2021 年 3 月 4 日

协定

关于通过联合国统一技术文件可移动的轮式车辆、设备和部件的规定安装和用于轮式车辆，以及相互承认根据这些联合国条例授予的批准*

（第 3 次修订，包括 2017 年 9 月 14 日生效的修订）

附录 154–第 155 号联合国条例

1958 年协定附件生效日期：2021 年 1 月 22 日

关于就网络安全和网络安全管理系统批准车辆的统一规定

本文档仅作为文档工具。具有法律约束力的真实文本为：ECE/TRANS/WP.29/2020/79（经 ECE/TRANS/WP.29/2020/94 和 ECE/TRANS/WP.29/2020/97 修订）。

联合国

*本协议以前的标题：

关于采用统一的批准和相互承认条件的协定，

1958 年 3 月 20 日在日内瓦完成的机动车设备和部件批准（原始版本）；

关于轮式车辆采用统一技术规范的协议，

可安装和用于轮式车辆的设备和零件，以及根据这些规定相互承认批准的条件，1995 年 10 月 5 日在日内瓦制定（第 2 版）。

联合国第 155 号条例

关于就网络安全和网络安全管理系统批准车辆的统一规定

目录

1. 范围

就网络安全而言，本法规适用于 M 和 N 类车辆。

1.1. 本法规还适用于 O 类车辆（如果至少安装了一个电子控制单元）。

1.2. 本法规也适用于 L6 和 L7 类车辆，如果从 3 级起配备了自动驾驶功能，如参考文件 WP.29 下的自动驾驶定义和联合国自动车辆法规制定的一般原则（ECE/TRANS/WP.29/1140）中所定义。

1.3. 本法规不影响其他联合国法规、区域或国家立法，这些法规管理授权方对车辆、车辆数据、功能和资源的访问，以及此类访问的条件。它也不妨碍国家和区域隐私立法的适用以及在处理自然人个人数据方面对自然人的保护。

1.4. 本法规不影响与网络安全相关的其他联合国法规、国家或地区法规，这些法规管理更换零件和组件（物理和数字）的开发和安装/系统集成。

2. 定义

就本法规而言，以下定义应适用：

2.1. “车辆类型”指至少在以下基本方面没有区别的车辆：

（a） 制造商对车辆类型的指定；

（b） 与网络安全相关的电气/电子体系结构和外部接口的基本方面。

2.2. “网络安全”是指保护道路车辆及其功能免受电气或电子部件网络威胁的情况。

2.3. “网络安全管理系统（CSMS）”是指一种基于风险的系统方法，定义组织流程、责任和治理，以处理与车辆网络威胁相关的风险，并保护车辆免受网络攻击。

2.4. “系统”是指实现一项或多项功能的一组组件和/或子系统。

2.5. “开发阶段”指车辆型式认证前的时期。

2.6. “生产阶段”指车型的生产持续时间。

2.7. “后期生产阶段”是指直到该车型下所有车辆的使用寿命结束时，不再生产该车型的时期。包含特定车型的车辆将在此阶段投入使用，但不再生产。当不再有任何特定车型的运行车辆时，该阶段结束。

2.8. “缓解”是指降低风险的措施。

2.9. “风险”是指给定威胁可能利用车辆的漏洞，从而对组织或个人造成伤害。

2.10. “风险评估”是指发现、识别和描述风险（风险识别）、理解风险性质和确定风险水平（风险分析），并将风险分析结果与风险标准进行比较，以确定风险和/或其大小是否可接受或可容忍（风险评估）。

2.11. “风险管理”指指导和控制组织风险的协调活动。

2.12. “威胁”是指可能对系统、组织或个人造成伤害的意外事件的潜在原因。

2.13. “漏洞”是指资产或缓解措施的弱点，可被一个或多个威胁利用。

3. 申请批准

3.1. 关于网络安全的车型认证申请应由车辆制造商或其正式授权代表提交。

3.2. 应随附下述文件一式三份，以及以下详细信息：

3.2.1. 关于本法规附件 1 中规定项目的车辆类型说明。

3.2.2. 如果显示信息包含在知识产权范围内或构成制造商或其供应商的特定专有技术，则制造商或其供应商应提供足够的信息，以便能够正确进行本法规中提及的检查。此类信息应在保密的基础上处理。

3.2.3. 符合本法规第 6 段要求的 CSM 合规证书。

3.3. 文件应分两部分提供：

（a） 认证的正式文件包，包含附录 1 中规定的材料，在提交类型认证申请时应提供给认证机构或其技术服务机构。审批机关或其技术服务机构应将本文件包用作审批流程的基本参考。认证机构或其技术服务机构应确保该文件包在车辆类型最终停止生产后至少 10 年内保持可用。

（b） 与本法规要求相关的附加材料可由制造商保留，但在类型认证时开放供检查。制造商应确保在类型认证时开放供检查的任何材料至少可供使用 10 年，从车辆最终停止生产时算起。

4. 标记

4.1. 应将国际认证标志粘贴在符合本法规下认证车型的每辆车辆的显眼位置和认证表上规定的易于接近的位置，该国际认证标志包括：

4.1.1. 一个环绕字母“E”的圆圈，其后是授予认证的国家的识别号。

4.1.2. 本法规编号后接字母“R”、破折号和认证号，位于段落 4.1.1.中所述圆圈右侧的上面。

4.2. 如果车辆符合根据本法规授予认证的国家协议所附的一个或多个其他法规认证的车型，则第 4.1.1.段中规定的符号。上述内容无需重复；在这种情况下，法规和认证号以及根据本法规授予认证的国家授予认证的所有法规的附加符号应置于第 4.1.1.段中规定符号右侧的垂直列中的上面。

4.3. 认证标志应清晰易读且不可擦除。

4.4. 认证标志应放置在制造商粘贴的车辆铭牌上或其附近。

4.5. 本法规附件 3 给出了认证标志布置的示例。

5. 批准

5.1. 认证机构应在适当情况下，仅向满足本法规要求的此类车型授予网络安全方面的类型认证。

5.1.1. 认证机构或技术服务机构应通过文件检查验证车辆制造商已采取与车型相关的必要措施，以：

（a） 通过供应链收集并验证本法规要求的信息，以证明已识别并管理供应商相关风险；

（b） 记录风险评估（在开发阶段或回顾阶段进行）、测试结果和适用于车型的缓解措施，包括支持风险评估的设计信息；

（c） 在车型设计中实施适当的网络安全措施；

（d） 检测并应对可能的网络安全攻击；

（e） 记录数据以支持网络攻击的检测，并提供数据取证能力，以便对未遂或成功的网络攻击进行分析。

5.1.2. 认证机构或技术服务机构应通过测试该车型的车辆来验证车辆制造商是否已实施其记录的网络安全措施。试验应由认证机构或技术服务机构自己或与车辆制造商合作通过抽样进行。抽样应重点但不限于风险评估期间评估为高的风险。

5.1.3. 如果车辆制造商未满足第 7.3.段中提及的一项或多项要求，则认证机构或技术服务机构应拒绝授予与网络安全相关的型式认证，尤其是：

（a） 车辆制造商未进行第 7.3.3.段中提及的详尽风险评估。包括制造商没有考虑与附件 5、A 部分所指的威胁有关的所有风险；

（b） 车辆制造商未针对车辆制造商风险评估中确定的风险保护车辆类型，或未按照第 7 段的要求实施相应的缓解措施。；

（c） 车辆制造商未采取适当和相称的措施，以确保车辆类型（如提供）上的专用环境，用于存储和执行售后市场软件、服务、应用程序或数据；

（d） 在批准之前，车辆制造商未进行适当且充分的测试，以验证所实施安全措施的有效性。

5.1.4 如果认证机构或技术服务部门没有从车辆制造商处收到足够的信息来评估车型的网络安全性，则评估认证机构也应拒绝授予网络安全方面的型式认证。

5.2. 根据本法规认证或延期或拒绝认证的通知应通过符合本法规附件 2 中所示格式的形式传达给采用本法规的 1958 年协议各方。

5.3. 认证机构不得在未验证制造商已制定了令人满意的安排和程序以正确管理本法规所涵盖的网络安全方面的情况下授予任何型式认证。

5.3.1. 除了 1958 年协议附表 2 中规定的标准外，认证机构及其技术服务机构应确保：

（a） 具备适当网络安全技能和特定汽车风险评估知识的称职人员；[1]

（b） 根据本法规实施统一评估程序。

5.3.2. 采用本法规的各缔约方应通知并由其认证机构通知采用本联合国法规的缔约方的其他认证机构，告知其作为依据的方法和标准，以评估根据本法规和本法规采取的措施的适当性特别是第 5.1、7.2.段。和 7.3。

该信息仅在（a）首次根据本法规授予认证之前和（b）每次更新评估方法或标准时共

享。

为了收集和分析最佳实践，并确保采用本法规的所有认证机构都能统一应用本法规，本信息旨在共享。

5.3.3. 第 5.3.2 段中提及的信息应在适当时间内，且不迟于根据相关评估方法和标准首次批准前 14 天，以英语上传至联合国欧洲经济委员会建立的安全互联网数据库“DETA”[2]。该信息应足以理解认证机构针对第 5.3.2 段中提及的每个具体要求采用的最低性能水平，以及其用于验证满足这些最低性能水平的流程和措施。[3]

5.3.4. 收到第 5.3.2 段所述信息的审批机关可在通知之日后 14 天内将意见上传至 DETA，从而向通知审批机关提交意见。

5.3.5. 如果授予审批机关无法考虑根据第 5.3.4.段收到的意见，则已发送意见的审批机关和授予审批机关应根据 1958 年协议附表 6 寻求进一步澄清。本法规世界车辆法规协调论坛（WP.29）的相关附属工作组[4]应就评估方法和标准的通用解释达成一致。[5]应实施通用解释，所有认证机构应根据本法规相应发布型式认证。

5.3.6. 根据本法规授予型式认证的各认证机构应将授予的认证通知其他认证机构。型式认证以及补充文件应由认证机构在授予 DETA 认证之日后 14 天内以英语上传。[6]

5.3.7. 缔约方可研究根据第 5.3.6.段上传的信息授予的批准。如果缔约方之间存在任何分歧，应根据 1958 年协定第 10 条和附表 6 解决。缔约方还应将 1958 年协议附表 6 所指的不同解释通知世界车辆法规协调论坛（WP.29）的相关附属工作组。相关工作组应支持解决分歧意见，必要时可就此咨询 WP.29。

5.4. 为了第 7.2 段的目的。根据本法规，制造商应确保实施本法规涵盖的网络安全方面。

6. 网络安全管理系统合规证书

6.1. 缔约方应指定一个认证机构对制造商进行评估，并颁发 CSM 合规证书。

6.2. 车辆制造商或其正式授权代表应提交网络安全管理系统合规证书申请。

6.3. 应随附下述文件一式三份，并随附以下文件：

6.3.1. 描述网络安全管理系统的文件。

6.3.2. 使用附件 1 附录 1 中定义的模型签署的声明。

6.4. 在评估过程中，制造商应使用附件 1 附录 1 中定义的模型进行声明，并向认证机构或其技术服务部门证明其具有符合本法规中所有网络安全要求的必要流程。

6.5. 当该评估已圆满完成，并收到制造商根据附件 1 附录 1 中定义的模型签署的声明后，本法规附件 4 中所述的 CSM 合格证书（以下简称 CSM 合格证书）应授予制造商。

6.6. 认证机构或其技术服务机构应使用本法规附件 4 中规定的模型作为 CSM 的合格证书。

6.7. CSMS 合规证书的有效期最长为三年，自证书颁发之日起计算，除非证书被撤销。

6.8. 授予 CSM 合规证书的审批机关可在任何时候验证是否继续满足其要求。如果不再满足本法规中规定的要求，认证机构应撤销 CSM 的合格证书。

6.9. 制造商应将影响 CSM 合规证书相关性的任何变更通知认证机构或其技术服务机构。与制造商协商后，认证机构或其技术服务机构应决定是否需要进行新的检查。

6.10. 在适当的时候，允许审批机关在 CSM 合规证书有效期结束前完成其评估，制造商应申请新的 CSM 合规证书或现有 CSM 合规证书的延期。审批机关应根据积极的评估，为 CSM 颁发新的合规证书或将其有效期再延长三年。认证机构应验证 CSM 是否继续符合本法规的要求。如果变更已提请审批机关或其技术服务机构注意，且已对变更进行了积极的重新评估，审批机关应颁发新的证书。

6.11. 对于与 CSM 相关的车型，应将 CSM 制造商合格证书的到期或撤销视为第 8 段中提到的认证修改，如果不再满足授予批准的条件，则可能包括撤销批准。

7. 规格

7.1. 一般规格

7.1.1. 本法规的要求不得限制其他联合国法规的规定或要求。

7.2. 网络安全管理系统的要求

7.2.1. 对于评估，认证机构或其技术服务机构应验证车辆制造商是否有网络安全管理系统，并应验证其是否符合本法规。

7.2.2. 网络安全管理体系应包括以下方面：

7.2.2.1. 车辆制造商应向认证机构或技术服务机构证明其网络安全管理系统适用于以下阶段：

（a） 发展阶段；

（b） 生产阶段；

（c） 后期制作阶段。

7.2.2.2. 车辆制造商应证明其网络安全管理系统中使用的过程确保充分考虑了安全性，包括附录 5 中列出的风险和缓解措施。这应包括：

（a） 制造商组织内部用于管理网络安全的流程；

（b） 用于识别车辆类型风险的过程。在这些过程中，应考虑附件 5 A 部分中的威胁和其他相关威胁；

（c） 用于评估、分类和处理已识别风险的流程；

（d） 用于验证已识别风险得到适当管理的流程；

（e） 用于测试车型网络安全性的流程；

（f） 用于确保风险评估保持最新的流程；

（g） 根据已识别的新网络威胁和漏洞，用于监测、检测和应对网络攻击、网络威胁和车辆类型漏洞的流程，以及用于评估实施的网络安全措施是否仍然有效的流程。

（h） 用于提供相关数据以支持对未遂或成功网络攻击的分析的过程。

7.2.2.3. 根据第 7.2.2.2（c）和 7.2.2.2（g）段中提及的分类，车辆制造商应证明其网络安全管理系统中使用的过程确保需要车辆制造商响应的网络威胁和漏洞应在合理的时间范围内缓解。

7.2.2.4. 车辆制造商应证明其网络安全管理系统确保第 7.2.2.2（g）段中提及的监控持续进行。这应：

（a） 将首次登记后的车辆纳入监控范围；

（b） 包括从车辆数据和车辆日志中分析和检测网络威胁、漏洞和网络攻击的能力。该能

力应符合第 1.3 段的要求。以及车主或司机的隐私权，特别是在同意方面。

7.2.2.5. 根据第 7.2.2.2.段的要求，车辆制造商应证明其网络安全管理系统将如何管理与合同供应商、服务提供商或制造商子组织之间可能存在的依赖关系。

7.3. 对车辆类型的要求

7.3.1. 制造商应具有与认证车型相关的网络安全管理系统的有效合格证书。

但是，对于 2024 年 7 月 1 日之前的类型认证，如果车辆制造商能够证明无法按照 CSMS 开发车型，则车辆制造商应证明在相关车型的开发阶段充分考虑了网络安全。

7.3.2. 对于正在批准的车型，车辆制造商应识别和管理与供应商相关的风险。

7.3.3. 车辆制造商应确定车辆类型的关键要素，并对车辆类型进行详尽的风险评估，并应适当处理/管理已识别的风险。风险评估应考虑车辆类型的各个要素及其相互作用。风险评估应进一步考虑与任何外部系统的相互作用。在评估风险时，车辆制造商应考虑与附件 5、A 部分所指的所有威胁相关的风险以及其他相关风险。

7.3.4. 车辆制造商应保护车辆类型免受车辆制造商风险评估中确定的风险。应采取相应的缓解措施，以保护车辆类型。实施的缓解措施应包括附件 5 第 B 部分和第 C 部分中提及的与所识别风险相关的所有缓解措施。但是，如果附件 5 第 B 部分或 C 部分中提及的缓解措施不相关或不足以识别风险，则车辆制造商应确保实施另一种适当的缓解措施。

特别是，对于 2024 年 7 月 1 日之前的类型认证，如果附件 5 第 B 或 C 部分中提到的缓解措施在技术上不可行，车辆制造商应确保实施另一种适当的缓解措施。制造商应向认证机构提供相应的技术可行性评估。

7.3.5. 车辆制造商应采取适当和相称的措施，以确保车辆类型（如提供）上的专用环境，用于存储和执行售后市场软件、服务、应用程序或数据。

7.3.6. 在类型认证之前，车辆制造商应进行适当且充分的试验，以验证所实施安全措施的有效性。

7.3.7. 车辆制造商应针对车辆类型采取措施，以：

（a） 检测并防止针对该车型车辆的网络攻击；

（b） 支持车辆制造商在检测与车型相关的威胁、漏洞和网络攻击方面的监控能力；

（c） 提供数据取证能力，以便对未遂或成功的网络攻击进行分析。

7.3.8. 本法规中使用的加密模块应符合一致标准。如果使用的加密模块不符合一致标准，则车辆制造商应证明其使用合理。

7.4. 报告规定

7.4.1. 根据第 7.2.2.2.（g）段的规定，车辆制造商应至少每年向认证机构或技术服务机构报告一次监测活动的结果，或更频繁地报告（如相关），其中应包括有关新网络攻击的相关信息。车辆制造商还应向认证机构或技术服务机构报告并确认，针对其车型实施的网络安全缓解措施仍然有效，并采取了任何其他措施。

7.4.2 如有必要，认证机构或技术服务机构应验证提供的信息，并要求车辆制造商纠正任何检测到的无效性。

如果报告或回复不充分，审批机关可根据第 6.8 段的规定决定撤销 CSM。

8．车辆类型的修改和扩展

8.1. 应将影响本法规要求的网络安全和/或文件技术性能的每项车型修改通知认证该车型的认证机构。
然后，审批机关可以：

8.1.1. 考虑到所做的修改仍然符合现有型式批准的要求和文件；或

8.1.2. 根据第 5 段进行必要的补充评估，并在相关情况下要求负责进行测试的技术服务机构提供进一步的测试报告。

8.1.3. 认证的确认、延期或拒绝（规定了变更）应通过符合本法规附件 2 中所示格式的通知表进行传达。发布认证延期的认证机构应为该延期指定一个序列号，并通过符合本法规附件 2 中所示格式的通知表通知采用本法规的 1958 年协议的其他缔约方。

9. 生产一致性

9.1. 生产一致性程序应符合 1958 年协议附表 1（E/ECE/TRANS/505/Rev.3）中规定的程序，并符合以下要求：

9.1.1. 认证持有者应确保记录生产一致性试验的结果，并确保所附文件在与认证机构或其技术服务机构商定的期限内保持可用。该期限不得超过 10 年，从生产最终停止时算起；

9.1.2. 授予型式认证的认证机构可随时验证各生产设施中采用的一致性控制方法。这些验证的正常频率应为每三年一次。

10. 对生产不合格的处罚

10.1. 如果不符合本法规中规定的要求或样车不符合本法规的要求，则可撤销根据本法规授予的车型认证。

10.2. 如果认证机构撤销其先前授予的认证，则应立即通过符合本法规附件 2 中所示格式的通知表通知采用本法规的缔约方。

11. 生产完全停止

11.1. 如果认证持有者完全停止生产根据本法规认证的车辆类型，则其应通知授予认证的机构。在收到相关通知后，该机构应通过一份认证表格的副本通知采用本法规的协议的其他缔约方，该批准表格的末尾应以大写字母注明已签字并注明日期的注释“停止生产”。

12 负责进行认证测试的技术服务机构的名称和地址，以及类型认证机构

12. 1. 采用本法规的协议缔约方应向联合国秘书处通报负责进行认证试验的技术服务机构和授予认证的型式认证机构的名称和地址，以及认证、延期、拒绝或撤销的证明表格将发送在其他国家签发的批准证书。

附件 1

信息文件

以下信息（如适用）应提供一式三份，并包括一份内容清单。任何图纸均应以适当比例提供，且应足够详细，尺寸为 A4 或 A4 格式的文件夹。照片（如有）应显示足够的细节。

1. 制造商（制造商的商品名）
2. 类型和一般商业说明
3. 型式识别方法（如果标记在车辆上）
4. 该标记的位置
5. 车辆类别
6. 制造商/制造商代表的名称和地址
7. 装配厂的名称和地址
8. 代表性车辆的照片和/或图纸
9. 网络安全

9.1. 车辆类型的一般结构特征，包括：

（a） 与车型网络安全相关的车辆系统；

（b） 与网络安全相关的系统组件；

（c） 这些系统与车辆类型和外部接口内的其他系统的相互作用。

9.2. 车辆类型的示意图

9.3. CSMS 合规证书编号

9.4. 描述其风险评估结果和识别风险的待认证车型文件

9.5. 待认证车型的文件，描述已在所列系统或车型上实施的缓解措施，以及它们如何解决所述风险

9.6. 待认证车型的文件，描述了售后市场软件、服务、应用程序或数据专用环境的保护

9.7. 待认证车型的文件，描述了用于验证车型及其系统网络安全性的试验以及这些试验的结果

9.8. 关于网络安全方面供应链考虑的说明

附件 1-附录 1

CSMS 的制造商合规声明模型

制造商关于符合网络安全管理系统要求的声明

制造商名称:.....

制造商地址:.....

.....（制造商名称）证明已安装并将维护符合联合国第 155 号法规第 7.2 段中规定的网络安全管理系统要求的必要程序。

完成地点:.....

日期:.....

签字人姓名:.....

签字人的职能：.....

.....

（制造商代表的印章和签名）

附件 2

表达

（最大格式：A4（210 x 297 mm））

发行人：管理机构名称：

.....
.....
.....

关于 [8]：

批准

批准延期

自年月日起撤销批准

拒绝批准

生产完全停止

符合联合国第 155 号法规的车辆类型

批准号：.....

分机号码：.....

延期原因：.....

1. 制造商（制造商的商品名）：.....
2. 类型和一般商业说明.....
3. 型式识别方法（如果标记在车辆上）：.....

3.1. 该标记位置：.....

4. 车辆类别：.....
5. 制造商/制造商代表的名称和地址：.....
6. 生产工厂的名称和地址.....
7. 网络安全管理系统合规证书编号：.....
8. 负责进行试验的技术服务部门：.....
9. 试验报告日期：.....
10. 试验报告数量:.....
11. 备注：（如有）.....
12. 地点：.....
13. 日期：.....
14. 签名：.....
15. 提交给审批机关的信息包索引（可根据要求获取）随附：

[7] 授予/延长/拒绝/撤销认证的国家的识别号（见本法规中的认证规定）。

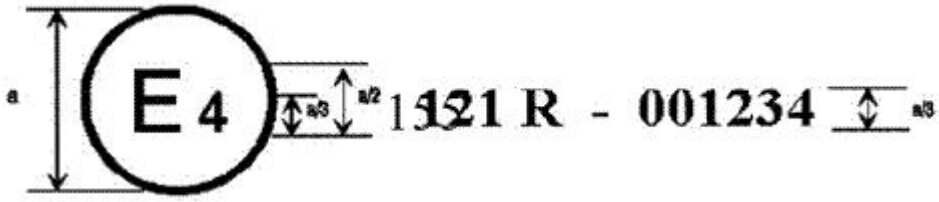
[8] 删除不适用的内容。

附件三

认证标志的排列

模型 A

（见本法规第 4.2 段）



a=最小 8 毫米。

附在车辆上的上述认证标志表明，已在荷兰（E 4）根据第 155 号法规认证了相关道路车辆类型，认证号为 001234。认证号的前两位数字表示认证是根据本法规原始形式（00）的要求授予的。

附件 4

CSMS 合规证书模型

网络安全管理系统合
规证书

联合国法规编号[本法规]证书编号

[参考编号]

[……批准机关]

证明

制造商：.....

制造商地址：.....

符合第 155 号法规第 7.2 段的规定

已对以下各项进行检查：.....

发件人（认证机构或技术服务机构的名称和地址）：.....

报告数量：.....

本证书有效期至[…..日期]

于[….日期]

在[….地点]

[……签字]

附件：制造商提供的网络安全管理系统说明。

附件五

威胁和相应缓解措施列表

1. 本附件由三部分组成。本附件 A 部分描述了威胁、漏洞和攻击方法的基线。本附录 B 部分描述了针对车辆类型的威胁的缓解措施。C 部分描述了针对车辆外部区域（如 IT 后端）的威胁缓解措施。

2. 车辆制造商实施的风险评估和缓解措施应考虑 A、B 和 C 部分。

3. 高级别漏洞及其相应示例已在 A 部分中编入索引。在 B 部分和 C 部分的表格中引用了相同的索引，以将每个攻击/漏洞与相应的缓解措施列表联系起来。

4. 威胁分析还应考虑可能的攻击影响。这些可能有助于确定风险的严重性并识别其他风险。可能的攻击影响可能包括：

（a） 受影响车辆的安全操作；

（b） 车辆功能停止工作；

（c） 软件修改，性能改变；

（d） 软件更改但无操作效果；

（e） 数据完整性破坏；

（f） 违反数据保密规定；

（g） 数据丢失；

（h） 其他，包括犯罪。

第 A 部分：与威胁相关的漏洞或攻击方法

1.表 A1 中列出了威胁和相关漏洞或攻击方法的高级描述。

第 B 部分：车辆威胁的缓解措施

1.“车辆通信通道”的缓解措施

表 B1 列出了与“车辆通信通道”相关的威胁缓解措施。

2.“更新过程”的缓解措施

表 B2 列出了与“更新过程”相关的威胁缓解措施。

3.“促进网络攻击的非预期人类行为”的缓解措施

表 B3 中列出了与“促进网络攻击的非预期人类行为”相关的威胁缓解措施。

4.“外部连接和连接”的缓解措施

表 B4 列出了与“外部连接和连接”相关的威胁缓解措施。

5.“攻击的潜在目标或动机”的缓解措施

表 B5 列出了与“攻击的潜在目标或动机”相关的威胁缓解措施。

6.“如果未充分保护或加固，可能被利用的潜在漏洞”的缓解措施

表 B6 中列出了与“如果未充分保护或加固，可能被利用的潜在漏洞”相关的威胁缓解措施。

7.“车辆数据丢失/数据泄露”的缓解措施

表 B7 列出了与“车辆数据丢失/数据泄露”相关的威胁缓解措施。

8.“对系统进行物理操作以启用攻击”的缓解措施

表 B8 列出了与“物理操纵系统以发起攻击”相关的威胁缓解措施。

第 C 部分：车辆外部威胁的缓解措施

1.“后端服务器”的缓解措施

表 C1 中列出了与“后端服务器”相关的威胁缓解措施。

2.“非预期人为行为”的缓解措施

表 C2 中列出了与“非预期人类行为”相关的威胁缓解措施。

[1]例如 ISO 26262-2018、ISO/PAS 21448、ISO/SAE 21434

[2]https://www.unece.org/trans/main/wp29/datasharing.html

[3]关于上传的详细信息（如方法、标准、绩效水平）的指南以及格式应在解释文件中给出，该文件由网络安全和空中问题工作组为 GRVA 第七届会议编写。

[4]自动/自动和连接车辆工作组（GRVA）

[5]该解释应反映在第 5.3.3 段脚注中提及的解释文件中。

[6]GRVA 将在其第七次会议期间制定关于文件包最低要求的进一步信息。