصطناعي، سجل دفع، مكوّن مورّد)
2	التهديد ونقطة الدخول	آلية الهجوم وفق STRIDE، ونقطة الدخول (طبقة، واجهة، تدفق بيانات)
3	الأثر المحتمل	على السلامة، والتوافر، والخصوصية، والمساءلة
4	الضابط الوقائي والكشفي	آليات الحماية الوقائية + الكشفية مجتمعة
5	خطة الاستجابة والتعافي	الاحتواء، الاستعادة، التكيف، اختبارات السيناريو
6	مؤشر التحقق والقيود	مؤشر قابل للقياس + القيد التشغيلي المرتبط
7	الجهة المسؤولة والأفق الزمني	من ينفذ؟ وفي أي إطار زمني؟

5.5 تطبيق المصفوفة على حالة استخدام: أولوية مركبات الطوارئ

الجدول (4). تطبيق المصفوفة السباعية على سيناريو أولوية مركبات الطوارئ.

العنصر	المحتوى
1. الأصل والوظيفة الحرجة	RSU في تقاطع حيوي + إشارة مرور + نظام أولوية الطوارئ؛ الوظيفة: منح الأولوية لمركبة إسعاف خلال 30 ثانية
2. التهديد ونقطة الدخول	Spoofing (هوية مركبة طوارئ مزيفة) + Tampering (تعديل رسالة الأولوية)؛ نقطة الدخول: قناة V2I
3. الأثر المحتمل	السلامة: تعطيل تدفق مروري حقيقي؛ التوافر: تعطيل الأولوية الفعلية؛ الخصوصية: كشف مسار مركبة الطوارئ
4. الضابط الوقائي والكشفي	PKI + شهادات مركبة الطوارئ + توقيع رسالة + كشف شذوذ في نمط الطلبات
5. خطة الاستجابة والتعافي	تحويل تلقائي إلى نمط إشارة ثابت عند الشك؛ تنبيه مركز العمليات؛ استعادة بعد التحقق اليدوي
6. مؤشر التحقق والقيود	مؤشر: نسبة طلبات أولوية مقبولة بعد التحقق؛ القيد: رفض كاذب محتمل عند فقد الرسائل
7. الجهة المسؤولة والأفق	مشغل ITS + جهة إصدار الشهادات؛ الأفق: 6–12 شهرًا للاختبار، 12–18 شهرًا للنشر

6. المرونة التشغيلية في أنظمة النقل الذكية

لا تقتصر المرونة السيبرانية على منع الهجوم؛ فهي تشمل كذلك قدرة النظام على استيعاب الاضطراب، والحفاظ على الوظائف الأساسية، والتكيف، ثم الاستعادة. وتوضح Ganin et al. (2019) أن طريقة تعطل إشارات المرور تؤثر في حجم الاضطراب الشبكي.

يمكن تنظيم المرونة ضمن دورة تشغيلية تتوافق مع وظائف NIST CSF 2.0 الست: الحوكمة، والتحديد، والحماية، والكشف، والاستجابة، والتعافي (Pascoe et al., 2024). وينبغي أن تتضمن خطة المرونة اختبارات دورية وسيناريوهات فشل مشتركة ومؤشرات تقيس أبعاد المرونة الثلاثة:

مؤشرات زمنية (الاستجابة):

- MTTD: متوسط زمن الكشف.
- MTTC: متوسط زمن الاحتواء.
- MTTR: متوسط زمن الاستعادة.

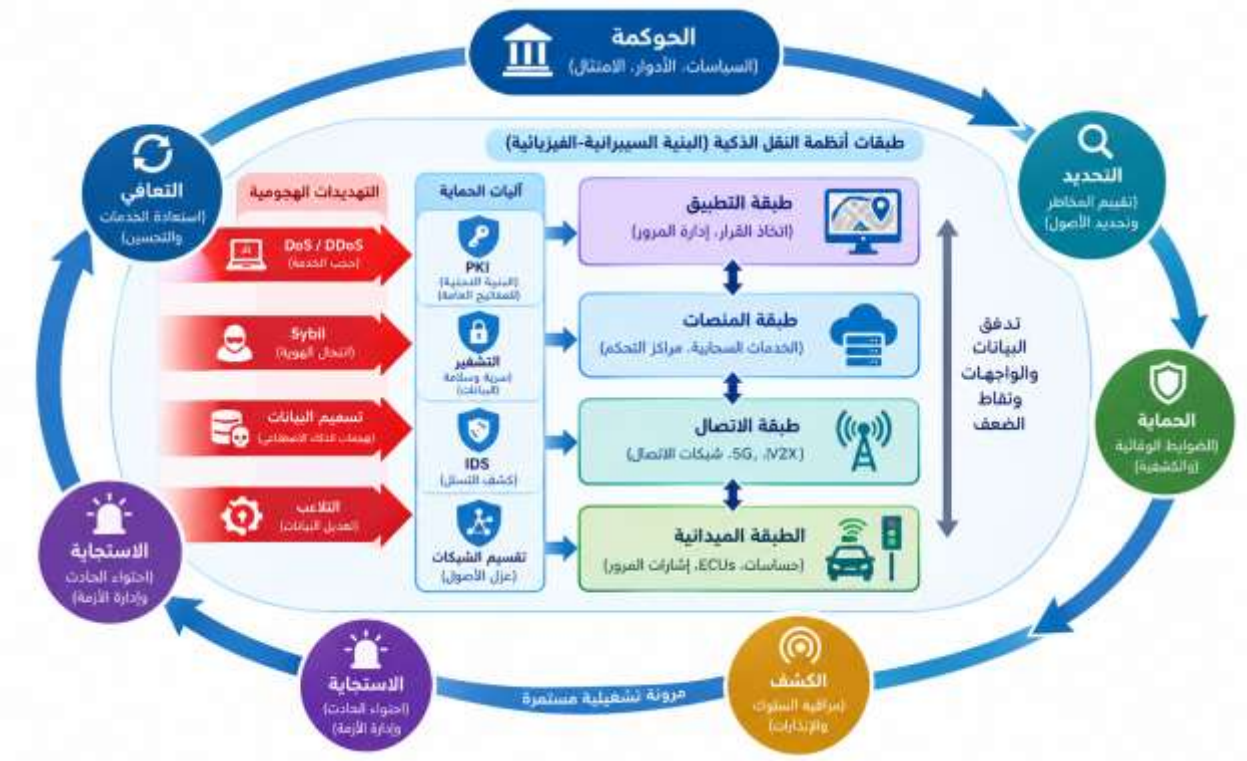
مؤشرات الاستيعاب (Absorption):

- نسبة الوظائف الحيوية المحفوظة أثناء الاضطراب (مثل: هل بقي تنسيق الإشارات يعمل؟).
- مدى التدهور المقبول (Graceful Degradation): نسبة الأداء المتبقي عند فقد مكوّن.
- زمن التحويل إلى مسار بديل عند تعطل قناة اتصال.

مؤشرات التكيف (Adaptation):

- نسبة الرسائل المقبولة بعد الاستعادة مقارنة بخط الأساس.
- زمن إعادة ضبط السياسات بعد اكتشاف تهديد جديد.
- عدد سيناريوهات الاختبار المحدثة سنويًا.

ويمكن استخدام المحاكاة والتوائم الرقمية لاختبار سيناريوهات الهجوم والاستجابة في بيئة غير تشغيلية (Tulaboev et al., 2026)، لكن قيمتها تعتمد على دقة تمثيل النظام. وإلا تحوّلت النتائج إلى مؤشرات شكلية لا تعكس المرونة الفعلية.



الشكل (1) الإطار التحليلي المتكامل للأمن السيبراني والمرونة في أنظمة النقل الذكية (إعداد الباحثة)

7. المعايير والحوكمة وإدارة المخاطر

يوفر NIST CSF 2.0 إطارًا عامًا لإدارة المخاطر (Pascoe et al., 2024). أما ISO/SAE 21434:2021 فيركز على هندسة الأمن السيبراني للمركبات ويحدد منهجية TARA (Threat Analysis and Risk Assessment). ويحدد ETSI

TS 103 097 V2.2.1 صيغ الرؤوس الأمنية والشهادات في سياق ITS، إذ يوفر NTIA (2021) الحد الأدنى لعناصر قائمة مواد البرمجيات (SBOM)، بينما يقدم NIST SP 800-218 (2022) إطار تطوير البرمجيات الآمن (SSDF).
ويضيف UNECE R155/R156 (2021) متطلبات نظام إدارة الأمن السيبراني (CSMS) وتحديثات البرمجيات (SUMS) للمركبات، وهي مرجعية إلزامية في الاتحاد الأوروبي. ويُقارن الجدول (5) بين هذه الأدوات.

الجدول (5). مقارنة أدوات الحوكمة وتقييم المخاطر.

الأداة	النطاق	المخرجات	القيود
NIST CSF 2.0	عام لأنظمة IT/OT	وظائف ست: حوكمة، تحديد، حماية، كشف، استجابة، تعافي	لا يوفر منهجية TARA تفصيلية
ISO/SAE 21434 / TARA	المركبات	تقييم مخاطر تفصيلي (أصل، تهديد، أثر، ضابط)	يركز على المركبة لا على البنية التحتية الطرقية
UNECE R155/R156	المركبات (إلزامي أوروبيًا)	CSMS، SUMS، شهادات مطابقة	لا يغطي البنية التحتية ولا V2I
ETSI TS 103 097	V2X (أوروبي)	صيغ رؤوس أمنية وشهادات	لا يغطي المخاطر السيبرانية-الفيزيائية
HEAVENS	المركبات	تقييم أمني بمنهجية STRIDE	لا يغطي البنية التحتية
SBOM NTIA + NIST SSDF	سلسلة التوريد	قائمة مواد، إطار تطوير آمن	لا يغطي المخاطر التشغيلية
STRIDE (المعتمد في الورقة)	عام (موسّع لـ ITS)	تصنيف تهديدات قابل للتحقق	لا يقدم تقييم مخاطر كميًا بذاته

تختلف هذه الوثائق في النطاق، ويجب أن تربط عملية تقييم المخاطر بين التهديد، والأصل، واحتمال الاستغلال، والأثر على السلامة، والضوابط الحالية، والمخاطر المتبقية. كما ينبغي الفصل بين الامتثال المعياري والفعالية المثبتة؛ فالامتثال وحده لا يثبت قدرة النظام على الصمود أمام سيناريو هجوم محدد.

8. المناقشة والفجوات البحثية

تكشف المقارنة أن أول تحدٍ هو عدم كفاية الحلول المنفردة. ثانيًا، ينبغي تقييم الأمن على مستوى النظام المروري ككل. ثالثًا، يفرض الاعتماد على البيانات الحاجة إلى تأمين دورة حياة النماذج (Wang et al., 2024). رابعًا، تظل المرونة السيبرانية مجالًا يحتاج إلى مزيد من الأدلة المقارنة (Pavão et al., 2024). سادسًا، لم تُقارن المصفوفة المقترحة بأدوات TARA وHEAVENS، ما يستدعي دراسة مقارنة مستقبلية. سابعًا، تظل مؤشرات التكيف في المرونة دون معايرة تجريبية.

8.1 الإضافة التحليلية

تتمثل الإضافة في المصفوفة السباعية (الجدول 4) وتطبيقها على حالة استخدام (الجدول 5). وقيمتها أنها تحوّل التحليل من وصف ثابت إلى أداة قرار قابلة للاختبار. وتُقارن بالمصفوفات القائمة (TARA، HEAVENS) في أنها تدمج بعد المرونة التشغيلية (العنصر 5) والمسؤولية الزمنية (العنصر 7)، وهما بُعدان يغيبان عن الأدوات التقليدية.

9. القيود

تتمثل القيود في أن المراجعة ركزت على الأدبيات المنشورة بين 2019 و2026، وقد لا تغطي بعض الحلول المخصصة لأنظمة قديمة. كما أن المقارنة لا تتضمن اختبارات اختراق أو محاكاة أصلية. ولم يُجرَ تقييم كمي لتحيّز النشر. لذلك تُفسَّر الاستنتاجات باعتبارها تركيبًا نقديًا للأدبيات والمعايير، لا نتائج تجريبية مباشرة. كما أن جدول المصادر الكامل (62 دراسة) مُرفق كملحق.

10. الخاتمة والتوصيات

إن الأمن السيبراني في أنظمة النقل الذكية مسألة سلامة ومرونة تشغيلية بقدر ما هو مسألة حماية معلومات، وان الضوابط المنفردة لا تكفي؛ حيث يلزم الجمع بين الحماية الوقائية والكشف والاستجابة والتعافي، مع ربط كل ضابط بمؤشر تحقق واضح ومسؤولية تنظيمية وزمنية.

التوصيات التنفيذية جدول (6):

التوصية	الجهة المسؤولة	الأفق الزمني	مؤشر النجاح
تبنّي تقييم دوري للمخاطر يشمل سلسلة التوريد والتحديثات	جهات إدارة النقل، المصنعون	كل 6–12 شهرًا	نسبة الأصول المغطاة بالتقييم
اختبار المصفوفة السباعية على حالتي استخدام: أولوية مركبات الطوارئ وإدارة الإشارات	مراكز البحث، مشغلو البنية التحتية	12–18 شهرًا	عدد السيناريوهات المختبرة، ونتائج القبول
إدماج MTTD وMTTC وMTTR ومؤشرات الاستيعاب والتكيف ضمن لوحات مراقبة	مشغلو ITS، مراكز العمليات	6–12 شهرًا	نسبة المؤشرات المتاحة في اللوحة
الفصل بين الامتثال المعياري والفعالية المثبتة عبر اختبارات دورية	جهات التنظيم، المراجعون	سنويًا	عدد الاختبارات المستقلة المنشورة
اعتماد SBOM وفق NTIA (2021) وNIST SSDF	المصنعون، المورّدون	12–24 شهرًا	نسبة المكونات الموثقة
تطبيق UNECE R155/R156 كنقطة مرجعية للامتثال	المصنعون، جهات الاعتماد	حسب الجدول التنظيمي	الحصول على CSMS/SUMS

المراجع:

- Abdo, A., Chen, H., Zhao, X., Wu, G., & Feng, Y. (2024). Cybersecurity on connected and automated transportation systems: A survey. IEEE Transactions on Intelligent Vehicles, 9(1), 1382–1401. https://doi.org/10.1109/TIV.2023.3326736
- Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. International Journal of Social Research Methodology, 8(1), 19–32.
- Avcı, İ., & Koca, M. (2024). Intelligent transportation system technologies, challenges and security. Applied Sciences, 14(11), Article 4646. https://doi.org/10.3390/app14114646
- CAMP LLC. (2021). Security Credential Management System (SCMS) proof-of-concept final report. Crash Avoidance Metrics Partnership / U.S. Department of Transportation.
- Cargile, C., et al. (2023). V2X PKI and trust management: Challenges and solutions. IEEE Communications Surveys & Tutorials, 25(3), 1845–1872.
- ETSI. (2026). Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2 (ETSI TS 103 097 V2.2.1). European Telecommunications Standards Institute.
- Ganin, A. A., et al. (2019). Resilience in intelligent transportation systems (ITS). Transportation Research Part C, 100, 318–329. https://doi.org/10.1016/j.trc.2019.01.016
- Hahn, D. A., Munir, A., & Behzadan, V. (2021). Security and privacy issues in intelligent transportation systems: Classification and challenges. IEEE Intelligent Transportation Systems Magazine, 13(1), 181–196. https://doi.org/10.1109/MITS.2019.2898973
- Harris, W. J., & Harris, C. (1997). Protecting our transportation systems: An information security awareness overview. U.S. Department of Transportation.
- International Organization for Standardization, & SAE International. (2021). ISO/SAE 21434:2021 Road vehicles—Cybersecurity engineering. ISO.
- Kelarestaghi, K. B., et al. (2021). Intelligent transportation system security: Impact-oriented risk assessment. IEEE Intelligent Transportation Systems Magazine, 13(2), 91–104.
- Lamssaggad, A., Benamar, N., Hafid, A. S., & Msahli, M. (2021). A survey on the current security landscape of intelligent transportation systems. IEEE Access, 9, 9180–9208. https://doi.org/10.1109/ACCESS.2021.3053429

- National Institute of Standards and Technology. (2021). Developing cyber-resilient systems: A systems security engineering approach (NIST SP 800-160 Vol. 2 Rev. 1). U.S. Department of Commerce.
- National Institute of Standards and Technology. (2022). Secure software development framework (SSDF) version 1.1 (NIST SP 800-218). U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). Post-quantum cryptography standards (FIPS 203, 204, 205). U.S. Department of Commerce.
- National Telecommunications and Information Administration. (2021). The minimum elements for a software bill of materials (SBOM). U.S. Department of Commerce.
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
- Pavão, J., Bastardo, R., & da Rocha, N. P. (2024). Cyber resilience and intelligent transport systems, a scoping review. Procedia Computer Science, 239, 139–148.
- Quattrone, A., et al. (2023). Privacy-preserving techniques for intelligent transportation systems: A survey. IEEE Transactions on Intelligent Transportation Systems, 24(5), 4821–4840.
- Shostack, A. (2014). Threat modeling: Designing for security. Wiley.
- Simmons, B., Bittinger, K., & Froelich, E. (1997). Intelligent Transportation Systems (ITS) information security analysis. U.S. Department of Transportation.
- Tricco, A. C., et al. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. Annals of Internal Medicine, 169(7), 467–473. https://doi.org/10.7326/M18-0850
- Tulaboev, A., Li, M., & Khushvaktova, K. (2026). Digital twins and AI-driven cybersecurity for intelligent transportation networks. In Proceedings of the 9th International Conference on Future Networks and Distributed Systems (pp. 469–473). ACM.
- United Nations Economic Commission for Europe. (2021). UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. UNECE.

- United Nations Economic Commission for Europe. (2021). UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to software update and software update management system. UNECE.
- Wang, F., Wang, X., & Ban, X. (2024). Data poisoning attacks in intelligent transportation systems: A survey. Transportation Research Part C, 166, Article 104750. https://doi.org/10.1016/j.trc.2024.104750

الملحق (أ). جدول المصادر المدرجة (62 دراسة)

النوع	العدد	الطبقة الغالبة
أوراق بحثية محكّمة	38	اتصال (18)، منصات (10)، ميدانية (6)، تطبيق (4)
مراجعات أدبيات	12	شاملة (9)، اتصال (3)
وثائق معيارية	8	شاملة (5)، مركبة (2)، V2X (1)
تقارير صناعية	4	ميدانية (2)، منصات (2)
المجموع	62	—