ICS 35.240.50
P 55

SL

中华人民共和国水利行业标准

SL/T 803—2020

水利网络安全保护技术规范

Technical specification for cybersecurity of water resources

2020-11-30 发布　　2021-02-28 实施

中华人民共和国水利部　发布

中华人民共和国水利部

关于批准发布《碾压式土石坝设计规范》等5项水利行业标准的公告

2020年第22号

中华人民共和国水利部批准《碾压式土石坝设计规范》（SL 274—2020）等5项为水利行业标准，现予以公布。

序号	标　准　名　称	标准编号	替代标准号	发布日期	实施日期
1	碾压式土石坝设计规范	SL 274—2020	SL 274—2001	2020.11.30	2021.2.28
2	水利水电工程进水口设计规范	SL 285—2020	SL 285—2003	2020.11.30	2021.2.28
3	绿色小水电评价标准	SL/T 752—2020	SL 752—2017	2020.11.30	2021.2.28
4	水利网络安全保护技术规范	SL/T 803—2020		2020.11.30	2021.2.28
5	淤地坝技术规范	SL/T 804—2020	SL 289—2003 SL 302—2004	2020.11.30	2021.2.28

水利部

2020年11月30日

目　　次

前　言

根据水利技术标准制修订计划安排，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》的要求，编制本标准。

本标准共10章和2个附录，主要技术内容有：

——总体要求；

——网络安全技术体系；

——安全纵深防御能力；

——安全监测预警能力；

——安全应急响应能力；

——安全运营；

——安全监督检查。

本标准批准部门：**中华人民共和国水利部**

本标准主持机构：**水利部网络安全与信息化领导小组办公室**

本标准解释单位：**水利部网络安全与信息化领导小组办公室**

本标准主编单位：**水利部信息中心**

本标准参编单位：**海河水利委员会水利信息网络中心**

本标准出版、发行单位：**中国水利水电出版社**

本标准主要起草人：**詹全忠　杨　旭　张　潮　周维续　黄　锐　沈智镔　陈　岚　张　洋　卢　青**

本标准审查会议技术负责人：**朱星明　吴恒清**

本标准体例格式审查人：**朱星明**

本标准在执行过程中，请各单位注意总结经验，积累资料，随时将有关意见和建议反馈给水利部国际合作与科技司（通信地址：北京市西城区白广路二条2号；邮政编码：100053；电话：010-63204533；电子邮箱：bzh@mwr.gov.cn），以供今后修订时参考。

水利网络安全保护技术规范

1 范围

本标准规定了水利网络安全保护总体要求、安全技术体系框架、安全纵深防御能力建设要求、安全监测预警能力建设要求、安全应急响应能力建设要求、安全运营要求和安全监督检查要求。

本标准适用于网络安全等级保护等级为一级、二级和三级的水利网络安全保护对象的网络安全保护。

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标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 50174—2017 数据中心设计规范

3 术语与缩略语

3.1 术语和定义

GB/T 32919、GB/T 22239、GB/T 25070、GB/T 20984、GB/T 28448 界定的以及下列术语和定义适用于本标准。

3.1.1

水利网络安全保护对象 water resources cybersecurity protection object

由计算机及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括水利基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、水利工程控制系统和水利业务应用系统（含采用移动互联技术的系统）等。

3.1.2

水利关键信息基础设施 water resources critical information infrastructure

一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的水利网络安全保护对象。例如：符合水利关键信息基础设施认定规则的大型水利枢纽、输水调水工程等重要基础设施的集中控制系统和水灾害防御、水资源管理等重要业务系统。

3.1.3

工业控制系统 industrial control system

工业生产中使用的控制系统，包括数据采集与监视控制系统（SCADA）、分散控制系统（DCS）和其他较小的控制系统，如：可编程逻辑控制器（PLC），现已广泛应用在工业部门和关键基础设施中。

［来源：GB/T 32919—2016，3.1］

3.1.4

安全保护能力　security protection capability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的能力。

［来源：GB/T 22239—2019，3.2］

3.1.5

安全计算环境　security computing environment

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

［来源：GB/T 25070—2019，3.4］

3.1.6

安全区域边界　security area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

［来源：GB/T 25070—2019，3.5］

3.1.7

安全通信网络　security communication network

对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。

［来源：GB/T 25070—2019，3.6］

3.1.8

安全管理中心　security management center

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台或区域。

［来源：GB/T 25070—2019，3.7］

3.1.9

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］

3.1.10

脆弱性　vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

［来源：GB/T 20984—2007，3.18］

3.1.11

（信息安全）风险评估　（information security）risk assessment

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

［来源：GB/T 20984—2007，3.7］

3.1.12

等级测评　testing and evaluation for classified cybersecurity protection

测评机构依据国家网络安全等级保护制度，按照有关管理规范和技术标准，对非涉及国家秘密的网络安全安全等级保护状况进行检测评估的活动。

［来源：GB/T 28448—2019，3.6］

3.1.13

网络安全应急响应能力　emergency response capability of cybersecurity

一个组织为了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的及时性、有效性以及可控性等。

3.2　缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control List）

DCS：分散控制系统（Distributed Control System）

DDoS：拒绝服务（Distributed Denial of Service）

DNS：域名系统（服务）协议（Domain Name System）

FTP：文件传输协议（File Transfer Protocol）

GIS：地理信息系统（Geographic Information System）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

ICS：工业控制系统（Industrial Control System）

IoT：物联网（Interent of Things）

MAC 地址：媒体存取控制位址（Media Access Control Address）

MCU：微控制单元（MicroController Unit）

PLC：可编程逻辑控制器（Programmable Logic Controller）

POP3：邮局协议版本 3（Post Office Protocol—Version 3）

SCADA：数据采集与监视控制系统（Supervisory Control And Data Acquisition System）

SMB：协议名（Server Message Bloc）

SSH：安全外壳协议（Secure Shell）

SSL：安全套接层（Secure Sockets Layer）

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

UDP：用户数据报协议（User Datagram Protocol）

VLAN：虚拟局域网（Virtual Local Area Network）

WAF：网站应用防火墙（Web Application Firewall）

4　总体要求

4.1　基本原则

水利网络安全建设应遵循以下基本原则：

a）全面完整原则：在进行网络安全建设时，应遵循本文件规定，结合实际，进行完整的网络安全体系架构设计，全面覆盖所有安全要素；

b）等级保护原则：应按照 GB/T 22240—2020，确定各类水利网络安全保护对象的保护等级；

c）同步要求原则：水利信息化项目在规划建设运行时，应将网络安全保护措施同步规划、同步建设、同步使用；

d）适当调整原则：在进行网络安全建设时，可根据水利网络安全保护对象具体情况和特点，适当调整部分安全要素的建设标准；

e）持续改进原则：应依据本标准和 GB/T 22239—2020 等国家标准规范要求持续完善网络安全体系。

4.2　一般要求

水利网络安全建设应满足以下一般要求：

a）设备安全要求：应优先选用稳定可靠的服务器、PLC、MCU、终端等计算设备，并根据需要进行计算设备安全评估；
b）软件安全要求：应优先选用稳定可靠的操作系统、PLC 系统、组态软件、应用软件等软件，并根据需要进行软件安全评估；
c）接入安全要求：可采用密码技术等保证接入网络的设备安全可信；
d）安全服务要求：应与产品、服务提供者签订安全保密协议，并约定其为产品、服务提供安全维护，在规定或者约定的期限内，不应终止提供安全维护；
e）容灾备份要求：应具备容灾备份措施对重要数据进行备份。

4.3 水利关键信息基础设施补充要求

水利关键信息基础设施网络安全建设，应满足以下补充要求：
a）设备安全要求：应对重要设备进行安全审查和评估；
b）软件安全要求：应对重要软件进行安全审查和评估；
c）协议安全要求：应采用具备安全校验机制的通信协议，重要的服务和通信连接应采取加密技术措施；
d）认证检测要求：关键设备和安全专用产品应当按照国家相关标准的强制性要求，采用安全认证或者安全检测合格的产品；
e）计算环境要求：应按不低于第三级网络安全保护对象的安全计算环境要求进行设计实施；
f）容灾备份要求：应具备异地容灾备份措施；
g）安全验收要求：竣工验收前，宜进行网络安全专项验收。

5 网络安全技术体系

5.1 体系架构

5.1.1 水利行业网络安全建设应包括纵深防御、统一安全服务、威胁感知预警、应急决策指挥，宜按照图 1 构建。其中纵深防御应包括安全物理环境、安全计算环境、安全区域边界、安全通信网络等部分。

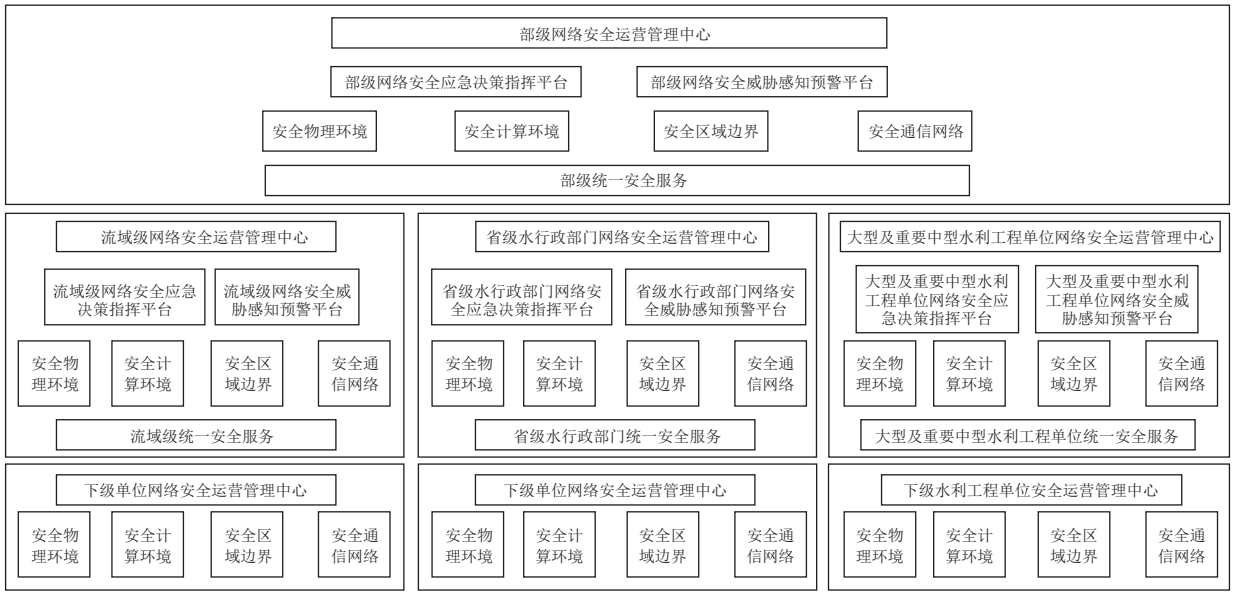

图 1 水利行业网络安全技术体系框架图

5.1.2 网络安全技术架构应包括以下内容：

a）应建设水利行业协同统一的网络安全服务体系，包括网络安全情报服务、灾备服务、密码服务、认证服务等；

b）在安全物理环境基础上，应构建安全计算环境、安全区域边界、安全通信网络的3层基础防护；

c）宜构建网络安全威胁感知预警平台和网络安全应急决策指挥平台，形成贯穿所有安全活动的安全运营管理中心。

5.1.3 纵深防御应建立完善合规的物理环境、计算环境、区域边界、通信网络防护。同时应针对公共的安全技术形成统一的安全服务，包括安全情报服务、灾备服务、密码服务、认证服务等4项服务。

5.1.4 监测预警应满足下列要求：

a）应建立采集流量数据、设备日志、主机日志、应用系统日志的数据采集系统；

b）应对采集数据进行分析，发现安全事件和潜在威胁，进行风险预警；

c）宜建设水利行业网络安全大数据平台，建立数据采集标准规范，对各级节点网络安全数据和关键网络安全数据进行威胁分析；

d）各级节点应建设共享交换机制，与上级节点实现关键流量数据、网络安全预警等数据交互。

5.1.5 应急响应应满足下列要求：

a）应建设行业应急决策指挥平台并制定网络安全事件相关数据交换标准；

b）各级节点可建设应急决策指挥平台，管理网内网络安全资源，对网内各类风险预警进行综合研判和闭环处置，实现应急预案管理与策略编排，并应与上级应急决策指挥平台进行数据交换。

5.1.6 安全运营应在纵深防御、监测预警、应急响应等各类安全设备（系统）的支撑下，建立网络安全运营体系，识别网络安全态势，优化网络安全防御措施。

5.2 建设要求

5.2.1 应开展网络安全纵深防御能力、网络安全监测预警能力、网络安全应急响应能力建设，宜建立与之对应的网络安全运营体系。

5.2.2 部级建设应满足下列要求：

a）应建设网络安全情报服务、灾备服务、统一密码服务、统一身份认证服务，为本级及下级网络节点提供服务共享；

b）应以不低于第三级系统安全要求开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设，应对水利关键信息基础设施采取措施进行重点保护；

c）应建设网络安全数据采集处理系统，建设威胁感知预警平台，对本级及下级网络节点的关键网络安全数据进行统一分析，及时发现网络安全威胁；

d）应建设网络安全应急决策指挥平台，对本级和行业内重要网络安全事件进行全流程处置指挥；

e）应建立以数据为核心，网络安全资源管理为支撑，涵盖威胁预防、威胁防护、持续监测、响应处置的闭环安全运营体系；

f）各下级网络节点应按最高级别网络安全保护对象相应等级保护级别安全要求开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设。

5.2.3 流域级建设应满足下列要求：

a）应在上级节点网络安全服务基础上，建设区域级网络安全情报服务、统一密码服务、统一身份认证服务，为本级及下级网络节点提供服务共享；

b）应以不低于第三级系统安全要求开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设，应对关键信息基础设施采取措施进行重点保护；

c）应建设网络安全数据采集处理系统，建设威胁感知预警平台，对本级及下级节点的网络安全数据进行统一分析，及时发现网络安全威胁，应与上级节点进行数据共享；

d）应依托上级节点或自行建设网络安全应急决策指挥平台，对网内重要网络安全事件进行全流程指挥处置，应与上级节点进行数据共享；

e）应建立以数据为核心，网络安全资源管理为支撑，涵盖威胁预防、威胁防护、持续监测、响应处置的闭环安全运营体系；

f）各下级节点应按最高级别网络安全保护对象相应等级保护级别安全要求开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设。

5.2.4 省级建设应满足下列要求：

a）可在上级节点网络安全服务基础上，建设区域级网络安全情报服务、统一密码服务、统一身份认证服务，为本级及下级单位提供服务共享；

b）应以不低于第三级系统安全要求开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设，应对关键信息基础设施采取措施进行重点保护；

c）应建设网络安全数据采集处理系统，自行或依托上级节点建设威胁感知预警平台，对本级及下级节点的网络安全数据进行统一分析，及时发现网络安全威胁，应与上级节点进行数据共享；

d）应依托上级节点或自行建设网络安全应急决策指挥平台，对本省（自治区、直辖市）内重要网络安全事件进行全流程指挥处置，应与上级节点进行数据共享；

e）应建立以数据为核心，网络安全资源管理为支撑，涵盖威胁预防、威胁防护、持续监测、响应处置的闭环安全运营体系；

f）各下级节点应按最高级别网络安全保护对象相应等级保护级别安全要求开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设。

5.2.5 市县级建设应满足下列要求：

a）应以不低于第二级系统安全要求开展有关的安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设；

b）应建设网络安全数据采集系统，宜依托上级节点威胁感知预警平台，对网络安全数据进行统一分析，及时发现网络安全威胁；

c）宜依托上级节点网络安全应急决策指挥平台，对重要网络安全事件进行全流程指挥处置；

d）应依托上级节点或自行建立以数据为核心，网络安全资源管理为支撑，涵盖威胁预防、威胁防护、持续监测、响应处置的闭环安全运营体系；

e）各下级节点应按最高级别网络安全保护对象相应等级保护级别安全要求，开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设。

5.2.6 大型（含重要中型）水利工程管理单位建设应满足下列要求：

a）应在上级节点网络安全服务基础上，建设网络安全情报服务、灾备服务、统一密码服务、统一身份认证服务，可根据水利工业控制系统实际情况，建设工业控制专用的网络安全情报服务、本地灾备服务、统一密码服务、身份认证服务；

b）应以不低于第三级系统安全要求（含工业控制系统扩展要求）开展安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设，并对关键信息基础设施采取措施进行重点保护；

c）应建设网络安全数据采集处理系统，自行或依托上级节点建设威胁感知预警平台，对网络安全数据进行统一分析，及时发现网络安全威胁，应与上级节点威胁感知预警平台进行数据

共享；

d）应依托上级节点或自行建设网络安全应急决策指挥平台，对重要网络安全事件进行全流程指挥处置，并与上级节点进行数据共享；

e）应建立以数据为核心，网络安全资源管理为支撑，涵盖威胁预防、威胁防护、持续监测、响应处置的闭环安全运营体系；

f）不具备三级及以上网络安全保护对象的单位可参照本标准对其他级别网络安全保护对象的要求进行建设。

5.2.7 中小型水利工程管理单位建设应满足下列要求：

a）应以不低于第二级系统安全要求（含工业控制系统扩展要求）开展有关的安全物理环境、安全计算环境、安全区域边界、安全通信网络等方面的网络安全纵深防御能力建设；

b）应建设网络安全数据采集系统，宜依托上级节点威胁感知预警平台，对网络安全数据进行统一分析，及时发现网络安全威胁；

c）宜依托上级节点网络安全应急决策指挥平台，对重要网络安全事件进行全流程指挥处置；

d）应依托上级节点或自行建立以数据为核心，网络安全资源管理为支撑，涵盖威胁预防、威胁防护、持续监测、响应处置的闭环安全运营体系；

e）具备三级及以上网络安全保护对象的单位，可参照本文件对大型及重要中型水利工程管理单位的网络建设要求进行建设。

6 安全纵深防御能力

6.1 基本要求

安全纵深防御能力建设基本要求应由安全物理环境、安全通信网络、安全区域边界和安全计算环境各部分组成，应根据承载网络安全保护对象的不同等级和类型情况，并按以下要求执行：

a）网络安全等级保护只有一级的水利网络安全保护对象，应采用 GB/T 22239—2019 第一级的安全要求；

b）网络安全等级保护为二级及以下的水利网络安全保护对象，应采用第二级安全要求开展安全纵深防御能力建设；

c）网络安全等级保护为三级的水利网络安全保护对象，应采用第三级安全要求开展安全纵深防御能力建设；

d）存在工业控制系统、云计算环境、移动互联和物联网应用的，应在以上基础上分别落实工业控制系统、云与虚拟化、移动互联和物联网扩展安全要求；

e）存在关键信息基础设施的，应在第三级安全要求的基础上落实关键信息基础设施扩展要求。

6.2 安全物理环境

6.2.1 安全物理环境应包括物理位置选择、机房环境安全、物理访问控制、安全分域、防盗窃、防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、设备设施安全、电力供应、监控审计、电磁防护和灾难备份中心等方面。

6.2.2 第二级要求应以承载最高网络安全保护等级为第二级的保护对象，应符合 GB/T 50174—2017 的 C 级标准和 GB/T 22239—2019 第二级的安全要求。

6.2.3 第三级要求应以承载最高网络安全保护等级为第三级的保护对象，除符合 GB/T 50174—2017 中 B 级标准和 GB/T 22239—2019 第三级的安全要求外，还应符合下列要求：

a）应对机房和设备间的进出访问进行控制，部署安全监控措施，进行安全巡检；

b）应对专用移动存储介质进行统一管理，记录介质领用、接入使用、交回、维修、报废、销毁

等情况。

6.2.4 关键信息基础设施安全除符合 6.2.3 要求外，还应符合下列要求：

a) 应对关键信息基础设施运行环境进行安全管理，确保物理环境安全可控；

b) 不应使用境外机构提供或位于境外的物理服务器或虚拟主机；

c) 应配备关键信息基础设施机房周边环境的边界安全控制人员；

d) 工业控制系统现地设备应置于安全的物理环境中，具备防火、防风、散热、防盗、防雨等能力；

e) 工业控制系统现地设备环境周边应采用围墙、门禁、密码锁、视频监控、专人值守、授权访问等安全措施；

f) 关键设备周边应采用自动化设备识别入侵，并进行报警，实施自动响应动作；

g) 应对关键信息基础设施设置独立的逻辑或物理区域，并根据业务功能、设备类型等划分子区域；

h) 宜对关键信息基础设施配置第二道电子门禁系统；

i) 应对关键信息基础设施核心设备持续运行提供备用电力供应；

j) 应对关键设备设置有专人值守的视频监控系统，定期审计监控系统记录；

k) 宜对网络设备、关键计算设备进行冗余配置，符合业务系统持续正常运行的要求；

l) 工业控制系统输出设备应放置在安全区域，并对设备进行授权访问控制、设备标记和实时监控；

m) 宜使用自动化措施对设备的访问日志进行记录，包括访问人员、目的、时间、鉴别形式、访问设备等；

n) 宜设置电磁屏蔽措施。

6.3 安全通信网络

6.3.1 构成

安全通信网络应包括网络架构、传输加密、安全审计等方面。

6.3.2 第二级要求

安全通信网络第二级要求应符合 GB/T 22239—2019 第二级的安全要求。

6.3.3 第三级要求

安全通信网络第三级要求除符合 GB/T 22239—2019 第三级安全要求外，还应符合下列要求：

a) 安全区域应根据业务属性划分，可划分为内部业务区、接入区、前置交换区、公众服务区、数据区和安全管理区等；

b) 数据通信应使用符合国家要求的密码技术；

c) 应提供通信线路、关键网络设备、安全设备的硬件冗余；

d) 应基于硬件设备，对重要通信过程进行加解密运算和密钥管理；

e) 应将攻击监测数据和审计数据进行统一分析。

6.3.4 关键信息基础设施安全要求

6.3.4.1 网络架构安全要求除符合第三级要求外，还应符合下列要求：

a) 关键信息基础设施信息系统，应与其他不同等级系统之间设置技术隔离措施，实施严格访问控制策略；

b）不应将高安全等级业务系统或其功能模块，部署到低安全等级区域；属于低安全等级区域的业务系统或其功能模块，可部署于高安全等级区域，并按照高安全等级区域的保护策略进行保护；

c）应提供通信线路、网络设备、安全设备和关键计算设备的硬件冗余。

6.3.4.2 传输加密安全要求除符合第三级要求外，还应符合下列要求：

a）通信信道应满足关键业务处理需求；

b）应对不同局域网之间的远程通信，采用密码技术进行加密传输；局域网内宜对关键、敏感数据进行加密；

c）应对关键数据进行校验，保证通信信息的完整性、可用性；

d）安全审计记录宜包括监测、记录系统运行状态、日常操作、故障维护、远程维护等，日志数据留存应不少于12个月。

6.4 安全区域边界

6.4.1 构成

安全区域边界构成宜符合以下要求：

a）水利网络安全保护对象区域边界可分成内部边界、互联网边界、水利业务网边界、外联网边界。安全区域边界构成见图2。安全区域划分方法，可参见附录A。

注：内部边界是指局域网内部各个安全域或计算环境之间的边界；互联网边界是指与互联网连接的安全域或网络边界；水利业务网边界是指与水利业务网连接的安全域或网络边界；外联网边界是指与其他外部网络之间的安全域或网络边界。

b）边界防护手段可包括边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计和可信验证等方面。

c）水利关键信息基础设施安全区域可涉及其中一种或多种网络边界，其边界防护应依据实际情况满足对应要求。

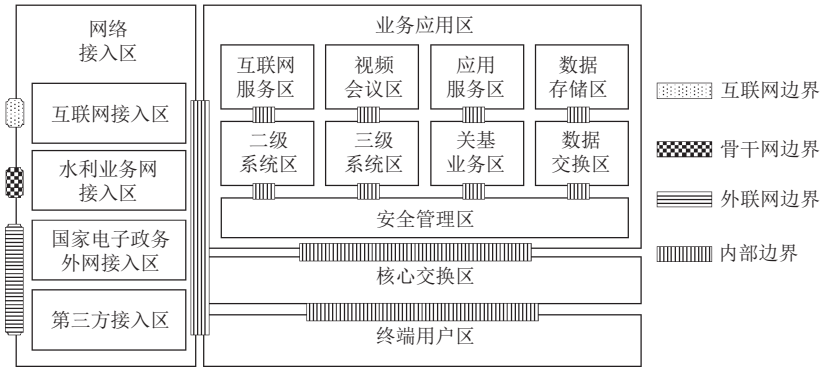

图2 安全区域边界构成图

6.4.2 第二级要求

6.4.2.1 安全区域边界第二级要求应符合GB/T 22239—2019第二级的安全要求。

6.4.2.2 内部边界安全应符合下列要求：

a）应根据访问控制策略，设置进出双向的访问控制规则，默认情况下（除允许的通信外）拒绝所有通信，删除多余或无效的访问控制规则，访问控制规则数量最小化；

b）应对存放集中访问控制权限或集中进行安全管理类设备或系统、认证类系统以及数据库系统边界进行网络安全审计，对重要的用户行为和重要网络安全事件进行审计。

6.4.2.3 互联网边界安全应符合下列要求：

a）应根据访问控制策略，设置进出双向的访问控制规则，默认情况下（除允许的通信外）拒绝所有通信，删除多余或无效的访问控制规则，访问控制规则数量最小化；

b）应在互联网网络边界，配置恶意代码防护措施；

c）应在互联网网络边界进行安全审计，审计重要用户行为和重要网络安全事件；

d）对审计记录应进行定期备份；

e）应能检测互联网网络边界的攻击行为，并进行告警。

6.4.2.4 水利业务网边界安全应符合下列要求：

a）应根据访问控制策略，设置进出双向的访问控制规则，默认情况下（除允许的通信外）拒绝所有通信，删除多余或无效的访问控制规则，访问控制规则数量最小化；

b）应能对访问本级网络的异常网络行为进行审计和告警。

6.4.2.5 外联网边界安全应符合下列要求：

a）应根据访问控制策略，设置进出双向的访问控制规则，默认情况下（除允许的通信外）拒绝所有通信，删除多余或无效的访问控制规则，访问控制规则数量最小化；

b）应在外联网边界进行安全审计，审计重要用户行为和重要网络安全事件。

6.4.3 第三级要求

6.4.3.1 安全区域边界第三级要求要求应符合 GB/T 22239—2019 第三级的安全要求。

6.4.3.2 内部边界安全应符合下列要求：

a）对区域边界数据流应实现基于应用协议和应用内容的监测和访问控制；

b）应能对非授权设备连接到内部网络的行为进行检查与限制；

c）应能对内部用户非授权连接到外部网络的行为进行检查与限制；

d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络；

e）当检测到攻击行为时，应能记录攻击源 IP、攻击类型、攻击目标、攻击时间；在发生严重入侵事件时，应提供报警；

f）对区域边界应进行安全审计，审计每个用户的用户行为和安全事件。

6.4.3.3 互联网边界安全应符合下列要求：

a）应在互联网边界对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；

b）宜对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；

c）应能对互联网边界数据流进行基于应用协议和应用内容的访问控制；

d）当检测到攻击行为时，网络安全措施应能记录攻击源 IP、攻击类型、攻击目标、攻击时间；在发生严重入侵事件时，应能报警，并宜实现自动阻断；

e）对互联网边界应进行安全审计，审计用户行为和安全事件；

f）网络攻击监测数据和审计数据，应进行统一分析。

6.4.3.4 水利业务网边界安全应符合下列要求：

a）对骨干网边界数据流，宜进行基于应用协议和应用内容的访问控制；

b）当检测到攻击行为时，网络安全措施应能记录攻击源 IP、攻击类型、攻击目标、攻击时间；在发生严重入侵事件时，应能报警，并宜实现自动阻断；

c）对骨干网边界应进行安全审计，审计重要用户行为和安全事件；

d）网络攻击监测数据和审计数据，应进行统一分析。

6.4.3.5 外联网边界安全应符合下列要求：

a）应能对远程访问、访问外联网等用户行为，进行行为审计和数据分析；

b）对外联网边界数据流，宜进行基于应用协议和应用内容的访问控制；

c）当检测到攻击行为时，应能记录攻击源 IP、攻击类型、攻击目标、攻击时间；在发生严重入侵事件时，应能报警，并宜实现自动阻断；

d）对外联网边界应进行安全审计，审计用户行为和安全事件；

e）网络攻击监测数据和审计数据，应进行统一分析。

6.4.4 关键信息基础设施安全要求

6.4.4.1 内部边界安全除符合第三级要求外，还应符合下列要求：

a）应通过逻辑隔离或物理隔离技术，实现内部区域边界的访问控制；

b）应对内部边界，设置严格的访问控制策略，访问控制策略达到端口级；

c）应能对内部网络的安全事件和威胁进行安全检测，基于流量检测多种网络协议中的攻击行为。

6.4.4.2 互联网边界安全除符合第三级要求外，还应符合下列要求：

a）应建立不同网络安全等级系统、不同业务系统、不同区域之间的安全互联和访问控制策略，策略达到端口级；

b）应对不同网络安全等级系统、不同业务系统、不同区域之间的互操作、数据交换和信息流量进行严格控制，限制数据从高等级系统流向低等级系统；

c）应对进出网络的数据流实现基于应用协议和应用内容的访问控制；

d）应采用严格的接入控制措施，对未授权设备进行动态检测及管控，仅允许通过授权和安全评估的软硬件运行，保证系统和设备接入的可信性；

e）应对不同局域网远程通信采用安全防护措施，采用密码技术对通信双方进行验证；

f）应在网络边界设置业务优先级，优先保障关键信息基础设施业务运行；

g）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

h）应能对高级威胁进行安全检测，基于流量检测多种网络协议中的攻击行为；

i）应在互联网边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为约定格式，发送至安全威胁感知预警平台。

6.4.4.3 水利业务网边界安全除符合第三级要求外，还应符合下列要求：

a）应通过逻辑隔离技术，实现骨干网边界的访问控制，访问控制策略达到 IP 地址级；

b）应在骨干网边界检测和限制从内部发起的网络攻击行为，对网络行为进行分析，实现对网络攻击特别是未知新型网络攻击的检测和分析；当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目的、攻击时间；在发生严重入侵事件时，应提供报警和阻断；

c）应能对高级威胁进行安全检测，基于流量检测多种网络协议中的攻击行为；

d）应在骨干网边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为约定格式，发送至安全威胁感知预警平台。

6.4.4.4 外联网边界安全除符合第三级要求外，还应符合下列要求：

a）应在外联网边界部署防恶意代码设备，实现区域边界的病毒防护以及恶意代码防范，并维护恶意代码防护机制的升级和更新；

b）应在外联网边界部署检测、防止或限制从外部发起的网络攻击行为的设备；

c）应在外联网边界对网络行为进行分析，实现对网络攻击特别是未知新型网络攻击的检测和分析；当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目的、攻击时间；在发生严重入侵事件时，应能报警，并宜实现自动阻断；

d）应能对高级威胁进行安全检测，基于流量检测多种网络协议中的攻击行为；

e）应在外联网边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为约定格式，发送至安全威胁感知预警平台。

6.5 安全计算环境

6.5.1 防护手段

安全计算环境防护手段应包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等方面。

6.5.2 第二级要求

安全计算环境除符合 GB/T 22239—2019 第二级安全要求外，还应符合下列要求：

a) 应采用集中统一管理方式，对终端计算机进行管理，统一软件下发、安装系统补丁、实施病毒库升级和病毒查杀；
b) 应定期开展针对终端的弱口令检查、病毒查杀、漏洞修补、操作行为管理和安全审计等工作；
c) 应避免网站系统后台管理页面和信息暴露在互联网，应严格管控门户网站信息的发布；
d) 应控制邮件系统用户注册审批和员工账户注销管理，不应将工作邮件自动转发至私人或境外邮箱；应避免系统存在弱口令，避免访问钓鱼邮件；
e) 应对 3 个月及其以上在线且未使用的水利网络安全保护对象采取断电、断网等下线措施；再次上线使用前，应先进行漏洞修补、病毒库更新等安全加固。

6.5.3 第三级要求

安全计算环境除符合 GB/T 22239—2019 第三级安全要求外，还应符合下列要求：

a) 应设置并启用管理终端外联控制策略，对管理终端未经授权的外联行为进行监测和处置，未经授权，不应通过任何形式连接外部网络；不应使用 USB 接口，为手机等外部设备充电；
b) 应对重要计算设备和系统采用密码技术、生物技术等两种或两种以上组合的鉴别技术鉴别用户身份；
c) 应对重要计算设备的入侵或异常行为进行实时监测，并在发生严重入侵事件时，提供报警和阻断；报警和审计记录，应发送至安全威胁感知预警平台；
d) 应采用密码技术，对身份鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据、重要个人信息、水利工程技术数据等数据的传输和存储进行加密；
e) 应对网站系统进行安全审计，包括前台用户的注册、登录、关键业务操作等行为日志记录，后台内容管理用户的登录、网站内容编辑、审核及发布等行为日志记录，系统管理用户的登录、账号及权限管理等系统管理操作日志记录；宜指定独立的审计管理员，负责管理审计日志；
f) 应提供重要数据处理系统的软硬件冗余；
g) 应将网络攻击监测数据和审计数据发送至安全威胁感知预警平台进行统一分析；
h) 在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应在境内存储。

6.5.4 关键信息基础设施安全要求

6.5.4.1 基础信息资源安全除符合第三级要求外，还应符合下列要求：

a) 应对关键信息基础设施操作系统进行统一安全配置和安全加固，仅安装需要的组件和应用程序，关闭不需要的服务、默认共享和高危端口；
b) 应采用可信令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护；

c）应对关键信息基础设施运行终端进行安全管控，设置访问控制策略，严格输入输出管理；
d）应采用统一的认证、加密技术，实现对关键信息基础设施的认证和加密；
e）应对关键信息基础设施服务器，部署统一的防病毒、防入侵和主机审计措施，应能及时发现漏洞、入侵行为和高级网络威胁，并在发生攻击事件时进行告警并阻断；
f）应对关键基础设施的基础信息资源部署数据灾备措施；
g）应对重要业务操作或异常用户操作行为形成记录清单；
h）应对重要业务数据资源的操作，基于安全标记等技术实现访问控制；
i）应使用自动化机制，来支持系统账户、配置库、漏洞库、补丁库、病毒库等的管理，漏洞和补丁应在经过验证后及时修补。

6.5.4.2 应用安全除符合第三级要求外，还应符合下列要求：
a）应建立覆盖应用系统全生命周期的安全机制，基于统一身份认证服务，实现基于风险的身份鉴别、访问控制、数据加密、安全审计等安全要求；
b）应对应用系统的安全性、可用性进行实时安全监测，监测内容包括内容篡改、木马植入、可用性以及网络攻击等；
c）宜实现关键信息基础设施核心应用的应用级灾备建设；
d）宜配置应用备用通信协议保障业务连续性。

6.5.4.3 数据安全除符合第三级要求外，还应符合下列要求：
a）在数据规划和创建阶段，应实现数据的分级分类，明确数据的重要性和敏感程度；
b）应采用密码技术、防泄漏技术等，保证重要数据在传输、存储过程中的完整性和保密性，包括但不限于身份鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；宜根据实际情况，与水利密码基础设施对接；
c）应采用数据隔离技术，建设数据交换平台，实现不同敏感程度网络之间的数据交换，增强数据在外部使用的安全性；
d）应建立数据异地备份机制，并定期对备份有效性进行测试，实现业务和数据抵御地域性灾难的风险，保证数据不丢失以及业务正常恢复，有效提高业务连续性与数据安全；
e）个人信息的收集、存储、使用、传输、披露应符合 GB/T 35273—2020 要求，严格控制重要数据的公开、分析、交换、共享和导出等关键环节，并采取加密、脱敏、去标识化等技术手段，保护敏感数据安全；
f）应建立业务连续性管理及容灾备份机制，重要系统和数据库应实现异地备份；安全性要求高的业务数据，宜实现数据的异地实时备份。

6.6 工业控制系统扩展安全

6.6.1 内容构成

工业控制系统扩展安全应针对工业控制系统中的现场控制和过程监控区，安全内容应包括工业控制系统的安全物理环境、安全分区原则、安全通信网络、安全区域边界、网络设备安全、工业控制设备本体安全、工业控制主机安全防护和安全计算环境等。

6.6.2 第二级要求

工业控制系统扩展安全应符合 GB/T 22239—2019 第二级的工业控制系统安全扩展要求。

6.6.3 第三级要求

工业控制系统扩展安全除符合 GB/T 22239—2019 第三级的工业控制系统安全扩展要求外，还应

符合下列要求：

a）服务器和客户端均应使用安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施；

b）应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口、多余网口或服务端口等；确需保留的服务，应通过相关的技术措施，进行安全防护和严格的监控管理；

c）应基于硬件密码模块，对重要通信过程进行加密；

d）应对控制设备和系统，在上线前进行安全性检测；

e）应对工业控制系统的开发、测试和运行，分别提供独立环境；

f）控制设备固件更新前应经过评估测试；

g）宜对工业控制系统的安全信息进行采集、分析与预警。

6.6.4 关键信息基础设施安全要求

6.6.4.1 安全分区原则安全分区应符合下列要求：

a）工业控制系统分区分域应符合保护核心、有效隔离原则，分成现场控制区、过程监控区；

b）对水利生产实现直接控制的系统、业务模块以及未来对水利生产有直接控制功能的业务系统置于现场控制区；

c）现场控制区、过程监控区和水利业务网之间，功能应相对独立，不应网络混用；

d）在现场控制区、过程监控区内，应根据网络应用特点、重要性程度等因素，划分不同的子网或区域；

e）不应将没有防护的工业控制网络与互联网连接。

注：现场控制区中的业务系统，包括实时闭环控制的 SCADA 系统、实时动态监测系统，安全自动控制系统及保护工作站，如闸门控制系统、机组监控系统、泵站监控系统、设备监测系统等。过程监控区中的业务系统，包括采集监测系统、生产数据采集分析系统等。

6.6.4.2 安全区域边界除符合第三级要求外，还应符合下列要求：

a）现场控制区与过程监控区之间，应采用具有访问控制功能安全可靠的设备实现逻辑隔离、报文过滤、访问控制等功能；设备功能、性能、电磁兼容性，应经过国家相关部门的认证和测试；

b）过程监控区与水利业务网之间，应进行物理隔离，或部署工业控制单向隔离装置进行访问控制；

c）现场控制区、过程监控区的边界，宜建立白名单机制，控制粒度达到工业协议内容级；

d）过程监控区与水利业务网边界，可部署网络入侵检测系统，合理设置检测规则；检测规则应包含工业控制系统专有攻击特征库，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计；

e）设备生产厂商或外部单位，不应远程连接现场控制区中的业务系统及设备；内部远程维护业务系统应进行会话控制，并采用会话认证、加密与抗抵赖等安全机制。

6.6.4.3 安全通信网络除符合第三级要求外，还应符合下列要求：

a）应采取逐级通信原则，仅允许上下级连接网络进行通信，不应越级通信；

b）现场控制区与上级网络连接，应使用独立的网络链路；

c）过程监控区系统与上级集控中心远程通信时，应采用认证、加密、访问控制等技术措施；

d）宜对关键节点、关键业务设备进行设备级标识和认证；

e）宜配备不同服务商的备用通信网络服务。

6.6.4.4 网络安全设备除符合第三级要求外，还应符合下列要求：

a）应通过安全配置确保现场控制区、过程监控区的核心交换机、汇聚交换机、边界防火墙、单向隔离装置等网络设备、安全设备自身的安全性；

b）对登录网络设备、安全设备的用户，应进行身份鉴别及权限控制，只允许相关管理、维护人员等登录设备；

c）远程登录网络设备、安全设备，应采用 HTTPS、SSH 等加密方式；

d）应限定远程管理网络设备、安全设备的 IP 地址；

e）网络设备、安全设备用户口令，应符合复杂度要求，并定期更换；条件允许时，可对安全设备的系统管理员、安全管理员、审计员等特权用户实施双因子认证；

f）应及时清理网络设备、安全设备上临时用户、多余用户。

6.6.4.5 工业控制设备本体安全除符合第三级要求外，还应符合下列要求：

a）应采用通过国家安全检测认证的工业控制设备和系统；

b）系统的可信技术应采用安全可控的技术机制；

c）宜支持安全芯片或安全固件等硬件级部件作为系统信任根，为现场设备的安全启动和数据安全提供安全保护；

d）应采取加密技术对 PLC 通信数据安全加密，宜采用具有通信数据加密功能的 PLC 设备；

e）宜采用应用程序白名单技术，对工业主机内业务组件、系统组件及安全软件等执行程序进行管控；

f）应具备防止、检测、报告和消减恶意代码或非授权软件影响的能力；

g）应对设备本体进行漏洞扫描和漏洞挖掘，及时修补并进行漏洞管理；

h）除安全接入区外，现场控制区及过程监控区，应禁止接入无线通信的设备。

6.6.4.6 工业控制主机安全防护除符合第三级要求外，还应符合下列要求：

a）应对现场控制区内部署防病毒软件等防止恶意代码攻击的技术措施，对代码特征库定期更新，并应在更新代码前进行测试；

b）对不适宜部署防病毒软件的服务器和客户端，应采用进程白名单管控安全防护技术；列入白名单内的软件进程，应遵循最小化原则；

c）过程监控区内的服务器和操作员终端操作系统，应及时升级系统补丁；

d）现场控制区、过程监控区设备，应通过主机白名单软件对 USB 外设管控，对移动介质的插入、复制、写入等操作安全审计；

e）不应在过程监控区和其他区域之间，交叉使用移动存储介质以及便携计算机；确需通过外设接入的设备，应采取安全监控措施，并履行安全接入审批手续，应在接入前采取病毒查杀等安全预防措施。

6.6.4.7 安全监测和审计除符合第三级要求外，还应符合下列要求：

a）应使用自动化工具，持续对工业控制系统进行安全监视，包括配置管理、系统变更、运行状态和运行环境安全等；

b）过程监控区内应部署工业控制流量审计系统对流量进行审计，应对工业控制协议进行深度包解析，自动识别工业控制设备的通信关系，及时发现隐藏在正常流量中的异常数据包，实时监测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入等异常行为；

c）过程监控区内应部署安全日志审计设备，应对操作系统、数据库、业务应用的重要操作进行记录、分析；远程用户登录本地系统的操作行为，应进行安全审计；

d）应包括对网络运行日志、操作系统运行日志、数据库访问日志、业务应用系统运行日志、安全设施运行日志等集中收集、自动分析、安全审计。

6.6.4.8 数据安全除符合第三级要求外，还应符合下列要求：

a）应识别和建立重要、关键工业控制业务数据清单；

b）应确保静态存储的重要工业控制业务数据，不被非法访问、删除、修改；应采用加密存储或隔离保护，设置访问控制功能；

c）应对动态传输重要工业控制业务数据，进行加密传输进行保护。

6.6.4.9 备份与容灾除符合第三级要求外，还应符合下列要求：

a）应结合自身业务和数据库实际，对生产监控系统的数据备份采取重要性分级管理，并确保重要业务数据至少可恢复至1天前；

b）关键主机设备、网络设备或关键部件，应配置冗余；

c）应定期对关键业务的数据进行备份，实现重要数据备份与恢复；备份系统存储容量，应至少满足12个月存储数据量要求；

d）应定期进行备份数据恢复测试，测试应在测试环境中进行，确保实际备份数据的异机可恢复性，测试过程应做好记录及分析；

e）应加强备份文件的自身安全管控，备份数据文件不应保存在本机磁盘、个人移动存储等存储介质上。

6.7 云与虚拟化扩展安全

6.7.1 第二级要求

云与虚拟化扩展安全应符合GB/T 22239—2019第二级的云计算安全扩展要求。

6.7.2 第三级要求

云与虚拟化扩展安全除符合GB/T 22239—2019第三级的云计算安全扩展要求外，还应符合下列要求：

a）应通过云安全管理平台，对物理和虚拟资源进行安全防护、监测、告警和攻击阻断；

b）应能检测虚拟机之间的资源隔离失效、非授权操作、恶意代码感染和入侵行为等异常，进行告警和管控。

6.7.3 关键信息基础设施安全要求

云与虚拟化扩展安全除符合第三级要求外，还应符合下列要求：

a）云平台应具备身份认证、访问控制、权限控制等功能；

b）应对虚拟机之间、虚拟机与宿主机之间的流量进行监控和访问控制；发现攻击行为，应能告警并阻断；

c）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；应采取密码技术或其他技术手段，防止虚拟机镜像、快照中可能存在敏感资源被非法访问；

d）应采用安全措施，实现虚机主机的防护、隔离、补丁修补和安全加固。

6.8 移动互联扩展安全

6.8.1 第二级要求

移动互联扩展安全应符合GB/T 22239—2019第二级的移动互联安全扩展要求。

6.8.2 第三级要求

移动互联扩展安全除符合GB/T 22239—2019第三级的移动互联安全扩展要求外，还应符合下列要求：

a）应对正式运行的移动应用客户端软件，在入网前进行安全评估检测；

b）宜监测非法移动应用客户端软件；

c）应对移动应用采集的个人相关信息，进行合规管控；

d）应采用统一的认证、加密技术，实现对移动应用的安全保护；

e）应采取网络准入技术，对无线接入设备进行管控。

6.8.3 关键信息基础设施安全要求

移动互联扩展安全应对 APP 在入网前进行隐私保护和漏洞安全检测，通过检测后方可入网。

6.9 物联网扩展安全

6.9.1 第二级要求

物联网扩展安全应符合 GB/T 22239—2019 第二级的物联网安全扩展要求。

6.9.2 第三级要求

物联网扩展安全应符合 GB/T 22239—2019 第三级的物联网安全扩展要求。

6.9.3 关键信息基础设施安全要求

物联网扩展安全采集或监控设备宜采用加密技术确保数据传输的保密性和完整性。

7 安全监测预警能力

7.1 基本要求

安全监测预警能力建设，应根据网络中承载的信息系统状况，按下列要求执行：

a）定级系统均为网络安全等级保护第二级及以下的，应采用第二级安全要求，开展安全监测预警能力建设；

b）定级系统最高等级含有网络安全等级保护第三级的，应采用第三级安全要求，开展安全监测预警能力建设；

c）存在工业控制系统的，应在 a）、b）规定基础上，落实工业控制系统扩展要求；

d）存在关键信息基础设施的，应在 a）、b）规定基础上，落实关键信息基础设施扩展要求；

e）宜建设网络安全威胁感知预警平台；预警平台宜具备安全信息采集、威胁感知、分析展示等功能。

7.2 安全信息采集

7.2.1 第二级安全要求

7.2.1.1 第二级安全要求应满足 GB/T 22239—2019 第二级的安全要求。

7.2.1.2 物理环境信息应满足如下要求：

a）应采集机房基础信息，包括物理位置、周边环境、出入口、电力供应、安防措施等信息；

b）应采集配线间信息，包括物理位置、消防设施、安防措施等信息；

c）应采集机房网络物理链路信息，包括设备连接、线路铺设、配线架部署等信息；

d）应实时采集机房人员出入信息，包括出入时间、所属单位、进入原因等信息；

e）应实时采集机房环境监控信息，包括电力、消防、温度、湿度等信息。

7.2.1.3 资产信息应满足如下要求：

a）应采集网络设备、安全设备信息，包括设备型号、固件版本、物理位置、设备用途、责任单位、责任人等；

b）应采集服务器信息，包括设备型号、操作系统版本、IP 地址/MAC 地址、应用部署、应用访问路径、在用端口、禁用端口、启用服务、中间件版本、数据库版本、安全软件安装情况、

物理位置、设备用途、责任单位、责任人等；

c）应采集存储设备信息，包括设备型号、系统版本、存储容量、物理位置、设备用途、责任单位、责任人等；

d）应采集终端设备信息，包括设备型号、操作系统版本、IP 地址/MAC 地址、安全软件安装情况、物理位置、设备用途、责任单位、责任人等；

e）应采集上位机、PLC 等设备信息，包括设备型号、固件版本、物理位置、设备用途、责任单位、责任人等；

f）应能对物理资产下各个服务进行管理，可对中间件、数据库、其他应用服务进行管理，可结合流量发现资产下的新型服务；

g）可通过 SNMP 获取、流量发现等手段自动发现未知资产的 IP 地址/MAC 地址、服务等情况；

h）可根据 SNMP 获取的资产信息生成网络拓扑。

7.2.1.4 运行状态信息应满足如下要求：

a）应采集网络中所有设备运行状态信息，包括但不限于设备 CPU、内存、存储、网络等利用率；

b）应采集网络中所有数据平台运行状态信息，包括命中率状况、数据库等待事件、共享存储的使用情况、排序使用的情况、登录用户情况、各数据库空间使用信息、segment、表、索引数据库逻辑读和物理读的比例情况、表空间使用情况、表和索引的存储分布情况、数据总线状态等；

c）应采集网络中所有中间件运行状态信息，包括中间件服务状态和基本性能、JVM 使用情况、JMS、JTA、执行队列情况、Web 应用监控、JDBC 连接池、Web 会话等；

d）应采集通用服务运行状态信息，包括能否显示各个系统的登录界面，如提供登录用户，应验证是否能登录；

e）应采集网络运行状态信息，包括网络通断情况、流量占用情况等。

7.2.1.5 脆弱性信息应满足如下要求：

a）应采集网络中所有的漏洞信息，包括漏洞名称、描述、风险级别、演变过程、受影响系统、危害、详细的解决办法和操作步骤等内容；

b）应采集外部厂商的漏洞报告，包括漏洞名称、描述、风险级别、演变过程、危害、详细的解决办法和操作步骤等内容。

7.2.1.6 安全日志信息应满足如下要求：

a）应采集所有网络设备、安全设备的配置变更信息，包括操作单位、操作人员、操作时间、变更原因、影响范围；

b）应采集网络拓扑情况，审批和监控改变网络拓扑的行为；采集信息包括操作单位、操作人员、变更对象、对拓扑变更操作的描述、起止时间等；

c）应实时采集主机病毒、木马查杀情况，且存储时间不应短于 6 个月。

7.2.1.7 网络流量信息应采集网络中主要节点的网络流量信息，包括流量大小、带宽情况、延迟情况、流量故障等。

7.2.2 第三级安全要求

7.2.2.1 第三级安全要求应满足 GB/T 22239—2019 第三级的安全要求。

7.2.2.2 物理环境信息在符合 7.2.1.2 要求基础上，还应满足如下要求：

a）应实时无死角采集机房内部和出入口视频影像、入侵报警信息，自动记录并推送机房入侵报警起止时间、入侵方式、入侵期间的视频影像；

b）应采集现场维护单位、维护人员、陪同人员、维护工具、维护对象信息，包括应用系统与设

备、对维护活动的描述、被转移或替换的设备列表（包括设备标识号、起止时间及现场视频）等信息。

7.2.2.3 资产信息应满足如下要求：

a）应实时采集网络设备信息，包括设备型号、固件版本、运行状态、在用端口、关闭端口、ACL、物理位置、设备用途、责任单位、责任人等；

b）应实时采集安全设备信息，包括设备型号、固件版本、运行状态、安全防护策略、物理位置、设备用途、责任单位、责任人等；

c）应实时采集服务器信息，包括设备型号、操作系统版本、IP 地址/MAC 地址、应用部署、应用访问路径、应用指纹（Web 开发语言、Web 前端框架）、运行状态（CPU 占用、内存占用、硬盘已用/可用容量）、在用端口、禁用端口、启用服务、中间件版本、安全软件安装情况、移动存储介质使用情况、数据库版本、物理位置、设备用途、责任单位、责任人等；

d）应实时采集存储设备信息，包括设备型号、系统版本、运行状态、存储已用容量、存储可用容量、物理位置、设备用途、责任单位、责任人等；

e）应实时采集终端设备信息，包括设备型号、操作系统版本、IP 地址/MAC 地址、安全软件安装情况、运行状态、移动存储介质使用情况、物理位置、设备用途、责任单位、责任人等；

f）应实时采集设备互访权限关系，包括访问路径、访问方式、业务描述等；

g）应实时采集设备运维信息，包括远程维护单位、维护人员、维护工具、维护对象（应用系统、设备等）、对维护活动的描述、起止时间等；

h）应建立动态资产管理库，自动实现资产关联、合并、去重，实时补充和更新资产数据。

7.2.2.4 运行状态信息在符合 7.2.1.4 要求基础上，还应满足如下要求：

a）应实时采集主机用户登录信息，内容包括用户身份、登录时间、注销时间等；

b）应实时采集主机状态信息，包括进程、服务、网络连接、文件变更、远程登录、敏感操作等。

7.2.2.5 脆弱性信息在符合 7.2.1.5 要求基础上，还应满足如下要求：

a）采集操作系统、数据库、中间件等漏洞信息时间间隔不应超过 3 个月，并应建立漏洞清单，漏洞清单应包含漏洞类型、发现时间、责任单位、整改方式、整改时间等信息；

b）采集平台及应用程序漏洞信息时间间隔不应超过 3 个月，并应建立漏洞清单，漏洞清单应包含漏洞类型、发现时间、责任单位、整改方式、整改时间等信息；

c）应通过第三方情报实时采集安全设备、计算设备、网络设备的漏洞信息。

7.2.2.6 安全日志信息在符合 7.2.1.6 要求基础上，还应满足如下要求：

a）应采集应用授权用户登录信息，包括用户身份、登录时间、登录 IP 等，且存储时间不应短于 6 个月；

b）应采集应用实时访问量；

c）应采集应用实时访问源地址。

7.2.2.7 网络流量信息应满足如下要求：

a）应实时采集网络边界和核心节点的网络流量信息，包括 HTTP、UDP、TCP、DNS、POP3、FTP、SSL、SSH 等协议会话的关键数据；

b）应实时采集 IP 资源情况，包括 IP 资源规划、已用 IP、可用 IP 等；

c）应实时采集 VLAN 划分情况；

d）应实时采集端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等信息，记录攻击源 IP、攻击类型、攻击目的、攻击时间等数据，且存储时间不应短于 6 个月；

e）应实时采集网络中所有接入设备的信息，包括设备类型、接入时间、责任单位、责任人等。

7.2.3 工业控制系统扩展要求

工业控制系统扩展应满足如下要求：

a) 应实时采集工业控制系统流量，包括但不限于 OPC、Modbus、Profinet、Ethernet/IP、IEC104 等协议流量；

b) 应实时采集工业控制系统控制器下装、上传、启动、停止等关键操作信息；

c) 应实时采集系统中软件安装及更新信息，并对其进行完整性校验；

d) 对系统平台进行完整性扫描时间间隔不应超过 6 个月，并应重新评估软件、固件和信息的完整性。

7.2.4 关键信息基础设施扩展要求

关键信息基础设施扩展应满足如下要求：

a) 应采集应用程序代码的数字签名，确保后期只有通过签名验证的 APP，才能被安装到终端上；

b) 应采集用户账号的多重并发会话行为，并及时告警；

c) 应实时采集用户的关键操作、重要行为、业务资源使用情况等重要事件，如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作；

d) 应采集系统中使用密钥的生成、发放、更新、注销信息，并进行统一监控、统一管理。

7.3 威胁感知

7.3.1 第三级安全要求

7.3.1.1 威胁感知要求应能对多源数据进行关联分析，准确发现、识别威胁，并对威胁严重性进行定级，满足 GB/T 22239—2019 第三级的安全要求。

7.3.1.2 威胁感知除符合 GB/T 22239—2019 第三级的安全要求外，还应符合下列要求：

a) 应能收集威胁情报，收集来源包括内部网络、终端和部署的安全设备产生的日志数据，订阅的安全厂商、行业组织产生的威胁数据，新闻网站、博客、论坛、社交网等发布的威胁情报；

b) 应实时从国家和地方应急响应组织及有关信息安全主管部门接收安全警报、建议和指示；

c) 应能对文件进行威胁鉴定，判定文件的安全性；

d) 应能发现应用系统的未知风险接口；

e) 应能准确识别漏洞、弱口令等系统风险点；

f) 应能准确识别拖库行为、0day 攻击行为、暴力破解、Web 攻击行为、邮件攻击行为、木马回连、DDOS 攻击、SMB 行为、违规登录行为、恶意 URL 检测、恶意 IP 检测、数据泄露、漏洞利用、主机异常、恶意程序、探测扫描、账号异常、隐蔽信道通信、FTP 异常行为、恶意 DNS 通信等威胁；

g) 应能准确识别攻击工具的种类、数量、方式等信息；

h) 应能准确判断攻击流量及发展趋势；

i) 应准确提供攻击源头的真实 IP 地址、地理位置等信息；

j) 应能准确识别攻击成功的威胁，包括漏洞攻击成功、Web 攻击成功、服务器被上传 Webshell 等；

k) 应能对攻击者的意图、时机、能力、破坏力进行评估；

l) 应能对攻击可能造成的影响进行评估，通过分析和推断对手信息，结合响应措施、漏洞、资产等其他己方信息，持续进行仿真计算，估算攻击造成影响的变化趋势。

7.3.2 用户行为分析

用户行为分析除符合 GB/T 22239—2019 第三级的安全要求外，还应符合下列要求：

a）应基于网络流量、日志记录、审计跟踪记录等数据，对用户行为进行持续自动评估，实时发现内部威胁和有针对的攻击；

b）用户行为分析可采用统计分析、聚类分析、关联规则分析、时序数据挖掘分析等大数据分析技术。

7.3.3 工业控制系统扩展要求

工业控制系统扩展要求除符合 GB/T 22239—2019 第三级的安全要求外，还应符合下列要求：

a）应能准确识别内网渗透威胁，包括渗透路径、起始时间、终止时间、渗透方法等；

b）应能准确识别主机被控威胁，包括控制方式、权限获取情况、影响范围等；

c）应能及时发现控制器的配置更改、代码更改和固件下载等行为，防止控制器出现故障或非授权的中断；

d）应能及时发现针对工业控制系统的攻击行为，包括工业控制器异常指令告警、流量异常告警，工业控制系统的异常登录、非法设备接入、违规外联，以及工业网络攻击事件、工业安全设备预警；

e）应能及时发现工业控制系统中的异常操作，包括工业控制器的异常下装行为、异常开启行为、关闭异常行为、DO 点异常行为、AO 点异常行为等。

7.3.4 关键信息基础设施扩展要求

关键信息基础设施扩展要求除符合 GB/T 22239—2019 第三级的安全要求外，还应符合下列要求：

a）应能准确识别主机被控威胁，包括控制方式、权限获取情况、影响范围等；

b）应能及时发现关键业务的配置变更、流程变更和代码变更等行为，防止出现非授权操作；

c）应能及时发现关键信息基础设施中的异常操作，包括登录行为异常、登录地点异常、操作频率异常、业务流量异常等；

d）应进行风险评估。

8 安全应急响应能力

8.1 应急决策指挥平台

8.1.1 宜建设网络安全应急决策指挥平台，支撑网络安全应急响应。指挥平台宜具备网络安全事件研判分析、事件响应处置、应急预案管理和网络安全设备或系统管理功能，实现网络安全事件的闭环处置。

8.1.2 威胁分析研判应满足如下要求：

a）应对监测到的网络安全隐患及网络安全事件进行数据分析、研判；

b）应提供分析研判可视化功能，支持从资产信息、漏洞信息、历史访问、攻击 IP 信息、攻击溯源、原始浏览日志、攻击载荷、算法模型溯源、相关网络安全设备日志等角度展示网络安全事件全貌，支持各类信息的深入溯源；

c）应通过研判分析，进行事件的真实性和紧急性确定，确认事件处理的网络安全运营负责人与业务负责人等信息。

8.1.3 事件响应处置应满足如下要求：

a）通过威胁分析研判，可对威胁感知系统发现的网络攻击、内部漏洞等网络安全事件进行全过程的管理，包括事件发现、分析研判、事件确定、指挥处置、溯源分析、策略优化等过程，形成网络安全待处理任务；

b）可进行资产、联系人、信息系统、事件类型等多角度的合并编辑，支持自定义的优先忽略等操作；

c）可对发现的安全事件的处置过程做全流程展示；

d）宜对发现的网络安全事件进行总结，形成知识库。

8.1.4 应急预案管理宜满足如下要求：

a）宜实现网络安全应急预案的电子化管理，为网络安全事件设定对应的应急预案；

b）宜与网络安全处置脚本保持联动；

c）可根据各类分析处置任务脚本，进行网络安全事件应急预案的自定义编排。

8.1.5 综合展示应满足如下要求：

a）宜以GIS地图、网络拓扑图等数据为基础，以饼状图、雷达图、热力图、漏斗图等多种可视化方式进行前端展示，直观展示网络安全态势、漏洞安全态势、威胁安全态势、安全事件安全态势；

b）可通过自定义的方式对显示进行编辑，支持调用大数据平台的分析结果作为大屏展示的数据源；

c）宜针对网络内重要的信息系统，以资产、威胁、事件等多角度进行全面的安全展示。

8.1.6 网络安全设备统一管理应满足如下要求：

a）可对防火墙、WAF、上网行为管理等网络安全设备进行统一管理；

b）可通过接口与网络安全设备进行对接，提供管理入口功能，支持不直连设备的情况下对设备进行配置管理；

c）可支持网络设备配置核查功能，及时发现网络安全设备因配置不合理导致的安全隐患，支持预置的核查模板检查和用户自定义核查模板检查。

8.1.7 通知通报应满足如下要求：

a）可支持多用户对网络安全事件的协同分析，可将分析信息和相关数据在多用户之间进行交换和集中展示；

b）可将网络安全事件信息第一时间自动发送给业务负责人、网络安全运营人员、网络安全责任人等，并将相关更新信息同步发送直至事件处置结束。

8.1.8 安全管理中心应满足如下要求：

a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；

c）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计，并应对这些操作进行审计；

d）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理；根据安全审计策略，对审计记录进行存储、管理和查询等；

e）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

f）应通过安全管理员对用户权限进行分配，保管所有除系统管理员以外的所有用户的ID标志符文件，查看用户审计日志以及审计管理员日志，但不能增删改日志内容。

8.2 应急预案

应急预案应满足如下要求：

a）应根据《水利网络安全事件应急预案》要求，制定或修订网络安全事件应急预案或实施细则。

b）网络安全事件应急预案中应明确事件应急组织职责、事件分级分类及应急响应流程，并满足以下要求：

1）应说明组织体系与职责；

2）应确立组织范围内的预警分级、预警监测、预警研判和发布、预警响应、预警解除等流程；

3）应对事件报告、应急响应、应急结束等程序做出规定；

4）应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施；

5）应对日常管理、预案演练、宣传与培训、重要敏感期的预防控制等进行规划；

6）应落实技术支撑队伍、技术保障单位、技术专家队伍、社会资源、信息共享与合作、经费等应急保障资源。

c）应对网络安全事件应急预案进行评估。

d）应将网络安全事件应急预案向相关人员、角色或部门进行通报。

e）应定期评估修订网络安全事件应急预案；当管理架构、信息系统或运行环境发生变更时，应及时更新网络安全事件应急预案。

f）当系统发生变更或在实施、执行、测试中遇到问题时，应及时修改网络安全事件应急预案并向相关人员、角色或部门及用户进行通报。

g）应防止网络安全事件应急预案非授权泄露和更改。

h）在发生安全事件时，应确保应急响应计划的实施能维持信息系统的基本业务功能，并最终完全恢复信息系统且不减弱原来的安全措施。

i）应指定专门的网络安全应急支撑队伍、专家队伍，保障网络安全事件得到及时有效处置。

8.3 应急演练

应急演练应满足如下要求：

a）每年应制定或修订应急演练计划；

b）每年应执行应急演练计划，并在演练开始前通知用户和相关部门；

c）应与水利网络安全工作部门和其他有关部门（如应急响应组织）进行沟通协调，为应急演练提供保障条件；

d）应记录和核查应急演练结果，并根据需要修正应急响应计划；

e）应保存演练记录、演练总结报告等；

f）应将信息系统备份及恢复能力列入应急演练计划，包括检验备份及恢复的可靠性和信息完整性；

g）应在替代的处理场所演练应急计划，使应急人员熟悉设施和可用资源，以评价该场所支持应急运行的能力；

h）应将全面恢复和重构信息系统到已知状态，作为应急演练计划的一部分。

注：应急演练流程可参见附录 B.1、B.2。

8.4 应急资源

应急资源应满足如下要求：

a）应落实事件处理所需的各类资源，为用户处理、报告安全事件提供咨询和帮助；

b）应使用自动机制，为事件处理提供进一步的资源支持；
c）应在事件处理部门和外部网络安全组织之间建立直接合作关系，能在必要时获得外部组织的协助。

8.5 应急恢复能力

8.5.1 应急恢复能力应按照 GB/T 20988—2007 等标准，制定灾难恢复计划，确保网络安全保护对象（含水利关键信息基础设施）能及时从网络安全事件中恢复。

8.5.2 统一容灾备份应满足如下要求：
a）应按照 GB/T 20988—2007 中第 3 级及以上灾难恢复能力的要求，选择灾难备份中心，避免灾难备份中心与主中心同时遭受同类风险（包括同城和异地两种类型），以规避不同影响范围的灾难风险；
b）应控制灾难备份中心位置信息的知悉范围；
c）应实现对重要系统和数据库进行容灾备份，完全数据备份至少每天 1 次；可在 1 天内多次利用通信网络，将关键数据定时批量传送至备用场地；
d）建设灾难备份中心，计算机机房应符合 GB/T 50174—2017 的要求，工作辅助设施和生活设施，应符合灾难恢复目标的要求；
e）灾难备份中心应提供与主场所同等的网络安全措施；
f）灾难备份中心应位于中华人民共和国境内。

8.5.3 恢复和重构应满足如下要求：
a）在信息系统遭到破坏或发生故障后，应及时恢复信息系统业务功能；
b）根据数据的重要性和数据对系统运行的影响，应制定数据的备份策略和恢复策略、备份流程和恢复流程等；
c）应为信息系统中基于事务的系统（如数据库管理系统和事务处理系统等）执行事务恢复，包括事务回滚、事务日志等；
d）应具有在指定的恢复时间内，根据完整性得到保护的磁盘映像，重构信息系统部件的功能。

8.5.4 业务连续性应满足如下要求：
a）应制定并实施业务连续性计划，确保业务的核心支撑能力在重大网络安全事件中不受到明显影响，支持业务稳定、持续运行；
b）应设置重要系统和数据处理设施冗余，满足系统可用性要求；
c）应确保水利关键信息基础设施必要时有能力应用备用协议以保障业务连续性；
d）应将网络安全连续性纳入业务连续性管理之中，确保在不利情况下，网络安全连续性达到要求的级别。

9 安全运营

9.1 基本要求

9.1.1 运营架构

安全运营应建立在纵深防御、监测预警、决策指挥等安全技术要素基础之上，应在运营中实现对各类安全资源的管理控制，使其发挥应有的作用。应从威胁预防、威胁防护、安全监测、响应处置等方面，建立闭环的安全运营体系。

9.1.2 三权分立

应对各类安全设备、安全系统、安全资源建立系统管理员、审计管理员、安全管理员账户，并赋

予相应权限。

9.1.3 运营体系

应参考图 3 对各类网络安全事件的运营活动制订符合实际的体系流程，宜在实际工作中向智能化、标准化方向发展。

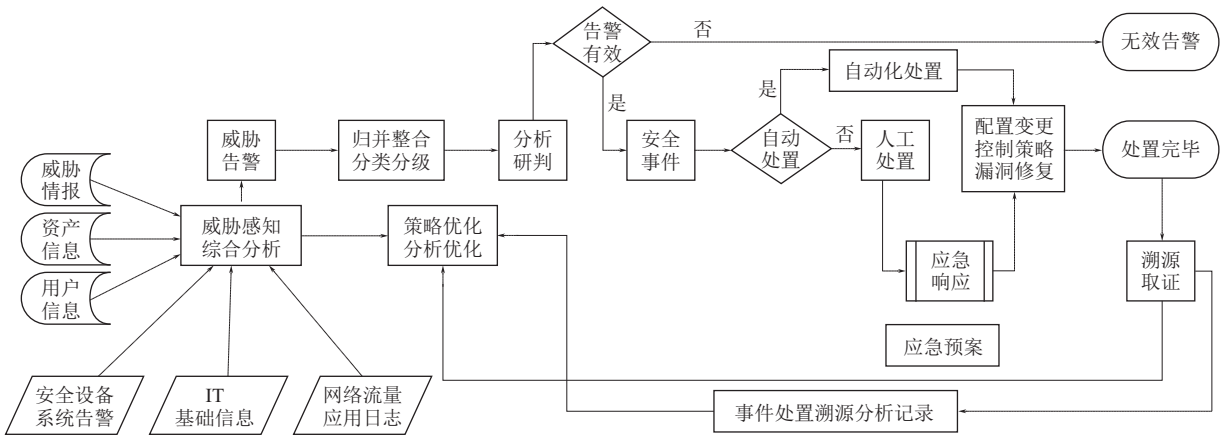

图 3　安全运营流程示例

9.2 运营要素

9.2.1 威胁防护

威胁防护应满足如下要求：

a) 安全基线：应从事件预防的角度，对主机系统、网络设备、业务应用的安全基线进行评估，对存在的安全风险，进行安全加固；

b) 安全运维：应开展安全产品和系统运行维护、安全审计日志分析及配置备份更新等，保障安全产品高效可靠地运行；

c) 策略优化：应基于预测及安全基线评估中发现的网络安全策略不足，针对性优化提升防护能力，对访问控制进行优化，增强访问控制、杜绝越权访问；

d) 全面审计：宜不断优化提升审计手段与审计内容，实现全面覆盖；

e) 安全评估：宜开展系统上线前及运行中周期性安全评估，通过代码检测、渗透测试、漏洞检测发现系统中存在的安全风险。

9.2.2 安全监测

安全监测应满足如下要求：

a) 应持续开展应用失陷检测，发现存在的各类漏洞并进行验证，经确认后及时整改；

b) 宜通过威胁感知对内部失陷、内部攻击、内部违规、外部攻击等行为进行事件研判分析，及时制止攻击行为，提高防护策略；

c) 应通过对终端安全分析发现账户安全、恶意文件、邮件病毒、APT、非法外联等事件，快速验证并进行改进；

d) 宜不断优化安全信息采集，采集各类安全告警、审计数据、网络流量等，进行标准化、丰富化处理；

e) 宜不断优化安全监测预警，利用关联分析、机器学习的行为分析、虚拟执行、情景分析，发现异常违规及可疑攻击，及时产生告警，并通过人工及风险识别工具进行风险评估；

f）应开展安全事件实时通报，按周、月、年或突发事件等维度，对安全事件进行通报，保障信息及时传达；对特殊安全事件，应制定相应安全应对方案。

9.2.3 响应处置

响应处置应满足如下要求：

a）应从事件控制的角度，对出现的安全事件，基于应急决策指挥系统展开安全事件研判分析，为安全应急响应提供决策依据，对重大安全事件，应直接按照应急预案启动应急响应；

b）应利用决策指挥平台，对告警进行人工综合分析判断，消除无效告警，确定真实告警事件，形成处置工单；

c）安全应急响应处置时，应进行抑制、清除、恢复等动作并形成处置报告，对真实告警事件，视分析研判结果，通过决策指挥平台进行自动化处置或通过通报流程进行人工处置，同时进行溯源和取证。

9.2.4 威胁预防

威胁预防应满足如下要求：

a）应从攻击预测的角度进行资产发现，梳理基础设备信息、基础设备开放端口信息、基础设备部署应用类型等，掌握信息资产运行情况；

b）应通过威胁情报收集安全漏洞、风险预警等信息，经审核验证确认后，应及时推送给相关用户，实现安全威胁预警；

c）在重大会议等活动时期前应加强开展主机、网络、应用、终端的安全检查，发现问题及时整改，并在重要时期安排技术人员安全值守保障全程安全；

d）在重大会议等活动时期前宜开展攻防演练、渗透测试等演练，检验安全技术、管理、运营体系的健壮性，应对重点时期安全保障要求；

e）在实际运营活动中，应不断优化分析研判支撑能力，引入相关的分析数据源；

f）在实际运营活动中，应在应急预案管理、应急演练、综合研判等方面不断优化应急决策指挥系统。

10 安全监督检查

10.1 监督检查内容

网络安全监督检查内容宜包括：责任落实及制度建立情况、日常管理情况、信息系统等级保护落实情况、安全运维管理情况、应急及安全培训情况、门户网站安全情况、网络及数据安全的防护情况、终端安全防护情况等。

10.2 监督检查方法

监督检查可采用攻防演练、渗透测试、在线监测、现场检查等方式，进行水利网络安全监督检查。

10.3 监督检查风险防控

监督检查风险防控应包括以下内容：

a）在监督检查实施过程中，应对实施人员进行身份背景、专业资格和资质的审查；应使用经相关部门认证和认可的专业工具，具有相应的过程控制规程和质量保证；

b）应与监督检查实施人员签署保密协议，对监督检查工作中产生的过程数据和结果数据严格保

密，未经授权不应泄露和利用；

c）应在与被检查方约定的监督检查范围和检查内容内进行全面检查；

d）应降低对被检查方网络安全保护对象正常运行可能造成的影响或干扰。

10.4 关键信息基础设施增强要求

10.4.1 自查关键信息基础设施自查应满足下列要求：

a）应自行或委托网络安全服务机构对关键信息基础设施的安全性每年进行至少1次安全评估。

b）应从合规检查、技术检测和分析评估3个主要环节开展安全评估。

c）检测内容可包括但不限于网络安全制度落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、安全防护情况、风险评估情况、应急演练情况、网络安全等级保护落实情况等。

d）应根据安全评估情况，对关键信息基础设施进行安全整改，降低风险水平。

e）应编制检测评估报告，内容包括：

1）检查对象基本情况，可包含关键信息基础设施的定义描述、主要核心资产情况、核心业务情况、面临的主要威胁和系统安全能力的描述等；

2）检查评估结果，应对发现的关键信息基础设施存在的主要问题进行分析说明。

f）应将检测评估报告及时发送至关键信息基础设施网络安全保护责任部门。

10.4.2 安全检测应选取关键信息基础设施网络安全保护责任部门认可的网络安全服务机构进行检测评估。信息系统应在检测评估发现的安全问题得到整改后方可上线运行。

10.4.3 安全抽查被抽检方应提供安全风险抽查检测所必需的资料和技术支持，包括网络安全管理制度、网络拓扑图、重要资产清单、关键业务介绍等；应针对抽查检测中发现的安全问题和风险进行及时整改。

注：安全监督检查流程可参见附录B.3、B.4。

附录 A
（资料性）
网络安全区域划分说明

网络区域划分可根据业务系统的保护等级、业务属性、业务功能、数据流量、访问主体和安全风险等综合分析进行划分，具有相同等级、相似的业务属性、同等级数据流向和相似安全风险的业务可划分为同一区域，不同等级、不同业务属性、不同数据流向和访问主体的业务划分成不同区域。网络信息系统可结合实际情况划分为内部业务区、接入区、前置交换区、公众服务区、数据区和安全管理区等。

例如，根据网络接入的边界不同可划分不同的网络接入区，包括互联网接入区、业务网接入区、城域网接入区以及电子政务外网等外联网接入区；根据提供服务类型、用户类型、业务属性等可划分业务服务区，进一步分成互联网服务区（公众服务区）、应用服务区（内部业务区）、数据库服务区（数据区）、视频会议区以及终端区，同时针对不同等级的保护对象应对应用服务区、数据库服务区进一步划分成二级系统区域以及三级系统区域，区域之间应该进行逻辑隔离；满足第三级安全保护要求应独立划分安全管理区；关键信息基础设施可设置独立的网络区域，并与二级、三级系统进行逻辑或物理隔离。

附录 B
（资料性）
检 查 过 程

B.1 攻防演练流程

B.1.1 准备阶段

B.1.1.1 演练组织

攻防演练组成单位一般包括组织单位、攻击单位和防守单位，攻击单位和防守单位由组织单位确定。

组织单位应负责演练总体把控、工作协调、制定规则、过程监督、风险控制、成果评判、问题通报和核查组织，并根据国家网络安全主管部门以及水利部要求进行备案。组织单位应成立演练总指挥部，具体负责攻防演练的组织实施。

攻击单位应根据组织单位授权，组建攻击队伍对演练目标系统进行网络攻击测试。

防守单位应组建防守队伍，对所负责的水利网络安全保护对象进行防护，并对网络攻击进行监测、溯源、处置。

组织单位和攻击单位双方应签署保密协议，攻击队伍成员应签署保密承诺书。

B.1.1.2 确定规模

组织单位应明确演练时长，明确参加演练的攻击单位数量及攻击队伍人数，明确防守单位数量。

B.1.1.3 制定方案

组织单位应制定攻击演练方案，方案的内容宜包括以下内容：

a）演练目标：包括目标系统、交付成果等内容；

b）人员组织：包括组织单位、攻击单位、防守单位等单位成员组成、成员角色与定义、成员职责等内容；

c）时间进度：攻防演练各阶段的时间进度安排；

d）演练规则：包括攻击规则、防守规则、成果评判标准、沟通协调机制、风险控制措施等内容。

B.1.2 实施阶段

B.1.2.1 演练启动

攻防演练应由演练总指挥宣布演练开始。

B.1.2.2 组织单位任务

组织单位应对演练全过程进行监督和评估。应对攻击队伍操作行为、攻击成果进行监督，对防守单位监测预警情况、应急处置情况、被攻击目标的运行状态进行监督。应研判并控制攻击对演练目标及相关水利网络安全保护对象所造成的危害，评估攻击的准确性、有效性，评估防守监测能力、预警响应能力、应急处置能力。

组织单位应建立演练指挥渠道。通过指挥渠道指挥演练活动，接收攻击单位、防守单位等单位的演练成果。

B.1.2.3 攻击单位任务

攻击单位应根据演练规则，组建攻击队伍，在保障演练目标及相关水利网络安全保护对象运

行安全的前提下，采取限制攻击目标、不限攻击路径的方式，利用演练目标及相关水利网络安全保护对象的安全防护薄弱环节，进行真实环境下有组织的网络攻击测试。攻击不应采用 DDoS 攻击、恶意蠕虫攻击等行为。攻击单位应通过演练指挥渠道及时向组织单位上报攻击成果。

B. 1. 2. 4　防守单位任务

防守单位应根据演练规则，以日常安全运维为基础组建防守队伍，明确分工及职责，以实战思维强化安全防护措施，完善监测预警，加强应急处置。防守单位应通过演练指挥渠道及时向组织单位上报防守成果。

B. 1. 2. 5　演练终止

根据演练方案，由总指挥部宣布演练结束，所有人员停止演练活动。

演练实施过程中，在出现突发情况时，总指挥部可以提前或暂时终止演练，包括：

a）出现真实突发事件，需要参演人员参与应急处置；

b）出现特殊意外情况，短时间内不能妥善解决。

B. 1. 3　总结阶段

演练结束，演练参与各方应及时进行总结评估。

组织单位应对攻击成果、防守成果及所有演练活动进行评估，对演练进行系统和全面的总结。演练总结报告宜包括：演练目的、时间和地点、演练范围、演练组织情况、攻击成果分析、防守成果分析、演练方案概要、发现的问题及原因分析、意见和建议等内容。

攻击单位应对整个演练活动的攻击组织情况、攻击技战法、攻击成果进行梳理，提出合理的整改建议，形成总结报告并上报组织单位。报告内容宜包括：攻击测试目的、测试范围、测试时间、实施流程、攻击队伍成员情况、攻击手段、风险漏洞及整改建议、成果汇总分析、问题及建议等内容。

防守单位应对整个演练活动的防守组织情况、防守技战法、防守成果进行梳理，形成总结报告并上报组织单位。报告内容宜包括：防守目的、时间和地点、防守范围、应急预案、防守队伍成员情况、防守措施、防守成果、汇总分析、问题及建设等内容。

B. 1. 4　成果运用

组织单位应对演练暴露出来的风险漏洞进行整理分析，提出整改建议，并根据《水利网络安全信息通报工作规范》要求，通报相关单位限期整改。相关单位应及时采取有效措施予以整改，并反馈整改情况。组织单位应要求攻击单位对相关单位整改情况进行核查。

B. 2　渗透测试流程

B. 2. 1　准备阶段

B. 2. 1. 1　明确职责

渗透测试组成单位一般包括组织单位、测试单位和被测试单位，测试单位和被测试单位由组织单位确定。

组织单位应负责渗透测试的总体把控、工作协调、过程监督、风险控制、成果评判、问题通报和核查组织，并根据国家网络安全主管部门以及水利部要求进行备案。

测试单位应根据组织单位授权，组建测试队伍对测试目标自身存在的可利用漏洞进行渗透。

采用白盒测试时，被测试单位应协助完成测试目标的漏洞挖掘，采用黑盒测试时，不要求被测试

单位协助。

组织单位和测试单位双方应签署保密协议，测试队伍成员应签署保密承诺书。

B.2.1.2 确定规模

组织单位应明确测试时长，明确测试单位数量及测试队伍人数，明确计划测试的水利网络安全保护对象数量及相关单位数量。

B.2.1.3 制定方案

组织单位应指定渗透测试方案，方案的内容宜包括以下内容：

a）渗透目标：包括测试范围、交付成果等内容；

b）实施组织：包括组织单位、测试单位、被测试单位等单位成员组成、成员角色与定义、成员职责等内容；

c）时间进度：包括渗透测试各阶段的时间进度安排等内容；

d）测试规则：包括测试方式、风险控制措施等内容。

B.2.2 实施阶段

B.2.2.1 组织单位任务

组织单位应对渗透测试全过程进行监督。应对测试队伍操作行为、渗透成果进行监督。应研判并控制测试对测试目标及相关水利网络安全保护对象所造成的危害。

B.2.2.2 测试单位任务

测试单位应组建攻击队伍，在受约束的测试路径与测试范围内，采用自动化及手工测试方法相结合的方式，发现测试目标自身存在的脆弱性及安全风险。

B.2.2.3 被测试单位任务

测试方式为白盒测试时，被测试单位应提供测试目标相关资料，包括网络拓扑、接口文档、代码等，配合完成指定为测试目标的水利网络安全保护对象的漏洞挖掘。测试方式为黑盒测试时，渗透测试将在不通知被测试单位的情况下完成。

B.2.2.4 测试终止

根据渗透测试方案，完成所有渗透测试任务后，所有人员停止渗透活动。

实施过程中，出现突发情况时，组织单位可以提前或暂时终止渗透，包括：

a）出现真实突发事件，需要被测试单位人员参与应急处置；

b）出现特殊意外情况，短时间内不能妥善解决。

B.2.3 总结阶段

组织单位应对测试成果及所有渗透测试活动进行评估，对渗透测试进行系统和全面的总结。测试总结报告的内容包括：测试目的、时间和地点、测试范围、测试方式、测试组织情况、成果分析、发现的问题及原因分析、意见和建议等。

测试单位应对整个渗透测试活动的组织情况、测试成果进行梳理，提出合理的整改建议，形成总结报告并上报组织单位。报告内容包括：攻击测试目的、测试范围、测试时间、实施流程、测试队伍成员情况、测试方法、风险漏洞及整改建议、成果汇总分析、问题及建议等。

B.2.4 成果运用

组织单位应对渗透测试暴露出来的风险漏洞进行整理分析，提出整改建议，并根据《水利网络安全信息通报工作规范》要求，通报相关单位限期整改。相关单位应及时采取有效措施予以整改，并反馈整改情况。组织单位应对整改情况进行核查。

B.3 现场检查流程

B.3.1 前期准备

在监督检查活动正式实施前做好前期准备，包括：

a）确定监督检查的目标；

b）确定监督检查的范围；

c）组建监督检查管理与实施团队；

d）开展前期系统调研。

B.3.2 确定范围

监督检查范围可以是一个单位整体网络安全情况，也可以一个具体的水利网络安全保护对象网络安全情况；可以是技术方面情况，也可以是管理方面情况。

B.3.3 组建团队

组织单位组建包括管理层、相关业务骨干、IT 技术工程师等人员的监督检查实施小组，设立负责人 1 名。必要时，可组建由监督检查方、被检查方领导和相关部门负责人参加的监督检查领导小组，或聘请相关专业的技术专家和技术骨干组成专家小组。

监督检查实施小组应做好评估前的表格、文档、检测工具等各项准备工作，开展网络安全检查实施工作的技术培训和保密教育，制定监督检查实施过程管理的相关规定。可根据被检查方要求，双方签署保密协议，或适情签署个人保密承诺书。

B.3.4 系统调研

监督检查小组应进行充分的系统调研，确定监督检查依据、方法和检查内容。调研内容至少应包括：

a）主要业务功能、业务范围和业务流程；

b）网络结构与网络区域划分，包括内部连接和外部连接；

c）系统边界，与其他系统的连接情况；

d）主要的软硬件资产；

e）系统和数据的敏感性；

f）维护和使用系统的人员；

g）管理制度、操作规程等文档。

系统调研采取问卷调查为主、现场访谈为辅的方式进行，在问卷调查不能完全达到系统调研目的的情况下，可结合现场访谈的方式进行。

B.3.5 确定依据

根据前期的系统调研结果，并依据业务实施对系统安全运行的需求，确定监督检查的依据和方法，使之能够与被检查对象的环境和安全要求相适应。监督检查依据包括（但不仅限于）：

a）国家法律、法规及有关规定；
b）现有国家标准、行业标准、地方标准、团体标准和企业标准等；
c）行业主管部门针对业务系统制定的要求和规定；
d）系统的安全保护等级要求；
e）系统互联单位的安全要求；
f）系统本身的实时性或性能要求等。

B.3.6 制定方案

监督检查小组应制定监督检查方案，方案的内容宜包括以下内容：
a）安全检查计划：监督检查各阶段的具体检查计划，包括检查目标、检查内容、检查范围、检查形式、检查交付成果等内容；
b）实施团队组织：包括监督检查团队成员组成、成员角色与定义、成员职责等内；
c）时间进度安排：监督检查工作实施的时间进度安排。

B.3.7 明确任务

将监督检查实施方案及时向监督检查实施小组的所有人员进行传达，明确相关人员在监督检查实施过程中的任务和责任，并就监督检查的相关内容开展培训和保密教育。

B.3.8 现场检查

B.3.8.1 首次会议

在现场检查正式实施前，检查实施方与被检查方应共同召开本次监督检查工作的首次会议。在首次会议上，监督检查方的项目负责人根据前期所确定的检查实施方案，介绍监督检查工作的大体流程、检查的目的与范围、检查工作的实施方法、工作交付成果等信息，与被检查方确认检查实施时间和检查计划、人员配合与沟通渠道，并向被检查方提供询问的机会，使与会人员能够对即将开始的监督检查工作有一个清晰、全面的认识。

B.3.8.2 检查实施

在现场检查的实施过程中，结合人员访谈、现场观察、实地查验、配置核查、文档审查、工具扫描等方式，监督检查人员应按照检查内容和检查条款进行逐项检查，对照被检查系统的实际安全状况如实、准确填写检查结果，形成检查结果原始记录，为后续的结果分析做准备。

B.3.8.3 过程控制

监督检查实施小组成员应严格按照监督检查方案和实施计划开展现场检查工作。必要时，为了更好地达到检查目的或适应实际环境变化的需求，可适当调整检查计划，及时告知被检查方，并与相关人员进行商榷，直到得到相关人员的认同。监督检查项目负责人应及时与被检查方的相关人员交换意见，对已收集获取的检查证据进行确认。对于被检查方存有异议的检查结果，应采取检查核对的方法进行再次确认。当收集到的检查证据不能达到检查目的时，应及时向被检查方报告理由，并商定相应的解决措施，包括调整检查计划，以及改变检查目的、检查范围等。

B.3.8.4 末次会议

在完成现场检查实施后，检查方与被检查方应共同召开本次监督检查工作的末次会议，除参与首次会议的各方人员外，与会人员还包括监督检查实施过程中被访谈对象、被调查对象以及其他相关参

与人员。在末次会议上，监督检查方的负责人根据现场检查的实施情况，向被检查方反馈监督检查中发现的具体问题和整体检查结果。

B.3.9 后期分析

检查方应根据现场收集获取的信息和检查结果原始记录，对被查系统的实际安全管理情况进行梳理和汇总，分析被检查系统的网络安全威胁和风险情况，评估其是否存在严重安全隐患，根据检查分析评估结果形成检查结论。

B.3.10 报告编制

检查方应在规定时间内编制完成监督检查报告，并反馈给被检查方。对监督检查过程中发现的共性问题，监督检查机构应及时通报行业主管部门，并协助其开展网络安全管理咨询、业务培训及安全整改工作。网络安全管理监督检查报告应清晰、准确、客观地给出监督检查的实施情况、检查结果和相关内容，说明被检查系统存在的安全隐患和缺陷，并给出改进建议。

安全管理监督检查报告至少应包含以下内容：检查系统名称；系统主管部门；检查时间和地点；监督检查依据；监督检查结论；报告编制人；报告审核人；报告批准人；检查结果汇总表；安全整改建议；检查实施机构的公章。

B.3.11 安全整改

监督检查发现存在安全隐患的，其主管、运维或使用单位应尽快组织实施安全整改工作，并及时向信息化主管部门及行业主管部门报告整改情况。对存在重大安全隐患的重点领域系统，通知被检查单位立即采取防护措施实施安全整改。监督检查方应及时对其安全整改情况进行复查，对已采取的安全整改措施应进一步考虑是否引入新的安全问题并进行检查和分析，督促其改进和完善信息安全管理技术措施。对于安全整改实施不到位的，要求被检查方继续进行安全整改。检查方通过现场检查和后期分析后确认被检查方网络安全不存在安全隐患的，或经安全整改后确认被检查方网络安全风险在可控范围内的，结束监督检查工作。

B.4 在线监测流程

B.4.1 准备阶段

B.4.1.1 明确职责

在线监测组成单位一般包括组织单位、监测单位和被监测单位，监测单位和被监测单位由组织单位确定。

组织单位应负责在线监测的总体把控、工作协调、过程监督、问题通报和核查组织。

B.4.1.2 确定范围

组织单位应明确在线监测范围，包括被监测单位、被监测系统域名或IP地址。

B.4.2 实施阶段

B.4.2.1 工作流程

监测单位应采用专用监测设备，对监测范围内的系统实行7×24小时不间断的监测，对于监测发现的问题，应由监测单位安排专人进行人工验证，并在确认后通知组织单位。

B.4.2.2 监测内容

监测内容宜包括以下内容：

a）系统可用性：包括系统首页访问时间、断网时间、DNS 解析时间等内容；

b）系统漏洞：包括系统 SQL 注入、跨站脚本、信息泄露、目录遍历等漏洞；

c）系统安全事件：包括挂马、篡改、暗链、敏感信息等安全事件。

B.4.3 成果运用

组织单位应根据《水利网络安全信息通报工作规范》要求，及时将在线监测发现的安全风险通报相关单位并限期整改。相关单位应及时采取有效措施予以整改，并反馈整改情况。组织单位应对整改情况进行核查。