ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 107-2022

车辆信息安全应急响应和漏洞管理技术要求

Technical requirements for incident/emergency response and vulnerabilitymanagement of vehicle information security

2022-11-02 发布　　2022-11-03 实施

吉林省汽车电子协会　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国第一汽车集团有限公司智能网联开发院、长春嘉诚信息技术股份有限公司联合提出。

本文件由吉林省汽车电子协会归口。

本文件起草单位：长春嘉诚信息技术股份有限公司、中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：李忆平、宋涛、田锰、李红澳、汤利鑫、朱琳、孙振、李佳桐、时晓亮、陈后立、边泽宇。

本文件参与起草单位：沙龙机甲科技有限公司、吉林大学汽车仿真与控制国家重点实验室、中国汽车工程研究院股份有限公司、一汽奔腾轿车有限公司、东风汽车集团有限公司技术中心、长春吉大正元信息技术股份有限公司、重庆长安汽车股份有限公司、一汽-大众汽车有限公司。

本文件参与起草人：王思涵、李杰、全代勇、雷凯、周海鹰、孙伟、苏日、汪向阳、王博。

本文件审查人：杨彦鼎（东风汽车集团有限公司技术中心）、夏国强（中国汽车工程研究院股份有限公司）、马文峰（一汽奔腾轿车有限公司）、马喜来（一汽解放汽车有限公司）、占锐（东风汽车集团有限公司技术中心）、孔晓霜（中国第一汽车集团有限公司创新技术研究院）。

本文件为首次发布。

引　言

随着我国汽车行业在信息化工作的深入开展，车辆信息系统已经进入运行维护阶段，然而，提供运行维护服务标准和规范还不够完善，车辆信息系统在运行中提供不同功能的新型服务，更需要一个系统的体系支撑起运行维护。

系统的运行维护主要由应急响应和漏洞管理两个方面进行技术支撑，对车辆信息系统中的所有车辆动态信息进行防护。

本文件规定了车辆信息系统运行维护组织在应急响应、漏洞管理过程和方法等，旨在建立高效车辆信息系统的应急、漏洞处理标准。

车辆信息安全应急响应和漏洞管理技术要求

1 范围

本文件规定了车辆信息安全应急响应与漏洞管理的技术要求。

本文件适用于车辆生产商、运营机构及车辆互联网生态系统信息安全相关方。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20985.2-2020 信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

GB/Z 20986-2007 信息安全事件分类分级指南

GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

车辆信息运营管理组织 vehicle information operation management organization

车辆信息系统建设或管理运营组织单位。

3.2

远程信息服务平台 remote vehicle cyber security platform

用于车辆管理或者提供信息服务的远程系统。

3.3

利益方 stakeholder

与车辆信息安全事件具备直接或间接利益关系的用户、部门、组织等。

3.4

网联汽车 connected vehicle

通过网络与远程信息服务平台连接并进行数据交换的汽车。

3.5

应急响应 incident response

为预防、监控、处置和管理车辆信息安全事件所采取的措施和活动。

3.6

应急响应组织 emergency response organization

管理应急响应事件的组织。

3.7

事件级别 event level

通过影响范围、影响程度决定事件处理的优先级。

3.8

漏洞 vulnerability

在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，使攻击者能够在未授权的情况下访问或破坏系统。

4 缩略语

下列缩略语适用于本文件：

CAN：控制器局域网络（Controller Area Network）；

ECU：电子控制单元（Electronic Control Unit）；

LIN：本地互联网络（Local Interconnect Network）；

T-Box：远程信息处理器（Telematics BOX）；

WiFi：无线（Wireless Fidelity）。

5 车辆信息安全应急响应要求

5.1 应急响应流程

车辆信息安全的应急响应流程分别按照应急准备、应急识别、应急处置、总结改进的流程进行概述，流程图如图1所示。

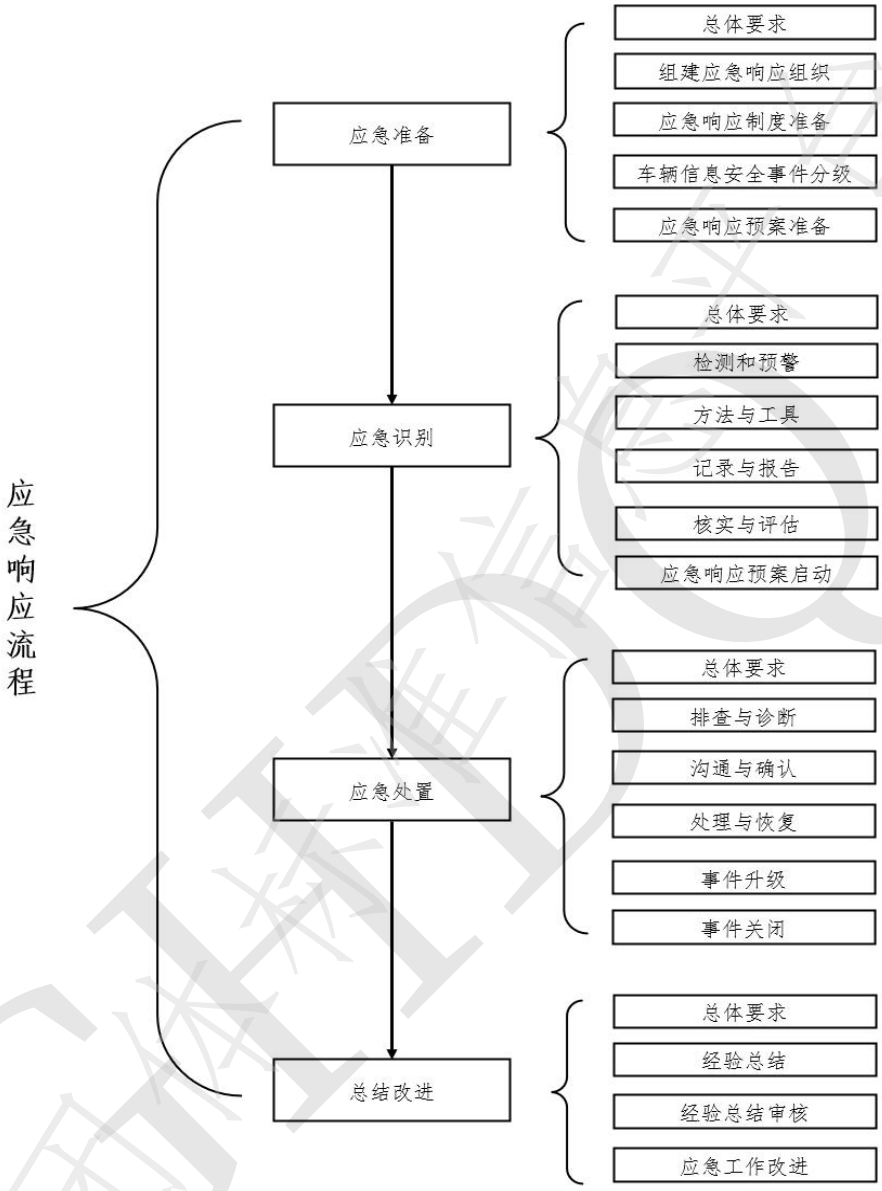

图1　应急相应流程

5.1.1　应急准备

5.1.1.1　总体要求

车辆信息安全事件应急响应策略应纳入车辆信息运营管理组织战略规划中，与组织的战略、目标和任务相统一，确保满足法律法规及相关标准体系的要求；采用自上而下的方式建立完善的应急响应组织架构，制定明确的应急响应过程制度文档，经过信息安全专家论证通过并取得高层管理者以及国家监管部门审批后正式实施运行，应急资源准备阶段组织应进行以下活动。

5.1.1.2　组建应急响应组织

组建车辆信息安全事件应急响应组织过程应满足以下要求：

a)　车辆信息安全应急响应组织可由车辆运营管理者、信息安全专家、车辆信息系统技术专家、软件开发人员、系统运维人员组成；

b)　应建立车辆信息安全应急响应领导小组，指导、管理和组织车辆信息安全应急响应整体工作；

c) 应规定运行维护服务及应急响应过程参与者角色及职责，关键角色岗位应建立人才储备机制；
d) 应根据应急响应服务的范围、要求等与相关利益方达成一致，并形成记录；
e) 应建立应急响应人员上岗培训制度，确保其具备岗位所需专业技能；
f) 应建立应急响应人员的定期考核制度，明确考核的指标、方法、周期，确保组织能够持续满足应急响应的要求；
g) 可建立应急响应监督管理委员会，对应急响应执行过程、制度执行情况等进行审查，记录审查过程及审查结果并妥善保存，针对审查发现的重大问题及时上报车辆信息安全应急响应领导小组并提供合理改进建议。

5.1.1.3 应急响应制度准备

车辆信息运营管理组织的应急响应制度应符合以下要求：
a) 应根据车辆信息安全需求制定车辆信息安全应急响应总体方针和策略，明确组织车辆信息安全应急响应工作的总体目标、范围、原则及应急响应框架；
b) 应对车辆信息安全应急响应活动中的各类管理内容制定应急响应制度；
c) 应对车辆信息安全应急响应管理人员或操作人员的日常操作建立操作规程；
d) 应定期对车辆信息安全应急响应制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
e) 应明确车辆信息安全相关应急响应管理制度和操作规程的发布流程并进行版本控制；
f) 发生重大安全事件或业务流程发生变动时，应根据最新情况及时调整车辆信息安全应急响应制度。

5.1.1.4 车辆信息安全事件级别划分

车辆信息安全事件分级标准应遵循在任何情况下，基于车辆信息安全事件对组织运营的实际或预计的不利影响做出车辆信息安全事件等级划分；在任何情况下，车辆信息安全事件直接或间接威胁车辆使用者主体的生命、财产等重大合法权益的应最优先处理。车辆信息安全事件分级标准用于对车辆信息安全事件等级排列：
a) 一般事件级：对车辆信息系统产生较小的影响，影响局部功能的正常运行；
b) 较大事件级：对车辆信息系统产生较大的影响，影响大部分功能的正常运行；
c) 重大事件级：对车辆信息系统产生严重的影响，导致车辆信息系统瘫痪无法正常运行。

注：具体级别划分可参考GB/Z 209860-2007的信息安全事件分类分级方法。

5.1.1.5 应急响应预案准备

车辆信息安全事件应急响应预案应满足以下要求：
a) 应根据车辆信息安全事件类别及级别制定相应应急响应预案；
b) 应定期开展车辆信息安全应急响应预案演练，并根据演练过程中发现存在的不足对应急响应预案进行修订。

5.1.2 应急识别

5.1.2.1 总体要求

为了确保能够快速识别和有效地响应车辆信息安全事件，车辆信息运营管理组织方宜采取必要的技术手段和其他方面的支持手段建立车辆信息安全威胁监测与预警平台，同时确保组织内部能够快速有效的对车辆信息安全事件达成一致响应方案，应急识别阶段组织宜进行以下活动。

5.1.2.2 监测与预警

车辆信息安全事件监测与预警实施过程应满足以下要求：
a) 应对车辆信息安全受威胁对象建立监测与预警机制，采用必要技术或管理手段对被监测对象的机密性、完整性、可用性等进行监测。监测对象包括：
1) 网络和通信监测对象如：车内通信、车外近距离通信、车外远距离通信；

2） 安全计算环境监测对象如：车载计算芯片、WIFI、远程信息服务平台的计算环境等；
3） 应用系统监测对象如：T-Box 系统、车载娱乐系统、远程信息服务平台等；
4） 数据安全监测对象如：车辆位置信息、车辆行驶记录等；
5） 车辆供应链系统安全监测对象如：车载娱乐系统、车辆通信协议、传感器硬件、ECU控制器等；
6） 车辆信息运营管理组织认定必要纳入监测的对象。

注1：车内通信即车内系统、组件之间的通信，例如CAN通信、LIN通信、以太网通信等。
注2：车外近距离通信是指蓝牙、近场无线通信和WiFi等.
注3：车外远距离通信是指车辆通过蜂窝移动通信、卫星通信与远距离终端或车辆远程服务平台进行通信。
注4：车辆供应链系统主要是指为在整车制造和流通过程中提供或参与车辆信息系统设计或制造相关实体方。

b） 应对被监测对象设置安全参考模型，确定被监测对象关联的车辆信息安全事件。

5.1.2.3 方法与工具

车辆信息运营管理组织可以采用自动监测工具与人工结合的方式对被监测对象开展日常监测与预警活动。活动过程中可能涉及多种方法与工具，可能包括：

a） 车辆信息安全监测预警、车辆信息安全漏洞管理、车辆信息安全风险管理、车辆信息安全人工分析；
b） 信息安全管理方法论、风险管理方法论等。

5.1.2.4 记录与报告

车辆信息安全事件记录与报告过程应满足以下要求。

a） 应建立车辆信息系统监测、预警的记录和报告制度，并按照约定的形式和时间间隔上报现场负责人。
b） 应定期备份监测、预警的记录，确保记录不会丢失。
c） 应对车辆信息安全事件保持持续性追踪。
d） 报告内容应包括：
1） 报告人；
2） 车辆信息安全事件发生的时间、地点、具体位置；
3） 车辆安全事件基本情况描述，事件类型；
4） 影响的范围；
5） 初步原因分析。

注：报告内容可参照GB/T 20985.2-2020中附录B的信息安全态势、事件和脆弱性报告及表单示例设计。

5.1.2.5 核实与评估

对车辆信息安全事件的核实与评估过程应满足以下要求：

a） 现场负责人应对报告内容进行逐项核实；
b） 核实确认后的车辆信息安全事件报告，应提交给应急响应责任者；
c） 车辆信息安全事件报告应作为事件级别评估的输入；
d） 应急响应负责人应根据事件级别定义，初步确定车辆信息安全事件所对应的事件级别。

5.1.2.6 应急响应预案启动

车辆信息安全事件应急响应预案启动过程应满足以下要求：

a） 应建立、审议应急响应预案启动的策略和程序，以控制预案启动的授权和实施；
b） 应对应急响应预案启动可能造成的影响进行评估；
c） 应按照预定方案通知相关利益方，确定相关利益方已知悉通知内容，并进行记录留存；
d） 根据前期处置要求进行应急响应预案的自动启动，或由应急响应责任人或现场负责人启动预案；
e） 应记录应急响应预案启动、实施过程及结果。

5.1.3 应急处置

5.1.3.1 总体要求

依据车辆信息安全事件的评估结果，一旦被确认且响应被确定，应急处置阶段组织宜进行以下活动。

5.1.3.2 排查与诊断

车辆信息安全事件的排查与诊断过程应满足以下要求：

a) 应及时调度处置人员赴现场排查诊断车辆故障；
b) 现场处置人员排查与诊断过程中遇到无法独立解决的问题应上报寻求人员及技术支持；
c) 现场处置人员进行故障排查和诊断时用到的各种工具应进行统计记录；
d) 现场处置人员应随时向上级汇报故障排查情况、诊断信息、故障定位的结果；
e) 应将排查与诊断的过程与结果信息进行整理与归档并定期进行备份。

5.1.3.3 沟通与确认

车辆信息安全事件的沟通与确认应满足以下要求：

a) 现场场处置人员应及时与相关利益方沟通，沟通内容主要包括系统故障点、造成故障的原因、排查诊断状况等；
b) 在处理故障前现场处置人员应及时上报排查诊断车辆故障结果及处置方案。

5.1.3.4 处理与恢复

对车辆信息安全事件的处理与恢复过程应满足以下要求：

a) 应控制处置活动造成的影响范围，降低事件损失；
b) 采用的方法、手段不应造成次生、衍生事件的发生；
c) 现场处置人员应记录处置与恢复过程及结果并上报；
d) 处置完毕后事件各方应对现场处置结果进行确认。

5.1.3.5 事件升级

车辆信息安全事件升级过程应满足以下要求：

a) 现场负责人应根据实际情况整理升级信息并通报相关利益方；
b) 信息通报时应验证双方身份，确保通报信息的真实性。

5.1.3.6 事件关闭

车辆信息安全事件关闭过程应满足以下要求：

a) 组织应建立、审议事件关闭的策略和程序，以控制事件关闭的实施；
b) 事件处置人员应按照事件关闭程序提出申请；
c) 事件关闭时应及时归档事件相关文档；
d) 事件关闭后应备份保留相关资料文档。

5.1.4 总结改进

5.1.4.1 总体要求

信息安全事件结束后，最重要的工作内容是车辆信息运营管理组织依据本次应急响应过程过程进行经验总结，总结经验的结果可以用于加强组织应急响应管理能力，总结经验阶段组织宜进行以下活动。

5.1.4.2 经验总结

在车辆信息系统中可以将事件作为进一步TARA分析的输入，进行自底向上的TARA分析从已知信息安全漏洞和脆弱性入手形成针对该信息安全事件的信息安全目标与应对措施，对该信息安全事件的再发性防范提供支撑。包括以下几项经验总结：

a) 应急响应工作参与方的工作绩效评估；
b) 应急准备工作的充分性和针对性；
c) 车辆信息安全事件发生的原因、次数、频率；

d） 车辆信息安全事件处置的经验；
e） 车辆信息安全事件的趋势信息；
f） 车辆信息系统中潜在的类似隐患。

5.1.4.3 经验总结审核

应进行以下几项总结审核：
a） 评审和识别应急响应活动中参与者执行既定的应急响应方案情况，执行过程中存在的问题或待改进之处；
b） 评审、识别和改进应急准备工作活动存在的不足之处或需增强的方面；
c） 评审和识别应急预案的实际执行过程中存在的问题或待改进之处；
d） 评审、识别和改进组织现有的应急响应管理制度；
e） 评审和识别近期应急响应事件存在问题的改善情况与实际应用效果；
f） 宜对全年发生的车辆信息安全事件进行统计分析及审核。

注：所有收集到的车辆信息安全事件的相关信息（信息安全事件信息可由本组织已发生的事件和从行业渠道或互联网收集的事件组成）宜存储在独立的安全数据库中。该数据库可作为威胁情报库。

5.1.4.4 应急工作改进

车辆信息运营管理组织宜根据信息安全事件的发展趋势或模式，基于以往的制度体系、知识及经验完善应急响应活动流程，优化活动过程各环节。

5.2 应急响应管理要求

5.2.1 应急准备

5.2.1.1 应急培训

制定应急响应培训计划与开展培训工作应满足以下要求：
a） 将应急响应预案作为培训的主要内容；
b） 参训人员应明确其在应急响应过程中的权责范围、接口关系，熟练掌握相关设备、系统及软硬件工具的操作规范和处置流程；
c） 培训训每年不少于一次。

5.2.1.2 应急演练

组织开展应急演练应满足以下要求：
a） 应预先制定演练计划；
b） 应记录演练的详细过程，并形成报告；
c） 演练不能影响车辆信息系统业务的正常运行；
d） 应根据演练对发现的问题及时进行整改。

5.2.2 应急识别

5.2.2.1 日常监测

应进行以下日常监测步骤：
a） 组织应定期与车辆信息系统运维人员沟通，掌握业务运行状态；
b） 组织应掌握应急设备、系统及应急工具的状态，确保其可用性和安全性。

5.2.2.2 技术管理

应进行以下技术管理步骤：
a） 应建立车辆应急知识库并保持更新；
b） 应积极组织相应人员对常见的攻击方式定期演练。

5.2.2.3 文档记录

应进行以下文档记录步骤：

a) 应定期备份监测、预警的记录，确保记录不会丢失；
b) 应建立有效的应急响应活动过程文档跟踪机制，保证对应急响应全流程活动的追踪回溯能力。

5.2.3 应急处置

5.2.3.1 人员管理要求

车辆信息安全事件应急响应处置人员管理应满足以下要求：
a) 处置人员应根据车辆信息系统事件现场的实际情况及时调整处置措施；
b) 对无法现场处置的问题，处置人员应及时上报并寻求远程技术支持；
c) 当现场处置人力不足时，处置人员应在开展处置工作的同时上报要求增派人员；
d) 原则上现场处置人员应全程负责完成应急处置工作，确需调换的人员应在确保不影响应急处置工作的前提下完成人员替换和工作交接。

5.2.3.2 事件处置管理

车辆信息安全事件处置管理应满足以下要求：
a) 事件发生时应按照应急流程迅速响应到全生命周期；
b) 事件升级时应根据实际情况整理升级信息并上报；
c) 事件关闭时应按照相应流程提出申请，并上交事件报告等材料；
d) 事件关闭后组织应审计事件处置过程，并备份归档事件材料。

5.2.4 总结改进

5.2.4.1 应急预防

车辆信息安全事件发生预防活动应满足以下要求：
a) 应建立应急响应活动参与方定期沟通交流机制，及时交流最新车辆信息安全事件态势，保持组织对车辆信息安全整体态势感知的敏感度；
b) 应建立车辆信息安全事件全网监测机制，关注车辆信息安全事件最新消息；
c) 应建立必要的车辆信息安全研究团队或与第三方安全机构合作对车辆信息系统进行攻防演练，包括不限于物理攻击、网络攻击等形式；
d) 应定期组织信息安全专家对车辆的安全防护设计方案进行论证，对发现的问题或不足之处制定相应处置方案。

5.2.4.2 管理改进

车辆信息安全事件关闭后应对组织人员管理、技术管理、制度管理等进行评估，评估后根据评估结果进行调整。

5.3 应急响应技术要求

5.3.1 应急准备

在应急准备阶段，技术层面应满足以下要求：
a) 应组建应急响应技术小组，包含总体技术负责人、车辆信息系统技术人员与信息安全技术人员等；
b) 在应急预案中应编制应急技术手段及流程，并在预案中阐述必要的应急工具，应急工具需涵盖车辆近场通讯、车内总线等场景检测需求；
c) 应急准备流程应满足网络安全等级保护制度的相关要求。

5.3.2 应急识别

5.3.2.1 攻击方式识别

应采用技术手段对车辆软件、硬件、通信环境至少涵盖以下攻击方式识别能力：
a) 远程程入侵攻击识别；

b） 抵近攻击识别；
c） 接触攻击识别；
d） 数据篡改攻击识别；
e） 拒绝服务攻击识别；
f） 未授权访问攻击识别。

5.3.2.2 事件登记评估

车辆信息安全事件等级评估应满足以下要求：
a） 应评估车辆信息安全事件的危害等级；
b） 应评估车辆信息安全事件的影响范围；
c） 应评估车辆信息安全事件的威胁类型；
d） 应评估车辆信息安全事件可接受响应时间。

5.3.2.3 潜在风险分析

开展车辆信息安全时间潜在风险分析活动应满足以下要求：
a） 应通过威胁情报库进行威胁建模分析识别车辆信息系统潜在威胁；
b） 应通过车辆信息系统故障报警识别潜在威胁；
c） 应通过车辆信息系统关联日志分析识别潜在威胁；
d） 宜在实验环境下通过实战攻击方法分析车辆信息系统潜在威胁。

5.3.3 应急处置

5.3.3.1 技术响应

采用技术手段对车辆信息安全事件进行响应活动应满足以下要求：
a） 应按照应急预案中的技术要求开展应急处置；
b） 应采用技术手段阻断事件扩散；
c） 应采用技术手段尽快恢复系统运行；
d） 应采用技术手段分析事件，对事件溯源。

5.3.3.2 补救措施

采用技术手段对车辆信息安全事件进行补救活动应满足以下要求：
a） 制定和发布补救计划，配套相应的技术方案；
b） 推荐适当的车辆应急响应工具；
c） 检测并清除相关车辆信息系统及其他受影响信息系统中的攻击实例；
d） 修复导致事件发生的信息系统漏洞；
e） 针对事件更新车辆信息系统安全策略，完善预警机制。

5.3.4 总结改进

5.3.4.1 事件复盘

应对车辆信息安全事件应急响应过程进行分析，从制度、预案、流程、管理、人员、处置等多个环节进行分析和评估。

5.3.4.2 技术改进

评估应急处置所采用技术手段的可用性、有效性和先进性以及技术短板，做出针对性改进。

6 车辆信息安全漏洞管理要求

6.1 漏洞管理流程

车辆信息安全的漏洞管理流程分别按照漏洞发现和报告整理、漏洞传递和接收、漏洞验证、漏洞处置、漏洞追踪的流程进行概述，流程图如图2所示：

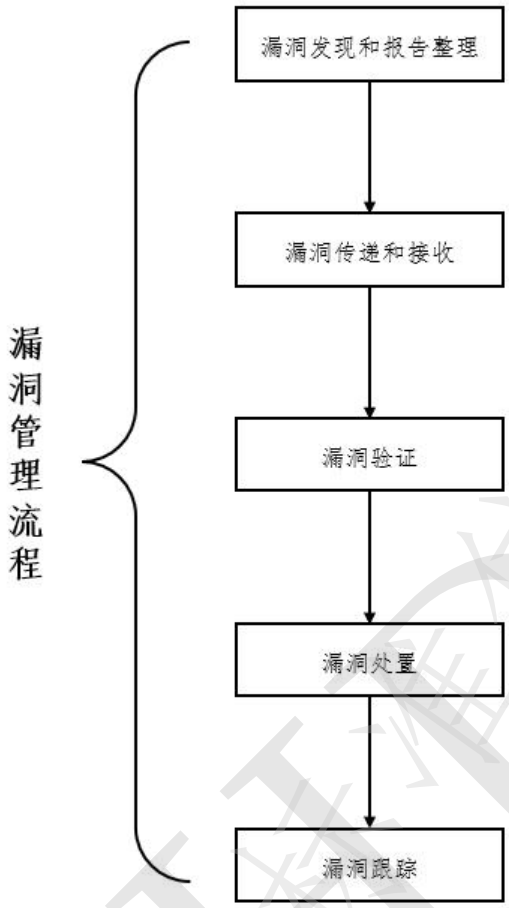

图2　漏洞管理流程

6.1.1　漏洞发现和报告整理

6.1.1.1　总体要求

漏洞发现是指在遵循国家相关法律、法规的前提下，可通过人工或自动化方法对车辆信息安全漏洞进行探测、分析，并证实漏洞存在的真实性的过程；漏洞报告整理是指在发现车辆信息安全漏洞后，对漏洞信息的描述以及组织内部全部漏洞信息的管理；漏洞发现和报告整理阶段应满足以下要求。

6.1.1.2　漏洞发现要求

车辆信息系统漏洞发现活动应满足以下要求：

a)　应在保证不影响车辆信息系统业务运行安全和数据安全的前提下实施漏洞发现活动；
b)　漏洞发现者应对发现的漏洞信息进行梳理形成形式化的漏洞报告单；
c)　漏洞告单应至少包含漏洞信息独有标识、漏洞利用方法、漏洞影响范围以及漏洞缓解或修复建议等内容。

6.1.1.3　漏洞报告整理要求

开展车辆信息系统漏洞报告整理活动应满足以下要求：

a)　应设立专职漏洞管理员编制车辆信息系统的漏洞应急预案，制定漏洞全生命周期管理监测流程；
b)　应采取必要的漏洞分类分级方法对漏洞进行规范管理；
c)　漏洞管理员应负责车辆信息系统的漏洞库更新、漏洞修复及策略更新工作；

d) 针对有必要在组织内部有限公开的漏洞信息，漏洞管理员应及时在组织内部通报漏洞信息，提供的漏洞信息包括：报告人、漏洞技术类型、技术环境信息，涉及的产品和系统、用于核验的技术内容等。

注：GB/T 30279-2020给出的网络安全漏洞分类分级方法可供参照。

6.1.2 漏洞传递和接收

6.1.2.1 总体要求

漏洞信息传递是指漏洞发现者上报车辆信息安全漏洞信息或漏洞管理员向组织内部特定接收对象共享车辆信息安全漏洞信息的过程；漏洞接收是指确认接收漏洞报告信息的过程；漏洞传递和接收阶段应满足以下要求。

6.1.2.2 漏洞传递要求

开展车辆信息系统漏洞传递活动应满足以下要求：

a) 应采用密码技术手段保证漏洞信息传递过程中机密性和完整性，防止漏洞信息泄露、被篡改；

b) 应采用身份鉴别技术对漏洞信息发送者的身份进行标识，保证漏洞信息接收者能对漏洞发送者身份真实性进行鉴别。

6.1.2.3 漏洞接收要求

漏洞接收者接收车辆信息系统漏洞应满足以下要求：

a) 应采取有效措施保护漏洞相关信息的访问、存储、使用安全；

b) 应采用身份鉴别技术对漏洞信息接收者的身份标识，保证漏洞信息发送者能对漏洞接收者身份真实性进行鉴别；

c) 漏洞接收者接收到漏洞信息后，应及时给予漏洞发送者确认和反馈；

d) 漏洞接收者应按照应有职责开展漏洞活动：

1) 漏洞管理员应对漏洞信息进行核查，并确定后续漏洞活动；

2) 漏洞管理员应对漏洞信息进行收录，并对漏洞活动过程必要文档进行归档；

3) 漏洞验证人员应在取得授权后开展漏洞验证活动；

4) 漏洞验证人员不得开展超出授权范围漏洞活动，或利用漏洞进行违法违规活动。

6.1.3 漏洞验证

漏洞验证是指在收到漏洞报告后，及时对漏洞的存在性、等级、类别等进行技术验证，向漏洞报告者发送漏洞报告接收确认或反馈的过程，漏洞验证阶段应满足以下要求：

a) 漏洞报告接收方应依据报告复现并核验漏洞的真实性和有效性；

b) 应明确权责分配，包括车辆信息系统漏洞修复的部门、供应链方、技术第三方、相关业务主管及开发和运维人员等；

c) 应依据漏洞修复的重要紧急程度明确漏洞相关方验证时限；

d) 应使用统一规范的漏洞定义语言，确保漏洞修复周期内各个环节获取的漏洞信息一致；

e) 验证完成后应及时通知与该漏洞相关联的漏洞提供者或管理者。

6.1.4 漏洞处置

漏洞处置是指通过对车辆信息系统的软硬件版本升级、补丁、更改配置等方式，对车辆信息系统漏洞进行修补的过程，漏洞处置阶段应满足以下要求：

a) 应建立漏洞处置工作流程，与车辆信息系统相关利益方协同开展漏洞处置工作；

b) 应对漏洞进行根本原因分析，判断该漏洞是否影响其他产品或服务；

c) 应对漏洞处置方法进行充分严格的有效性和安全性测试，避免因漏洞处置活动衍生安全问题；

d) 漏洞处置人员应在规定的时间范围内完成漏洞处置活动；

e) 对于不能直接或立即修复的漏洞问题，应提出有效的临时处置建议并出具处置技术指导说明；

f） 宜对漏洞处置活动关键过程进行审计记录（升级日志、记录表单等）。

6.1.5 漏洞跟踪

漏洞跟踪是指车辆信息安全漏洞修复后，对与该漏洞相关的产品、服务进行监控，收集用户使用反馈信息，确认漏洞修复效果的过程；漏洞跟踪阶段应督促并监督车辆信息系统漏洞管理活动的实施情况。需督促并监督的情况如下。

a） 应督促漏洞相关联利益方及时升级修复补丁；
b） 应跟踪并监督漏洞管理活动的实施情况，定期对漏洞管理的实施效果进行核查，核查内容包括：
   1） 已发现的漏洞是否得到有效处置；
   2） 参与漏洞管理的各方是否协调一致；
   3） 漏洞处理过程是否符合及时处理规范和安全风险最小化等原则。

6.2 漏洞管理要求

6.2.1 漏洞发现和报告整理

在漏洞发现和报告整理阶段，管理层面应满足以下要求：

a） 在进行漏洞检测前，应有专业人员主动评估可能存在的安全风险并告知被测方；
b） 在实施漏洞发现活动时应遵守相关法律法规，不应对用户的系统运行和数据安全造成影响和损害，不应存在为了发现漏洞而侵犯其他组织的业务运行和数据安全的行为；
c） 对测评结果存在的漏洞进行分析证实漏洞存在的真实性，应及时将漏洞信息整理上报；
d） 报告漏洞时，应客观、真实地对漏洞进行描述，应采取有效措施防止信息泄露。

6.2.2 漏洞报告传递接收

在漏洞报告传递接收阶段，管理层面应满足以下要求：

a） 应设立加密的传输信道，保障漏洞报告的安全发送与接收，确保漏洞相关信息的安全性和保密性，防止漏洞信息泄露；
b） 在收到漏洞报告者的漏洞报告后，应及时给予漏洞报告者确认或反馈；
c） 如果发现漏洞涉及其他利益方，及时向相关利益方通告，需要协调时可请求漏洞应急组织的帮助。

6.2.3 漏洞验证

在漏洞验证阶段，管理层面应满足以下要求：

a） 应对漏洞的存在性、等级、类别等进行技术验证；
b） 如果该漏洞涉及其他利益方，应及时通知相关提供者或网络运营者共同进行验证；
c） 如果报告的漏洞是在提供者或网络运营者目前不提供支持的产品或服务中发现的，提供者或网络运营者应继续完成调查和漏洞验证，并确认该漏洞对其他支持的产品的影响；
d） 在漏洞验证后，应根据漏洞验证情况对漏洞进行描述，并及时向漏洞管理员上报；
e） 在漏洞验证过程中发生如下情况时，可以终止后续的漏洞管理阶段，并及时向漏洞管理员反馈：
   1） 重复漏洞：该漏洞是个已重复的漏洞，已解决或已修复的漏洞；
   2） 无法验证漏洞：该漏洞是漏洞发现者、组织等无法验证的漏洞；
   3） 无危害漏洞：该漏洞是一个无安全影响，或无法被现有技术利用的漏洞。

6.2.4 漏洞处置

在漏洞处置阶段，管理层面应满足以下要求：

a） 应与漏洞相关利益方协同开展漏洞处置工作；
b） 在漏洞处置过程中应进行深入分析，判断该漏洞是否影响其他产品或服务；
c） 应对已经确认的漏洞，根据漏洞严重程度、受影响用户的范围立即进行漏洞修复或制定防范措施；

d) 在对漏洞修复过程中，不应影响其他业务的正常运行；
e) 在发布补丁和升级版本前应进行充分严格的有效性和安全性测试，避免补丁衍生出现安全缺陷。对于不能通过补丁或版本升级解决的漏洞风险，应提出有效的临时处置建议，出具指导技术说明；
f) 若不能立即给出修复措施，应给出有效的临时防护建议，并可联合漏洞应急组织根据漏洞影响范围及发展情况制定下一步处置方案和解决措施；
g) 应向漏洞报告者和用户及时告知漏洞的处置措施；
h) 应对受影响的用户提供必要的技术支持，支持其完成漏洞修复；
i) 应采取必要手段保护漏洞处置活动过程的安全，防止发生信息泄露等安全事件发生。

6.2.5 漏洞跟踪

在漏洞跟踪阶段，管理层面应满足以下要求：
a) 应实时关注漏洞处理信息，避免出现衍生漏洞，给系统带来新的危害；
b) 应收集用户的反馈信息，监测产品或服务是否稳定运行，并对漏洞修复或防范措施做进一步改进，确认漏洞彻底解决。

6.3 漏洞管理技术要求

6.3.1 漏洞发现和报告整理

6.3.1.1 检测车辆信息系统漏洞

开展车辆信息系统漏洞检测活动应满足以下要求：
a) 在进行漏洞检测前，应对系统进行调研了解系统覆盖范围、具体资产确定测评对象；
b) 应使用正版的工具或具备合格产品证书的设备进行漏洞检测；
c) 应确保漏洞的真实性和有效性。

6.3.1.2 漏洞报告编制

开展车辆信息系统漏洞报告编制活动应满足以下要求：
a) 应编写漏洞技术报告；
b) 漏洞报告应具备技术论证内容。

6.3.2 漏洞报告传递接收

在漏洞报告传递接收阶段，技术层面应满足以下要求：
a) 应采用技术手段保证在漏洞相关信息传输过程中的机密性、完整性；
b) 应采用技术手段保证漏洞相关信息发送方与接收方身份的真实性。

6.3.3 漏洞验证

在漏洞验证阶段，技术层面应满足以下要求：
a) 应采用漏洞验证技术对已发现的漏洞的真实性进行验证；
b) 应保证漏洞验证结果的可重复性和可再现性；
c) 应依据 GB/T 28458-2020 中 5.3 的要求对已验证的漏洞进行描述。

6.3.4 漏洞处置

6.3.4.1 处置原则

开展车辆信息系统漏洞处置活动应满足以下原则：
a) 软件无后门原则，应禁止车辆信息系统预留具有后门功能的代码，防止发生后门被利用对车辆信息系统造成破坏；
b) 最小化授权原则，漏洞处置活动应只授予必要的、最小满足业务的权限，防止权限过大带来的风险；
c) 权限分离原则，重要保护对象的漏洞处置活动应具备两个或两个以上的权限，各权限应相互分离和单独授予；

d) 业务适用性原则，漏洞处置流程设计应结合业务或功能环境的实际需求，修复系统漏洞时应不影响其他业务和功能的正常使用。

6.3.4.2 处置要求

开展车辆信息系统漏洞处置活动应满足以下要求：

a) 应根据影响范围和事件级别对存在的漏洞进行分类；
b) 一般在七个工作日内修复高危漏洞；
c) 一般在十五个工作日内修复中危漏洞；
d) 一般在三十个工作日内修复低危漏洞；
e) 可能直接或间接威胁车辆使用者主体的生命、财产等重大合法权益的漏洞应在最小可接受时限内修复。

6.3.4.3 漏洞防护

车辆信息系统开展漏洞防护活动应满足以下要求：

a) 纵深防御
根据保护对象所处的环境条件和信息安全管理的要求，应由外到内对保护的对象实施层层防御的防护措施，各层次的安全措施应相互依托，形成系统化的防护机制，从而提高系统的整体抗攻击能力。
b) 主动防御
主动防御应采用包括但不限于情报共享、入侵检测技术、信息安全策略动态调整和各信息安全模块之间协同等措施，以降低信息系统在遭受网络攻击时所面临的风险。
c) 韧性防御
韧性防御信息安全设计应综合考虑可靠性、功能安全等多个方面的工程设计，以提高系统的生存能力和自愈能力。
d) 被动防御
当系统受到入侵或者损害时，应具备快速修复能力，具有完整的修复团队和技术支撑可以应对各种等级的安全事件。

6.3.5 漏洞追踪

在漏洞追踪阶段，应对已修复的漏洞采用技术手段对修复后的车辆信息系统进行分析，确保无残余风险。

参 考 文 献

[1] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范
[2] GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南