v.2, n.1, 2026

REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

REVISÃO CRÍTICA NARRATIVA DO ESTADO DA ARTE DA ISO/SAE 21434: EVOLUÇÃO CIENTÍFICA, REQUISITOS, APLICAÇÕES, LIMITAÇÕES E PERSPECTIVAS DA CIBERSEGURANÇA AUTOMOTIVA

A CRITICAL NARRATIVE STATE-OF-THE-ART REVIEW OF ISO/SAE 21434: SCIENTIFIC EVOLUTION, REQUIREMENTS, APPLICATIONS, LIMITATIONS AND PROSPECTS FOR AUTOMOTIVE CYBERSECURITY

REVISIÓN CRÍTICA NARRATIVA DEL ESTADO DEL ARTE DE LA ISO/SAE 21434: EVOLUCIÓN CIENTÍFICA, REQUISITOS, APLICACIONES, LIMITACIONES Y PERSPECTIVAS DE LA CIBERSEGURIDAD AUTOMOTRIZ

Alexandre Lopes[1], Angelo Machado de Souza[2], Davis Souza Alves[3]

e2140
https://doi.org/10.67553/sol21.v.2i1.40

PUBLICADO: 10/2026

RESUMO

A ISO/SAE 21434 organiza a engenharia de cibersegurança automotiva, cuja relação com a literatura precisa ser examinada junto aos métodos de análise de riscos, controles técnicos e evidências de aplicação. Este artigo apresenta uma revisão crítica narrativa de estado da arte, com busca web orientada por temas e seleção intencional, sobre publicações de janeiro de 2016 a 12 de setembro de 2026. O corpus reúne 28 estudos, analisados por problema, método, resultado e alcance da validação: 19 com consulta dirigida ao texto completo, sete por resumo ou material de apresentação e dois por metadados e documentação dos autores. A descoberta inicial não é integralmente reproduzível e a consulta normativa é parcial. Os antecedentes selecionados desenvolveram modelos de risco, detecção de intrusões e atualização segura. A literatura posterior examinada adapta a análise de ameaças e avaliação de riscos (Threat Analysis and Risk Assessment, TARA), automatiza artefatos e estrutura argumentos de *assurance* e sua manutenção entre fornecedores e versões do produto. Experimentos em redes veiculares e carregamento elétrico fornecem evidência técnica específica; avaliações de processo concentram-se em exemplos, estudos de caso e participação de especialistas. As lacunas do corpus dizem respeito à reprodutibilidade das decisões de risco, representatividade dos testes e atualização distribuída das evidências. Os estudos não estabelecem equivalência entre conformidade normativa, completude da análise e eficácia operacional. A agenda proposta combina avaliação adversarial, comparação independente de métodos e acompanhamento longitudinal de mudanças no produto.

PALAVRAS-CHAVE: ISO/SAE 21434. Cibersegurança automotiva. TARA. A*ssurance.* Revisão crítica narrativa.

---

[1] Fundador e CEO, lidero o direcionamento estratégico global do grupo, a consolidação das operações regionais e o desenvolvimento de parcerias internacionais, atuando diretamente junto a C-Levels e Conselhos na tomada de decisões críticas de governança e expansão.

[2] Profissional Especialista em Segurança da Informação | Cibersegurança | Governança de TI | Privacidade de Dados, na área de Tecnologia da Informação, com ênfase em Segurança da Informação, Governança de TI e Privacidade de Dados. Foco estratégico na proteção de ativos digitais e no fortalecimento da resiliência cibernética frente aos desafios do ambiente digital atual. Mestrado em Segurança da Informação pela Florida Christian University, com pesquisa voltada à conformidade com a LGPD. MBA em Gerenciamento de Projetos de TI e certificações internacionais, como Certified Information Security Officer (CISO), ISO/IEC 27001 Lead Implementer e DPO – EXIN. Competência comprovada em: Conformidade com normas e legislações: ISO/IEC 27001, ISO 27002, LGPD, ITIL, ISO 31000, ISO 27005. Gestão de riscos e implementação de controles e políticas de segurança. Resposta a incidentes, análise de ameaças e continuidade de negócios. Coordenação de projetos de cibersegurança e gestão de equipes técnicas. Apoio a auditorias, criação de planos diretores de tecnologia (PDTI) e campanhas de conscientização. Alinhamento entre TI, compliance e objetivos de negócio, com forte habilidade de comunicação com stakeholders.

[3] Doutor em Administração de TI - Ph.D na Florida Christian University (EUA), Mestre em Administração com foco em TI Verde, Extensão em Gestão de TI pela FGV/SP, Pós-graduado em Gerenciamento de Projeto), Graduado em Redes de Computadores e Internet. Possui as certificações PMP®, ITIL® Expert, C|EH®, ITIL® Professional (4 MP), COBIT®, ISO-20000®, ISO-27002®, EXIN® Agile Scrum Master, Lean IT, Green IT, ICS MCSA® Windows Server 2003, Cloud Computing, EXIN® Data Protection Officer (DPO), & EXIN ISO-27001 Professional (ISMP), Cyber Security, CompTIA Security+, EC-Council Certified Ethical Hacker, Psicanalista, CompuTIA Security+, DAC® Wireless, DCP® Switching, DSS® IP Surveillance. É consultor de Gestão de Sustentabilidade de TI, com produtos e consultorias em Green IT para órgãos públicos municipais do Brasil, além de Consultor em Privacidade de Dados (LGPD).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

ABSTRACT
ISO/SAE 21434 provides a framework for automotive cybersecurity engineering, whose relationship with the literature needs to be examined alongside risk assessment methods, technical controls and application evidence. This paper presents a critical narrative state-of-the-art review based on theme-guided web searches and purposive selection, covering publications from January 2016 to September 12, 2026. The corpus comprises 28 studies assessed by problem, method, result and validation scope: 19 through targeted full-text consultation, seven through abstracts or presentation material, and two through metadata and author documentation. Initial discovery is not fully reproducible, and access to normative content is partial. The selected earlier studies developed risk models, intrusion detection and secure updates. The selected later literature adapts threat analysis and risk assessment (TARA), automates artifacts, structures assurance arguments and examines their maintenance across suppliers and product versions. Vehicle-network and electric-charging experiments provide specific technical evidence; process evaluations largely rely on examples, case studies and expert participation. Evidence gaps within the corpus concern reproducible risk decisions, representative testing and distributed maintenance of evidence. The studies do not establish equivalence between normative compliance, analytical completeness and operational effectiveness. The proposed research agenda combines adversarial evaluation, independent method comparisons and longitudinal observation of product changes.

KEYWORDS: *ISO/SAE 21434. Automotive cybersecurity. TARA. Assurance. Critical narrative review.*

RESUMEN
La ISO/SAE 21434 organiza la ingeniería de ciberseguridad automotriz, cuya relación con la literatura debe examinarse junto con los métodos de análisis de riesgos, los controles técnicos y las evidencias de aplicación. Este artículo presenta una revisión crítica narrativa del estado del arte, con búsqueda web orientada por temas y selección intencional, sobre publicaciones de enero de 2016 al 12 de septiembre de 2026. El corpus comprende 28 estudios analizados por problema, método, resultado y alcance de la validación: 19 mediante consulta dirigida del texto completo, siete mediante resúmenes o material de presentación y dos mediante metadatos y documentación de los autores. La fase inicial de descubrimiento no es íntegramente reproducible y el acceso al contenido normativo es parcial. Los antecedentes seleccionados desarrollaron modelos de riesgo, detección de intrusiones y actualización segura. La literatura posterior examinada adapta el análisis de amenazas y evaluación de riesgos (Threat Analysis and Risk Assessment, TARA), automatiza artefactos y estructura argumentos de aseguramiento y su mantenimiento entre proveedores y versiones del producto. Los experimentos en redes vehiculares y carga eléctrica aportan evidencia técnica específica; las evaluaciones de procesos se concentran en ejemplos, estudios de caso y participación de especialistas. Las lagunas del corpus conciernen a la reproducibilidad de las decisiones de riesgo, la representatividad de las pruebas y la actualización distribuida de las evidencias. Los estudios no establecen equivalencia entre conformidad normativa, completitud del análisis y eficacia operativa. La agenda propuesta combina evaluación adversarial, comparación independiente de métodos y seguimiento longitudinal de cambios en el producto.

PALABRAS CLAVE: *ISO/SAE 21434. Ciberseguridad automotriz. TARA. Aseguramiento. Revisión crítica narrativa.*

1 INTRODUÇÃO

A cibersegurança automotiva envolve tanto a resistência de componentes e interfaces a ataques quanto a capacidade de justificar e atualizar decisões de engenharia. Um sistema de detecção de intrusões (intrusion detection system, IDS) pode apresentar bons resultados no

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

experimento e falhar diante de outro adversário. Um processo pode produzir os documentos previstos sem demonstrar que as hipóteses usadas continuam válidas. A comparação entre identificação temporal de unidades eletrônicas de controle (electronic control units, ECUs), ataques de evasão e métodos de asseguramento de cibersegurança (*assurance*) torna essa diferença observável na literatura (Cho; Shin, 2016; Ying *et al.*, 2019; Mohamad *et al.*, 2023).

Segundo o catálogo oficial da ISO, a ISO/SAE 21434, publicada em 2021, estabelece requisitos de engenharia para gestão de riscos cibernéticos no ciclo de vida de sistemas elétricos e eletrônicos (E/E) veiculares, sem prescrever tecnologias específicas. O catálogo mantém a edição de 2021 como publicada e registra revisão sistemática da norma iniciada em julho de 2026; esse procedimento normativo não corresponde a uma nova edição nem ao desenho desta revisão da literatura (ISO; SAE International, 2021).

O problema de pesquisa é delimitar quais evidências do corpus sustentam os métodos e controles relacionados à ISO/SAE 21434 e até onde seus resultados permitem concluir sobre aplicação e eficácia. A revisão crítica narrativa de estado da arte se justifica pela necessidade de distinguir requisitos de processo, contribuições acadêmicas e demonstrações técnicas. O objetivo geral é explicar como esse conhecimento se articula nos estudos selecionados e quais problemas permanecem abertos nesse conjunto. Os objetivos específicos são examinar antecedentes da norma, comparar métodos e aplicações, analisar o alcance das validações e identificar lacunas sustentadas pelo corpus. A análise combina estudos explicitamente dedicados à ISO/SAE 21434 e trabalhos técnicos cuja relação com suas atividades é estabelecida retrospectivamente. Essa distinção evita atribuir conformidade a pesquisas que antecedem a publicação da norma.

A busca web orientada por temas e a seleção intencional são organizadas em quatro questões centrais, formuladas no Quadro 1 e relacionadas às seções, estudos, tabelas e sínteses que as respondem. Elas cobrem antecedentes e evolução, análise de ameaças e avaliação de riscos (Threat Analysis and Risk Assessment, TARA) e processos, integração normativa, aplicações e validação, limites das evidências e perspectivas de pesquisa. A contribuição é uma síntese comparativa de um corpus delimitado. Não se pretende estimar toda a produção mundial nem realizar uma auditoria de conformidade normativa.

2 REFERENCIAL TEÓRICO

2.1 Antecedentes e formação do campo

No início do período analisado, a literatura já discutia questões de engenharia, além de demonstrar ataques. SAE J3061:2016 oferece orientação de alto nível para um ciclo de vida de cibersegurança. No mesmo ano, Macher *et al.* revisam métodos de análise de ameaças e riscos em relação ao contexto automotivo e às interfaces com segurança funcional. Como seu texto completo

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

não foi obtido, esse estudo sustenta a localização histórica do debate, sem permitir reproduzir sua seleção bibliográfica (SAE International, 2016; Macher *et al.*, 2016).

Islam *et al.* apresentam um precursor do modelo HEAVENS que relaciona ativos e ameaças, combina avaliações de ameaça e impacto e deriva requisitos. O exemplo de limitador de velocidade mostra a passagem da análise para requisitos de alto nível; seleção e implementação das contramedidas ficam fora do escopo declarado. A contribuição antecede a ISO/SAE 21434 e não demonstra atendimento à sua edição final (Islam *et al.*, 2016).

EVITA constitui um antecedente anterior ao recorte, discutido aqui por meio de estudos elegíveis. Sua influência aparece na avaliação do potencial de ataque e em modelos de arquitetura. Plappert *et al.* revisitam pressupostos tecnológicos ao tratar superfícies de ataque contemporâneas. Assim, a continuidade entre modelos antigos e recentes exige reavaliar premissas sobre acesso, recursos do atacante e mecanismos de proteção, em vez de reutilizar classificações sem exame (Plappert *et al.*, 2021).

Também em 2016, a identificação de ECUs por características temporais e a arquitetura Uptane tratavam, respectivamente, detecção na rede *Controller Area Network* (CAN) e atualização segura. São linhas técnicas que coexistem com o desenvolvimento dos processos. A posterior publicação da norma oferece uma linguagem para relacionar essas contribuições ao ciclo de vida; não é evidência de que tenha causado seu surgimento (Cho; Shin, 2016; Kuppusamy *et al.*, 2016).

2.2 Processos e conceitos da ISO/SAE 21434

Na amostra autorizada, o escopo da ISO/SAE 21434 abrange sistemas E/E de veículos de produção em série, componentes e interfaces, cujo desenvolvimento ou modificação se inicia após a publicação. Sistemas externos, como servidores back-end, podem integrar o contexto considerado, mas não passam automaticamente a pertencer ao escopo normativo. A Tabela 1 resume a estrutura descrita na amostra, sem reconstruir as disposições completas indisponíveis (ISO; SAE International, 2021).

Tabela 1. Estrutura da ISO/SAE 21434 descrita na amostra autorizada.

Cláusulas	Descrição resumida na amostra autorizada
5 e 6	Gestão organizacional e gestão por projeto
7	Atividades distribuídas entre cliente e fornecedor
8	Atividades contínuas e gestão de vulnerabilidades
9	Conceito, riscos e requisitos do item
10 e 11	Desenvolvimento, verificação e validação no veículo
12	Produção e montagem

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Cláusulas	Descrição resumida na amostra autorizada
13 e 14	Operação, manutenção, fim do suporte e descomissionamento
15	Métodos de análise de ameaças e avaliação de riscos

Fonte: síntese da estrutura descrita na amostra autorizada (ISO; SAE International, 2021). A identificação das cláusulas não implica consulta às suas disposições completas.

Na amostra autorizada, *cybersecurity goal* é um requisito no conceito associado a cenários de ameaça; *cybersecurity claim* é uma declaração sobre risco; *cybersecurity case* reúne argumento e evidências sobre riscos não desarrazoados. Os produtos de trabalho (*work products*) registram resultados das atividades. A amostra também distingue requisitos, recomendações e permissões e esclarece que a ordem das cláusulas não estabelece sequência obrigatória de execução (ISO; SAE International, 2021).

A interpretação de engenharia exige separar esses conceitos do formato usado para implementá-los. Dobaj *et al.* propõem um desenvolvimento iterativo centrado em modelagem de ameaças, com ações e produtos de trabalho demonstrados em direção assistida. O estudo ajuda a relacionar requisitos e níveis de arquitetura, mas seus artefatos são uma proposta dos autores. Embora publicado no volume de 2023, teve publicação *online* em 2021 e discute a norma como então emergente (Dobaj *et al.*, 2023).

A definição de acordo de interface de cibersegurança (*cybersecurity interface agreement*) entre cliente e fornecedor está confirmada na amostra autorizada. Segundo Grimm *et al.*, a dificuldade prática é manter coerentes as hipóteses do fornecedor e aquelas assumidas na integração do veículo. Os autores propõem gestão de TARA entre sistemas, organizações e fases. A crítica é sobre a explicitação e coordenação do processo; não autoriza afirmar que a norma desconhece vulnerabilidades, monitoramento ou resposta a incidentes (ISO; SAE International, 2021; Grimm *et al.*, 2023).

2.3 TARA e métodos de análise de riscos

Nos métodos analisados, a definição do item delimita funções, interfaces e contexto. A análise relaciona ativos às propriedades comprometidas e aos cenários de dano (*damage scenarios*). Cenários de ameaça (*threat scenarios*) descrevem ameaças pertinentes; caminhos de ataque (*attack paths*) representam ações necessárias à sua realização. A classificação do impacto e a viabilidade do ataque (*attack feasibility*) sustentam a determinação do risco e a decisão de tratamento. Essa exposição sintetiza os métodos estudados; não transcreve a cláusula 15 nem estabelece uma ordem normativa de execução (Lautenbach; Almgren; Olovsson, 2021; Plappert *et al.*, 2021).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

A viabilidade caracteriza a facilidade de realizar um caminho. Transformá-la em probabilidade observada exige outro modelo e dados que sustentem a conversão. Essa diferença é visível em Plappert *et al.*: controles alteram a categoria de viabilidade nos exemplos, mas a alteração não mede uma redução observada de incidentes. O trabalho utiliza o projeto de norma internacional (Draft International Standard, DIS) de 2020; seu alinhamento declarado não deve ser reclassificado como avaliação da edição final (Plappert *et al.*, 2021).

Tabela 2. Métodos e função na análise de riscos.

Abordagem e estudos	Função	Limite de interpretação
HEAVENS e HEAVENS 2.0, Islam e Lautenbach	Relacionar ativos, ameaças, impacto e decisões	Propostas externas; conformidade declarada não é certificação
SARA, Monteuuis *et al.*	Ampliar modelagem para direção autônoma e privacidade	Casos específicos; resumo consultado
STRIDE e árvores/grafos, Lautenbach et al.	Classificar ameaças e representar caminhos	Não constituem, isoladamente, TARA completa
THREATGET e SOA, Chlup e Dantas	Gerar ameaças e caminhos a partir de modelos	Cobertura depende das entradas e regras
Redes Bayesianas, Comert *et al.*	Representar dependências probabilísticas	*Preprint*; parâmetros não são frequências de frota
Inteligência artificial (IA), Ahmad et al.	Apoiar classificação de ameaças e viabilidade	Validação detalhada não verificada no acesso disponível

Fonte: síntese dos métodos e estudos citados na seção 2.3; não representa validação comparativa independente. SOA: service-oriented architecture (arquitetura orientada a serviços).

HEAVENS 2.0 explicita a adaptação de um método à nova referência normativa: Lautenbach, Almgren e Olovsson propõem alterações para tratar diferenças em relação à ISO/SAE 21434 e limitações do modelo anterior. O exemplo deriva objetivos ligados a autenticação, *replay* e adulteração. Esse resultado mostra a utilidade de um procedimento para produzir decisões rastreáveis; sua eficácia depende da qualidade dos ativos, cenários e premissas informados (Lautenbach; Almgren; Olovsson, 2021).

SARA (*Security* Automotive Risk Analysis) acrescenta questões de vinculabilidade (linkability) e confusão em veículos autônomos e demonstra o método em casos de rastreamento e frenagem. A consulta ao resumo permite caracterizar essa ampliação, mas não comparar rigorosamente sua cobertura com HEAVENS. Tampouco se pode assumir que diferenças de terminologia correspondam a superioridade de um método (Monteuuis *et al.*, 2018).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) organiza tipos de ameaça; árvores e grafos representam combinações e dependências. Sua utilização deve ser avaliada pela pergunta que ajudam a responder. A discussão de HEAVENS 2.0 inclui abordagens baseadas em potencial de ataque e no Common Vulnerability Scoring System (CVSS). O corpus não contém uma validação autônoma suficiente para eleger CVSS como medida geral de risco automotivo. Uma pontuação de vulnerabilidade não substitui a análise dos danos do item (Lautenbach; Almgren; Olovsson, 2021).

Como contraponto, Comert, Chowdhury e Nicol empregam redes Bayesianas para examinar vulnerabilidade e efeitos no desempenho de sistemas de transporte e controle cooperativo. Os exemplos numéricos mostram como dependências e redundância alteram resultados do modelo. O trabalho permanece identificado como *preprint*: não foi localizada uma versão revisada correspondente. Sua quantificação probabilística é externa à norma e não calibra automaticamente escalas qualitativas de TARA (Comert; Chowdhury; Nicol, 2020).

Tratamento de risco, *cybersecurity goals* e *cybersecurity claims* também não são intercambiáveis. Um objetivo orienta requisitos de proteção; uma declaração pode justificar a posição adotada diante de um risco. O resultado precisa conservar premissas e vínculos com a análise, para que uma mudança no item permita reconhecer decisões que deixaram de ser sustentadas. Esta é uma inferência da revisão a partir da integração entre métodos de TARA, desenvolvimento e *assurance*, e não um requisito específico verificado nas cláusulas não consultadas (Islam *et al.*, 2016; Dobaj *et al.*, 2023; Mohamad *et al.*, 2023).

2.4 Relação com normas e regulamentos

CSMS (Cyber *Security* Management System) designa o sistema de gestão de cibersegurança; SUMS (Software Update Management System), o sistema de gestão de atualizações de software. OTA (over-the-air) identifica a modalidade de atualização remota sem fio. A Tabela 3 distingue o objeto dos documentos oficiais acessíveis, sem presumir sua aplicação automática a uma jurisdição.

Tabela 3. Natureza e relação dos documentos examinados.

Documento	Natureza	Distinção necessária
SAE J3061:2016	Prática recomendada e guia	Antecedente; catálogo também mantém edição estabilizada de 2021
ISO/SAE 21434:2021	Norma internacional	Requisitos de engenharia segundo catálogo e amostra; não equivale a homologação
UN R155	Regulamento ONU	Distingue certificado do CSMS e aprovação do tipo veicular

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Documento	Natureza	Distinção necessária
UN R156	Regulamento ONU	Trata SUMS e atualizações; não se restringe a OTA
ISO 26262	Série de segurança funcional	Comportamento defeituoso e perigos; objeto complementar
ISO/PAS 5112:2022	Especificação publicamente disponível	Orientação para auditoria de CSMS; não para *cybersecurity assessments*
ISO/DTS 5112	Projeto de especificação técnica	Projeto em aprovação na consulta registrada; não é edição final publicada

Fonte: catálogos e documentos oficiais citados na seção 2.4; versões e limites de acesso descritos no texto.

A J3061 de 2016 permanece relevante como antecedente bibliográfico, enquanto seu registro SAE de 2021 aparece como estabilizado. Esses estados documentais não devem ser reduzidos à afirmação genérica de que o guia foi simplesmente retirado (SAE International, 2016; SAE International, 2021).

Na reprodução oficial da UN R155 consultada, certificado de CSMS e aprovação do tipo veicular são atos distintos. Processos de gestão de riscos, dependências de fornecedores, testes e acompanhamento pós-produção integram a análise regulatória. Esta revisão interpreta que a ISO/SAE 21434 pode apoiar a organização dessas evidências; a conformidade declarada à norma não substitui os atos e verificações do regulamento. A entrada em vigor internacional de R155 ocorreu em janeiro de 2021, o que não se confunde com aplicação por cada jurisdição (UNECE, 2025; United Nations, 2026b).

A reprodução de R156 consultada contempla gestão de atualizações, identificação de versões, compatibilidade, autenticidade e integridade, com disposições adicionais para OTA. Ela é de 2021. Uma notificação oficial confirma emenda vigente desde 4 de junho de 2026, cujo conteúdo material não foi recuperado. A análise não apresenta a reprodução antiga como versão consolidada até o corte da revisão (UNECE, 2021; United Nations, 2026a).

A parte de vocabulário da ISO 26262 foi consultada por catálogo, sem substituir a leitura das demais partes da série. Sua relação com cibersegurança é examinada pelos estudos de coanálise, preservando a diferença entre perigos associados a comportamento defeituoso e cenários de ataque (ISO, 2018; Li *et al.*, 2024).

A ISO/PAS 5112:2022 orienta auditorias organizacionais de CSMS e explicita que não fornece orientação para *cybersecurity assessments*. Seu sucessor ISO/DTS 5112 estava em aprovação em 12 de setembro de 2026. Confundir PAS publicada, projeto DTS e especificação final produziria um requisito documental inexistente na data da consulta (ISO, 2022; ISO, 2026).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

3 METODOLOGIA

3.1 Desenho, recorte e elegibilidade

Desenho e recorte. Foi conduzida uma revisão crítica narrativa de estado da arte, com busca web orientada por temas e seleção intencional. O período coberto compreende 1º de janeiro de 2016 a 12 de setembro de 2026. A unidade de análise é o estudo, e não cada arquivo ou versão recuperada. Documentos normativos e regulatórios foram examinados separadamente e não integram a contagem dos 28 estudos.

Critérios de inclusão: trabalhos identificáveis por título, autoria e fonte, dentro do recorte, que tratassem de cibersegurança automotiva, análise de riscos, controles, *assurance* ou processos de engenharia e permitissem caracterizar ao menos a contribuição e seu escopo. O corpus reúne artigos de periódicos e eventos, um documento técnico de evento e um *preprint* explicitamente identificado. Critérios de exclusão: fontes promocionais, registros sem identificação suficiente e versões duplicadas. O texto completo não foi condição obrigatória de inclusão; a profundidade da análise foi limitada pelo material consultado. Essa decisão introduz assimetria de evidência entre os estudos.

3.2 Descoberta, confirmação e tratamento das versões

Mecanismo de descoberta e fontes de confirmação. A descoberta ocorreu pelo mecanismo de busca web disponível no ambiente de trabalho, cuja identificação específica não está informada nos materiais disponíveis. Seguiu-se consulta a registros ou textos de SpringerLink, ACM, SAE Mobilus, MDPI, PLOS, SCITEPRESS, USENIX e NDSS, além de repositórios institucionais e autorais e de fontes oficiais da ISO, SAE, ONU e EUR-Lex. IEEE Xplore apresentou restrições de acesso; conforme o estudo, utilizaram-se metadados depositados pela editora no Crossref e manuscritos autorais. Não foram pesquisados diretamente Scopus, Web of Science, ScienceDirect ou Google Scholar. Essas plataformas editoriais e fontes de confirmação não são apresentadas como bases bibliográficas submetidas a uma estratégia de busca estruturada.

Tabela 4. Frentes temáticas de descoberta e fontes de confirmação.

Frente	Expressões orientadoras	Materiais e fontes de confirmação
Norma e processos	“ISO/SAE 21434”; “SAE J3061”; *cybersecurity assurance*; CSMS	Documentos oficiais e estudos de implementação
Riscos	(“*automotive*” AND “*risk assessment*”); TARA; HEAVENS; *model-based*; *automation*	Editora, repositório institucional e DOI

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Frente	Expressões orientadoras	Materiais e fontes de confirmação
Controles e aplicações	CAN IDS; SOME/IP; V2X; OTA; *electric vehicle charging*; *software-defined vehicles*	Artigos, *benchmarks* e documentação dos autores
Regulação e auditoria	“UN R155”; “UN R156”; “ISO/PAS 5112”; “ISO/DTS 5112”	ISO, SAE, ONU e reprodução oficial EUR-Lex

Fonte: registros de elaboração da revisão. As expressões sintetizam os temas utilizados; não constituem transcrição integral das consultas nem estratégia validada para uma base específica. SOME/IP: Scalable service-Oriented MiddlewarE over IP; V2X: vehicle-to-everything.

As expressões foram combinadas com títulos e autores para recuperar versões e conferir referências. DOI, título normalizado e relações entre versões orientaram a deduplicação. O relatório técnico de Dantas *et al.*, de 2022, e a publicação de 2023 representam um estudo. Para a contagem anual, adotou-se o ano bibliográfico da versão selecionada, com registro separado de publicação *online* quando diferente. Dobaj *et al.* são contabilizados em 2023, embora publicados *online* em 2021; THREATGET é de fascículo de 2023, com publicação *online* em dezembro de 2022. De Vincenzi *et al.* já estavam disponíveis *online* em junho de 2026; os metadados atribuem o trabalho a fascículo datado de outubro de 2026, posterior ao corte. Sua inclusão se apoia na disponibilidade *online*, sem antecipar a publicação do fascículo (Dantas *et al.*, 2023; Dobaj *et al.*, 2023; Chlup *et al.*, 2023; De Vincenzi *et al.*, 2026).

3.3 Extração, síntese e limites de reprodutibilidade

Níveis de acesso. O corpus final contém 28 estudos, com registro agregado de 19 consultas dirigidas ao texto completo, sete análises por resumo ou material de apresentação e duas por metadados e/ou documentação dos autores. Essas categorias descrevem o material acessível, sem constituir escala de qualidade científica ou maturidade. A associação individual de parte dos estudos às categorias não está explicitada no texto e depende da documentação suplementar indicada na seção 3.3.

Método de extração. Foram considerados objetivo, método, tecnologia, resultado, validação e limitações. A consulta ao texto completo foi dirigida às seções necessárias à análise; não significa leitura linha a linha, reprodução de experimentos ou verificação de todas as demonstrações. Com resumo, material de apresentação, metadados ou documentação autoral, a síntese foi limitada a esse conteúdo. A matriz suplementar registra referência, ano, tipo, versão, DOI ou fonte, tema, material analisado, acesso, contribuição, método, validação e limitações, identificando os campos não individualizados.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Método de síntese. Os estudos foram agrupados por problema e comparados quanto ao desenho e alcance da validação: proposta de método, modelo ou simulação, experimento em bancada ou veículo e investigação industrial. Não foram atribuídos escores globais de qualidade nem níveis de maturidade tecnológica. Países e instituições não foram quantificados porque as afiliações não foram extraídas uniformemente. As contagens descrevem somente o corpus; a classificação temática não permite inferir crescimento ou predominância no campo. O Quadro 1 relaciona as quatro questões centrais à análise realizada.

Quadro 1. Questões de pesquisa e correspondência com a análise.

Questão de pesquisa	Seções	Estudos e tabelas principais	Síntese da resposta
RQ1. Como os estudos selecionados articulam antecedentes e evolução da cibersegurança automotiva em relação à ISO/SAE 21434?	2.1; 4.2	Islam; Cho; Uptane; Mohamad (2020); Dobaj; THREATGET. Tabela 5.	Processos e controles coexistem antes e depois da norma; a distribuição do corpus não demonstra causalidade.
RQ2. Como o corpus relaciona TARA, processos e assurance à ISO/SAE 21434 e a normas e regulamentos complementares?	2.2–2.4; 4.1.1; 4.1.5	HEAVENS 2.0; Plappert; Dantas; Grimm; CASCADE; Li; documentos oficiais. Tabelas 1–3.	A literatura propõe adaptações e integração; documentos oficiais delimitam escopos, sem equivalência com homologação ou eficácia.
RQ3. Quais aplicações e controles do corpus apresentam implementação e validação, e qual é o alcance dessas evidências?	4.1.1–4.1.5; 4.3	THREATGET; Cho; Ying; CANet; ROAD; Luo; VeReMi; Uptane; Baker; Brokenwire; De Vincenzi.	Modelos, experimentos, casos e participação industrial oferecem evidência delimitada; acesso indireto restringe conclusões.
RQ4. Quais limites, lacunas do corpus e perspectivas de pesquisa são sustentados pelo material acessível?	3.3; 4.3–4.5	HEAVENS 2.0; Plappert; Dantas; THREATGET; CANet; ROAD; VeReMi; Grimm; CASCADE; Li; Püllen. Tabela 6.	Reprodutibilidade, testes e manutenção de evidências motivam pesquisas; as propostas não provam lacunas globais.

Fonte: elaboração a partir das seções e estudos já analisados. As respostas referem-se ao corpus selecionado.

Documentação suplementar e reprodutibilidade. Os registros de elaboração são designados Dossiê das etapas 1 a 6 e Auditoria das fontes, com informações sobre composição do corpus, versões, acesso e extração. Sua identificação e disponibilização como materiais suplementares permanecem pendentes de confirmação pelos autores. A matriz suplementar consolida os dados apresentados no artigo, identifica os campos não individualizados e não substitui esses registros.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Não foi preservado inventário completo dos resultados retornados, consultas exatas, ordem de triagem ou motivos individuais de exclusão; não há totais de identificação, exclusão ou deduplicação nem diagrama PRISMA. Registros de composição e contagem permitem conferir o corpus, mas não reproduzem a descoberta inicial. Uma reprodução completa exigiria novo levantamento com consultas e exportações preservadas desde a identificação, o que não foi executado. Não se trata de revisão sistemática, seleção com saturação demonstrada ou amostra representativa da produção mundial.

Origem das afirmações normativas. A análise baseou-se em catálogos oficiais, amostra autorizada e trechos regulatórios acessíveis. O restante da cláusula 5 e as disposições completas das cláusulas 6–15 da ISO/SAE 21434 não foram consultados. Informações confirmadas nesses materiais oficiais são diferenciadas de afirmações da literatura e de interpretações desta revisão, como nas seções 2.2–2.4. A exposição de métodos não reconstrói requisitos normativos não consultados.

3.4 Declaração de uso de IA

Os autores declaram que utilizaram o ChatGPT, da OpenAI, no ambiente Codex, na versão 5.6 Sol Máximo, em 12 de setembro de 2026, exclusivamente para revisão linguística e ajustes de coerência e coesão textual do manuscrito. A ferramenta não foi utilizada para outras finalidades.

Após o uso da ferramenta, os autores revisaram e editaram o texto e assumem responsabilidade pelo conteúdo final do artigo.

Não foram coletados dados de participantes nesta revisão. Não houve testes em seres humanos. A conferência indicada refere-se à revisão do artigo pelos autores.

4 RESULTADOS E DISCUSSÃO

4.1 Estado da arte no corpus selecionado por problema

4.1.1 Automação da análise e qualidade das entradas

Dantas *et al.* automatizam artefatos de análise de ameaças em uma arquitetura orientada a serviços (service-oriented architecture, SOA), com rastreabilidade a cenários de perda. A avaliação usa um modelo do Apollo. A versão publicada é de 2023; os detalhes consultados provêm do relatório técnico de 2022, cujo resumo foi confrontado com o registro final. Nesse relatório, comportamento e verificação de protocolos permanecem como extensões futuras. A enumeração de caminhos é, portanto, relativa à abstração adotada, e não uma demonstração de completude do sistema real (Dantas *et al.*, 2023).

THREATGET associa regras e capacidades a um modelo arquitetural para propagar ameaças e gerar árvores de ataque. Nas aplicações paralelas relatadas, tanto a análise humana

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

quanto a ferramenta identificaram fraquezas que a outra abordagem não encontrou; os achados humanos também levaram a ajustes das regras. O resultado sustenta uma relação de complementaridade. A ferramenta automatiza a enumeração, mas a própria avaliação mostra por que sua base de conhecimento precisa ser revisada (Chlup *et al.*, 2023).

A proposta para veículos pesados de Mairaj ud din e Ahmed reúne representação de arquitetura, identificação de ameaças, risco e controles. O resumo informa um estudo de caso, sem permitir quantificar ganhos frente a análises independentes. Ahmad, Han e Mahmood combinam aprendizado de máquina e otimização para apoiar TARA. A avaliação integral dos dados, partições e validação externa não foi possível; por isso, a acurácia informada no resumo não é usada como prova de superioridade (Mairaj ud din; Ahmed, 2024; Ahmad; Han; Mahmood, 2025).

Essas abordagens têm escopos diferentes. Dantas enfatiza rastreabilidade no modelo; THREATGET explicita propagação por regras; as outras propostas ampliam a automatização de classificação e tratamento. Compará-las apenas pela quantidade de ameaças geradas confundiria abrangência com duplicação ou falsos caminhos. Uma avaliação útil deve examinar pertinência, omissões, esforço de revisão e manutenção após alterações de arquitetura. Trata-se de critério proposto nesta síntese, não de resultado já obtido pelos estudos.

4.1.2 CAN, IDS e resistência a adversários adaptativos

Cho e Shin usam diferenças de relógio para identificar ECUs e detectar desvios no tráfego CAN. A avaliação inclui protótipo e veículo, mas parte dos ataques é emulada por filtragem de mensagens. Ying *et al.* estudam um adversário capaz de ajustar os intervalos de transmissão e reproduzir a característica temporal esperada. A evasão dos detectores avaliados não demonstra inutilidade de toda detecção temporal; delimita uma condição em que a hipótese de identificação deixa de sustentar a decisão (Cho; Shin, 2016; Ying *et al.*, 2019).

CANet desloca o foco para dependências nos sinais, combinando estruturas recorrentes e reconstrução não supervisionada. A síntese usa um manuscrito autoral, sem presumir identidade integral com a versão editorial: nele, dados reais e sintéticos com ataques simulados mostram desempenho dependente do tipo de ataque. A ausência de tráfego real publicável, a exclusão de certas transições operacionais e o custo de execução limitam a extrapolação. Aprender padrões de conteúdo das mensagens (*payload*) amplia o objeto detectável, mas não resolve automaticamente cobertura de cenários ou implantação (Hanselmann *et al.*, 2020).

O ROAD responde a parte do problema de evidência ao disponibilizar capturas CAN e documentar ataques com efeitos físicos. Seus autores distinguem ataques reais de alterações feitas após a coleta e apontam limitações dos *datasets* existentes. O conjunto ainda deriva de um veículo e inclui variantes simuladas; não contém toda a diversidade de ataques necessária para todos os

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

IDSs. Sua contribuição é permitir examinar as condições da avaliação, sem apresentar um ranking de detectores (Verma *et al.*, 2024).

A sequência desses estudos não descreve uma substituição linear de técnicas simples por técnicas superiores. Ela mostra mudanças no adversário, no sinal observado e na qualidade do experimento. Para relacionar um IDS à ISO/SAE 21434, a questão é quais cenários e requisitos seus testes sustentam e quais permanecem descobertos. Essa relação é analítica; os artigos técnicos não realizam, por esse motivo, uma avaliação completa do processo normativo.

4.1.3 *Automotive Ethernet* e V2X

Luo *et al.* combinam verificações de protocolo e temporização com uma rede neural para Scalable service-Oriented MiddlewarE over IP (SOME/IP). O estudo mede desempenho em plataforma de processamento embarcado, mas utiliza dados de controle de cruzeiro adaptativo simulado. Os autores reconhecem que a falta de dados de veículo real limita a avaliação da operação em tempo real. Assim, medidas por pacote e acurácia do classificador devem ser lidas junto à carga, à sequência processada e à localização do detector na arquitetura (Luo *et al.*, 2023).

Em comunicações vehicle-to-everything (V2X), a assinatura ou a origem reconhecida de uma mensagem não garante, por si só, que seu conteúdo esteja correto. VeReMi oferece dados simulados para comparar detecção de comportamento incorreto e evidencia complementaridade entre verificações de plausibilidade. Seus limites incluem ataques não representados e avaliação não interativa, que não mede a resposta do sistema após detectar uma mensagem problemática (Van der Heijden; Lukaseder; Kargl, 2018).

VeReMi Extension acrescenta modelos de erro e ataques que alteram diferentes atributos. A documentação dos autores de VeReMi NextGen, de 2026, apresenta separação geográfica entre conjuntos e maior variedade de cenários. Os artigos completos dessas duas extensões não foram consultados; a síntese apoia-se em metadados e documentação autoral, sem reproduzir métricas de detecção. A interpretação desta revisão é que a documentação indica maior organização e diversidade do *benchmark*, ainda baseado em simulação (Kamel *et al.*, 2020; Hermann *et al.*, 2026).

Esses trabalhos tornam explícito um problema transversal: testar uma função de detecção exige representar tanto o comportamento malicioso quanto as variações legítimas que podem produzir falsos alertas. A evidência de CAN, SOME/IP e V2X não forma um único conjunto intercambiável. Arquitetura, semântica e condições de uso delimitam a validade de cada comparação.

4.1.4 Atualizações, veículos elétricos e sistemas definidos por *software*

Uptane distribui funções de confiança para proteger atualizações veiculares mesmo sob comprometimento parcial. Sua análise distingue combinações de chaves e capacidades de

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

verificação das ECUs. As garantias variam com essas condições, especialmente para unidades com verificação parcial. O estudo fornece um antecedente concreto para integridade de atualizações e gestão de confiança, sem estabelecer que a ISO/SAE 21434 exija nominalmente essa arquitetura (Kuppusamy *et al.*, 2016).

Os trabalhos de carregamento elétrico expõem ameaças que ultrapassam o software de aplicação. Baker e Martinovic estudam a exposição da comunicação pela linha de energia (power line communication, PLC); sua errata corrige a identificação dos veículos observados para DIN 70121 e esclarece que os comportamentos não violavam os padrões escolhidos. A vulnerabilidade observada, portanto, não deve ser apresentada como não conformidade à ISO 15118. Brokenwire demonstra interrupção de sessões do Combined Charging System (CCS) por perturbação da comunicação; a leitura de resumo e slides sustenta esse resultado, sem confirmar a eficácia das mitigações sugeridas (Baker; Martinovic, 2019; Köhler *et al.*, 2023).

De Vincenzi *et al.* combinam revisão sobre veículos definidos por software (software-defined vehicles, SDV) com um questionário industrial exploratório. O estudo reúne superfícies de ataque, integração entre veículo e nuvem, software de criticidade mista e atualizações. As 11 respostas completas não autorizam estimar a prevalência de práticas em toda a indústria. Sua contribuição está em relacionar problemas que se tornam dependentes entre si quando funções e configurações mudam ao longo da operação (De Vincenzi *et al.*, 2026).

Esta revisão interpreta que a implicação para TARA é delimitar o item e as interfaces relevantes. Incluir uma ameaça que atravessa o carregador, o serviço de atualização ou a nuvem não equivale a estender automaticamente o escopo da norma a todo esse ambiente. A relação proposta entre essas aplicações e TARA é analítica: é preciso explicitar qual parte se modela, que evidência se obtém e quais dependências externas permanecem como hipóteses.

4.1.5 Assurance, integração entre segurança funcional e cibersegurança e continuidade operacional

Mohamad *et al.* investigaram necessidades de *assurance cases* com participantes de dois fabricantes europeus antes da edição final da norma. O resumo fornece evidência de uma demanda organizacional, mas não permite reconstruir todos os resultados qualitativos. CASCADE, publicado posteriormente, organiza argumentos por ativos e diferencia alegações sobre o produto daquelas sobre a qualidade do próprio *case*. Sua avaliação combina construção do método, exemplo e especialistas (Mohamad *et al.*, 2020; Mohamad *et al.*, 2023).

Esta revisão interpreta que a existência de um documento não constitui evidência suficiente de sua conclusão. Alegações genéricas de um argumento de *assurance* não devem ser confundidas com a definição específica de *cybersecurity claim* confirmada na amostra autorizada. Um argumento

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

é examinável quando a relação entre alegação e evidência é explícita; sua manutenção precisa reconhecer evidências que deixaram de se aplicar depois de uma alteração.

Li *et al.* propõem uma coanálise baseada em System-Theoretic Process Analysis (STPA) para aproximar segurança funcional e cibersegurança na fase de conceito, demonstrada em frenagem automática de emergência. Püllen, Liske e Katzenbeisser usam dependências entre ativos e cenários de dano para avaliar incidentes conforme condições operacionais. O segundo estudo referencia o DIS de 2020 e foi consultado apenas em resumo. Ambos conectam ameaças a consequências físicas, mas os casos não demonstram resposta segura para toda condição de condução (Li *et al.*, 2024; Püllen; Liske; Katzenbeisser, 2021).

A discussão de atividades contínuas retoma o vínculo entre operação e desenvolvimento. Monitoramento e gestão de vulnerabilidades precisam fornecer informação que possa ser relacionada aos itens e às decisões afetadas. Grimm *et al.* propõem explicitar preparação, iteração e análise posterior no tratamento de incidentes. Esses passos são apresentados como extensão acadêmica do processo, não como transcrição verificada da cláusula 13 (Grimm *et al.*, 2023).

4.2 Análise temporal e distribuição do corpus

Tabela 5. Distribuição dos estudos selecionados por ano e período.

Período	Contagem anual	Total
2016–2020	2016: 4; 2017: 0; 2018: 2; 2019: 2; 2020: 4	12
2021–2022	2021: 3; 2022: 0	3
2023–2026	2023: 7; 2024: 3; 2025: 1; 2026: 2	13

Fonte: corpus da revisão (n = 28). Zero significa ausência de trabalho selecionado naquele ano, não ausência de produção científica. Os períodos têm durações distintas e 2026 é parcial.

A codificação temática registrada atribui 11 estudos à TARA e quatro à detecção e avaliação em CAN, as categorias mais representadas no corpus. Essa distribuição resulta da seleção intencional e não estima a atenção relativa de toda a comunidade científica. O registro individual dessa codificação depende do Dossiê. A matriz suplementar descreve os temas tratados nos estudos, sem reconstruir a classificação estatística.

No período de 2016–2020 coexistem modelos de risco, detecção, atualização segura, *benchmarks* e necessidades de *assurance*. A amostra não sustenta descrever esse intervalo como uma fase exclusivamente técnica ou sem gestão. HEAVENS, SAE J3061 e o estudo industrial de *assurance* mostram que processos e controles já eram investigados em paralelo (Islam *et al.*, 2016; SAE International, 2016; Mohamad *et al.*, 2020).

Em 2021–2022, HEAVENS 2.0 e estudos ligados ao DIS explicitam a adaptação de métodos à linguagem normativa. É necessário separar a data do artigo da versão da norma que ele

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

utiliza. A contagem por fascículo também desloca para 2023 trabalhos publicados *online* anteriormente, como Dobaj e THREATGET. A distribuição anual não é, portanto, uma medida direta da data em que cada ideia surgiu (Lautenbach; Almgren; Olovsson, 2021; Plappert *et al.*, 2021; Püllen; Liske; Katzenbeisser, 2021; Dobaj *et al.*, 2023; Chlup *et al.*, 2023).

Entre 2023 e 2026, o corpus reúne automação, manutenção de TARA, argumentos de *assurance* e ampliação de *benchmarks*. A continuidade de CAN e V2X contraria uma narrativa de abandono dessas tecnologias em favor de SDV ou IA. O que se observa é a coexistência de problemas de detecção e de integração processual. Não se pode atribuir causalmente essa distribuição à publicação da ISO/SAE 21434, pois a seleção foi intencional e não controla outros fatores.

4.3 Evidência e maturidade

A revisão crítica narrativa sustenta, no corpus selecionado, graus diferentes de conhecimento conforme a pergunta. Ensaios em veículo e carregamento demonstram comportamentos em implementações delimitadas. Modelos de TARA produzem classificações e requisitos; estudos de *assurance* estruturam justificativas; entrevistas e questionários identificam necessidades e percepções. Não é adequado ordenar todos por uma única escala e concluir que um caso de uso vale como prova de eficácia de processo. O nível de acesso da revisão tampouco é um indicador automático de qualidade do estudo.

Na dimensão experimental, CAN e carregamento apresentam exemplos concretos de ataques e observação de seus efeitos. Isso permite discutir hipóteses de proteção e falhas específicas, mas não estabelece segurança geral das tecnologias. Na dimensão metodológica, TARA e *assurance* possuem procedimentos explícitos, porém a aplicação demonstrada não equivale a validação longitudinal. A maturidade aqui é uma interpretação por dimensão da evidência, não uma classificação dos setores por níveis de maturidade tecnológica (technology readiness levels, TRL).

Duas tensões atravessam os estudos. A primeira é entre padronização e contexto: um vocabulário comum favorece a comparação, enquanto categorias de risco dependem do item, do atacante e dos danos. A segunda é entre automação e cobertura: gerar mais caminhos pode revelar dependências ou apenas reproduzir o que a base de regras já representa. O resultado precisa ser confrontado com revisão independente e com evidência de execução quando a alegação for operacional.

A distinção entre conformidade e resistência a ataques é particularmente clara no caso de carregamento corrigido por errata. Ela também aparece, sob outra forma, na detecção temporal: a eficácia observada depende das capacidades atribuídas ao adversário. Tais estudos não invalidam

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

a engenharia por processos; mostram por que ela precisa conservar o vínculo entre hipótese, teste e conclusão (Baker; Martinovic, 2019; Ying *et al.*, 2019).

Há limitações próprias desta revisão, concentradas na seção 3.3: descoberta web sem registro integral, seleção intencional, acesso desigual às fontes, uso de versões autorais e consulta normativa parcial. O conteúdo material da emenda de R156 em 2026 não foi recuperado. A falta de individualização de parte dos níveis de acesso na documentação disponibilizada limita sua conferência por estudo. Essas restrições impedem afirmar quais temas dominam globalmente ou que as lacunas do corpus não tenham sido tratadas fora dele.

4.4 Lacunas e agenda de pesquisa

As lacunas abaixo se referem ao material efetivamente acessível dos estudos selecionados. As ações propostas são interpretações desta síntese e indicam resultados verificáveis, sem pressupor responsáveis ou prazos. Informação não verificada por acesso parcial não é tratada como avaliação inexistente no estudo.

Tabela 6. Lacunas delimitadas no corpus e pesquisas propostas para investigá-las.

Problema e base	Evidência que falta	Pesquisa e verificação proposta
Consistência da TARA, HEAVENS 2.0 e Plappert	Concordância entre avaliadores e sensibilidade às premissas	Analisar os mesmos itens independentemente; comparar classes e decisões de tratamento
Cobertura da automação, Dantas e THREATGET	Comparação externa de caminhos pertinentes, omissões e manutenção	Avaliar arquiteturas não usadas na construção; medir erros e esforço incluindo revisão humana
Validade dos testes, CANet, ROAD e VeReMi	Transferência entre veículos, sessões e adversários	Separar treino/teste por domínio; reportar cobertura, atraso, falsos alertas e custo
Continuidade de TARA e *assurance*, Grimm, Dobaj e CASCADE	Acompanhamento de evidências após mudanças sucessivas	Registrar versões, dependências e testes; verificar omissões e tempo de propagação
Resposta e consequências físicas, Püllen e Li	Em Püllen, validação detalhada não verificável no resumo; em Li, limitada ao caso	Avaliar resposta em simulação e bancada com cenários de dano e restrições de segurança funcional

Fonte: elaboração a partir dos estudos discutidos e dos limites de acesso descritos nas seções 3.3 e 4.1; matriz suplementar. As propostas são desta revisão.

A primeira lacuna não exige converter julgamentos qualitativos em probabilidades artificiais. O resultado de interesse é saber se avaliadores com a mesma informação chegam a decisões

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

compatíveis e quais premissas explicam divergências. Para modelos probabilísticos, a tarefa adicional é justificar parâmetros e examinar sensibilidade, sem apresentá-los como frequência empírica (Lautenbach; Almgren; Olovsson, 2021; Plappert *et al.*, 2021; Comert; Chowdhury; Nicol, 2020).

Na automação, a avaliação de THREATGET já fornece evidência de complementaridade e cobertura incompleta; isso é mais informativo que presumir a substituição dos especialistas. Uma comparação futura deve incluir o custo de preparar a arquitetura e corrigir as saídas. Para a proposta de IA consultada apenas em resumo, a pendência imediata é obter o texto e examinar a composição dos dados e a separação de treino e teste. A ausência desse acesso não prova que os autores tenham omitido tais avaliações (Chlup *et al.*, 2023; Ahmad; Han; Mahmood, 2025).

A manutenção distribuída merece um desenho distinto de um teste pontual de ferramenta. Mudanças controladas de componente podem ser acompanhadas até a atualização de caminhos, requisitos e argumentos afetados. A completude dessa propagação e os erros de reconciliação entre organizações seriam resultados mensuráveis. Uma eventual associação com incidentes exigiria controlar exposição e definições, não apenas comparar contagens antes e depois (Grimm *et al.*, 2023; Dobaj *et al.*, 2023; Mohamad *et al.*, 2023).

Produção, fim do suporte e descomissionamento tiveram pouca representação específica nesta seleção, embora integrem o escopo examinado. Isso é uma insuficiência de cobertura do levantamento, não prova de ausência de pesquisa. Antes de propor uma lacuna global nessas fases, é necessário ampliar a busca e recuperar estudos industriais pertinentes.

4.5 Tendências e perspectivas

A automação baseada em modelos é uma tendência observada no corpus recente, sustentada por Dantas, THREATGET e a aplicação a veículos pesados. O uso de IA em TARA é uma proposta presente na literatura de 2025; sua maturidade não pode ser equiparada à de técnicas cuja avaliação foi examinada em maior detalhe. Não foi encontrada neste conjunto base para afirmar substituição generalizada do julgamento técnico por IA (Dantas *et al.*, 2023; Chlup *et al.*, 2023; Mairaj ud din; Ahmed, 2024; Ahmad; Han; Mahmood, 2025).

A documentação autoral de VeReMi NextGen indica ampliação de cenários e organização dos conjuntos de avaliação; o artigo completo não foi consultado nesta síntese. A revisão sobre veículos definidos por software conecta atualização contínua, dependências de software e integração com serviços externos. São movimentos observados no material dos trabalhos selecionados, e não previsões de adoção universal (Hermann *et al.*, 2026; De Vincenzi *et al.*, 2026).

Esta revisão interpreta a ligação versionada entre TARA, requisitos, verificações e *assurance* como uma direção de pesquisa que une essas frentes. A hipótese é que essa integração

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

possa reduzir decisões baseadas em evidência desatualizada. A hipótese precisa ser testada pelos desenhos longitudinais propostos; não deve ser apresentada como benefício já demonstrado.

5 CONSIDERAÇÕES E RECOMENDAÇÕES

Esta revisão crítica narrativa de estado da arte, baseada em busca web orientada por temas e seleção intencional de 28 estudos, responde à RQ1: no corpus, antecedentes de análise de riscos, detecção e atualização segura coexistem com adaptações posteriores de TARA, automação e *assurance*. A distribuição temporal não demonstra que a publicação da ISO/SAE 21434 tenha causado essa evolução.

Quanto à RQ2, os estudos relacionam métodos de TARA, desenvolvimento e *assurance* à ISO/SAE 21434 e discutem sua complementaridade com segurança funcional, gestão regulatória e auditoria. Essas adaptações são contribuições da literatura; os documentos oficiais acessíveis sustentam distinções de escopo e natureza, sem permitir reconstruir as cláusulas não consultadas.

Em resposta à RQ3, CAN, SOME/IP, V2X, atualização segura, carregamento elétrico e veículos definidos por software apresentam aplicações e controles com validação delimitada. Experimentos demonstram comportamentos específicos; exemplos, estudos de caso e participação de especialistas sustentam propostas de processo. Evidências recuperadas apenas por resumo, metadados ou documentação autoral permitem conclusões mais restritas. O corpus não estabelece equivalência entre conformidade, completude da análise e eficácia operacional.

Quanto à RQ4, as lacunas delimitadas dizem respeito à reprodutibilidade das decisões de risco, representatividade dos testes e manutenção das evidências entre versões e fornecedores. A agenda propõe comparação independente, avaliação adversarial e acompanhamento longitudinal. São propostas desta revisão, limitadas pela seleção intencional, pela descoberta não integralmente reproduzível, pelo acesso parcial e pela consulta normativa incompleta; não demonstram ausência global de pesquisa nem benefícios já comprovados.

DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL

Os autores declaram que, durante a preparação deste trabalho, utilizaram a ferramenta ChatGPT, da OpenAI, na versão 5.6 Sol Máximo, exclusivamente para revisão linguística e ajustes de coerência e coesão textual. A ferramenta não foi utilizada para outras finalidades. Após o uso desta ferramenta, os autores revisaram, editaram e assumem total responsabilidade pelo conteúdo final da publicação. A Inteligência Artificial não é listada como autora, não possui responsabilidade legal pelo manuscrito e não foi utilizada para a geração de dados primários, manipulação de resultados ou conclusões científicas.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REFERÊNCIAS

AHMAD, U.; HAN, M.; MAHMOOD, S. AI-Enhanced *threat analysis and risk assessment* for connected and autonomous vehicles. ***Software* Quality Journal**, v. 33, n. 3, artigo 26, 2025. DOI: 10.1007/s11219-025-09723-6. Disponível em: https://doi.org/10.1007/s11219-025-09723-6. Acesso em: 07 set. 2026.

BAKER, R.; MARTINOVIC, I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In: USENIX *SECURITY* SYMPOSIUM, 28., 2019. **Anais [...]**. [S. l.]: USENIX Association, 2019. p. 407–424. Disponível em: https://www.usenix.org/conference/usenixsecurity19/presentation/baker. Acesso em: 07 set. 2026. Errata consultada: https://www.usenix.org/system/files/sec19_errata_baker.pdf.

CHLUP, S. *et al.* THREATGET: Towards Automated Attack Tree Analysis for *Automotive* Cybersecurity. **Information**, v. 14, n. 1, artigo 14, 2023. DOI: 10.3390/info14010014. Disponível em: https://doi.org/10.3390/info14010014. Acesso em: 04 set. 2026. Publicação online em dez. 2022; fascículo de 2023.

CHO, K.-T.; SHIN, K. G. *Fingerprinting* Electronic Control Units for Vehicle Intrusion Detection. In: USENIX *SECURITY* SYMPOSIUM, 25., 2016, Austin. **Anais [...]**. [S. l.]: USENIX Association, 2016. p. 911–927. Disponível em: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cho. Acesso em: 07 set. 2026.

COMERT, G.; CHOWDHURY, M.; NICOL, D. M. Assessment of System-Level Cyber Attack Vulnerability for Connected and Autonomous Vehicles Using Bayesian Networks. **arXiv:2011.09436**, 2020. DOI: 10.48550/arXiv.2011.09436. *Preprint*. Disponível em: https://doi.org/10.48550/arXiv.2011.09436. Acesso em: 12 ago. 2026.

DANTAS, Y. *et al.* Automating Vehicle SOA Threat Analysis Using a *Model-Based* Methodology. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS *SECURITY* AND PRIVACY (ICISSP), 9., 2023. **Anais [...]**. [S. l.]: SCITEPRESS, 2023. p. 180–191. (v. 1). DOI: 10.5220/0011786400003405. Disponível em: https://doi.org/10.5220/0011786400003405. Acesso em: 19 jul. 2026. Versão técnica consultada: https://arxiv.org/abs/2212.12347. Relatório técnico autoral de 2022; contado com a publicação de 2023 como um único estudo.

DE VINCENZI, M. *et al.* Contextualizing *Security* and Privacy of *Software-Defined Vehicles*: A Literature Review and Industry Perspectives. **ACM Computing Surveys**, v. 58, n. 13, p. 1–36, 2026. DOI: 10.1145/3814955. Disponível em: https://doi.org/10.1145/3814955. Acesso em: 21 ago. 2026. Publicado *online* em: 23 jun. 2026; fascículo com data de out. 2026. Registro de publicação online anterior ao fascículo (online-first).

DOBAJ, J. *et al.* Towards a *security*-driven *automotive* development lifecycle. **Journal of *Software*: Evolution and Process**, v. 35, n. 8, e2407, 2023. DOI: 10.1002/smr.2407. Disponível em: https://doi.org/10.1002/smr.2407. Acesso em: 14 ago. 2026. Publicação online em 2021; fascículo de 2023.

GRIMM, D. *et al.* Gap Analysis of ISO/SAE 21434 – Improving the *Automotive* Cybersecurity Engineering Life Cycle. In: IEEE INTERNATIONAL CONFERENCE ON INTELLIGENT TRANSPORTATION SYSTEMS (ITSC), 26., 2023, Bilbao. **Anais [...]**. [S. l.]: IEEE, 2023. p. 1904–1911. DOI: 10.1109/ITSC57777.2023.10422100. Disponível em: https://doi.org/10.1109/ITSC57777.2023.10422100. Acesso em: 17 ago. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

HANSELMANN, M. *et al.* CANet: An Unsupervised *Intrusion Detection System* for High Dimensional CAN Bus Data. **IEEE Access**, v. 8, p. 58194–58205, 2020. DOI: 10.1109/ACCESS.2020.2982544. Disponível em: https://doi.org/10.1109/ACCESS.2020.2982544. Acesso em: 10 ago. 2026. Manuscrito autoral consultado.

HERMANN, A. *et al.* VeReMi NextGen: A *Dataset* for Evaluating Misbehavior Detection Systems in VANETs. In: IEEE VEHICULAR NETWORKING CONFERENCE (VNC), 2026, Montreal. **Anais [...]**. [S. l.]: IEEE, 2026. Disponível em: https://ieeexplore.ieee.org/abstract/document/11629123. Acesso em: 08 ago. 2026. Documentação consultada: https://veremi-*dataset*.github.io/veremi-nextgen.

ISLAM, M. M. *et al.* A *Risk Assessment* Framework for *Automotive* Embedded Systems. In: ACM INTERNATIONAL WORKSHOP ON CYBER-PHYSICAL SYSTEM *SECURITY* (CPSS), 2., 2016. **Anais [...]**. [S. l.]: ACM, 2016. p. 3–14. DOI: 10.1145/2899015.2899018. Disponível em: https://doi.org/10.1145/2899015.2899018. Acesso em: 23 ago. 2026.

ISO. **ISO 26262-1:2018: Road vehicles: Functional *safety*: Part 1: Vocabulary**. 2018. Disponível em: https://www.iso.org/standard/68383.html. Acesso em: 12 ago. 2026.

ISO. **ISO/PAS 5112:2022: Road vehicles: Guidelines for auditing cybersecurity engineering**. 2022. Disponível em: https://www.iso.org/standard/80840.html. Acesso em: 07 set. 2026.

ISO. **ISO/DTS 5112: Road vehicles: Guidelines for auditing cybersecurity engineering**. 2026. Catálogo de projeto em desenvolvimento. Disponível em: https://www.iso.org/standard/92730.html. Acesso em: 19 ago. 2026.

ISO; SAE INTERNATIONAL. **ISO/SAE 21434:2021: Road vehicles: Cybersecurity engineering**. 2021. *Preview* autorizado: https://cdn.standards.iteh.ai/sist-preview/70918/aa7103c3560f406c86ccdbfec4a0d8de/ISO-SAE-21434-2021.pdf. Disponível em: https://www.iso.org/standard/70918.html. Acesso em: 27 jul. 2026.

KAMEL, J. *et al.* VeReMi Extension: A *Dataset* for Comparable Evaluation of Misbehavior Detection in VANETs. In: IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC), 2020. **Anais [...]**. [S. l.]: IEEE, 2020. p. 1–6. DOI: 10.1109/ICC40277.2020.9149132. Disponível em: https://doi.org/10.1109/ICC40277.2020.9149132. Acesso em: 02 set. 2026. Documentação consultada: https://veremi-*dataset*.github.io/veremi-extension.

KÖHLER, S. *et al.* Brokenwire: Wireless Disruption of CCS *Electric Vehicle Charging*. In: NETWORK AND DISTRIBUTED SYSTEM *SECURITY* SYMPOSIUM (NDSS), 2023. **Anais [...]**. [S. l.: s. n.], 2023. Disponível em: https://www.ndss-symposium.org/ndss-paper/brokenwire-wireless-disruption-of-ccs-electric-vehicle-charging/. Acesso em: 22 ago. 2026.

KUPPUSAMY, T. K. *et al.* Uptane: Securing *Software* Updates for Automobiles. In: ESCAR EUROPE, 14., 2016. **Anais [...]**. [S. l.: s. n.], 2016. Disponível em: https://ssl.engineering.nyu.edu/papers/kuppusamy_escar_16.pdf. Acesso em: 21 jul. 2026.

LAUTENBACH, A.; ALMGREN, M.; OLOVSSON, T. Proposing HEAVENS 2.0 – an *automotive risk assessment* model. In: COMPUTER SCIENCE IN CARS SYMPOSIUM (CSCS), 2021. **Anais [...]**. [S. l.]: ACM, 2021. p. 1–12. DOI: 10.1145/3488904.3493378. Disponível em: https://doi.org/10.1145/3488904.3493378. Acesso em: 15 ago. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

LI, Y. *et al.* Complying with ISO 26262 and ISO/SAE 21434: A *Safety* and *Security* Co-Analysis Method for Intelligent Connected Vehicle. **Sensors**, v. 24, n. 6, artigo 1848, 2024. DOI: 10.3390/s24061848. Disponível em: https://doi.org/10.3390/s24061848. Acesso em: 29 jul. 2026.

LUO, F. *et al.* A Multi-Layer *Intrusion Detection System* for SOME/IP-Based In-Vehicle Network. **Sensors**, v. 23, n. 9, artigo 4376, 2023. DOI: 10.3390/s23094376. Disponível em: https://doi.org/10.3390/s23094376. Acesso em: 11 ago. 2026.

MACHER, G. *et al.* A Review of *Threat Analysis and Risk Assessment* Methods in the *Automotive* Context. In: COMPUTER *SAFETY*, RELIABILITY, AND *SECURITY* (SAFECOMP), 2016. **Anais [...]**. [S. l.]: Springer, 2016. p. 130–141. (Lecture Notes in Computer Science, v. 9922). DOI: 10.1007/978-3-319-45477-1_11. Disponível em: https://doi.org/10.1007/978-3-319-45477-1_11. Acesso em: 22 jul. 2026.

MAIRAJ UD DIN, Q.; AHMED, Q. Automated TARA Framework for Cybersecurity Compliance of Heavy Duty Vehicles. SAE Technical Paper 2024-01-2809. Documento técnico apresentado no WCX SAE World Congress Experience, 2024. DOI: 10.4271/2024-01-2809. Disponível em: https://doi.org/10.4271/2024-01-2809. Acesso em: 05 set. 2026.

MOHAMAD, M. *et al. Security Assurance Cases* for Road Vehicles: An Industry Perspective. In: INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND *SECURITY* (ARES), 15., 2020. **Anais [...]**. [S. l.]: ACM, 2020. p. 1–6. DOI: 10.1145/3407023.3407033. Disponível em: https://doi.org/10.1145/3407023.3407033. Acesso em: 12 ago. 2026.

MOHAMAD, M. *et al.* CASCADE: An Asset-driven Approach to Build *Security Assurance Cases* for *Automotive* Systems. **ACM Transactions on Cyber-Physical Systems**, v. 7, n. 1, artigo 3, p. 1–26, 2023. DOI: 10.1145/3569459. Disponível em: https://doi.org/10.1145/3569459. Acesso em: 25 ago. 2026.

MONTEUUIS, J.-P. *et al.* SARA: *Security Automotive* Risk Analysis Method. In: ACM WORKSHOP ON CYBER-PHYSICAL SYSTEM *SECURITY* (CPSS), 4., 2018. **Anais [...]**. [S. l.]: ACM, 2018. p. 3–14. DOI: 10.1145/3198458.3198465. Disponível em: https://doi.org/10.1145/3198458.3198465. Acesso em: 04 set. 2026.

PLAPPERT, C. *et al.* Attack Surface Assessment for Cybersecurity Engineering in the *Automotive* Domain. In: EUROMICRO INTERNATIONAL CONFERENCE ON PARALLEL, DISTRIBUTED AND NETWORK-BASED PROCESSING (PDP), 29., 2021. **Anais [...]**. [S. l.]: IEEE, 2021. p. 266–275. DOI: 10.1109/PDP52278.2021.00050. Disponível em: https://doi.org/10.1109/PDP52278.2021.00050. Acesso em: 15 ago. 2026.

PÜLLEN, D.; LISKE, J.; KATZENBEISSER, S. ISO/SAE 21434-Based *Risk Assessment* of *Security* Incidents in Automated Road Vehicles. In: COMPUTER *SAFETY*, RELIABILITY, AND *SECURITY* (SAFECOMP), 2021. **Anais [...]**. [S. l.]: Springer, 2021. p. 82–97. (Lecture Notes in Computer Science, v. 12852). DOI: 10.1007/978-3-030-83903-1_6. Disponível em: https://doi.org/10.1007/978-3-030-83903-1_6. Acesso em: 21 jul. 2026.

SAE INTERNATIONAL. **SAE J3061_201601: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems**. 2016. DOI: 10.4271/J3061_201601. Disponível em: https://saemobilus.sae.org/standards/j3061_201601-cybersecurity-guidebook-cyber-physical-vehicle-systems. Acesso em: 08 set. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

SAE INTERNATIONAL. **SAE J3061_202112: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems**. 2021. DOI: 10.4271/J3061_202112. Disponível em: https://saemobilus.sae.org/standards/j3061_202112-cybersecurity-guidebook-cyber-physical-vehicle-systems. Acesso em: 06 ago. 2026.

UNECE. **UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to *software* update and *software* updates management system [2021/388]**. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:42021X0388. Acesso em: 10 set. 2026.

UNECE. **UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cyber *security* and cyber *security* management system [2025/5]**. 2025. Disponível em: https://eur-lex.europa.eu/eli/reg/2025/5/oj/eng. Acesso em: 08 set. 2026.

UNITED NATIONS. **C.N.237. 2026.TREATIES-XI.B.16.156: Amendments to United Nations Regulation No. 156**. 2026a. Disponível em: https://treaties.un.org/doc/Publication/CN/2026/CN.237.2026-Eng.pdf. Acesso em: 07 set. 2026.

UNITED NATIONS. **United Nations Regulation No. 155: Treaty status**. 2026b. Disponível em: https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20XI/XI-B-16-155.en.xml. Acesso em: 12 ago. 2026.

VAN DER HEIJDEN, R. W.; LUKASEDER, T.; KARGL, F. VeReMi: A *Dataset* for Comparable Evaluation of Misbehavior Detection in VANETs. In: *SECURITY* AND PRIVACY IN COMMUNICATION NETWORKS (SECURECOMM), 2018. **Anais [...]**. [S. l.]: Springer, 2018. p. 318–337. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, v. 254). DOI: 10.1007/978-3-030-01701-9_18. Disponível em: https://doi.org/10.1007/978-3-030-01701-9_18. Acesso em: 22 jul. 2026.

VERMA, M. E. *et al.* A comprehensive guide to CAN IDS data and introduction of the ROAD *dataset*. **PLOS ONE**, v. 19, n. 1, artigo e0296879, 2024. DOI: 10.1371/journal.pone.0296879. Disponível em: https://doi.org/10.1371/journal.pone.0296879. Acesso em: 11 set. 2026.

YING, X. *et al.* Shape of the Cloak: Formal Analysis of *Clock Skew*-Based *Intrusion Detection System* in Controller Area Networks. **IEEE Transactions on Information Forensics and *Security***, v. 14, n. 9, p. 2300–2314, 2019. DOI: 10.1109/TIFS.2019.2895957. Disponível em: https://doi.org/10.1109/TIFS.2019.2895957. Acesso em: 08 set. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.