ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 117-2022

车内以太网通信网络安全的入侵检测和态势感知技术要求

Technical requirements for intrusion detection and situation awareness of in vehicle Ethernet communication network security

2022-12-13 发布　　2022-12-14 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、长春吉大正元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。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：中电信数智科技有限公司长春分公司、中电福富信息科技有限公司。

本文件主要起草人：高深、孙冰楠、谢辉、黄丽荣、于鑫淼、薛炜晨、陈绍军、李新坚、陈鑫、郑俊、蔡悦贞。

本文件参与起草单位：中国第一汽车集团有限公司智能网联开发院、联通（吉林）产业互联网有限公司、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、联通智网科技股份有限公司、东风汽车集团有限公司技术中心、上汽通用五菱汽车股份有限公司、智车信安（苏州）信息安全科技有限公司、武汉路特斯科技有限公司、吉林大学软件学院、岚图汽车科技有限公司。

本文件参与起草人：陈后立、李木犀、高子平、李杰、全代勇、雷凯、刘书勇、孙伟、周海鹰、张亮、黎飞、陈炼松、路海峰、刘建鑫、王健、汪涛。

本文件审查人：孙航（中国汽车技术研究中心有限公司）、孟令军（东软集团股份有限公司）、刘健皓（北京百度智行科技有限公司）、王建（华为技术有限公司）、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

本文件针对目前车联网暴露的诸多信息安全的问题，比如车内无线通信领域的信号窃取与干扰等，这些问题容易导致车载终端受到恶意攻击，干扰汽车整车信息安全，故就此提出相应的信息安全技术设计要求。

为了确保标准的规范化和普适性，本文件编制一个基础性标准对车内以太网通信安全的入侵检测和态势感知安全技术要点进行规范化要求，统一设计要点，形成平台化技术要求，以保证车内通信信息安全设计的安全性和过程一致性，以形成通用性的技术要求。

车内以太网通信网络安全的入侵检测和态势感知技术要求

1 范围

本文件规定了车内以太网通信网络安全的入侵检测和态势感知的技术要求，以描述车内以太网通信网络安全入侵检测的系统结构，功能要求，设计要求和态势感知的技术总体要求、数据采集要素要求、数据存储要求、数据分析要求、数据处理要求、可视化呈现要求等内容。提供车内以太网通信网络安全进行系统建设时的基本要求。

本文件适用于为企业生产智能网联汽车提出关于车内以太网通信网络安全的入侵检测和态势感知的相应参考标准，也适用于为相关方提供选择技术路线的参考标准。

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 25068.1-2012 信息技术安全技术IT网络安全 第1部分：网络安全管理

GB/T 20275-2021 信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T 25069-2022 信息安全技术 术语

T/GHDQ 114-2022 车载CAN网络入侵检测和态势感知技术要求

T/GHDQ 115-2022 车辆控制器系统的入侵检测和态势感知技术要求

3 术语和定义

GB/T 25069-2022 和 GB/T 20275-2021 界定的以及下列术语和定义适用于本文件。

3.1

系统日志 SYSLOG

是一种用来在互联网协议(TCP/IP)的网络中传递记录档讯息的标准。在网络管理领域，Syslog协议提供了一个传递方式，允许一个设备通过网络把事件信息传递给事件信息接受者(也称之为日志服务器)。

3.2

域名系统 Domain Name System:DNS

因特网上作为域名和IP地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。

3.3

网络流量数据包 Netflow

提供网络流量的会话级视图，记录下每个TCP/IP事务的信息。一个NetFlow流定义为在一个源IP地址和目的IP地址间传输的单向数据包流，且所有数据包具有共同的传输层源、目的端口号。

3.4

远程登录会话安全性协议 Secure Shell:SSH

由 IETF 的网络工作小组(Network Working Group)所制定，为建立在应用层和传输层基础上的安全协议。是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。

3.5

文件传输协议 File Transfer Protocol:FTP

是 TCP/IP 协议组中的协议之一。FTP协议包括两个组成部分，其一为FTP服务器，其二为FTP客户端。其中FTP服务器用来存储文件，用户可以使用FTP客户端通过FTP协议访问位于FTP服务器上的资源。

3.6

关键字 keyValue

key value 根据关键字取值

3.7

基于以太网的入侵检测系统 Ethernet-Based Intrusion Detection System:EIDS

是用于检测Hacker或Cracker通过网络进行的入侵行为。EIDS的运行方式有两种，一种是在目标主机上运行以监测其本身的通信信息,另一种是在一台单独的机器上运行以监测所有网络设备的通信信息，比如Hub、路由器。

3.8

虚拟局域网标签 VLAN TAG

配合企业网络使用政策，区分不同的VLAN网段，隔离并保护公司内部重要资讯。

4 缩略语

表1中的缩略语适用于本文件。

表1 缩略语

缩写	解释	中文释义
IVI	In-Vehicle Infotainment	车载信息娱乐系统
OBU	On-board Unit	车载单元
ADAS	Advanced Driver Assistance System	高级驾驶辅助系统
NFC	Near Field Communication	近距离无线通讯
OBD	On-board Diagnostics	车载自动诊断系统
T-BOX	Telematics BOX	车联网通讯终端
CGW	Communication Gateway	中央网关
IDS	Intrusion Detection Systems	入侵检测系统
ECU	Electronic Control Unit	电子控制单元
SDK	Software Development Kit	软件开发工具包

5　基于以太网的入侵检测技术要求

5.1　系统结构

基于以太网的入侵检测系统通过车载控制器-（安全SDK）对系统的各种异常行为进行检测，将检测结果发送给管理节点（日志收集汇总），由管理节点将安全事件上报到云端管理平台，进行可视化呈现。通过识别针对ECU或是整车系统的异常事件、攻击事件，采取措施进行网络安全防御，从而保障车内以太网网络系统的应用安全、通信安全、系统安全、访问点安全、数据安全，如图1。

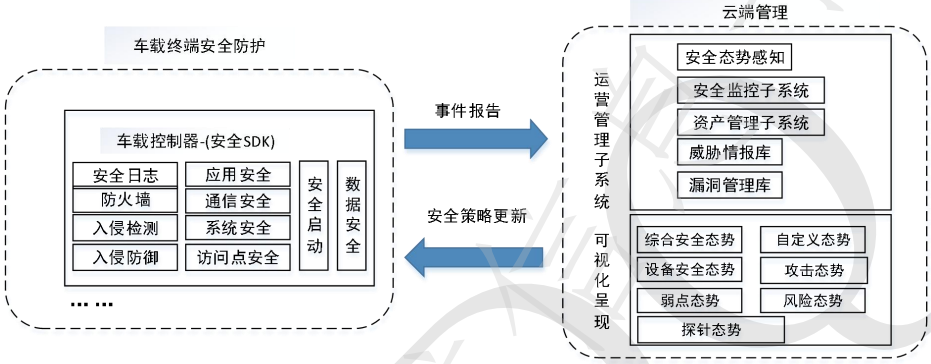

图1　基于以太网的入侵检测及态势感知系统参考结构

5.2　系统功能要求

5.2.1　功能概述

基于以太网的入侵检测系统应提供对车内以太网安全的全面监控，保障车辆的主机和控制器安全，对汽车进行安全管理和应急响应，其功能包括入侵检测、安全日志、系统安全、防火墙和动态策略库管理、恶意代码检测能力等。

5.2.2　入侵检测

应具有入侵检测功能，应具有识别网络入侵攻击行为、实时检测网络异常、预置网络检测策略、拒绝不符合策略的访问并阻断、记录审计信息等功能。

5.2.3　安全日志

根据车载终端系统日志和应用日志，应具备可通过被动采集或主动查询等检测方法，检测系统的异常行为；根据对系统CPU、内存、网络连接状态等系统运行环境（系统日志中有包含此类信息）的监控，应能实时检测系统的安全状态。（以上日志都归类为安全日志，安全日志应当能负责对日志进行采集、存储、上报和导出）

5.2.4　入侵防御

入侵防御要求如下：

a)　系统防御：应通过访问限制来阻止直接或间接非法入侵；应预置访问控制策略；应拒绝不符合策略并且阻断、记录审计信息；

b)　告警响应：入侵检测系统输出安全事件，管理节点调用日志库上报到云端管理平台，实现事件告警响应。

5.2.5 防火墙

防火墙要求如下：

a) 应能对所有接入数据进行智能过滤（即根据自定义规则自动化过滤），防止非法控车操作指令；
b) 应具备动态策略库管理：支持策略库的更新、策略库本地加密存储、应急规则推送更新、个性化策略配置；
c) 应能对策略库的更新传输过程进行数据完整性校验和数据加密，保证数据的完整性和保密性；
d) 应具备对策略库的更新进行权限验证，保证操作的合法性。

5.3 系统设计要求

5.3.1 总体设计原则

总体设计原则如下：

a） EIDS网络入侵检测系统应具备可根据整车安全设计的需求，结合整车网络架构，在满足相应的资源和处理能力的控制器中部署探针，即，在支持LINUX/QNX/ANDROID等操作系统的控制器中部署探针，对整车的控制器安全进行全面的监控；
b） 部署在车端各零部件中的EIDS探针应当将安全事件统一上报给云端管理平台；
c） 在日志文件无法加密的情况下，任何被认为需要加密的敏感数据都应匿名；
d） 密码和密钥不能写入日志；
e） 记录操作不影响用户体验。

5.3.2 日志监控模块

5.3.2.1 日志采集

日志采集要求如下：

a） 日志采集方法应包括：
   1） 被动采集：读取系统和应用的日志信息，将日志信息与自定义规则进行匹配，输出告警事件，上报到管理节点或云端管理平台；
   2） 主动采集：EIDS周期性地下发命令，查询其当前的系统安全状态，将历史信息与当前信息进行比对，发现系统中当前的异常状态。

备注：EIDS利用一个运行在随机模式下的网络适配器来实时监视并分析通过网络的所有通信业务。由于随着交换带宽的不断增长,并非所有的网络流量都会反映在监听端口或镜像端口上，并非所有的交换设备都提供类似的监听端口或镜像端口。所以需要IDS选择挂接在流量最大的上下行端口上,用来截获进出内外网的数据流量。

b） 日志监控对象应包括：
   1） 系统日志监控——系统的SYSLOG等的监控；
   2） 应用日志监控——全部应用程序的监控；
   3） 系统行为监控——SSH、FTP方式异常登录、越权访问等行为的监控，如：多次连续的密码鉴别失败，意味着出现了暴力破解的恶意行为；
   4） 系统环境监控——系统CPU、内存、网络连接状态等系统运行环境的监控。
c） 日志监控流程应包括：
   1） 通过主动采集或被动采集的方式采集系统日志和应用日志；
   2） 将采集的日志，进行解析和范式化，便于入侵检测系统对各种来源的日志进行统一的规则匹配和分析；

3） 输出规则匹配结果，将异常行为和安全事件告警上报管理节点或云端管理平台，或根据已配置的响应策略直接进行本地响应处理。

5.3.2.2 日志存储

日志存储要求如下：

a） 日志应支持加密并进行本地存储；

b） 每次更新日志之后，校验码也需对应更新；

c） 上传日志或写新的日志时，应能对日志内容进行校验，防止日志被篡改，同时还应对日志进行加密，防止日志被窃取，导致信息泄露的风险；

d） 日志系统应能保存最近至少6个月的日志，应能自动删除规定时间段之外的日志。

5.3.2.3 日志上传

存储在本地的日志上传至云端，其要求如下：

a） 日志上传需支持出错自动重传；

b） 日志应支持定时批量上传；

c） 日志上传的数据文件应能够压缩，提高文件传输效率；

d） 日志模块应能上传最近6个月以上的安全日志。

5.3.3 防火墙

以太网防火墙应具备可依据规则对以太网帧报文进行解析和匹配，并根据匹配结果对帧报文进行以下处理：

a） 过滤：基于提前定义好的通讯矩阵（白名单）去过滤，满足条件的数据就转发或者使用，否则就丢弃的规则，防火墙需要拦截非法的数据，避免其进入其他安全区域，白名单设定规则应包括以下三个部分：

1） 针对MAC帧，需要检查MAC帧中的虚拟局域网标签（VLAN TAG）是否与整车通讯数据库定义的一致，对于路由器或者终端节点，还应该检查收到的MAC帧中的MAC地址。如果是单播报文，应该与自己的MAC地址一致；如果是组播报文，则本节点应该属于组播域内的一员；

2） 针对IP数据包，需要检查IP头中的IP地址及其类型；

3） 针对TCP、UDP链接，需要检查协议头和链接状态跟踪；

4） 能够支持按照整车通讯数据库限制通讯的TCP或者UDP端口。

b） 记录：防火墙的相关数据，例如拦截数据流量、防火墙故障状态和防火墙规则数量等，需要存储在相应的安全区域。这部分数据需要能够配合其他功能，例如结合诊断功能报告故障码，又或者传递给网络入侵检测系统以分析入侵情况。

5.3.4 入侵检测规则与内容要求

以太网网络入侵检测的原理是基于规则匹配的方式判断以太网网络是否异常，因此对入侵检测的规则和内容要求如下：

a） 入侵检测宜通过日志解析规则对截取或旁路拷贝的报文进行检查，对判定为异常的报文调用日志模块和报警模块进行记录以及报警。

b） 检测规则库应主要包含规则数据和规则加载程序两个部分；

c） 入侵检测内容应包括以下五个部分：

1） 报文健康检查：检查报文的长度、携带的信号的范围等；

2）报文周期检查：检查周期报文的间隔时间；
3）信号关系检查：检查某些存在关联的两个信号之间的关系；
4）报文异常分析：检查报文序列是否正常出现及其出现的频率；
5）负载率监控：监控以太网网络上负载情况。

6 态势感知技术要求

6.1 态势感知总体要求

态势感知平台应具备能够利用云端的安全性、网络带宽及稳定性优势，为后期的数据分析提供基础数据和能力，应提供一套管理界面，以支持管理员能配置防火墙、防御规则，并能对车辆安全态势进行可视化展示，应能支持对事件、日志、流量的采集，应提供数据库实现对平台业务数据的存取和查询。

6.2 数据采集要素要求

数据采集要素要求如下：

a） 采集对象应包括：
1） 设备进程。如车机、T-BOX、仪表、OBU、CGW 中央网关等设备上运行的所有进程；
2） 设备文件。如车机、T-BOX、仪表、OBU、CGW 中央网关等设备上的二进制文件、敏感文件（如应能采集车辆的安全事件日志）；
3） 设备 DNS。如车机、T-BOX、仪表、OBU、CGW 中央网关等设备的 DNS 通信信息（支持配置过滤规则对采集内容进行过滤）；
4） 设备 Netflow。如车机、T-BOX、仪表、OBU、CGW 中央网关等设备与外界通信的 Netflow 信息。

b） 采集方式应包括：
1） 主动采集：管理平台可实时或定期收集、获取车辆设备终端本身的数据；
2） 被动采集：被动采集数据包括威胁情报、漏洞库信息等。

c） 数据源应包括：
1） 车辆设备终端基础数据应包括设备终端编号、设备终端型号、设备终端名称、设备终端软件版本、设备终端类型等；
2） 管理平台数据应包括平台IP、域名、提供的服务类型等；
3） 安全事件日志应包括设备终端型号、事件类型、事件时间、事件内容；
4） 应支持能周期性地采集安全数据，或在采集条数累积到一定值时，进行数据上传；
5） 应支持分类分级，针对重要、敏感数据应能进行脱敏处理，保证数据安全。

d） 漏洞信息应包括：
1） 漏洞名称、编号、简介；
2） 威胁等级、参考网址；
3） 受影响实体等信息。

6.3 数据处理要求

为了满足安全分析对数据质量的要求，应支持将采集到的数据进行格式化、清洗、转换、标签化等处理，包括以下操作：

a） 应对采集的各类异构的数据进行统一格式化处理，并保存原始采集数据。各数据满足针对数据格式定义的要求。如：能根据每种类型数据的标准定义字段规则，实现相关字段的标准化能

力；能够以分隔符、键值对等多种格式数据解析，并可通过正则表达式等手段对解析后的内容进行统一格式化处理；

b） 应能通过自定义过滤字段进行数据的清洗过滤，对于数据格式不一致、数据输入错误、数据不完整等问题，支持对数据进行转换和加工（替换）；

c） 能够提供常见的数据转换算子，如数据过滤，字段替换，动态补全，静态补全，keyValue，时间转换，字段截取，子域名拆分，数据脱敏，字段合并，IP解析扩展，字段移除等；

d） 支持对于不同类型的数据进行关联补齐；

e） 支持将数据标签化，基于关联补齐后的数据，结合数据所属车辆设备终端类型等信息，在原数据基础上进行标记；

f） 支持将数据分析结果以可视化方式进行展示。

6.4 数据存储要求

数据存储要求如下：

a） 应支持结构化数据、半结构化数据和非结构化数据的存储；

b） 应支持将采集和处理获取的原始数据、预处理后的数据、告警数据进行存储；

c） 应支持包括安全策略数据、用户数据、系统日志、操作日志等管理数据的存储；

d） 应支持包括漏洞信息库、威胁情报库等知识库数据的存储；

e） 应支持日志系统能保存最近至少6个月的日志。

6.5 数据分析要求

数据分析要求如下：

a） 应支持对车辆设备终端的安全事件日志、流量等数据建立数据分析模型的能力，对采集的数据进行集中、动态和自动化分析；

b） 应能通过技术手段（如统计学、聚类/分类识别、关联分析等），识别复杂攻击和深度威胁；

c） 对采集的各类安全事件日志进行深度分析，提取有效告警信息，并标记事件的可信度、攻击阶段、是否攻击成功等；

d） 宜支持对告警信息进行追踪、溯源，并提供规则库的扩展；

e） 宜支持对数据源进行预处理、支持数据融合并进行多层次多维度的态势呈现，提供决策数据；

f） 宜具备安全策略库，支持灵活的规则配置。

6.6 可视化展示要求

6.6.1 安全管理

安全管理要求如下：

a） 安全监控管理：

1） 应支持对车内系统安全日志事件的展示；

2） 应支持对车端入侵监测系统的防火墙规则进行配置，防火墙规则支持黑白名单模式；

3） 应支持对车端入侵监测系统的网络防御规则进行配置；

4） 应支持对车端入侵监测系统上传的事件日志和流量数据进行审计；

5） 应支持对安全事件、漏洞信息的风险预警及应急响应处置；告警方式应至少包含以下一种：平台、短信、邮件、即时通信等；

6） 应具备系统平台管理功能，支持在平台上提供统一的用户、角色、权限（菜单）分配。

b） 设备管理：

1） 应具备对车型、设备、车辆等基础信息的展示；
2） 应具备按月份统计车辆总数、车辆新增数、发生的安全事件数，日志累计数，风险预警次数和响应处理次数，并生成月度统计报表；
3） 设备类型应包括车载终端设备，应用，云端安全类资产等，如车载终端设备（T-BOX）、IVI、OBU、车身控制器、ADAS感知系统、NFC、OBD等。

c） 威胁情报管理：
1） 应具备对威胁情报信息的展示；
2） 应具备对威胁情报信息实时或者周期性更新；
3） 应具备对车内系统进行实时威胁情报获取。

d） 漏洞管理：
1） 应具备对漏洞信息的展示；
2） 应具备对漏洞信息实时或者周期性更新；
3） 应具备对车内系统进行漏洞探测。

6.6.2 安全态势展示

安全态势展示要求如下：

a） 应支持车端和云端管理平台多层级的安全态势展示，应包括：
1） 综合安全态势；
2） 设备安全态势；
3） 攻击态势；
4） 弱点态势；
5） 风险态势；
6） 探针态势等。

b） 应支持按车载终端类型的安全态势展示和按地区或按时间段的设备安全态势展示；

c） 应支持对车联网安全风险过去和当前趋势进行可视化展示；

d） 应支持安全态势可选择性展示，通过筛选条件选择展示的内容，可支持按车型、监控的设备类型进行查询；

e） 应支持以两种或两种以上视图展示以上各维度安全态势细节，包括但不限于以下几种：
1） 地理信息图关联关系图；
2） 趋势图；
3） 柱状图、饼图。

6.6.3 数据展示

数据展示要求如下：

a） 态势展示的类别和内容，应包括见表2。

表2　态势展示类别和内容

安全态势	展示类别	展示内容
综合安全态势	1、车辆设备受攻击态势地图； 2、车辆设备呈现被防护对象的安全态势； 3、安全威胁趋势； 4、全网告警分布； 5、全网漏洞及配置弱点分布；	1、车型类别，车辆总数、安全事件总数； 2、攻击类型种类、受攻击设备数量； 3、安全事件描述、危险等级、发生时间。 4、风险评估项； 5、IP地址、所属地域、所属单位、责任人、厂商、发行版本、来源系统等； 6、当前发现漏洞的总数量、高危漏洞数量、新增漏洞数、长期未处理的漏洞情况； 7、设备类型、分布地域、漏洞类型； 8、漏洞处置状态； 9、安全组件类型； 10、车辆使用年限、保养频率展示、车况分析； 11、驾驶行为异常行为、异常地点； 12、探针部署位置等；
设备安全态势	1、车辆地域分布地图； 2、车辆设备呈现被防护对象的安全态势； 3、车辆可用性情况列表等； 4、车辆预测风险分布地图；	
弱点态势	1、漏洞概要统计信息列表； 2、漏洞总体安全趋势图； 3、漏洞类型分布TOP列表； 4、漏洞数量趋势图； 5、漏洞处置情况列表；	
攻击态势	1、车辆设备受攻击情况列表； 2、车联网平台和车辆安全事件的攻击类型TOP列表； 3、攻击事件的被攻击的地理区域和攻击来源国家TOP列表； 4、攻击事件的车型TOP列表； 5、攻击事件详情列表等；	
风险态势	1、车辆风险值地域分布地图； 2、安全风险要素列表等； 3、车辆风险值分布TOP列表； 4、周期性风险值分布趋势；	
探针态势	1、探针地域分布地图； 2、探针运行健康状态； 3、探针部署情况列表； 4、探针收集信息数量列表；	

b） 应支持按关键字查询攻击条目或进行攻击事件导出；

c） 系统能提供自定义态势能力，用户能够根据自身需求，通过平台低代码组件，配置相关的数据源，数据过滤条件，拖拉拽的方式调用相关呈现组件，形成用户自定义大屏。

7　安全要求

以下为安全性要求细则：

a） 态势感知系统内部组件之间应具备数据安全传输能力，通过建立加密通道进行数据传输；

b） 态势感知系统同其他系统间互通在性能允许情况下应具备安全的加密通讯连接；

c） 态势感知系统应保证自身的应用安全，包括不限于：密码的存储与传输禁止使用明文、禁止在COOKIE中保存用户密码、防止跨站伪造、进行异常输入验证等安全防护能力、防止网页篡改等；
d） 态势感知系统的用户宜纳入4A管理；
e） 态势感知系统对于敏感数据的存储和传输，宜采取加密或脱敏等措施。

8 性能要求

性能要求如下：
a） 态势感知系统应能够连续7×24小时不间断工作；
b） 态势感知系统应支持TB级或以上级别海量数据的采集、分布式存储和分布式运算；
c） 态势感知系统应支持分钟级运算和查询；
d） 入侵检测系统应支持分钟级实时数据采集。