ICS 29.240.01
CCS F 23

团　体　标　准

T/EPIAJL 23-2025

吉林电网便携式运维网关集中管控技术规范

Specification for portable operation and maintenance gateway centralized management system of Jilin power grid

2025-12-05 发布　　2025-12-30 实施

吉林省电力行业协会　　发　布

全国团体标准信息平台

目　　次

目次.....I
前言.....II
1 范围.....1
2 规范性引用文件.....1
3 术语和定义.....1
4 缩略语.....2
5 总体架构.....3
6 功能要求.....4
6.1 人员管理.....4
6.2 运维网关管理.....4
6.3 工单管理.....4
6.4 规则库管理.....4
6.5 日志管理.....4
6.6 基础信息管理.....5
6.7 与运维网关的级联通信.....5
7 性能要求.....5
7.1 运维网关性能要求.....5
7.2 集中管控性能要求.....6
8 安全要求.....6
8.1 运维网关安全要求.....6
8.2 集中管控安全要求.....6
附录A（资料性）运维网关与集中管控级联通信规范.....8
A.1 概述.....8
A.2 通信协议基础.....8
A.3 通信流程说明.....8
A.4 密钥交换说明.....9
A.5 业务报文说明.....9
A.6 基础业务请求接口说明.....15
A.7 日志上送请求接口说明.....20
A.8 数据下发请求接口说明.....30
A.9 网关升级请求接口说明.....36
附录B（资料性）运维网关与集中管控级联通信代码示例.....42
B.1 概述.....42
B.2 代码示例.....42
B.3 固件压缩包样式示例.....50
参考文献.....51

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》给出的规则起草。

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这些专利的责任。

本文件由吉林省电力行业协会提出并归口 。

本文件起草单位：国网吉林省电力有限公司、国网吉林省电力有限公司电力科学研究院、国网长春供电公司、国网吉林供电公司、国网松原供电公司、国网延边供电公司、国网四平供电公司、国网辽源供电公司、国网白山供电公司、国网通化供电公司、国网白城供电公司、国网吉林省电力有限公司超高压公司、南京南瑞信息通信科技有限公司、珠海市鸿瑞信息技术股份有限公司。

本文件主要起草人：张继国、周玉光、赵巍、姜楠、王伟、付宇泽、姚卓宏、李佳、高奇、张丹、姜海峰、刘畅、周宏伟、宋玉飞、吕东、李天权、赵亮、孙佳龙、柴源、姜书鹏、王一琳、赵新、白帆、卢浩然、司聪、刘博龙、周家名、宋柏岩、冷淼、王成慧、赵德智、郭淼、于永生、杨红柳、方雅民、方昊。

本文件在执行过程中的意见或建议反馈至吉林省电力行业协会（吉林省长春市南关区通化路1100号，130022）。

全国团体标准信息平台

吉林电网便携式运维网关集中管控技术规范

1 范 围

本文件规定了吉林电网电力监控系统便携式运维网关集中管控的总体架构、功能要求、性能要求、安全要求以及与便携式运维网关之间的级联通信规范。

本文件适用于吉林电网内调度控制中心主站、集控站、配网自动化主站等电力监控系统便携式运维网关集中管控的设计、调试和验收要求，同时也适用于吉林电网电力监控系统便携式运维网关的设计研发、调试和验收要求，单机容量为200MW及以上等级燃煤发电机组电力监控系统运维可参照本文件执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 36572 电力监控系统网络安全防护导则

国家发改委令〔2024〕27号 电力监控系统安全防护规定

3 术语和定义

GB/T 36572 界定的以及下列术语适用于本文件。

3.1

电力监控系统 Electric power system supervision and control

用于监视和控制电力生产及供应过程的、基于计算机及网络技术的业务系统及设备，以及作为基础支撑的通信设施及数据网络等，包括但不限于实现继电保护和安全自动控制、调度监控、变电站（换流站）监控、发电厂监控、新能源发电监控、分布式电源监控、储能电站监控、虚拟电厂监控、配电自动化、变电站集控、发电集中监视、发电机励磁和调速、电力现货市场交易、直流控制保护、负荷监控、计费控制等功能的系统，以及支撑以上功能的通信设施、数据网络及配套网管系统。

[来源：GB/T 36572-2018，3.1，有修改]

3.2

便携式运维网关 Portable operation and maintenance gateway

一种运维安全边界设备，通过串接在运维终端与被运维对象之间，对运维操作进行实时监视、风险管控和工作记录。下文中简称“运维网关”。

3.3

便携式运维网关集中管控 Portable operation and maintenance gateway centralized management system

由设备管理、工单管理、规则库更新、运维日志管理等功能构成，用于集中接入和统一管理运维网关。下文中简称“集中管控”。

3.4

SM2算法 SM2 algorithm

国密算法中的一种，是一种椭圆曲线公钥密码算法，其密钥长度为256比特，属于非对称加密算法。

3.5

SM3算法 SM3 algorithm

国密算法中的一种，是一种密码摘要算法，其摘要长度为256比特，主要用于数字签名及验证、消息认证码生成及验证、随机数生成等，属于哈希算法。

3.6

SM4算法 SM4 algorithm

国密算法中的一种，是一种分组密码算法，其分组长度一般为128比特，密钥长度也为128比特，属于对称加密算法。

3.7

ECDHE密钥协商算法 ECDHE key exchange algorithm

一种基于椭圆曲线的密钥交换算法，主要用于密钥交换场景。

4 缩略语

下列缩略语适用于本文件

ARP：地址解析协议（Address Resolution Protocol）

DoS：拒绝服务（Denial of Service）

FTP：文件传输协议（File Transfer Protocol）

ICMP：互联网控制报文协议（Internet Control Message Protocol）

IP：互联网协议（Internet Protocol）

KVM：键盘、显示器、鼠标（Keyboard Video Mouse）

OMS：调度管理系统（Operation Management System）

PMS：电力生产管理系统（Power Management System）

RS232：串行数据接口标准（Recommended Standard 232）

SCP：安全复制协议（Secure Copy Protocol）

SFTP：安全文件传输协议（Secret File Transfer Protocol）

SSH：安全外壳协议（Secure Shell）

SYN：同步序列编号（Synchronize Sequence Numbers）

TCP：传输控制协议（Transmission Control Protocol）

TELNET：远程登录服务（Telecommunications Network）

USB：通用串行总线（Universal Serial Bus）

5 总体架构

集中管控应通过内部专用网络实现与运维网关的级联通信，实现运维网关统一管控，集中审计的管理机制。集中管控应部署在主站侧，按照电力监控系统网络安全防护规定要求，应经网络安全防护装置与运维网关、网安平台及OMS系统、PMS系统、风控平台、调控云等外部系统进行通信。集中管控与运维网关总体架构简图见图5.1。

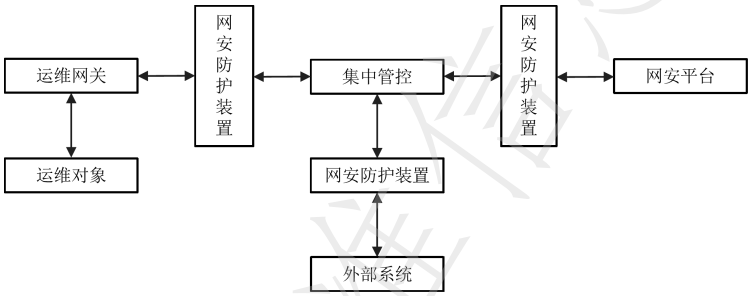


图5.1 总体架构简图

集中管控各个支撑模块要求如下：

a) 内部网安平台通信模块，应包含获取告警分析、设备台账、恶意代码库、组织机构信息以及工单中转信息等模组；

b) 外部系统对接通信模块，应具备与OMS系统、PMS系统、风控平台、调控云等外部系统对接通信模组；

c) 基础支撑模块，应包含运维网关备案管理、运维网关运行管理、运维网关升级管理、组织机构管理以及站点信息管理等模组；

d) 日志集中管理模块，应包含告警日志、运维日志、运维文件等日志集中管理等模组；

e) 规则及规则库管理模块，应包含规则库、操作指令规则、控制指令规则、高危端口规则等自动更新模组；

f) 工单统一管理模块，应包含运维任务管理、资产信息维护等模组；

g) 统计分析模块，应包含综合监视分析、统计报表、日志审计、执行情况分析等模组；

h) 与运维网关级联通信模块，应具备接收注册、网关监测、日志收取、规则下发、工单下发、恶意代码库下发、固件下发等模组。

运维网关与集中管控级联通信模块应包括网关注册、心跳数据、日志上送、规则获取、工单获取、恶意代码库获取、固件获取、账户管理、USB key管理、指令规则管理与获取、高危端口管理与获取、全过程运维管理以及本身设备日志上送等模组，运维网关与集中管控级联通信应遵照附录A中给出的通信规范。

6 功能要求

6.1 人员管理

应具备人员用户管理功能，具体要求如下：

a) 应支持对用户信息、角色信息的添加、编辑、删除等功能，支持对用户名的唯一性进行校验；
b) 应支持针对用户身份赋予对应的角色，对平台进行不同维度管理；
c) 应支持对角色进行权限设置，采用三权分立原则，不存在特权或超级用户。

6.2 运维网关管理

运维网关管理应满足如下要求：

a) 应支持对运维网关进行备案，实现已备案运维网关的安全接入；
b) 应支持对运维网关名称、厂商、型号等信息进行查看；
c) 应支持对运维网关连接状态、CPU、内存、磁盘、电量等信息进行查看；
d) 应支持对运维网关的运维工作情况进行查看；
e) 应支持运维网关恶意代码特征库的管理和远程升级，恶意代码特征库升级方式应电力监控系统网络安全要求；
f) 应支持运维网关固件的管理和远程升级。

6.3 工单管理

工单管理应满足如下要求：

a) 应支持同步外部系统工单或工作票信息，应支持接收运维网关创建的工单；
b) 应支持创建工单，至少包含工单下发人、工单接收人、工作任务、计划开始时间、计划结束时间、运维站点等内容；
c) 应支持对工单信息进行编辑；
d) 应支持将工单下发至运维网关，并支持查看下发状态。

6.4 规则库管理

集中管控应能根据实际运维工作场景创建多种规则库，应满足如下要求：

a) 应支持规则库及规则库中规则的增删改查，规则库包括：操作指令规则库、控制指令规则库、高危端口规则库；
b) 应支持规则库分组下发至运维网关；
c) 应支持运维网关主动获取规则库；
d) 应支持规则库下发状态的查看；
e) 应支持默认规则库的管理。

6.5 日志管理

日志管理应具备以下功能：

a) 应支持接收运维网关上送的告警日志，包括：高风险指令告警、违规外联告警、攻击告警、恶意代码告警、高危端口通信告警和二次授权记录等；

b） 应支持接收运维网关上送的运维日志，包括：认证登录日志、操作日志、设备插拔日志、文件传输日志等；
c） 应支持接收运维网关上送的运维日志文件，包括：录屏文件、通信报文、指令记录、键盘记录等；
d） 应支持告警日志、运维日志的查看和导出，并将导出行为生成日志；
e） 应支持运维日志文件的导出，并将导出行为生成日志。

6.6 基础信息管理

基础信息管理具备以下功能：
a） 应支持维护和管理组织机构的信息，包括：组织机构编号、组织机构名称等内容；
b） 应支持建立组织机构和厂站之间的运维关系；
c） 应支持建立组织机构和运维网关的归属使用关系；
d） 宜支持维护组织机构和组织机构下运维人员的人员架构关系。

6.7 与运维网关的级联通信

集中管控应接入运维网关，满足运维网关管理、工单管理、规则库管理、日志管理等功能要求，具体接入要求及协议明细见附录 A 和附录 B 。

7 性能要求

7.1 运维网关性能要求

运维网关性能应满足如下要求：
a） 处理器应采用非 x86 架构；
b） 推荐内存容量不低于 4GB；
c） 固态硬盘存储容量不低于 1TB；
d） 至少应配备 2 个 HDMI 接口；
e） 至少应配备 2 个千兆电口；
f） 至少应配备 2 个 DB9（R232）接口；
g） 至少应配备 4 个 USB 接口；
h） 至少应配备 1 个内置高清摄像头，推荐分辨率不低于 800 万像素；
i） 至少应配备 4 个 USB 接口；
j） 至少应配备 5 个 USB key，并适配 Windows7、Windows10、Linux 等操作系统；
k） 至少应配备 1 个指纹识别模块；
l） 至少应配备 1 个 7 英寸（约 178mm）的触摸屏，推荐 10 英寸；
m） 外观尺寸应不超过 300mm×200mm×80mm（长×宽×高）；
n） 整机质量应不大于 2.0kg；
o） 进出接口应对侧布置；
p） 开机时长应低于 1min；
q） 运维操作响应及高风险指令识别延迟应低于 200ms；

r） 违规外联、攻击行为识别及阻断响应时间应低于 3s；
s） 应支持对 WIFI、蓝牙、双网卡方式违规外联行为检测；
t） 应支持 NTP 通过网络服务方式对时；
u） 提供的配线应采用通用线序；
v） 常规条件下，电池续航时间应不低于 4h。

7.2 集中管控性能要求

集中管控性能如下要求：
a） 应支持多客户端并发访问数量应不低于 20 个；
b） 应支持接入运维网关数量应大于 500 台；
c） 应支持常规数据访问的响应时间应不低于 3s；
d） 应支持统计分析类数据访问的响应时间应不低于 5s；
e） 应支持 1000 条以上级别数据导出的响应时间应不低于 10s；
f） 应支持对传输带宽进行配置，确保不阻塞网络带宽。

8 安全要求

8.1 运维网关安全要求

运维网关应满足如下安全要求：
a） 不应内置后门，不存在已知缓冲区溢出等安全漏洞；
b） 不应配备 WIFI、蓝牙等无线通信硬件模块；
c） 应关闭默认共享、高危端口等通用服务以及不必要的系统服务；
d） 应具备检测并抵御常见网络攻击和渗透攻击的能力；
e） 应支持用户口令复杂度检测、口令过期提醒、口令过期时间可配置；
f） 应采用国密算法保证鉴别信息和重要业务数据等敏感信息存储的保密性；
g） 应具备进程守护机制，确保程序本身的安全可靠运行；
h） 应具备开机硬件检测功能，在发现硬盘等硬件被更换后不应启动操作系统；
i） 应采用安全可控的操作系统。

8.2 集中管控安全要求

集中管控应依据所在安全分区等级保护分级，满足GB/T 22239-2019中第6～10章对应分级的等级保护要求，集中管控通用安全要求如下：
a） 不应存在弱口令，初始口令首次登录时应进行修改；
b） 不应存在后门及高危安全漏洞；
c） 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
d） 应按照三权分立的原则，建立不同角色用户，实现权限相互独立、相互制约；
e） 应采用国密算法保证鉴别信息和重要业务数据等敏感信息在数据存储和传输时的机密性、完整性；

f) 应提供自身审计数据的查阅功能；
g) 应关闭不需要的系统服务、默认共享和高危端口；
h) 集中管控应用程序运行时，不应对操作系统、其他业务系统的安全性与稳定性造成影响；
i) 应采用安全可控的操作系统；
j) 宜采用基于调度数字证书的加密认证技术保障重要应用功能的安全性；
k) 宜采用安全可控的数据库、中间件。

全国团体标准信息平台

附 录 A
（资料性）
运维网关与集中管控级联通信规范

A.1 概述

运维网关与集中管控的级联通信要求如下：

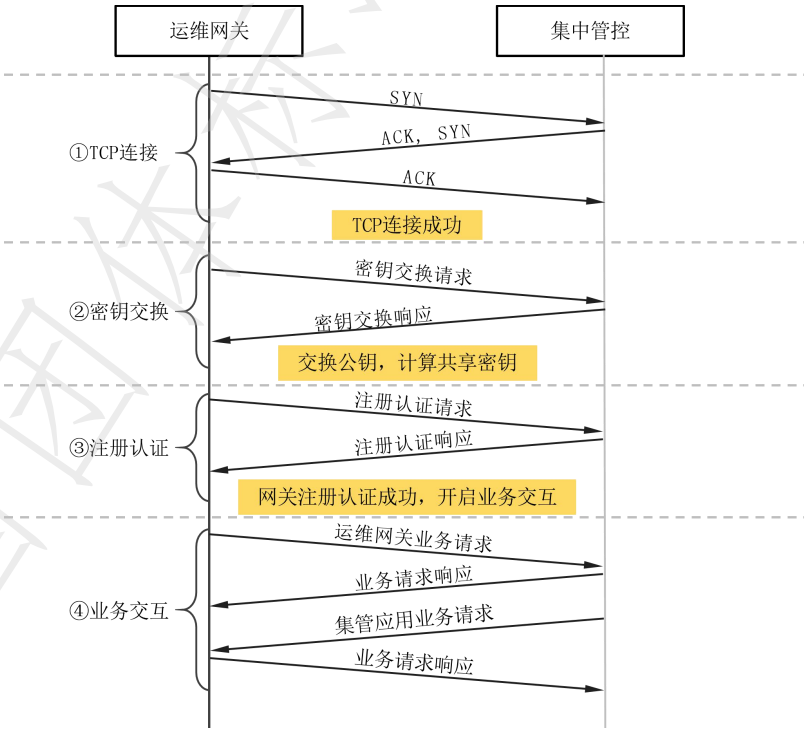
a） 应支持接收集中管控下发的规则库，作为风险管控依据；
b） 应支持接收集中管控下发的运维工单，开展对应的运维工作；
c） 应支持将运维日志、告警日志、运维文件等信息上传至集中管控；
d） 应支持从集中管控查询恶意代码特征库信息，应支持下载更新；
e） 应支持从集中管控查询网关固件信息，应支持下载更新。

A.2 通信协议基础

运维网关与集中管控应的级联通信采用 TCP 作为传输层协议，运维网关作为客户端，集中管控应作为服务端，默认端口为 62099，支持自定义配置。

A.3 通信流程说明

运维网关与集中管控的通信流程见图 A.1。



图A.1 通信流程示意图

运维网关（或通过扩展底座）与集中管控网络连通之后：

a） 运维网关作为客户端请求建立与集中管控的 TCP 连接；
b） 运维网关发起密钥交换请求，用 ECDHE 算法生成通信密钥；

c） 运维网关发起注册认证请求，并用通信密钥进行业务数据加密；
d） 认证通过后，进行日志上送、规则库下发、运维工单下发等业务数据交互，并用通信密钥进行业务数据加密。

A.4 密钥交换说明

运维网关与集中管控成功建立 TCP 连接后，应使用 SM2 算法和 sm2p256v1 曲线生成己方公私钥，明文发送密钥交换请求交换公钥用于计算通信密钥。密钥交换请求报文格式见表 A.1。

表A.1 密钥交换请求报文格式

数据项	长度及类型	说明
Magic Number - 0	1 字节	恒为 0xAC
Magic Number - 1	1 字节	恒为 0xFC
版本号	2 字节 uint16，网络序	当前版本为 0x0001
本连接运维网关侧能提供的最大并发服务数	2 字节 uint16，网络序	可为 0，最大 1024。缺省建议使用 8，若双方协商不一致，按较小值运行
本连接希望集中管控能够支持的并发请求数	2 字节 uint16，网络序	可为 0，最大 1024。缺省建议使用 8，若双方协商不一致，按较小值运行
加密算法组	1 字节	当前传 0x12，即散列算法用 SM3，非对称加密算法用 SM2(sm2p256v1)，对称加密算法用 SM4/CTR/NoPadding
保留	1 字节	
密钥长度	2 字节 uint16	网络序
密钥内容	若干字节	十六进制格式(不进行 Base64 等任何编码)，用于 ECDHE 密钥交换的公钥

集中管控回复的密钥交换响应报文格式见表 A.2。

表A.2 密钥交换响应报文格式

数据项	长度及类型	说明
Magic Number - 0	1 字节	恒为 0xAC
返回码	1 字节	正常时为 0，连接异常为 1
保留	2 字节	
本连接集中管控侧能够提供的最大并发服务数	2 字节 uint16，网络序	可为 0，最大 1024。缺省建议使用 8，若双方协商不一致，按较小值运行
本连接希望运维网关侧能够支持的并发请求数	2 字节 uint16，网络序	可为 0，最大 1024。缺省建议使用 8，若双方协商不一致，按较小值运行
保留	2 字节	
密钥长度	2 字节 uint16	网络序
密钥内容	若干字节	十六进制格式（不进行 Base64 等任何编码），用于 ECDHE 密钥交换的公钥

A.5 业务报文说明

A.5.1 业务报文格式

运维网关和集中管控均可主动发起业务交互请求，并由对端进行响应，请求和响应报文格式见表 A.3。

表A.3 业务报文格式

一级划分	二级划分	长度及类型	说明
数据头	请求/响应标识	2 字节，网络序	详见 A.5.1.1
	控制号	2 字节，网络序	请求报文中为业务请求码，响应报文中为业务返回码
	时间戳	8 字节，网络序	毫秒时间戳，返回消息的时间戳和对应的请求消息的时间戳保持一致
	通信控制标记	1 字节	详见 A.5.1.2
	确认字节	1 字节	详见 A.5.1.3
业务数据	数据长度	4 字节，网络序	描述业务数据长度，可为 0
	数据内容	若干字节	业务数据内容，可以没有
校验	校验	8 字节，网络序	详见 A.5.1.4

A.5.1.1 请求/响应标识

请求/响应标识为 16 位 2 进制数据，具体说明见表 A.4。

表A.4 请求/响应标识说明

0（高位）	1	2	3	4	5	6	...	15（低位）
通信标识			请求序列号			通道号		
001 为请求 011 为响应			每次请求应在上次请求的基础上+1，响应消息应和对应的请求消息序列号保持一致			最大支持 1024 个通道(通常通道数小于 32)，在连接建立时双方需协商该通道数，按较小值运行		

A.5.1.2 通信控制标记

通信控制标记共 8 个二进制位，详见表 A.5。

表A.5 通信控制标记说明

位置	作用	描述
7（低位）	是否有业务数据	1 – 该请求/响应含有业务数据，0 – 该请求/响应无业务数据
6	是否无需回应	1 – 该请求为一个无需回应的请求，0 – 该请求需要接收方在处理完成后回复请求方。正常业务均设为 0
5	是否加密	1-加密，0-不加密，加密仅针对业务数据部分
4	业务数据格式	1-二进制格式，0-Json 格式，除文件外都用 Json 传输
3	是否文件传输请求	1 文件传输，0-非文件传输，注：文件描述包也设置为 1
2	保留	
1	保留	
0（高位）	保留	

A.5.1.3 确认字节

通信报文的第 14 字节作为确认字节，用于对协议报文的开始部分进行检查。发送方应设置该字节的值为前 13 个字节逐字节异或的结果再与 0x66 异或得出的最终值。接收方应校

验该值，以确认前 14 个字节为一个业务交互报文的开始部分。该字节并非用于传输错误校验或恢复。

A.5.1.4 校验

从请求/响应标识起到业务数据的所有字节均参与校验，应使用 SM3 散列算法计算出散列值，按每 8 个字节分组并进行异或运算，产生一个 8 字节的校验值。

A.5.2 数据加密说明

加密控制：A.5.1.2 通信控制标记中第 5 位，值为 1 代表加密，值为 0 代表不加密；

加密范围：A.5.1 业务报文格式中的业务数据内容；

加密密钥:A.4 密钥交换说明中用 ECDHE 算法计算得出的通信密钥,使用通信密钥的 0-15 字节作为 SM4 加密密钥，16-31 字节作为初始向量（IV）；

加密算法：SM4 对称加密算法，加密模式为 CTR，填充方式为 NoPadding；

解密说明：接收方收到业务报文后，根据加密控制位判断是否需要解密，若需解密则用通信密钥采用同样的方式进行解密。

A.5.3 文件传输说明

业务报文也支持对文件的传输，文件传输采用分包发送的机制，数据包的通信控制标记中是否文件传输均设置为 1-文件传输，业务数据格式及文件传输包分类按表 A.6 中的说明进行设置。

表A.6 文件传输数据包分类

数据包类型	数据包数量	业务数据格式	描述
文件描述包	1	Json	文件传输过程的第一帧数据包，主要描述所传文件的信息。一次完整的文件传输过程应发送两种类型的数据包：一个文件描述包和干文件内容包。详见表 A.5.3.1
文件内容包	n	二进制	文件一般需要拆分成多个数据包进行发送，一个文件数据包推荐为 50KB，接收方收到数据后按照一定的规则组装还原文件。文件传输应先发送文件描述包，成功发送并收到确认响应后，依次按顺序发送文件内容包。详见表 A.5.3.2

A.5.3.1 文件描述包

文件描述包用来传输当前发送的文件的描述信息，例如文件名称、文件类型、Hash 校验值等。具体业务数据字段说明见表 A.7。

表A.7 文件描述包业务数据格式

业务请求码		详见表 A.11，通用文件上传为 0x6151		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填

3	wo_no	工单编号	字符型（128）	运维文件上传有工单编号，非必填，
4	log_file_type	文件类型	整数型（1）	1：录屏文件；2：通信报文；3：串口通信；4：SSH、Telnet、RS232 字符指令；5：传输文件；6：键盘记录；7：工作票照片；8：恶意代码特征库升级包；9：固件升级包；10：通用工单文件；11：其他。必填
5	biz_info	业务描述信息	Json 对象	传输文件需要的业务字段信息放到该对象中，非必填
6	file_name	文件名称	字符型（256）	包括后缀，必填
7	file_type	文件类型	字符型（32）	指文件后缀，非必填
8	file_path	文件原路径	字符型（256）	非必填
9	file_size	文件大小	整数型（8）	文件字节大小，纯数字，单位 B，必填
10	create_time	文件创建时间	字符型（32）	例如:2018-07-13 12:34:56，必填
11	update_time	文件修改时间	字符型（32）	例如:2018-07-13 12:34:56，必填
12	file_code	文件标识	整数型（8）	文件的唯一标识，接收方按此唯一标识归集文件。必填
13	slice_count	分包总数	整数型（4）	本次文件传输一共分了多少数据包，包含文件描述包，必填
14	slice_no	包序号	整数型（4）	当前文件包是本次文件传输的第几个包，文件描述包为第一个包，文件内容包按顺序排，必填
15	slice_size	文件分包大小	整数型（2）	本次文件传输的文件分片大小，单位 KB，比如 500K 的文件，一包 50K 进行传输，该字段可用于断点续传，如需进行断点续传需确保分片大小一致。该值最大可设置为 1024K，必填
16	hash_code	文件哈希	字符型（64）	SM3 算法计算的文件哈希值，接收方组装完成文件后用该哈希值进行完整性校验，必填
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
3	slice_count	分包总数	整数型（4）	本次文件传输一共分了多少数据包，包含文件描述包，必填
4	slice_no	包序号	整数型（4）	当前文件包是本次文件传输的第几个包，文件描述包为第一个包，文件内容包按顺序排，必填
5	file_code	文件标识	整数型（8）	必填
6	next_no	接收方需要的下一个包序号	整数型（4）	接收方需要的下一个数据包序号。目的为了实现断点续传，后续发送方只需要按着返回值发送下一个包即可，必填

A.5.3.2 文件内容包

文件内容包的业务数据格式为二进制形式，其中第 1～8 八字节为文件标识，第 9～12 四个字节为分包总数，第 13～16 四个字节为包序号，剩余字节为当前报文包含的文件数据，推荐的分包大小为 50kB。详见表 A.8。

表A.8 文件内容包业务数据字节描述

1～8	9～12	13～16	17	18	...	n
文件标识（网络序）	分包总数（网络序）	包序号（网络序）	一包文件数据			

回复确认包的业务数据格式见表A.9。

表A.9 文件内容包响应业务数据格式

返回码	0-成功，其他见表A.12 业务返回码对照表			
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一ID，必填
3	slice_count	分包总数	整数型（4）	本次文件传输一共分了多少数据包，包含文件描述包，必填
4	slice_no	包序号	整数型（4）	当前文件包是本次文件传输的第几个包，文件描述包为第一个包，文件内容包按顺序排，必填
5	file_code	文件标识	整数型（8）	必填

A.5.3.3 文件传输数据包示例

表A.10是一次文件发送过程的分包示例，接收方收到所有数据包后应按顺序组装文件数据。

表A.10 文件传输数据包示例表

数据包	文件标识	数据包总数	数据包序号	数据包内容	描述
文件描述包	123456	36	1	Json	文件描述信息
文件内容包1			2	二进制	第一包文件数据
文件内容包2			3	二进制	第二包文件数据
文件内容包3			4	二进制	第三包文件数据
...			...	...	...
文件内容包34			35	二进制	第34包文件数据
文件内容包35			36	二进制	第35包文件数据

A.5.4 业务请求说明

业务数据传输请求包含基础业务、日志上送、规则库下发、运维工单下发、更新升级等部分，具体业务请求明细及对应的业务请求码见表A.11。

表A.11 业务请求码对照表

业务类型	类型编码	业务子类型	编码	业务请求码	请求发起方
基础业务	0x00	注册认证	0x64	0x0064	运维网关
		心跳数据	0x66	0x0066	运维网关
		版本上报	0x68	0x0068	运维网关
		配置下发	0x70	0x0070	集中管控
运维日志上送	0x29	认证登录日志	0x01	0x2901	运维网关
		操作日志	0x02	0x2902	
		文件传输日志	0x03	0x2903	

		设备插拔日志	0x04	0x2904	
		运维任务信息	0x06	0x2906	
		日志统计信息	0x07	0x2907	
告警日志上送	0x30	高风险指令告警	0x01	0x3001	运维网关
		违规外联告警	0x02	0x3002	
		攻击告警	0x03	0x3003	
		恶意代码告警	0x04	0x3004	
		高危端口告警	0x06	0x3006	
		二次授权记录	0x05	0x3005	
通用文件上送	0x61	通用文件上传	0x51	0x6151	运维网关
规则库下发	0x51	高危端口规则下发	0x01	0x5101	集中管控
		操作类指令规则下发	0x02	0x5102	集中管控
		控制类指令规则下发	0x03	0x5103	集中管控
		高危端口规则获取	0x51	0x5151	运维网关
		操作类指令规则获取	0x52	0x5152	运维网关
		控制类指令规则获取	0x53	0x5153	运维网关
运维工单下发	0x52	运维工单下发	0x04	0x5204	集中管控
		运维工单获取	0x05	0x5205	运维网关
		资产信息确认	0x21	0x5221	运维网关
更新升级相关	0x61	恶意代码库更新请求	0x11	0x6111	运维网关
		恶意代码库下发	0x01	0x6101	集中管控
		网关固件更新请求	0x12	0x6112	运维网关
		网关固件下发	0x02	0x6102	集中管控

A.5.5 业务返回码对照

接收方在获取业务请求后，应根据处理结果向发送方回复响应消息，响应报文中的业务返回码应能反映本次业务请求结果，具体的业务返回码对照见表 A.12。

表A.12 业务返回码对照表

返回码	十六进制	返回码说明
0	0x0000	成功
1	0x0001	成功，有更新
2	0x0002	成功，无更新
3	0x0003	成功，清空数据，清空运维网关侧对应类型的业务数据
4	0x0004	成功，无需上传
10001	0x2711	未备案
10002	0x2712	已冻结
10003	0x2713	已注销
10004	0x2714	证书验证失败
10005	0x2715	设备序列号缺失
10006	0x2716	运维网关证书缺失
10007	0x2717	运维网关签名缺失
10008	0x2718	设备厂商名称缺失
10009	0x2719	ip 地址缺失
10010	0x271A	网关端固件版本号缺失

10011	0x271B	网关使用的恶意代码引擎厂商缺失
10012	0x271C	网关当前的恶意代码库版本号缺失
10013	0x271D	设备 UID 缺失
10014	0x271E	设备 UID 无效
10015	0x271F	数据格式版本缺失
10016	0x2720	数据格式版本错误
10017	0x2721	设备厂商名称无效
10018	0x2722	参数错误，请核实必填信息
10019	0x2723	工单编号缺失
10020	0x2724	时间格式错误
10021	0x2725	联系方式格式错误
10022	0x2726	区域编码格式错误
10023	0x2727	数据长度错误
10024	0x2728	任务状态格式错误
10025	0x2729	检修类型格式错误
10026	0x273A	同文件标识的文件已接收完成，文件重复
10027	0x273B	文件重复，工单编号、文件名称、创建时间、hash 值、文件大小一样
10028	0x273C	未知业务请求，业务请求码无法识别
10029	0x273D	集中管控内部错误
10030	0x273E	暂不支持该功能，如恶意代码特征库升级功能不支持
11000	0x2AF8	其他错误

A.6 基础业务请求接口说明

A.6.1 注册认证

通信连接建立后，运维网关应向集中管控发送自身信息以完成注册认证流程，使集中管控能够验证运维网关身份并为其分配唯一标识符，注册认证数据包格式见表 A.13。

表A.13 注册认证业务数据格式

业务请求码		0x0064，即为十进制 100		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	client_pem	运维网关证书	长字符串	CA 格式证书，必填
2	client_sign	运维网关签名	长字符串	对 ECDHE 交换后得到的通信密钥（全长）进行 SM3 散列计算，然后用 SM2/SM3 算法签名后的值，必填。 证书校验及验签过程见下文注 1 描述。
3	version	数据格式版本	整数型（1）	当前固定为 1，必填
4	manufacturer	设备厂家名称	整数型（1）	常量整数，传输公司对应的序号即可 1：北京国泰网信科技有限公司； 2：北京科东电力控制系统有限责任公司； 3：北京珞安科技有限责任公司； 4：湖南匡安网络技术有限公司； 5：积成电子股份有限公司； 6：南京南瑞信息通信科技有限公司；

				7：许继电气股份有限公司； 8：浙江齐安信息科技有限公司； 9：浙江齐治科技股份有限公司； 10：珠海市鸿瑞信息技术股份有限公司； 11：其它。 必填
5	serial	设备序列号	字符型（32）	最长 32 位，必填
6	ip	ip 地址	字符型（16）	网关 ip 地址，必填
7	mac	Mac 地址	字符型（32）	例如：00-16-EA-AE-3C-40，非必填
8	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，第一次注册时该项不适用，后续每次请求均携带。生成规则：厂商名称首字母缩写_网关设备序列号
9	model	设备型号	字符型（32）	运维网关的设备型号，非必填
10	dev_name	网关设备名称	字符型（64）	运维网关上设置的设备名称，非必填
11	dock_mac	底座 MAC 地址	字符型（16）	底座 MAC 地址，如无底座，非必填
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	server_pem	集中管控端证书	长字符串	CA 格式证书，必填
2	server_sign	集中管控端签名	长字符串	对 ECDHE 交换后得到的通信密钥（全长）进行 SM3 散列计算，然后用 SM2/SM3 算法签名后的值，必填。 证书校验及验签过程见下文注 1 描述。
3	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，由集中管控分配，后续日志上送、业务交互均需携带，必填
4	message	消息	字符型（256）	提示消息，选填

注 1：证书校验及验签过程：

运维网关和集中管控应包含的信息：私钥、公钥证书、CA 证书。

通信双方发送自身验证信息的过程：

a) ECDHE 得到 SM4 通信密钥；

b) 通信密钥做 SM3 得到 hash 值；

c) hash 值经过 SM2/SM3 私钥签名，即为注册认证的 client_sign/server_sign 字段；

d) 通信双方验证对方身份的过程：

e) 利用 CA 证书校验收到的公钥证书（client_pem/server_pem）的合法性；

f) 利用收到的公钥证书验签收到的签名（client_sign/server_sign），原文为 b）的结果。

在运维网关通过扩展底座接入集中管控的场景中，运维网关只需将底座 MAC 地址发送给集中管控即可。

A.6.2 心跳数据

运维网关认证成功后，应每 1 分钟上报 1 次心跳数据到集中管控，心跳数据包括电量、CPU、内存等信息。心跳数据的业务数据格式见表 A.14。

表A.14 心跳数据业务数据格式

业务请求码		0x0066，即为十进制 102		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	battery_percent	电量信息	浮点数（4）	电量百分比数值，必填
4	cpu_usage	总 CPU 使用率	浮点数（4）	百分比数值，必填
5	memory_size	内存大小	整数型（8）	单位 B，必填
6	memory_usage	内存使用率	浮点数（4）	百分比数值，必填
7	disk_size	数据盘大小	整数型（8）	单位 B，仅传运维数据存储的盘的大小，必填
8	disk_usage	数据盘使用率	浮点数（4）	百分比数值，仅传运维数据存储的盘的使用率，必填
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，非必填
2	dev_id	网关唯一标识	字符型（64）	注册后返回的网关唯一 ID 必填

A.6.3 版本上报

运维网关注册认证成功后，应定期（默认 1 小时）将自身固件版本、恶意代码特征库版本、规则库版本等信息上报至集中管控，并根据返回信息判断是否有待更新的数据。

当运维网关侧相关版本发生变更时，也应及时调用版本上报接口将最新版本上报至集中管控。版本上报接口的业务数据格式见表 A.15。

表A.15 版本上报业务数据格式

业务请求码		0x0068		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	software_version	网关端固件版本号	字符型（64）	最长 64 位，必填
4	software_valid_date	网关端固件许可证有效期	字符型（32）	例如： 2024-07-13 12:34:56，非必填，不填代表无授权到期时间
5	virus_vendor	网关使用的恶意代码引擎厂商	字符型（64）	厂商名称名称，最长 50 位，必填 可选值：[瑞星;江民;绿盟;政采]

6	virus_version	网关当前的恶意代码库版本号	字符型（64）	最长 64 位，必填
7	virus_valid_date	网关当前的恶意代码库许可证有效期	字符型（32）	例如： 2024-07-13 12:34:56，非必填，不填代表无授权到期时间
8	os_type	网关操作系统类型	字符型（64）	例如：KylinSec OS Linux，非必填
9	os_version	网关操作系统版本号	字符型（64）	最长 64 位，非必填
10	os_valid_date	网关操作系统有效期	字符型（32）	例如:2024-07-13 12:34:56，非必填
11	port_base_id	端口规则库 ID	整数型（4）	网关侧端口规则库的唯一标识，初始值为 0，非必填，不填代表没同步过规则库
12	port_base_version	端口规则版本	整数型（8）	网关侧端口规则库的版本号，初始值为 0，非必填，不填代表没同步过规则库
13	operate_base_id	操作指令规则库 ID	整数型（4）	非必填，不填代表没同步过规则库
14	operate_base_version	操作指令规则库版本	整数型（8）	非必填，不填代表没同步过规则库
15	control_base_id	控制指令规则库 ID	整数型（4）	非必填，不填代表没同步过规则库
16	control_base_version	控制指令规则库版本	整数型（8）	非必填，不填代表没同步过规则库
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
3	software_version	集中管控端维护的固件版本号	字符型（64）	最长 64 位，必填
4	software_version_list	待升级的网关固件版本列表	JSON 数组	具体格式见表 A.16。 网关固件升级到最新版本需要的版本列表信息,通常是最新一次全量程序包以及该版本之后的增量包,非必填
5	virus_vendor	恶意代码库厂商	字符型（64）	与网关所提交的一致，非必填
6	virus_version	集中管控端维护的恶意代码库最新版本号	字符型（64）	如不具备提供对应的升级包,该项不使用，非必填
7	virus_version_list	待升级的恶意代码库版本列表	JSON 数组	具体格式见表 A.16。 恶意代码特征库升级到最新版本需要的版本列表信息,通常是最新一次全量程序包以及该版本之后的增量包，非必填
8	port_base_id	端口规则库 ID	整数型（4）	集中管控侧该网关对应的端口规则库的唯一标识，非必填

9	port_base_version	端口规则版本	整数型（8）	集中管控侧该网关对应的端口规则库的最新版本号(版本号建议以时间戳递增），非必填
10	operate_base_id	操作指令规则库ID	整数型（4）	集中管控侧该网关对应的操作指令规则库的唯一标识，非必填
11	operate_base_version	操作指令规则库版本	整数型（8）	集中管控侧该网关对应的操作指令规则库的最新版本号(版本号建议以时间戳递增），非必填
12	control_base_id	控制指令规则库ID	整数型（4）	集中管控侧该网关对应的控制指令规则库的唯一标识，非必填
13	control_base_version	控制指令规则库版本	整数型（8）	集中管控侧该网关对应的控制指令规则库的最新版本号(版本号建议以时间戳递增），非必填

版本信息数据格式见表A.16。

表A.16 版本信息数据格式

序号	字段	字段名称	字段类型	描述及要求
1	version	版本号	字符型（64）	升级包的版本号，必填
2	file_code	文件标识	整数型（8）	文件的唯一标识，必填
3	hash_code	文件哈希	字符型（64）	SM3算法计算的哈希值，16进制字符串，必填
4	update_type	升级包类型	整数型（1）	升级包类型，非必填。1：全量升级包；2：增量升级包
5	start_version	增量起点版本	字符型（256）	该升级包的升级起点版本，非必填，多个值用英文逗号分隔
6	publish_time	发布时间	整数型（1）	升级包的发布时间，以厂家发布的时间为准，主要用作升级参考及排序参考，必填
7	file_size	文件大小	整数型（8）	文件字节大小，纯数字，单位B，非必填
8	version_des	版本描述	字符型（512）	版本描述信息，非必填

A.6.4 配置下发

运维网关认证成功后，集中管控应同步一次基础配置信息，包括网关配置信息、组织机构信息、站点信息列表等。配置下发数据格式见表A.17。

表A.17 配置下发业务数据格式

业务请求码	0x0070			
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一ID，必填
2	version	数据格式版本	整数型（1）	当前固定为1，必填
3	config	网关配置信息	Json对象	非必填，字段待定
4	org_info	组织机构信息	Json对象	具体字段见A.18，非必填
5	station_list	站点信息列表	Json数组	站点数据列表，具体字段见A.19，非必填
6	user_list	人员账号列表	Json数组	具体字段待定，非必填

返回码		0-成功，其他见表A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型(256)	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一ID，必填

组织机构信息字段说明见表A.18。

表A.18 组织机构信息字段说明

序号	字段	字段名称	字段类型	描述及要求
1	org_id	组织机构编号	字符型（64）	必填
2	org_name	组织机构名称	字符型（128）	必填
3	org_type	组织机构类型	字符型（32）	非必填

站点信息字段说明见表A.19。

表A.19 站点信息字段说明

序号	字段	字段名称	字段类型	描述及要求
1	station_id	站点编号	字符型（64）	例如：1，集中管控中唯一标识 必填
2	station_name	站点名称	字符型（64）	例如：xx 电厂 必填
3	voltage_level	电压等级	字符型（32）	例如：30kV 非必填
4	station_type	站点类型	整数型（1）	1：发电厂 2：变电站 3：换流站 4：其他 必填

A.7 日志上送请求接口说明

A.7.1 概述

运维网关认证成功后，应支持将运维过程中产生的运维日志、告警日志、运维文件等信息及时上送至集中管控。

A.7.2 日志上送列表

日志类型见表表A.20。

表A.20 日志类型

日志类型	日志子类型	上传频率
运维日志	认证登录日志	空闲时统一上传
	操作日志	空闲时统一上传
	文件传输日志	空闲时统一上传

日志类型	日志子类型	上传频率
	设备插拔日志	空闲时统一上传
	运维任务信息	空闲时统一上传
	日志统计信息	空闲时统一上传
告警日志	高风险指令告警	空闲时统一上传
	违规外联告警	空闲时统一上传
	攻击告警	空闲时统一上传
	恶意代码告警	空闲时统一上传
	高危端口通信告警	空闲时统一上传
	二次授权记录	空闲时统一上传
运维文件	录屏文件、通信报文、指令记录、键盘记录	优先级最低，其他所有数据传完后开始传输

A.7.3 日志上送通用返回

集中管控收到运维网关上送的运维日志、告警日志后，需要返回一帧报文以响应处理结果，旨在让运维网关确认所上送的日志是否已被接收并成功处理。具体的返回格式见表 A.21。

表A.21 日志上送通用返回业务数据格式

返回码	0-上送成功，其他见表 A.12 业务返回码对照表			
返回报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	设备 UID	字符型（64）	网关注册后返回的网关唯一 ID，必填

A.7.4 运维日志

运维日志是运维网关在日常使用及运维过程中产生的记录类信息，运维网关与集中管控连接成功后应先该数据上送至集中管控。主要包括认证登录日志、操作日志、文件传输日志、设备插拔日志、运维任务信息、日志统计信息六个接口，具体说明及业务数据格式见下文。

A.7.4.1 认证登录日志

认证登录日志包含的字段信息如下表所示，第二列（字段）是发送到集中管控上所包含的字段。

表A.22 认证登录日志业务数据格式

业务请求码	0x2901			
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID,必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	log_time	日志产生时间	字符型（32）	例如： 2018-07-13 12:34:56，必填
4	login_action	登录/注销动作	整数型（1）	0：代表登录成功；1：代表注销；2：代表登录失败；必填
5	user_name	登录用户名	字符型（32）	必填
6	login_type	登录方式	整数型（1）	0：无意义；1：用户名登录；2：双因子登录；必填

A.7.4.2 操作日志

操作日志包含的字段信息见表 A.23

表A.23 操作日志业务数据格式

业务请求码		0x2902		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	log_time	日志产生时间	字符型（32）	例：2018-07-13 12:34:56，必填
4	wo_no	工单编号	字符型（128）	必填
5	resource_info	目的资源 IP 地址和端口	Json	一个 Json 数组，非必填
6	station_name	站点名称	字符型（64）	非必填
7	duration_time	运维持续时长	整数型（4）	运维持续时间，秒数 非必填
8	net_int_use	网口使用	字符型（256）	多个数据，采用中文顿号分隔，非必填
9	rs_int_use	串口使用	字符型（256）	非必填
10	usb_int_use	USB 口使用	字符型（256）	非必填
11	video_int_use	视频接口使用	字符型（256）	非必填
12	warning_qty	告警数量	整数型（2）	必填，可为 0
13	illegal_warning	违规外联告警	整数型（2）	必填，可为 0
14	attack_warning	攻击告警	整数型（2）	必填，可为 0
15	virus_warning	恶意代码告警	整数型（2）	必填，可为 0
16	hr_cmd_warning	高风险指令告警	整数型（2）	必填，可为 0
17	key_bp_warning	USB Key 旁路告警	整数型（1）	必填，0：表示未旁路， 1：表示旁路
18	video_file_name	录屏文件	字符型（256）	非必填
19	net_pac_name	通信报文	字符型（256）	非必填
20	rs_pac_name	串口通信报文	字符型（256）	非必填
21	char_cmd_name	SSH、Telnet、RS232 字符指令	字符型（256）	非必填
22	trans_file_name	传输文件	字符型（256）	非必填
23	key_record	键盘记录	字符型（256）	非必填
24	source_addr	源地址	字符型（512）	多个地址用英文逗号分隔 非必填
25	description	运维总结描述	字符型（512）	本次运维工作的自动总结描述，不超过 340 个汉字 选填

A.7.4.3 文件传输日志

文件传输日志包含的字段信息如表 A.24 所示，第二列（字段）是发送到集中管控上所包含的字段。

表A.24 文件传输日志业务数据格式

业务请求码	0x2903			
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一ID，必填
2	version	数据格式版本	整数型（1）	当前固定为1，必填
3	log_time	日志产生时间	字符型（32）	例如:2018-07-13 12:34:56，必填
4	wo_no	工单编号	字符型（128）	非必填
5	file_name	文件名称	字符型（256）	必填，带上后缀名的名称
6	file_type	类型	字符型（32）	非必填
7	file_path	路径	字符型（256）	非必填
8	file_size	大小	整数型（8）	文件字节大小，纯数字，单位B，必填
9	operate_type	传输方式	整数型（1）	1：表示FTP方式 2：表示SFTP方式 3：表示SCP方式 4：表示外部存储介质方式 5：表示DL/T 634.5104方式 6：表示DL/T 860方式 必填
10	resource_addr	目的资源地址	字符型（16）	被运维对象IP，非必填
11	virus_qty	恶意代码数量	整数型（2）	必填，没有填0
12	exc_qty	添加信任数量	整数型（2）	必填，没有填0
13	operate_direct	数据方向	整数型（1）	1：表示上行（上传至被运维对象） 2：表示下行（从被运维对象下载） 必填
14	operate_duration	传输时长	整数型（4）	传输秒数，例如：60 非必填

A.7.4.4 设备插拔日志

设备插拔日志包含的字段信息如下表A.25所示，第二列（字段）是发送到集中管控上所包含的字段。

表A.25 设备插拔日志业务数据格式

业务请求码	0x2904			
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一ID，必填
2	version	数据格式版本	整数型（1）	当前固定为1，必填
3	log_time	日志产生时间	字符型（32）	例如:2018-07-13 12:34:56，必填
4	wo_no	工单编号	字符型（128）	非必填

5	resource_addr	目的资源地址	字符型（16）	被运维对象 IP，选填
6	source_addr	源地址	字符型（16）	网口运维有意义，选填
7	dev_type	设备类型	字符型（32）	如：KVM-USB 接口，非必填
8	ext_dev_type	外设类型	字符型（32）	如：USB OUT，非必填
9	status	插拔状态	整数型（1）	必填，1：接口插入， 2：接口拔出
10	description	描述信息	字符型（512）	如：装置在 2023-06-28 11:39:59，进行接口插入，接口类型：装置串口，外设类型：CONSOLE 调试口，非必填

A.7.4.5 运维任务信息

运维任务信息包含的字段信息如下表 A.26 所示，第二列（字段）是发送到集中管控上所包含的字段。

表A.26 运维任务信息业务数据格式

业务请求码		0x2906		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	wo_name	任务名称	字符型（128）	任务名称，必填，例如：快速运维 090501
4	wo_no	工单编号	字符型（128）	必填，由于各网关上自建工单的编号有可能重复，所以这里上传的自建的工单编号是网关唯一标识+下划线+工单的编号，如“3233_41”，针对这个工单上传的日志也应一样处理工单编号
5	admin_name	工作负责人全名	字符型（128）	必填，快速运维时传当前登录的账号
6	operator_name	工作班成员全名	字符型（512）	多人时，以逗号分隔，非必填
7	station_name	站点名称	字符型（64）	厂站的名称，最长 32 位，非必填
8	station_id	站点编号	字符型（64）	厂站的 ID，非必填
9	begin_time	任务开始时间	字符型（32）	例如:2023-07-13 12:34:56，必填
10	end_time	任务结束时间	字符型（32）	例如:2023-07-16 12:34:56，必填
11	telephone	联系方式	字符型（32）	工作负责人手机号，非必填
12	device_info	运维对象信息	Json 数组	参考表 A.27，非必填
13	task_type	任务类型	整数型（1）	0：计划工单（例如：OMS 系统同步的工单）；1：临时工单（例如：集中管控自建工单；2：快速工单（例如：运维网关自建工单）；3：通用工单（例如：调查问卷运维方式）；必填。运维网关上传的均为 2（快速工单）
14	task_status	任务状态	整数型（1）	1：未启动 （默认未启动）；2：

				运行中；3：已停止；4：已结束。必填
15	task_content	工作内容	字符型（1024）	非必填
16	effect_scope	影响范围	字符型（1024）	非必填
17	safety_measure	安全措施	字符型（1024）	非必填
18	desc	其他描述信息	字符型（512）	非必填

运维对象信息字段包含调控标识、运维对象名称、运维对象地址，运维对象信息字段见表A.27所示。

表A.27 运维对象信息字段

序号	字段	字段名称	字段类型	描述及要求
1	device_id	调控标识	字符型（32）	非必填，运维对象在 OMS/调控云中的唯一 ID，便于反向完善运维对象信息 非必填
2	device_name	运维对象名称	字符型（64）	运维设备名称，最长 32，非必填
3	device_ip	运维对象地址	字符型（32）	运维设备对象地址，非必填

A.7.4.6 日志统计信息

日志统计信息包含的字段信息如表 A.28 所示，第二列（字段）是发送到集中管控上所包含的字段。

表A.28 日志统计信息业务数据格式

业务请求码	0x2907			
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	log_time	日志产生时间	字符型（32）	例 如 :2018-07-13 12:34:56，必填
4	wo_no	工单编号	字符型(128)	必填
5	task_status	运维任务状态	字符型（32）	1：未启动（默认未启动） 2：运行中 3：已停止 4：已结束 必填，产生该日志时均为 4-已结束
6	start_time	实际运维开始时间	字符型（32）	该工单的实际运维开始时间，必填
7	end_time	实际运维结束时间	字符型（32）	该工单的实际运维结束时间，必填

8	wo_log_num	运维日志总数量	整数型（2）	必填，可为 0
9	wo_warn_num	告警日志总数量	整数型（2）	必填，可为 0
10	wo_file_num	运维文件总数量	整数型（2）	必填，可为 0
11	operation_log_num	操作日志数量	整数型（2）	必填，可为 0
12	file_trans_num	文件传输日志数量	整数型（2）	必填，可为 0
13	dev_action_num	设备插拔日志数量	整数型（2）	必填，可为 0
14	hr_cmd_warn_num	高风险指令告警数量	整数型（2）	必填，可为 0
15	illegal_warn_num	违规外联告警数量	整数型（2）	必填，可为 0
16	attack_warn_num	攻击告警数量	整数型（2）	必填，可为 0
17	virus_warn_num	恶意代码告警数量	整数型（2）	必填，可为 0
18	hr_port_warn_num	高危端口通信告警数量	整数型（2）	必填，可为 0
19	auth_num	二次授权记录数量	整数型（2）	必填，可为 0
20	video_file_num	录屏文件数量	整数型（2）	必填，可为 0
21	net_pac_num	通信报文文件数量	整数型（2）	必填，可为 0
22	char_cmd_num	指令记录文件数量	整数型（2）	必填，可为 0
23	key_record_num	键盘记录文件数量	整数型（2）	必填，可为 0

A.7.5 告警日志

告警日志主要包括高风险指令告警、违规外联告警、攻击告警、恶意代码告警、高危端口通信告警、二次授权记录等。鉴于各类告警日志存在的共性字段，已对该部分字段进行抽取，详见 A.7.5.1 告警日志公共字段，从 A.7.5.2 开始是各告警日志的补充字段。运维网关记录及上报数据时，应同时包含公共字段与补充字段。

A.7.5.1 告警日志公共字段

告警日志公共字段格式见表 A.29，第二列（字段）是发送到集中管控上所包含的字段。

表A.29 告警日志公共字段格式

序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	log_time	日志产生时间	字符型（32）	例如:2018-07-13 12:34:56，必填
4	wo_no	工单编号	字符型(128)	必填
5	resource_addr	目的资源地址	字符型（16）	被运维对象 IP，非必填
6	resource_port	目的资源端口	整数型（4）	非必填
7	executor_name	指令操作人名称	字符型（32）	非必填
8	source_addr	源地址	字符型（16）	网口运维有意义，非必填
9	description	描述信息	字符型(256)	描述信息，补充信息可放此处非必填

A.7.5.2 高风险指令告警

高风险指令告警（含操作类指令和控制类指令）的补充字段格式见表 A.30，第二列（字

段）是发送到集中管控上所包含的字段。

表A.30 高风险指令告警补充字段格式

业务请求码		0x3001		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
10	action_id	记录动作	整数型（1）	1：申请被批准 2：申请被拒绝 3：申请超时（指令阻断） 非必填
11	operate_content	执行的高风险指令	字符型（128）	记录执行的高风险指令，必填
12	cmd_type	指令类型	整数型（1）	1：操作指令 2：控制指令 必填
13	protocol_type	协议类型	字符型（32）	包括：串行协议(rs232、DL/T 634.5101、DL/T 634.5103、Modbus_Rtu)、网口协议(tcp、udp、vnc、telnet、rdp、ssh、xdmcp、ftp、DL/T 634.5104、DL/T 860、Modbus、Q/GDW 273)区分大小写 必填

A.7.5.3 违规外联告警

违规外联告警的补充字段格式见表A.31，第二列（字段）是发送到集中管控上所包含的字段。

表A.31 违规外联告警补充字段格式

业务请求码		0x3002		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
10	ex_device_os	运维终端系统类型	字符型（32）	记录操作系统类型名，非必填
11	ex_device_mac	运维终端Mac地址	字符型（32）	E4-54-E8-DB-7E-9A，非必填
12	ex_host_name	运维终端主机名称	字符型（32）	记录主机名，非必填
13	ex_info	外联标识（描述）	字符型（32）	例如外联的WIFI名称，TP-LINK_BDC，非必填

A.7.5.4 攻击告警

攻击告警的补充字段格式见表A.32，第二列（字段）是发送到集中管控上所包含的字段。

表A.32 攻击告警补充字段格式

业务请求码		0x3003		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
10	attack_type	攻击类型	整数型（1）	1：ARP 攻击 2：DoS 攻击 3：IP 扫描 4：通信端口扫描

				必填
11	operate_content	攻击内容	字符型(128)	非必填
12	source_mac	源 Mac 地址	字符型（32）	E4-54-E8-DB-7E-9A 非必填
13	source_port	源端口	整数型（4）	59046，非必填
14	attack_detail	攻击详情	整数型（1）	1：Syn flood 防御 2：Udp flood 防御 3：ICMP flood 防御 4：DNS flood 防御 5：HTTP flood 防御 6：ICMP 超长包防御 7：NTP flood 防御 8：端口扫描防御 9：ARP 攻击防御 10：WinNuke 防御 11：Smurf 防御 12：Land 防御 13：Teardrop 防御 14：IP 扫描防御 必填

A.7.5.5 恶意代码告警

恶意代码告警的补充字段格式见表 A.33，第二列（字段）是发送到集中管控上所包含的字段。

表A.33 恶意代码告警补充字段格式

业务请求码		0x3004		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
10	file_name	文件名称	字符型（256）	必填，带上后缀名的名称
11	file_type	文件类型	字符型（32）	非必填
12	file_path	文件路径	字符型（256）	非必填
13	file_size	大小	整数型（8）	文件字节大小，纯数字，单位 B 必填
14	operate_type	传输方式	整数型（1）	1：表示 FTP 方式 2：表示 SFTP 方式 3：表示 SCP 方式 4：表示外部存储介质方式 5：表示 DL/T 634.5104 方式 6：表示 DL/T 860 方式 必填
15	virus_type	恶意代码类型	字符型（64）	非必填
16	action_id	记录动作	整数型（1）	1：信任后拷贝 2：删除后拷贝 3：取消拷贝 必填

A.7.5.6 高危端口通信告警

高危端口通信告警的补充字段格式见表 A.34，第二列（字段）是发送到集中管控上所包含的字段。

表A.34 高危端口通信告警补充字段格式

业务请求码		0x3006		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
10	operate_content	执行的高危端口	字符型（128）	执行的高危端口，必填
11	action_id	记录动作	整数型（1）	0：放行（记录） 1：申请被批准 2：申请被拒绝 3：申请超时（阻断），必填

A.7.5.7 二次授权记录

二次授权记录的补充字段格式见表 A.35，第二列（字段）是发送到集中管控上所包含的字段。

若不同类型二次授权记录有额外的补充字段信息，可统一放到公共字段的描述信息（description）里。

表A.35 二次授权记录补充字段格式

业务请求码		0x3005		
请求报文字段列表				
序号	字段	字段名称	字段类型	描述及要求
10	auth_status	授权状态	整数型（1）	1：授权通过 2：授权被拒绝 3：授权超时自动拒绝 4：其他。必填
11	auth_content	授权内容	字符型（128）	填被授权的高风险操作指令、控制指令的标识码、高危端口、文件名称等，非必填
12	auth_type	二次授权类型	整数型（1）	1：高风险操作指令二次授权 2：控制指令二次授权 3：高危端口通信二次授权 4：渗透测试场景二次授权 5：疑似恶意代码文件解除隔离二次授权 6：文件拷出二次授权 7：USB Key 旁路模式二次授权 必填
13	protocol_type	协议类型	字符型（32）	包括：串行协议(rs232、DL/T 634.5101、DL/T 634.5103、Modbus_Rtu)、网口协议(tcp、udp、vnc、telnet、rdp、ssh、xdmcp、ftp、DL/T 634.5104、DL/T 860、Modbus、Q/GDW 273) 区分大小写。非必填

A.7.6 运维文件

运维文件应包括录屏文件、通信报文、指令记录、键盘记录等运维过程中产生的文件。运维文件的上传应参考 A.5.3 文件传输说明，文件描述包的文件类型应设置对应的文件类型：1-录屏文件，2-通信报文，3-指令记录，4-键盘记录。上传时还需补充描述当前运维文件的记录开始时间及记录停止时间，通过文件描述包中的 biz_info 字段上传，biz_info 的字段说明详见表 A.36。

表A.36 运维文件上传biz_info字段说明

序号	字段	字段名称	字段类型	描述及要求
1	start_time	开始时间	字符型（32）	文件内容的开始时间，非必填
2	end_time	结束时间	字符型（32）	文件内容的结束时间，非必填

A.8 数据下发请求接口说明

A.8.1 概述

数据下发主要包括规则库下发、运维工单下发等。规则库和运维工单等业务数据下发，既可由集中管控主动下发，也可由运维网关主动获取，具体调用逻辑如下：

集中管控主动下发接口调用逻辑说明：

a) 支持业务数据（规则库、运维工单等）有新增或变更时，直接下发给范围内的在线运维网关；

b) 支持从集中管控手动点击下发按钮，直接下发给范围内的在线运维网关。

c) 运维网关主动获取接口调用说明：

d) 通过版本上报接口判断规则库有变化时，应调用规则库获取接口获取最新规则数据，版本信息上报接口可定期调用，推荐调用时间间隔 1 个小时；

e) 成功连接集中管控后，直接调用一次运维工单获取接口，应定期调用运维工单获取接口获取运维工单数据，推荐调用时间间隔 1 个小时。

注：数据下发和数据获取动作注意控制不能同时进行，以免产生逻辑混乱，集中管控和运维网关程序注意做好策略控制。

A.8.2 规则库下发

同一类规则可以新建不同的规则库，例如发电厂和变电站的运维网关可以对应不同的规则库，规则库发生变更时需记录一个规则库版本号，例如对高危端口变电站规则库进行新增、删除、修改等操作后，可以点击发布生成新的规则版本号，版本号推荐使用毫秒时间戳表示。

A.8.2.1 集中管控主动下发

集中管控在规则库下发请求见表 A.37。

表A.37 规则库下发业务数据格式

业务请求码	高危端口规则-0x5101，操作类指令规则-0x5102，控制类指令规则-0x5103			
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	rule_base_id	规则库 ID	整数型（4）	当前下发的规则库的唯一标识，集中管控会以规则库的形式来维护一批规则，不同的运维网关可能会对

				应不同的规则库，必填
4	rule_base_version	规则版本	整数型（8）	当前下发的版本，可以是毫秒时间戳，版本有更新需重新下发，必填
5	data	规则列表	Json 数组	规则数据列表，具体字段见 A.8.2.3， 列表为空代表需要清空运维网关本地规则、网关侧使用默认规则，必填，可以为空数组。
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册返回的网关唯一 ID，必填

A.8.2.2 运维网关主动获取

运维网关与集中管控成功建立连接后，应定期从集中管控获取最新版规则库，具体接口字段说明见表 A.38。

表A.38 规则库获取业务数据格式

业务请求码		高危端口规则-0x5151，操作类指令规则-0x5152，控制类指令规则-0x5153		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	rule_base_id	规则库 ID	整数型（4）	运维网关现有规则库的唯一标识，非必填
4	rule_base_version	规则版本	整数型（8）	运维网关现有规则库的版本，非必填
5	request_type	规则请求类型	整数型（1）	0：获取更新，集中管控侧有数据变更才返回数据，否则返回无更新 1：强制获取，集中管控侧有数据变更返回最新数据，数据无变更则返回当前规则库版本的数据 非必填，不填代表 0-获取更新
返回码		1-成功，有更新，2-成功-无更新，3-成功-清空数据，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
3	version	数据格式版本	整数型（1）	当前固定为 1，必填
4	rule_base_id	规则库 ID	整数型（4）	当前返回的规则库的唯一标识，集中管控会以规则库的形式来维护一批规则，不同的运维网关可能会对应不同的规则库，必填
5	rule_base_version	规则版本	整数型（8）	当前返回的规则库的版本，可以是毫秒时间戳，版本有更新需重新下发，必填
6	data	规则列表	Json 数组	规则数据列表，具体字段见 A.8.2.3 规则字段说明，列表为空代表需要清空运维网关本地规则、网关侧使用默认规则，必填，可以为空数组。

A.8.2.3 规则字段说明

高危端口规则的字段说明见表 A.39。

表A.39 高危端口规则字段说明

序号	字段	字段名称	字段类型	描述及要求
1	id	规则编号	字符型（32）	1，集中管控中规则唯一标识，必填
2	port	端口	整数型（4）	例如：8080，必填
3	port_des	端口描述	字符型(256)	例如：Tomcat 服务器常用端口，非必填
4	strategy	执行策略	整数型（1）	1：申请确认；2：阻断；3：放行（只记录）；必填
5	protocol	协议名称	字符型（32）	例如：tcp，具体协议名称（大小写、空格）按照表 A.42 协议进行定义，非必填。若不传，则代表对 tcp、udp 协议均生效。
6	description	规则描述	字符型(256)	例如：Tomcat 服务端口申请确认，非必填
7	status	启用状态	整数型（1）	0：禁用；1：启用；非必填，不填代表启用

操作类指令规则的字段说明见表 A.40。

表A.40 操作类指令规则字段说明

序号	字段	字段名称	字段类型	描述及要求
1	id	规则编号	字符型（32）	例如：1，集中管控中规则唯一标识，必填
2	cmd	命令	字符型（32）	例如：rm -rf，必填
3	cmd_des	命令描述	字符型（128）	例如：杀死 12345 进程，非必填
4	strategy	执行策略	整数型（1）	1：申请确认；2：指令阻断；3：会话阻断；4：告警执行； 必填
5	is_regular	是否正则形式	整数型（1）	0：否 1：是 必填
6	description	规则描述	字符型（256）	非必填
7	status	规则启用状态	整数型（1）	0：禁用 1：启用 非必填 不填代表启用
8	protocol	协议名称	字符型（32）	例如：ssh，具体协议名称（大小写、空格）严格按照表 A.42 协议对照说明 进行定义，非必填。 若不传,则代表对 ssh、telnet、rs232 三种协议均生效

控制类指令规则的字段说明见表 A.41。

表A.41 控制类指令规则字段说明

序号	字段	字段名称	字段类型	描述及要求
1	id	规则编号	字符型（32）	1，集中管控中规则唯一标识，必填
2	protocol	协议名称	字符型（32）	例如：DL/T 634.5104，具体协议名称（大小写、空格）严格按照表 A.42 协议对照说明 进行定义 必填
3	cmd_code	命令标识码	字符型（32）	58（根据不同协议，标识码不同），必填

4	cmd_code_des	标识码描述	字符型（128）	带时标 CP56Time2a 的单命令（遥控） 非必填
5	cmd_function	指令功能说明	字符型（128）	带时标单点遥控，非必填
6	strategy	执行策略	整数型（1）	1：申请确认 2：指令阻断 3：会话阻断 4：告警执行 必填
7	description	规则描述	字符型（256）	非必填
8	status	规则启用状态	整数型（1）	0：禁用 1：启用 非必填 不填代表启用

协议定义的字段对照说明见表 A.42。

表A.42 协议对照说明

序号	协议名称
1	tcp
2	udp
3	vnc
4	telnet
5	rdp
6	ssh
7	xdmcp
8	ftp
9	DL/T 634.5104
10	DL/T 860
11	Modbus
12	Q/GDW 273
13	DL/T 634.5101
14	DL/T 634.5103
15	rs232

A.8.3 运维工单下发

运维工单下发时，非“已结束”状态的工单均需下发，下发范围为运维工单对应的站点的运维单位下所有的运维网关。实际运维时需由工作负责人来执行自己负责的工单。

A.8.3.1 工单数据格式

运维工单的字段对照说明见表A.43。

表A.43 运维工单字段说明

序号	字段	字段名称	字段类型	描述及要求
1	wo_name	任务名称	字符型（128）	任务名称，必填，例如：运维工单090501
2	wo_no	工单编号	字符型（128）	必填
3	admin_name	工作负责人全名	字符型（128）	必填

4	operator_name	工作班成员全名	字符型（512）	多人时，以逗号分隔，非必填
5	station_name	站点名称	字符型（64）	厂站的名称，最长 32 位，非必填
6	station_id	站点编号	字符型（64）	厂站的 ID，非必填
7	begin_time	任务开始时间	字符型（32）	例如:2023-07-13 12:34:56，必填
8	end_time	任务结束时间	字符型（32）	例如:2023-07-16 12:34:56，必填
9	telephone	联系方式	字符型（32）	工作负责人手机号，非必填
10	device_info	运维对象信息	Json 数组	参考表 A.44，非必填
11	task_type	任务类型	整数型（1）	0：计划工单（例如：OMS 系统同步的工单） 1：临时工单（例如：集中管控自建工单） 2：快速工单（例如：运维网关自建工单） 3：通用工单（例如：调查问卷运维方式） 必填，运维网关上传的均为 2-快速工单
12	task_status	任务状态	整数型（1）	1：未启动 （默认未启动）；2：运行中；3：已停止；4：已结束 必填
13	task_content	工作内容	字符型（1024）	非必填
14	effect_scope	影响范围	字符型（1024）	非必填
15	safety_measure	安全措施	字符型（1024）	非必填
16	desc	其他描述信息	字符型（512）	非必填
17	upload_regular_file	是否需上报信息	整数型(1)	针对通用工单可能需要运维网关上报一些信息到集中管控，用这个字段判定，非必填 1：无需上传；2：需要上传

运维对象的字段说明见表A.44。

表A.44 运维对象字段说明

序号	字段	字段名称	字段类型	描述及要求
1	device_id	调控标识	字符型（32）	运维对象在 OMS/调控云中的唯一 ID，便于反向完善运维对象信息 非必填
2	device_name	运维对象名称	字符型（64）	运维设备名称，最长 32，非必填
3	device_ip	运维对象地址	字符型（32）	运维设备对象地址，非必填

A.8.3.2 集中管控主动下发

集中管控的运维工单下发请求见表 A.45。

表A.45 运维工单下发业务数据格式

业务请求码		0x5204		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	data	运维工单列表	Json 数组	运维工单数据列表，具体字段见 A.43 运维工单字段说明，必填
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填

A.8.3.3 运维网关主动获取

运维网关与集中管控成功建立连接后，应定期从集中管控获取运维工单，具体接口字段说明见表 A.46。

表A.46 运维工单获取业务数据格式

业务请求码		0x5205		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
3	data	工单详情列表	Json 数组	运维工单数据列表，具体字段见 A.43 运维工单字段说明，非必填，为空代表没有运维工单

A.8.3.4 资产信息确认（扩展功能）

运维网关资产信息确认接口字段说明见表 A.47。

表A.47 资产信息确认业务数据格式

业务请求码		0x5221		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	data	已确认的资产数据	Json 数组	数据格式见表 A.44，已经确认好的资产信息，一个资产的 IP 一般仅为一个值，必填

返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填

A.9 网关升级请求接口说明

A.9.1 概述

网关升级主要包含恶意代码特征库升级和网关固件升级等。

A.9.2 恶意代码特征库升级

集中管控支持对恶意代码特征库进行统一维护及管理，并将新的特征库版本返回给运维网关。恶意代码特征库的升级动作应由运维网关发起，主要流程如下：

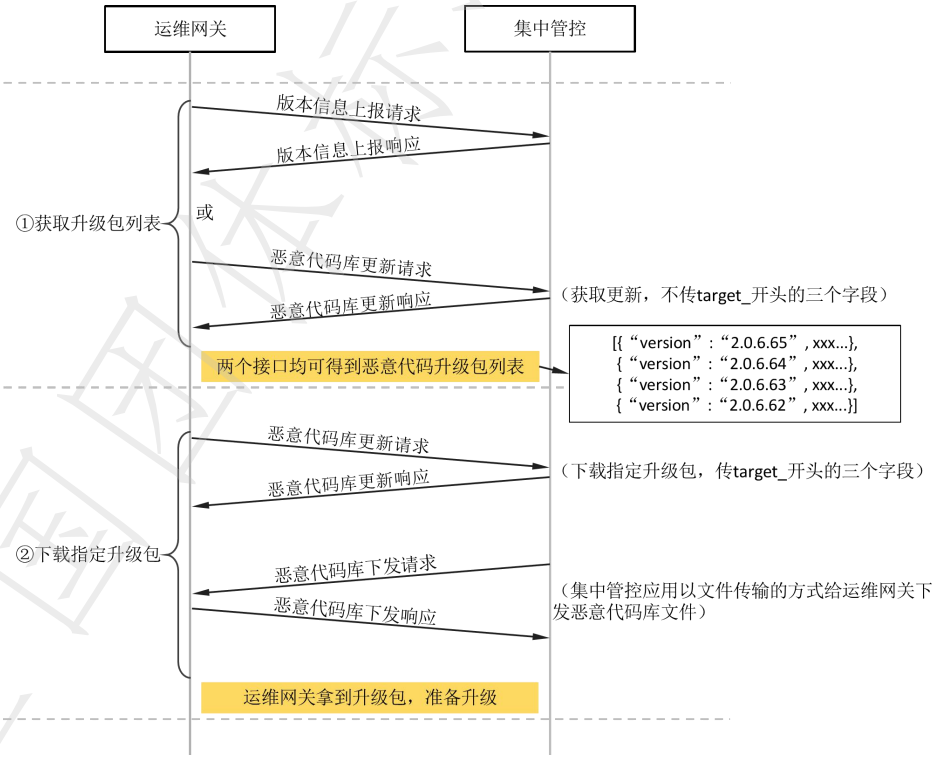
a） A.6.3 版本上报接口，会返回升级到最新版本恶意代码库所需要的升级包列表信息；

b） A.9.2.1 恶意代码库更新请求，获取更新，得到返回数据中的 depends 信息，代表升级到最新版本恶意代码库所需要的升级包列表信息；

c） 调用 A.9.2.1 恶意代码库更新请求，最终下载到指定升级包。

注：a）和 b）两种接口的使用目的一致，均是为了得到升级到最新恶意代码特征库需要的版本列表。

恶意代码升级流程示意图见图 A.2。



图A.2 恶意代码升级流程示意图

A.9.2.1 恶意代码库更新请求

恶意代码库更新请求有两种调用方式：

a) 获取更新：请求报文不传 target_virus_version、target_file_code、target_hash_code 三个字段，代表检查是否有版本更新，集中管控收到请求后会将待更新的包列表放在返回报文的 depends 字段；

b) 获取指定升级包：请求报文传 target_virus_version，target_file_code、target_hash_code 三个字段，代表获取指定的升级包，集中管控收到请求后会调用恶意代码库下发接口以文件传输的方式下发对应的升级包。

恶意代码库更新请求业务数据格式见表 A.48。

表A.48 恶意代码库更新请求业务数据格式

业务请求码		0x6111		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
2	version	数据格式版本	整数型（1）	当前固定为 1，必填
3	virus_vendor	网关使用的恶意代码引擎厂商	字符型（64）	厂商名称名称，最长 50 位，必填 可选值:[瑞星;江民;绿盟;政采]
4	virus_version	网关当前的恶意代码库版本号	字符型（64）	最长 64 位 必填
5	virus_valid_date	网关当前的恶意代码库许可证有效期	字符型（32）	例如:2024-07-13 12:34:56，必填
6	target_virus_version	获取的目标版本	字符型（64）	获取更新时不传该字段，获取指定升级包时传该字段。
7	target_file_code	获取的目标版本的文件标识	整数型（8）	指定升级包的唯一标识 非必填
8	target_hash_code	获取的目标版本的文件哈希	字符型（64）	当目标版本号无法唯一标记一个升级包时，用该字段进行辅助判断，非必填
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息，选填
2	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID，必填
3	virus_vendor	恶意代码库厂商	字符型（64）	与网关所提交的一致，选填
4	virus_version	集中管控端维护的恶意代码库最新版本号	字符型（64）	选填
5	depends	升级最新版本需要的升级包信息	JSON 数组	具体格式见表 A.49。 恶意代码特征库升级到最新版本需要的版本列表信息，通常是最新一次全量程序包以及该版本之后的增量包，非必填。

版本信息数据格式见表 A.49。

表A.49 版本信息数据格式

序号	字段	字段名称	字段类型	描述及要求
1	version	版本号	字符型（64）	升级包的版本号，必填
2	file_code	文件标识	整数型（8）	文件的唯一标识，必填
3	hash_code	文件哈希	字符型（64）	SM3 算法计算的哈希值，16 进制字符串，必填
4	update_type	升级包类型	整数型（1）	升级包类型，非必填： 1：全量升级包 2：增量升级包
5	start_version	增量起点版本	字符型（256）	该升级包的升级起点版本，非必填，多个值用英文逗号分隔
6	publish_time	发布时间	整数型（1）	升级包的发布时间，以厂家发布的时间为准，主要用作升级参考及排序参考，必填
7	file_size	文件大小	整数型（8）	文件字节大小，纯数字，单位 B，非必填
8	version_des	版本描述	字符型（512）	版本描述信息，非必填

A.9.2.2 恶意代码库下发请求

集中管控调用恶意代码库下发接口下发特征库文件时，应补充描述下发的恶意代码特征库厂商和版本号，通过文件描述包中的 biz_info 信息传送，biz_info 的字段说明见表 A.50。

表A.50 恶意代码特征库下发biz_info字段说明

序号	字段	字段名称	字段类型	描述及要求
1	virus_vendor	恶意代码引擎厂商	字符型（64）	下发的恶意代码厂商名称，必填 可选值：[瑞星;江民;绿盟;政采]
2	virus_version	恶意代码库版本号	字符型（64）	下发的恶意代码特征库版本号，必填
3	update_type	升级包类型	整数型（1）	升级包类型，非必填： 1：全量升级包 2：增量升级包
4	start_version	增量起点版本	字符型（256）	该升级包的升级起点版本，非必填，多个值用英文逗号分隔

A.9.3 网关固件升级

集中管控支持对网关固件升级包进行统一维护及管理，并将新的网关固件版本返回给运维网关。出于安全及谨慎等方面的考虑，网关固件的升级动作应由运维网关发起，主要流程如下：

a） A.6.3 版本上报接口，会返回升级到最新版本网关固件所需要的升级包列表信息；

b） A.9.3.2 网关固件更新请求，获取更新，得到返回数据中的 depends 信息，代表升级到最新版本网关固件所需要的升级包列表信息；

c） 调用 A.9.3.3 网关固件更新请求，最终下载到指定升级包。

注：a）和 b）两种接口的使用目的一致，均是为了得到升级到最新网关固件需要的版本列表。

A.9.3.1 网关固件管理

各厂商提的固件升级包需按照指定的格式，外层是一个 zip 包，zip 包里面包含两个文件，版本描述文件 version.json 和固件升级文件压缩包（格式由厂商自定义），平台下发

文件为整个 zip 包文件,网关自行解压

版本描述文件 version.json 应包含字段见表 A.51。

表A.51 版本描述文件信息

序号	字段	字段名称	字段类型	是否必填	说明
1	software_vendor	网关软件厂商	整数型（1）	必填	常量整数 对应序号如下： 1：北京国泰网信科技有限公司 2：北京科东电力控制系统有限责任公司 3：北京珞安科技有限责任公司 4：湖南匡安网络技术有限公司 5：积成电子股份有限公司 6：南京南瑞信息通信科技有限公司 7：许继电气股份有限公司 8：浙江齐安信息科技有限公司 9：浙江齐治科技股份有限公司 10：珠海市鸿瑞信息技术股份有限公司 11：其它
2	software_version	软件版本号	字符型（64）	必填	
3	software_file_name	升级包名称	字符型（256）	非必填	软件升级包名称
4	publish_time	发布时间	字符型（64）	必填	2024-12-30 12:30:30
5	hash_code	文件哈希值	字符型（64）	必填	SM3 算法计算的 压缩包内升级文件的 hash 值
6	update_type	升级包类型	整数型（1）	非必填	升级包类型： 1：全量升级包 2：增量升级包
7	start_version	增量起点版本	字符型（256）	非必填	该升级包的升级起点版本，多个值用英文逗号分隔
8	description	描述	字符型（256）	非必填	文件描述

A.9.3.2 网关固件更新请求

网关固件更新请求有两种调用方式：

a) 获取更新：请求报文不传 target_software_version、target_file_code、target_hash_code 三个字段，代表检查是否有版本更新，集中管控收到请求后会

将待更新的包列表放在返回报文的 depends 字段；

b) 获取指定升级包：请求报文传 target_virus_version，target_file_code、target_hash_code 三个字段，代表获取指定的升级包，集中管控收到请求后会调用网关固件下发接口以文件传输的方式下发对应的升级包。

网关固件更新请求业务数据格式见表 A.52。

表A.52 网关固件更新请求业务数据格式

业务请求码		0x6112		
请求对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	dev_id	网关唯一标识	字符型（64）	网关注册后返回的网关唯一 ID 必填
2	version	数据格式版本	整数型（1）	当前固定为 1 必填
3	software_version	网关端软件版本号	字符型（64）	最长 64 位，（是网关当前的版本号） 必填
4	software_valid_date	网关端软件许可证有效期	字符型（32）	例如:2024-07-13 12:34:56 非必填
5	target_software_version	获取的目标版本	字符型（64）	获取更新时不传该字段； 获取指定升级包时传该字段。
6	target_file_code	获取的目标版本的文件标识	整数型（8）	指定升级包的唯一标识 非必填
7	target_hash_code	获取的目标版本的文件哈希	字符型（64）	当目标版本号无法唯一标记一个升级包时，用该字段进行辅助判断 非必填
返回码		0-成功，其他见表 A.12 业务返回码对照表		
返回对象字段列表				
序号	字段	字段名称	字段类型	描述及要求
1	message	消息	字符型（256）	提示消息 选填
2	dev_id	网关唯集中管控一标识	字符型（64）	网关注册后返回的网关唯一 ID 必填
3	software_version	端维护的软件版本号	字符型（64）	选填
4	depends	升级最新版本需要的其他依赖版本	Json 数组	具体格式见表 A.49。 网关固件升级到最新版本需要的版本列表信息，通常是最新一次全量程序包以及该版本之后的增量包 非必填

A.9.3.3 网关固件下发请求

集中管控调用网关固件下发接口下发网关固件升级包时，需要补充描述下发的网关固件厂商和版本号等信息，通过文件描述包中的 biz_info 信息传送，biz_info 的字段说明见表 A.53。

表A.53 网关固件下发biz_info字段说明

序号	字段	字段名称	字段类型	描述及要求
1	software_vendor	网关软件厂商	整数型（1）	常量整数，传输公司对应的序号即可 1：北京国泰网信科技有限公司 2：北京科东电力控制系统有限责任公司 3：北京珞安科技有限责任公司 4：湖南匡安网络技术有限公司 5：积成电子股份有限公司 6：南京南瑞信息通信科技有限公司 7：许继电气股份有限公司 8：浙江齐安信息科技有限公司 9：浙江齐治科技股份有限公司 10：珠海市鸿瑞信息技术股份有限公司 11：其它 必填
2	software_version	网关软件版本号	字符型（64）	下发的网关软件版本号，必填
3	update_type	升级包类型	整数型（1）	升级包类型，非必填 1：全量升级包 2：增量升级包
4	start_version	增量起点版本	字符型（256）	该升级包的升级起点版本，非必填，多个值用英文逗号分隔

全国团体标准信息平台

附 录 B
（资料性）
运维网关与集中管控级联通信代码示例

B.1 概述

本附录为运维网关和集中管控之间的级联通信部分代码和固件压缩包样式示例。

B.2 代码示例

运维网关和集中管控之间的级联通信文件描述包和注册认证代码示例见表 B.1。

表B.1 文件描述包数据代码示例

对应通讯环节	代码示例

文件描述包	{
	"dev_id": "24533",
	"version": 1,
	"wo_no": "nx202011061",
	"log_file_type": 1,
	"biz_info": {
	"start_time": "2020-05-07 14:11:37",
	"end_time": "2020-05-07 15:02:12"
	}
	"file_name": "1717082466678.mp4",
	"file_type": "mp4",
	"file_path": "/home/data/",
	"file_size": 110730905,
	"create_time": "2020-05-07 22:11:37",
	"update_time": "2020-05-07 22:11:37",
	"file_code": "1234567",
	"slice_count": 121,
	"slice_no": 1,
	"slice_size": 50,
	"hash_code":
	"4bd9de6be70eadf1599e0a96bc99f8a3dd7d4fde8d31ffac723c54f23cb230ae"
	}

注册认证申请	{
	"client_pem": "vvvvvvvv",
	"client_sign": "xxxxxx",
	"version": 1,
	"manufacturer": 1,
	"serial": "FSDHAJFKKD",
	"ip": "192.168.2.132",
	"mac": "02:42:62:78:5b:c5",
	"dev_id": null,
	"model": "KA-POM",
	"dev_name": "测试网关",
	"dock_mac": "02:42:46:55:36:66"
	}

注册认证成功返回	{
	"server_pem": "yyyyyy",
	"server_sign": "uuuuuu",
	"dev_id": "KA_FSDHAJFKKD",
	"message": "成功"
	}

运维网关和集中管控之间的级联通信发送心跳数据和版本上报及返回代码示例见表B.2。

表B.2 发送心跳数据和版本上报及返回代码示例

对应通讯环节	代码示例

运维网关发送心跳数据	{
	"dev_id": "24533",
	"version": 1,
	"battery_percent": 80.3,
	"cpu_usage": 16.8,
	"memory_size": 33740730368,
	"memory_usage": 24.3,
	"disk_size": 337407303680,
	"disk_usage": 60.3
	}

版本上报	{
	"dev_id": "24533",
	"version": 1,
	"software_version": "1.2.0",
	"software_valid_date": "2024-07-13 12:34:56",
	"virus_vendor": "瑞星",
	"virus_version": "2.0.3.64",
	"virus_valid_date": "2024-07-13 12:34:56",
	"os_type": "KylinSec",
	"os_version": "4.8.123.11",
	"os_valid_date": "2024-07-13 12:34:56",
	"port_base_id": 1,
	"port_base_version": 1734406392012,
	"operate_base_id": 2,
	"operate_base_version": 1734406392012,
	"control_base_id": 3,
	"control_base_version": 1734406392012
	}

版本上报返回	{
	"message": "成功",
	"dev_id": "24533",
	"software_version": "1.2.1",
	"software_version_list": [{
	"version": "1.0.1","hash_code":
	"D0D2A990A9AEB988FBC77A3741563841A7F0ECD8E57BF088AAC8099BD38AB4BA",
	"update_type": 2,"start_version": "1.0.0, 0.9.0",
	"publish_time": "2024-12-29 15:12:08"
	}],
	"virus_vendor": "瑞星",
	"virus_version": "2.0.3.65",
	"virus_version_list": [{
	"version": "2.0.6.65","hash_code":
	"42C239A76EBE463845EA74B981329A0D4F01961A70FAC4799E81E9C5885C97FA",
	"update_type": 1,"start_version": "",
	"publish_time": "2024-08-10 12:23:37"
	}],
	"port_base_id": 1,
	"port_base_version": 1734406392012,
	"operate_base_id": 2,
	"operate_base_version": 1734406392012,
	"control_base_id": 3,
	"control_base_version": 1734406392012
	}

运维网关和集中管控之间的级联通信基础配置下发和认证登录日志及日志操作代码示例见表 B.3。

表B.3 基础配置下发和认证登录日志及日志操作代码示例

对应通讯环节	代码示例

基础配置下发	{
	"dev_id": "24533",
	"version": 1,
	"config": null,
	"org_info": {
	"org_id": "12323",
	"org_name": "xx 班组",
	"org_type": "班组"
	},
	"station_list": [{
	"station_id": "13232",
	"station_name": "xx 电厂",
	"voltage_level": "35kv",
	"station_type": "发电厂"
	}],
	"user_list": null
	}

认证登录日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:27",
	"login_action": 0,
	"user_name": "sysadmin",
	"login_type": 1
	}

操作日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:37",
	"wo_no": "nx202011061",
	"resource_info": [{"ip": "192.168.1.111","ports": "22,33,3306"}],
	"station_name": "x 厂站",
	"duration_time": "600",
	"net_int_use": "eth1、eth2",
	"rs_int_use": "",
	"usb_int_use": "",
	"video_int_use": "HDMI1",
	"warning_qty": 4,
	"illegal_warning": 0,
	"attack_warning": 2,
	"virus_warning": 1,
	"hr_cmd_warning": 2,
	"key_bp_warning": 0,
	"video_file_name": "2021061101.mp4",
	"net_pac_name": "2021061101.pcap",
	"rs_pac_name": "",
	"char_cmd_name": "c_c_2021061101.txt",
	"trans_file_name": "test.doc",
	"key_record": "k_2021061101.txt",
	"source_addr": "192.168.100.30",
	"description": "运维顺利完成,无较大异常"
	}

运维网关和集中管控之间的级联通信文件传输日志和设备插拔日志及运维对象字段代码示例见表 B.4。

表B.4 文件传输日志和设备插拔日志及运维对象字段代码示例

对应通讯环节	代码示例

文件传输日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:37",
	"wo_no": "nx202011061",
	"file_name": "测试.txt",
	"file_type": "txt",
	"file_path": "C:\",
	"file_size": "110730905",
	"operate_type": 1,
	"resource_addr": "172.16.69.210",
	"virus_qty": 4,
	"exc_qty": 2,
	"operation_direct": 1,
	"operate_duration": 60
	}

设备插拔日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:37",
	"wo_no": "nx202011061",
	"resource_addr": "172.16.69.210",
	"source_addr": "192.168.100.30",
	"dev_type": "KVM-USB 接口",
	"ext_dev_type": "USB OUT",
	"status": 1,
	"description": "k22 运维任务"
	}

运维对象字段	{
	"dev_id": "24533",
	"version": 1, "wo_name": "快速运维 090501",
	"wo_no": "nr_3233_41",
	"admin_name": "wangwu","operator_name": "zhangsan,lisi",
	"station_name": "灵泉变","station_id": "01111468123",
	"begin_time": "2023-07-13 12:34:56",
	"end_time": "2023-07-13 18:34:56",
	"telephone": "13965836333",
	"device_info": [{
	"device_id": "123","device_name": "网监 1",
	“device_ip": "192.168.1.211"
	}, {
	"device_id": "124",
	"device_name": "网监 2",
	"device_ip": "192.168.1.212"
	}],
	"task_type": 2,
	"task_status": 4,
	"task_content": "xxxxx",
	"impact_scope": "yyyyy",
	"safety_measure": "zzzzz",
	"desc": "qqqqq"
	}

运维网关和集中管控之间的级联通信日志统计业务和高风险指令 kill 及违规外联发送日志代码示例见表 B.5。

表B.5 日志统计业务和高风险指令kill及违规外联发送日志代码示例

对应通讯环节	代码示例

日志统计业务	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:37",
	"wo_no": "nx202011061",
	"task_status": 4,
	"start_time": "2020-05-06 22:11:37",
	"end_time": "2020-05-07 22:11:37",
	"wo_log_num": 12, "wo_warn_num": 12,
	"wo_file_num": 12, "operation_log_num": 12,
	"file_trans_num": 12, "dev_action_num": 12,
	"hr_cmd_warn_num": 12, "illegal_warn_num": 12,
	"attack_warn_num": 12, "virus_warn_num": 12,
	"hr_port_warn_num": 12,"auth_num": 12,
	"video_file_num": 12, "net_pac_num": 12,
	"char_cmd_num": 12, "key_record_num": 12
	}

高风险指令 kill	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:27",
	"wo_no": "nx202011061",
	"resource_addr": "172.16.69.210",
	"resource_port": 8088,
	"executor_name": "王五",
	"source_addr": "192.168.100.30",
	"description": "触发了高危指令 kill",
	"action_id": 1,
	"operate_content": "kill",
	"cmd_type": 1,
	"protocol_type": "ssh"
	}

违规外联发送日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:27",
	"wo_no": "nx202011061",
	"resource_addr": "172.16.69.210",
	"resource_port": 8088,
	"executor_name": "王五",
	"source_addr": "192.168.100.30",
	"description": "发生了违规外联，外联 WIFI：TP-LINK_BDC",
	"ex_device_os": "Linx 6.0.80",
	"ex_device_mac": "E4-54-E8-DB-7E-9A",
	"ex_host_name": "lishi",
	"ex_info": "TP-LINK_BDC"
	}

全国团体标准信息平台

运维网关和集中管控之间的级联通信发生攻击和发现恶意代码及发生高危端口通讯时发送日志代码示例见表 B.6。

表B.6 发生攻击和发现恶意代码及发生高危端口通讯时发送日志代码示例

对应通讯环节	代码示例

发生攻击时发送日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:27",
	"wo_no": "nx202011061",
	"resource_addr": "172.16.69.210",
	"resource_port": 8088,
	"executor_name": "王五",
	"source_addr": "192.168.100.30",
	"description": "发生了 ARP 攻击告警",
	"attack_type": 1,
	"operate_content": "ARP",
	"source_mac": "E4-54-E8-DB-7E-9A",
	"source_port": 59046,
	"attack_detail": 1
	}

发现恶意代码是发送日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:27",
	"wo_no": "nx202011061",
	"resource_addr": "172.16.69.210",
	"resource_port": 8088,
	"executor_name": "王五",
	"source_addr": "192.168.100.30",
	"description": "检测到恶意代码，xx",
	"file_name": "narit_csm.jar",
	"file_type": "jar",
	"file_path": "/home/data/",
	"file_size": 110730905,
	"operate_type": 1,
	"virus_type": "aa",
	"action_id": 1
	}

发生高危端口通讯时发送日志	{
	"dev_id": "24533",
	"version": 1,
	"log_time": "2020-05-07 22:11:27",
	"wo_no": "nx202011061",
	"resource_addr": "172.16.69.210",
	"resource_port": 8088,
	"executor_name": "王五",
	"source_addr": "192.168.100.30",
	"description": "连接了高危端口 22，xx",
	"operate_content": "22",
	"action_id": 1
	}

运维网关和集中管控之间的级联通信高危端口下发规则库及有更新返回时代码示例见表 B.7。

表B.7 高危端口下发规则库及有更新返回时代码示例

对应通讯环节	代码示例
集中管控下发高危端口规则库	{ "dev_id": "24533", "version": 1, "rule_base_id": 101, "rule_base_version": 1716861816445, "data": [{ "id": "123", "port": 22, "port_des": "SSH 服务", "strategy": 1, "protocol": "tcp", "description": "22 端口阻断", "status": 1 }, { "id": "124", "port": 110, "port_des": "POP3 邮件服务", "strategy": 3, "protocol": "tcp", "description": "110 端口告警", "status": 1 }] }
当运维网关获取操作类指令规则时有更新返回	{ "message": "成功，有更新", "dev_id": "24533", "version": 1, "rule_base_id": 101, "rule_base_version": 1716861816446, "data": [{ "id": "125", "cmd": "reboot", "cmd_des": "重启", "strategy": 1, "is_regular": 0, "description": "reboot 指令申请确认", "status": 1, "protocol": null }, { "id": "126", "cmd": "kill", "cmd_des": "杀死进程", "strategy": 2, "is_regular": 0, "description": "kill 指令阻断", "status": 1, "protocol": null }] }

运维网关和集中管控之间的级联通信下发运维工单和获取工单返回数据代码示例见表B.8。

表B.8 下发运维工单和获取工单返回数据代码示例

对应通讯环节	代码示例

集中管控下发运维工单时	{
	"dev_id": "24533",
	"version": 1,
	"data": [{
	"wo_name": "xxx 任务",
	"wo_no": "112233",
	"admin_name": "zhangsan",
	"operator_name": "lisi,wangyan",
	"station_name": "灵泉变",
	"station_id": "213123",
	"begin_time": "2023-07-13 12:34:56",
	"end_time": "2023-07-13 18:34:56",
	"telephone": "13596590999",
	"device_info": [{
	"device_id": "213",
	"device_name": "xxx",
	"device_ip": "1.1.2.3"
	}],
	"task_type": 0,
	"task_status": 1,
	"task_content": "xx",
	"impact_scope": "yy",
	"safety_measure": "zz",
	"desc": "cc"
	}]
	}

运维网关获取运维工单返回数据	{
	"message": "成功",
	"dev_id": "24533",
	"data": [{
	"wo_name": "xxx 任务",
	"wo_no": "112233",
	"admin_name": "zhangsan",
	"operator_name": "lisi,wangyan",
	"station_name": "灵泉变",
	"station_id": "213123",
	"begin_time": "2023-07-13 12:34:56",
	"end_time": "2023-07-13 18:34:56",
	"telephone": "13596590999",
	"device_info": [{
	"device_id": "213",
	"device_name": "xxx",
	"device_ip": "1.1.2.3"
	}],
	"task_type": 0,
	"task_status": 1,
	"task_content": "xx",
	"impact_scope": "yy",
	"safety_measure": "zz",
	"desc": "cc"
	}]
	}

全国电力智能运维信息平台

B.3 固件压缩包样式示例

各厂商提的固件升级包需按照指定的格式，外层是一个 zip 包，zip 包里面包含两个文件，版本描述文件 version.json 和固件升级文件压缩包（格式由厂商自定义），平台下发文件为整个 zip 包文件,运维网关自行解压，zip 压缩包样式见表 B.9。

表B.9 固件升级文件压缩包样式

对应通讯环节	样式示例
运维网关固件管理	zip 包结构示例： |--V1.5.0_2024102501.zip |--V1.5.0_2024102501.xxx |--version.json

全国团体标准信息平台

参考文献

[1] Q/GDW 11914—2018 电力监控系统网络安全监测装置技术规范
[2] Q/GDW 12195—2021 电力监控系统恶意代码监测系统技术规范
[3] Q/GDW 12297—2024 调度自动化系统主站运维网关技术规范
[4] Q/GDW 12472—2024 电力监控系统便携式运维网关技术规范

全国团体标准信息平台