ICS 35.020
CCS M 57

DB61

陕 西 省 地 方 标 准

DB 61/T 1614—2022

高速公路机电系统网络安全运行规范

Specification for Cybersecurity Operation of Expressway Electromechanical System

2022－10－12 发布　　2022－11－12 实施

陕西省市场监督管理局　　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。

本文件由陕西省交通运输厅提出并归口。

本文件起草单位：陕西高速电子工程有限公司、陕西交通控股集团有限公司、西安电子科技大学、陕西交控科技发展集团有限公司、长安大学。

本文件主要起草人：张建会、范耀东、崔艳鹏、柯翔、边艳妮、许宏科、刘晓娜、胡建伟、何国涛、张文华、王小博、王坚、汪文妹、沈纲、田浩帅。

本文件由陕西高速电子工程有限公司解释。

本文件首次发布。

联系信息如下：

单位：陕西高速电子工程有限公司

电话：029-87553894-6018

地址：西安市友谊东路428号

邮编：710054

高速公路机电系统网络安全运行规范

1 范围

本文件规定了高速公路机电系统网络安全运行的术语和定义、一般规定、资产梳理、基线核查、人员与第三方供应链安全要求、日常监测以及应急响应的要求。

本文件适用于高速公路机电系统的网络安全运行工作，其他等级公路可参照使用。

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 36637 信息安全技术 ICT供应链安全风险管理指南

GB/T 38645 信息安全技术 网络安全事件应急演练指南

GB 50174 数据中心设计规范

3 术语和定义

GB/T 22239界定的以及下列术语和定义适用于本文件。

3.1

高速公路机电系统 expressway electromechanical system

高速公路监控系统（含隧道）、收费系统、通信系统及供配电等相关系统的总称。

3.2

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239—2019，3.1]

3.3

网络安全事件 cybersecurity incident

由于人为原因，软硬件缺陷或故障、自然灾害等，对网络与信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

3.4

资产梳理 assets management

对高速公路（运营）管理单位具有价值的、安全策略保护的数字资源进行识别、标记、分类和统计分析。

3.5

基线 baseline

满足最小网络安全保证的基本要求，规定了软硬件系统的最低安全配置要求。

3.6

应急响应 emergency response

为应对网络安全事件的发生所做的准备以及在事件发生后所采取的措施。

4 一般规定

4.1 高速公路机电系统应符合国家相应网络安全等级保护要求。

4.2 网络安全核查不应影响高速公路机电系统的正常运行。

5 资产梳理

5.1 基本要求

5.1.1 应从网络、端口、主机和应用、互联网暴露资产和数据等维度进行动态管理。

5.1.2 应及时编制、更新、完善并保存资产清单。

5.1.3 应对资产进行安全属性关联分析，进行全方位的风险评估。

5.2 网络

5.2.1 应对网络拓扑、传输链路以及安全域等信息进行梳理归档。

5.2.2 应对网络中的主机、网络设备、安全设备、物联网设备、工控设备及其 MAC 地址、IP 地址和主机名信息进行梳理归档。

5.2.3 网络资产信息统计见图 A.1 和表 A.1。

5.3 端口

5.3.1 应对交换机、路由器等网络设备的物理端口及其使用情况进行梳理，确保端口没有非授权使用。

5.3.2 应对逻辑端口进行梳理，将存活 IP 和端口进行协议和服务识别，协议识别输出的信息至少包含 IP、端口、协议、服务名、标志以及证书等。

5.3.3 端口、协议和服务资产信息统计见表 A.2。

5.4 主机和应用

5.4.1 应对主机操作系统的系统信息和内核信息、环境变量信息、存在的漏洞和已知补丁信息进行梳理。

5.4.2 应对应用开放的服务信息、使用的中间件、数据库、编程语言、端口号以及 Web 应用框架等信息进行梳理。

5.4.3 主机和应用资产信息统计见表 A.3 和 A.4。

5.5 互联网暴露资产

5.5.1 应定期以 IP 地址段信息和关键字信息作为基础数据，结合域名、证书关联、单位关系探测、微信小程序、系统名称、单位标志等多种信息进行互联网空间隐形资产和未知资产的发现，建立资产归属数据库。

5.5.2 互联网暴露资产信息统计见表 A.5。

5.6 数据

5.6.1 应按照数据的来源、规模、存储位置、服务对象和敏感程度等属性进行梳理。

5.6.2 应对数据按照重要程度和敏感程度进行分类分级管理，明确每类数据的安全运行要求。

5.6.3 数据资产信息统计见表 A.6。

6 基线核查

6.1 基本要求

6.1.1 应建立适应的基线，并按照附录 B 定期核查。

6.1.2 对基线核查发现问题应及时处置，并记录和反馈。

6.2 机房安全

6.2.1 机房安全应符合 GB 50174 的规定。

6.2.2 应在机房安装防盗、防火等装置，出入口安装门禁控制系统、监控系统，在出入口显要位置张贴安全警示标识，视频监控确保三个月内可查询追溯、调阅分析。

6.2.3 应保证机房供配电设施运行正常，并安装电磁防护的相关措施，将各类机柜、设施以及设备等通过接地系统安全接地。应确保 UPS、发电机等后备供电设施的安全运行，对于 UPS 后备电池状态应至少每季度检测一次。

6.2.4 应确保消防系统各防火分区的消防器材正常运行，消防气体压力充足，每年至少检测一次。

6.3 网络环境安全

6.3.1 应在重要区域边界部署防火墙、安全分析和管控工具，检查边界安全控制策略。

6.3.2 应检查网络设备、安全设备和主机的安全配置。

6.3.3 应核查无线网络访问控制策略，对接入无线网络的设备进行实时控制和安全审计，确保无线网络入网实名认证及访问安全。

6.4 设备安全

6.4.1 应核查设备准入控制策略，实现对所有网络设备、主机和用户的准入管理，并对非授权访问绝对禁止。

6.4.2 应对违规外联行为进行日常化、无感知检查，并进行实时监测、告警和限制。

6.4.3 应核查机电系统网络边界、重要网络节点和基础环境的安全审计策略，对重要设备登录需实现双因素认证，对高危行为进行实时阻断和告警。

6.4.4 应核查统一管理和定期审计策略，审计日志留存应不少于 6 个月。

6.5 系统安全

6.5.1 应对系统的用户、权限、文件和网络等配置进行安全基线核查。

6.5.2 应对系统的重要服务和数据库进行安全基线核查。
6.5.3 应对系统安全补丁实施定期更新和修补，对必须修补的重要安全漏洞进行加固测试或补丁安全确认，测试或确认无误后，经授权才能修复漏洞，每月至少进行一次安全漏洞扫描。
6.5.4 应核查恶意代码防范软件的正版情况，及时升级恶意代码库以及安全软件版本。

6.6 应用安全

6.6.1 应定期对梳理后的应用（代码）、服务（接口）和中间件资产进行脆弱性扫描，及时发现安全漏洞并采取更新安全补丁等措施。
6.6.2 核查应用信息系统权限开放范围和审批流程。
6.6.3 网站类应用系统在升级时应进行脆弱性检测且每月至少进行一次检测，其他类应用系统在升级时应进行脆弱性检测且每半年至少进行一次检测。
6.6.4 网络和信息系统上线前，需通过具有资质的第三方的安全测评、等保备案和等级测评、密码应用安全性评估，涉及移动终端应用的需开展移动终端应用安全测评，确保高速公路机电系统的安全合规上线。

6.7 数据安全

6.7.1 应核查机电系统数据采集、存储、处理、传输、交换、销毁各数据全生命周期安全防护要求，对发现数据安全缺陷、漏洞等风险，应当立即采取补救和加固措施。
6.7.2 应保证机电重要信息系统和数据的容灾备份功能和恢复测式。

7 人员与第三方供应链安全要求

7.1 人员

7.1.1 上岗前应进行业务和安全责任教育培训，每年培训和考核次数不少于 1 次。
7.1.2 离岗时应进行工作交接，并收回安全工作所需的各类凭证与权限，登记备案。

7.2 第三方供应链

7.2.1 第三方供应链提供的产品和服务应符合 GB/T 36637 的规定。
7.2.2 应签订安全保密协议，明确安全保密的义务和责任。
7.2.3 派驻现场的第三方供应链人员应具备网络安全相关从业资格。
7.2.4 应明确第三方合作伙伴的工作专区、使用介质及其访问控制措施等。

8 日常监测

8.1 应建立网络安全监测预警和信息通报工作流程。
8.2 应从流量、文件、进程、系统和日志等方面开展常态化网络安全巡检工作。
8.3 以网络安全大数据为基础，感知网络安全威胁态势、网络及应用运行健康状态。

9 应急响应

9.1 应急预案

9.1.1 应健全应急工作机制、建立网络安全应急响应队伍，并明确人员构成和责任。

9.1.2 应按照网络安全事件分类的标准制定应急预案，包括但不限于启动预案的条件、应急组织构成、应急资源保障、应急通报流程、应急处置流程、响应时间、响应结束认定、事后教育和培训等内容。网络安全事件分类见附录 C。

9.1.3 应至少每年开展一次网络安全应急演练和渗透测试，具体组织方式和要求按照 GB/T 38645 的规定执行。

9.1.4 根据预案执行效果，及时对预案进行修订。

9.2 应急处置

9.2.1 发生网络安全事件，按照要求将事件相关情况报告安全负责人，启动应急预案进行处置操作，续报应急处置进展情况，直至应急事件处置结束，涉及违法犯罪的向所在地公安机关报案。

9.2.2 对有害程序事件，应首先将被感染主机从网络上隔离，做系统备份，分析评估有害程序感染范围和破坏程度，查明有害程序入侵途径。

9.2.3 对网络攻击事件，通过网络边界防护设备对攻击来源 IP 地址进行阻断或分流，分析攻击来源、攻击方式和被攻击对象，评估攻击影响范围和损失，优化边界防护设备访问控制策略，安装系统补丁，修复安全漏洞，恢复被攻击系统。

9.2.4 对信息破坏事件，应立即为受影响主机做镜像备份，从备份数据中恢复受破坏的最新信息数据，分析受破坏原因。对人为攻击引起的信息破坏，分析被利用漏洞并修复，追溯攻击者。

9.2.5 对信息内容安全事件，立刻关闭受影响系统，切换备用系统提供服务。对受影响系统做镜像备份，分析信息内容事件原因和攻击路径，及时修复安全漏洞，溯源攻击者。恢复系统正常信息内容，恢复对外服务。

9.2.6 对设备设施故障事件，应立即核查故障设备情况，如果能够自行恢复，应立即用备件替换受损部件；如不能自行恢复的，立即与设备供应商联系，请求派维护人员维修，并分析评估事件影响。

9.2.7 对灾害性事件，评估灾害性事件对机房、网络及信息系统的影响程度。机房不能提供服务的，应及时启动切换容灾机房业务系统。尽可能备份受灾机房中信息和系统数据，机房设备无法使用的，彻底清除数据、消磁处理，避免数据泄露。

9.3 总结评估

9.3.1 应在应急响应结束后 30 天内完成事件的调查处理和总结评估工作。

9.3.2 应对安全事件的起因、性质、影响和责任等进行分析评估，撰写并提交正式书面报告。

附 录 A
（规范性）
资产信息统计图表

填报单位：　　填报人：　　填报时间：

图A.1 网络拓扑图

表A.1 网络资产信息统计表

序号	路段名称	分中心/所/站	责任部门	重要程度	本地交换设备									接入设备				
					设备名称	部署位置	品牌型号	IP 地址	域	vlan	vlan IP	物理端口	端口状态（UP/down）	设备名称	品牌型号	互联端口	IP 地址/或互联地址	MAC 地址

注：①本地交换设备包括接入层、汇聚层、核心层网络设备；
②接入层设备包括与本地交换设备连接的重要网络节点，包括网络设备、安全设备、物联网设备、工控设备等；
③本表可根据运营管理需求，以使用单位为单元统计、归档，定期更新。

表A.2　端口、协议和服务资产信息统计表

应用名称	责任部门	重要程度	部署位置	源IP	源端口	目标IP	目标端口	协议方式	通信方向	数字证书	业务内容	备注

注：①端口号范围为 0-65535；

②协议方式主要包括UDP、TCP、HTTP 等方式；

③通信方向：主要描述业务数据流传输方向，如：车道工控机至收费站服务器方向。

表A.3　主机资产信息统计表

序号	主机名称	IP 地址	网络状态	品牌型号	操作系统版本	用途	用户名、密码合规性	漏洞	未安装补丁	病毒	责任人	资产状态	备注

注：①该表适用范围：服务器、管理机、工控机等计算机类设备；

②漏洞、未安装补丁、病毒按内容逐一填写，可利用专业软件等自动化手段；

③资产状态：包括在用、停用、报废；

④用户名密码为极敏感信息，由使用责任人负责管理，本表只需填写是否合规。

表A.4　应用资产信息统计表

序号	应用系统名称	操作系统及版本	编程语言及版本	服务信息	端口	数据库及版本	中间件及版本	应用框架及版本	IP 地址	协议	资产状态	责任人	漏洞与补丁	备注

注：①该表适用范围：高速公路各种应用与业务系统；

②应用系统按功能逐一填写，可利用专业软件等自动化手段；

③资产状态：包括在用、停用、报废。

表A.5　互联网暴露资产信息统计表

序号	资产名称	责任部门	重要程度	部署位置	IP 地址	域名	应用类型	责任人	备注

注：①互联网暴露资产包括域名、IP 地址、电子邮箱、公众号，以及发表的论文，文库资料等与高速公路机电系统相关的信息等；

②部署位置，如采用桩号+应用系统所在机房或主机等。

表A.6　数据资产信息统计表

序号	数据来源	数据规模/（年）	存储位置	服务对象	数据增量/（月）	数据中心名称	责任部门	责任人	统计截至时间	备注

注：①数据来源包括收费、监控等业务数据；

②数据规模：按照近两年数据年度总量均值划分为 PB、TB、GB、MB 四级；

③服务对象分为省中心、区域中心、路段分中心、站级四级；

④敏感程度分为重要数据、隐私数据（机构或公民的专有数据）、可公开数据三级；

⑤数据增量：按照近两年数据每月增长均值划分为 PB、TB、GB、MB 四级。

附 录 B
（资料性）
基线核查工作表

表B.1 基线核查工作表

序号	核查项目	核查内容	指标要求	检查记录	结论（符合/部分符合/不符合）
1	机房安全	机房安全制度	1）制定安全管理制度； 2）出入口张贴警示标示。		
		机房监控	1）7×24 小时不间断监测； 2）故障预警； 3）监控覆盖重点区域； 4）存储 3 个月以上。		
		物理安全	安装防火、防盗装置。		
		门禁系统	记录出入人员信息。		
		供配电系统	1）安装电磁防护设施； 2）满足安全接地要求； 3）确保后备供电设施的安全运行，后备电池每半年检测一次。		
		消防系统	确保消防器材正常运行，至少每年检测一次。		
2	网络环境安全	区域边界防护	1）部署防火墙； 2）满足边界防护策略； 3）检查边界安全控制策略。		
		基础安全配置	检查网络设备、安全设备和主机等。		
		无线安全防护	1）设置访问控制措施； 2）部署上网管理系统； 3）安全审计。		
3	设备安全	准入控制系统	禁止非授权访问，包括非法用户操作和合法用户未授权操作。		
		日志审计系统	1）网络安全设备、网络设备和服务器的安全审计； 2）定期审计，审计日志留存 6 个月以上。		
		防火墙	1）开启防火墙入侵检测防御； 2）开启防病毒功能。		

表 B.1 （续）

序号	核查项目	核查内容	指标要求	检查记录	结论（符合/部分符合/不符合）
4	系统安全	用户权限分配	1）建立安全运维账号，满足最小授权原则； 2）对系统用户、权限等安全核查。		
		数据库安全	1）身份鉴别可采用密码技术实现，若只采用“用户名+口令”鉴别方式，用户口令须由大小写英文字母、数字、特殊字符3种以上组成、长度不少于 8 位，每 90 天更换； 2）应对数据库的用户分配账户和权限； 3）应对审计记录进行保护，定期备份； 4）满足数据保密性相关要求。		
		系统安全加固	1）系统安全补丁； 2）进行漏洞扫描； 3）恶意代码软件的正版情况检查，至少每周升级一次恶意代码库及安全软件版本。		
5	应用安全	脆弱性检查	1）对应用（代码）、服务（接口）及中间件程序进行检查； 2）定期使用漏扫工具自查。		
		应用系统权限检查	1）明确权限开放范围和审批流程； 2）满足接口调用、数据调用的控制要求； 3）配置 ACL 策略限制。		
		风险评估	1）上线前测评； 2）网站类每月至少一次，其他类每半年至少一次。		
6	数据安全	存储	1）存储方式：本地存储、异地灾备、云端存储、离线存储、其他； 2）数据存储地点； 3）数据的容灾备份功能和恢复测式。		
		传输	1）采取专网传输； 2）采用密码技术保证数据的保密性、完整性； 3）检查加密技术； 4）网络传输协议。		
		使用	1）密码强度设置； 2）脆弱性检查； 3）分权限访问； 4）恶意代码检测。		

附 录 C
（资料性）
网络安全事件分类

网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件。

（1） 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2） 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3） 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4） 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

（5） 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6） 灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。