汽车网络安全管理系统实践探索

呼啸，陶述斌*，王海均

中国汽车技术研究中心有限公司，天津 300163

摘要：随着智能网联汽车领域飞速发展，汽车信息化水平大幅提升，信息交互的场景繁杂、种类多样、数量庞大，汽车网络安全风险日益加剧。伴随着国内外相关标准法规不断完善，相关部门监管力度逐渐深化的大背景，以本领域相关理论知识为依托，结合主流汽车企业及零部件供应商的实践经验积累，本文设计并开发一套汽车网络安全管理系统。该系统对汽车网络安全管理体系的建设进行分析及探索，并阐明体系建设的必要性，旨在为汽车产业链上下游相关企业搭建汽车网络安全管理体系提供建设思路，以便系统性化解网络安全风险。助力汽车企业在满足合规要求的同时，强化自身内控机制，保障业务连续性，在智能网联的快车道上高质量发展。

关键词：智能网联；汽车网络安全；信息安全；管理系统

DOI: 10.57237/j.cst.2024.01.003

Practice and Exploration of Cyber Security Management System

Hu Xiao, Tao Shubin, Wang Haijun

China Automotive Technology and Research Center Co., Ltd., Tianjin, 300163, China

Abstract: With the rapid development of the field of intelligent network connected vehicles, the level of automobile informatization has been greatly improved. The scene of information interaction is more and more complex, the type of information is more and more diverse, at the same time, the amount of information is more and more huge. Therefore, automobile enterprises are facing more and more security risks in network security. Under the background of continuous improvement of relevant standards and regulations at home and abroad and gradual deepening of supervision by relevant departments, this paper designs and develops a set of automobile network security management system, based on relevant theoretical knowledge in this field and the practical experience of mainstream automobile enterprises and parts suppliers. The system analyzes and explores the construction of automobile network security management system, and clarifies the necessity of system construction, aiming to provide construction ideas for relevant enterprises in the upstream and downstream of automobile industry chain to build automobile network security management system, so as to systematically resolve network security risks. This system helps automobile enterprises to meet compliance related requirements, while strengthening their own internal control mechanism, ensuring business continuity, and developing high-quality in the fast lane of intelligent networking.

Keywords: Intelligent Connected Vehicle; Cyber Security; Information Security; Management System

*通信作者：陶述斌, taoshubin@catarc.ac.cn

收稿日期: 2022-09-12; 接受日期: 2022-10-09; 在线出版日期: 2024-01-20

1 前言

当网联化使汽车由封闭系统走向开放的同时，尤其是汽车通过通信网络接入互联网连接到云端之后，汽车可以被黑客攻击的风险也大量增加[1]。现阶段，国内大部分主机厂、零部件供应商等汽车产业链相关企业的汽车网络安全管理体系正处于建设中或需进一步完善的阶段，且已有的网络安全保障能力参差不齐，无法满足车联网相关业务快速发展的需求。由汽车网络安全带来的风险种类不断增加，危害程度不断加剧，产业链相关企业应尽早准备，采取相关措施，以免日后在业务扩展或法规层面上的被动。

2 汽车网络安全行业政策背景

2.1 国际情况

2020 年 6 月，UNECE 下属联合国世界车辆法规协调论坛（简称 UN/WP.29）发布了全球首个汽车网络安全领域的强制性法规：《网络安全与网络安全管理系统》（以下简称 R155），并于 2021 年 1 月正式生效。该法规将智能汽车网络安全准入的要求划分为两个部分，一是针对智能汽车车辆制造商的网络安全管理体系要求，二是针对车辆产品的网络安全能力要求，并明确前者是后者的先决条件。

2020 年 12 月，德国汽车工业协会质量管理中心 VDA QMC 发布了《汽车网络安全管理体系审核》（通常称为“VDA 红皮书”）。作为审核支撑类文件，VDA 红皮书可对 R155 法规中 CSMS 认证部分的审核提供指导，在审核内容方面给出了最低通过要求。

2021 年 8 月 31 日，ISO（国际标准化组织）和 SAE（美国汽车工程师学会）联合发布了汽车网络安全领域首个国际标准：ISO/SAE 21434《道路车辆-网络安全工程》（以下简称 ISO/SAE 21434）。该标准主要应用于道路车辆原始设备制造商以及各级供应商。ISO/SAE 21434 定义了汽车网络安全的完整框架和产品全生命周期的相关流程,可作为 R155《网络安全与网络安全管理体系》中网络安全管理体系建设的落地指导文件,从而帮助汽车产业链上下游企业有效应对网络安全风险。

2022 年 3 月 31 日，ISO（国际标准化组织）发布了汽车网络安全领域审核类标准：ISO/PAS 5112《道路车辆-网络安全工程审核指南》(以下简称 ISO/PAS 5112)，该文件紧密衔接 ISO/SAE 21434 的相关要求，可对 ISO/SAE 21434 标准条款进行审计，考虑到 ISO/SAE 21434 是针对 R155 法规实践落地的指导文件，故 ISO/PAS 5112 也可以帮助相关人员从审核的角度去理解汽车网络安全体系的内容，从而更好的进行实施搭建。

2.2 国内情况

2021 年 8 月 12 日，工业和信息化部发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》，文中明确提到：应加强汽车的网络安全管理，企业应当建立汽车网络安全管理制度，依法落实网络安全等级保护制度和车联网卡实名登记管理要求，明确网络安全责任部门和负责人[2]。

2021 年 9 月 16 日，工业和信息化部发布的《关于加强车联网网络安全和数据安全工作的通知》从网络安全和数据安全基本要求、汽车安全防护、网络安全防护等六个方面强调了管理要求。如：落实安全主体责任。各相关企业要建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任。强化企业内部监督管理，加大资源保障力度，及时发现并解决安全隐患。加强网络安全和数据安全宣传、教育和培训[3]。

2021 年 7 月 13 日，三部门联合发布的《网络产品安全漏洞管理规定》，对网络产品安全漏洞的发现、报告、修补和发布进行了规范。文中明确提到：网络产品提供者、网络运营者和网络产品安全漏洞收集平台应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，留存网络产品安全漏洞信息接收日志不少于 6 个月。网络运营者发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证并完成修补[4]等相关要求。

3 汽车网络安全管理体系建设的必要性

3.1 满足合规要求

与信息系统网络安全相类似，智能网联汽车除了车辆和车联网采取合理安全策略和应用适当安全产品，也面临着政策标准合规等安全相关业务需求[5]。随着

国际国内相关法规政策的不断出台，监管要求逐渐深化，汽车网络安全的合规性已经从过去的符合标准进入到遵循法规的时代，对企业网络安全管理体系的要求也提出了新的挑战，迈上了新的台阶。相关企业需尽早建立完善管理制度、采取有效手段，保障自身在满足合规要求的条件下，进行生产经营活动，避免由此带来的负面影响。智能网联汽车的网络和数据安全问题不仅关系到汽车产业的健康有序发展，更关系到人身安全、社会安全和国家安全，安全形势严峻而监管需求迫切[6]。

3.2 保证业务连续性

随着社会经济的飞速发展，汽车行业的队伍也在不断壮大。未来中国汽车行业的市场需求还将会进一步增加，业务范围也会再进一步拓展。业务连续性管理是企业经营一体化的管理流程，使企业对潜在的威胁与冲击加以辨识分析，能够为企业提供业务中断及恢复的战略和操作层面的框架[7]。企业需意识到，汽车网络安全工作对业务连续性的重要性，而不仅仅是停留在攻防层面。

4 汽车网络安全管理系统设计方案

4.1 方案简介

本文以当下汽车网络安全标准法规为依托，结合汽车企业实际的操作规范及流程，设计一套管理系统，在保证合规的基础上，提升工作效率。该管理系统的设计思路总体上是将汽车网络安全分为核心业务模块和辅助功能模块两大类。

4.2 核心业务模块

治理文化：包含制度文件、文化宣贯、安全培训等子模块。制度文件是对汽车网络安全管理体系的各级文件进行管理，需明确文件的版本号、生效日期、适用范围、审核批准等信息，并对历史变更的版本及情况说明保留痕迹。文化宣贯和安全培训需记录计划开展时间、实际开展时间、负责人、参与人及活动相关素材等信息。该模块主要用于协助组织进行制度和文化的建设，并切实提升网络安全意识及能力。

信息共享：需明确涉及汽车网络安全共享信息的基本情况，如负责人、信息所属部门、保密级别、类型等。在对此类信息进行共享前，需要提交申请流程，经该信息负责人、申请方领导、负责方领导审批通过后，方可进行分享操作，整个过程保留相关痕迹。

工具管理：此处的工具管理并非传统意义上的维修工具，而是指与汽车网络安全相关的工具，如在使用中与相关项或组件进行交互的工具、用于评估或判断相关项或组件安全状态的工具等。首先需建立台账并明确责任人，台账信息应包含但不限于工具识别号、名称、版本、类型、存放位置、责任部门、责任人、简介等相关信息。此外还需要工具维护及报废的情况进行记录，包含但不限于时间、责任人、内容等相关信息。如果是涉及软件的工具，需维护授权情况及操作说明书等。

安全审计：分为内部评审和管理评审两类，可按照准备阶段、实施阶段、监督整改阶段进行管理。准备计划阶段需明确审核组成员、受审的部门、评审的依据及内容等。实施阶段需明确不符合项及严重程度，与受审部门确认情况，审核结果审核后进行发布。监督整改阶段需针对不符合项制定整改措施计划，确认、实施、验证。

研发阶段：应包含项目信息、相关性判断、网络安全计划、原始需求收集、项目定义、TATA 分析、目标及概念、网络安全方案、安全需求分发、网络安全详细设计、系统集成与测试、网络安全确认、后生产发布等关键环节，可根据实际情况进行裁剪。

生产阶段：主要涉及生产控制计划，应确保汽车产品在生产过程中遵守研发阶段所确定的网络安全规范，能够执行并防范引进新的网络安全漏洞。

运维阶段：应广泛收集各个渠道涉及网络安全的风险，记录情报来源、情报类别、所关联的产品信息、上报人信息等。然后进行信息的初筛，按漏洞流程或事件流程进行处置。两个流程中均需对情报进行定级、方案制定与验证、方案实施、有效性验证、达标判断等操作。事件的根本原因可能是漏洞，漏洞也可能升级为事件，建设时需考虑流程转换。

供应商管理：在传统供应商管理的基础上，重点关注与网络安全相关的事项，涉及准入/定点评价项、接口协议检查项、合同条款、绩效评价项等方面。

4.3 辅助功能模块

看板管理：该板块面向的对象主要是中高层领导。通过归纳、总结系统表单录入的原始业务数据，根据

不同统计维度，借助环形图、气泡图、趋势图等多种图表形式进行展示，可将整体业务流程的开展情况直观的呈现出来，便于使用者从宏观的角度对整体状况进行把握。

权限管理：该板块面向的对象主要是系统管理员及开发管理员。本文的设计是从菜单权限、数据权限、逻辑权限、按钮权限等维度进行管理，实现让对应的人聚焦于做对应的事。

预警管理：该板块面向的对象主要是中层领导及业务人员。系统支持自定义需要预警的活动节点及预警的时间，相对于传统的预警模式来说，形式更加灵活。预警的结果可从预警消息处查看，同时也可在有时效性限制的看板模块直观的看到。

5 结论

智能网联汽车是多种先进信息网络技术与装备制造技术融合的产物，软件大规模应用、外部连通性增强、网络威胁复杂等特点，使智能网联汽车面临的安全威胁非常突出，必须通过应用和提高网络安全技术手段来强化保障能力[8]。

对于我国来说，智能网联汽车行业属于新兴行业，其中应用的信息安全技术较为薄弱，需要进一步进行完善[9]。本文基于国际、国内汽车网络安全方面的法规标准情况，从满足合规要求、保证业务连续性等方面讲述了汽车网络安全管理体系建设的必要性，并以主辅结合的形式，给出了一套汽车网络安全管理系统的设计方案。

智能网联汽车是汽车全产业链价值链、车联网生态、互联网生态等相互衔接融合的枢纽[10],汽车网络安全作为汽车企业安全中的关键一环，需引起足够重视，及时采取措施，推动汽车产业高质量发展。

参考文献

[1] 胡欣宇，张洁．车联网的发展与挑战 [J]．物联网技术，2017, 7 (2): 56-59.

[2] 关于加强智能网联汽车生产企业及产品准入管理的意见 [S].

[3] 关于加强车联网网络安全和数据安全工作的通知 [S].

[4] 工业和信息化部，国家互联网信息办公室，公安部关于印发网络产品安全漏洞管理规定的通知 [J]．中华人民共和国国务院公报. 2021 (28): 49-51.

[5] 李端，闫寒．浅析智能网联汽车网络安全 [J]．工业信息安全, 2022 (3): 97-103.

[6] 冯聪．智能网联汽车网络安全问题的治理与执法探索 [A]．公安部网络安全保卫局．2020 互联网安全与治理论坛论文集 [C]．公安部网络安全保卫局：《信息网络安全》北京编辑部, 2020: 4.

[7] 丁辉．企业安全管理和业务连续性管理 [J]．中国标准化，2016, 0 (1): 107-110.

[8] 安晖．如何保障智能网联汽车的网络安全性 [J]．软件和集成电路, 2021 (11): 26-27.

[9] 赵馨月．智能网联汽车信息安全关键技术 [J]．时代汽车，2021 (1): 18-19. DOI: 10.3969/j.issn.1672-9668.2021.01.008.

[10] Wai CHEN，李源，刘玮．车联网产业进展及关键技术分析 [J]．中兴通讯技术, 2020, 26 (01): 5-11.