目　次

前　言 **1**

1　范围 **3**

2　规范性引用文件 **3**

3　术语与缩略语 **3**

4　总体要求 **6**

4.1 一般要求 6

4.2 同步要求 7

4.3 通用要求 8

4.4 水利关键信息基础设施增强通用要求 8

5　安全技术体系框架 **9**

5.1 建设要求 9

5.2 体系结构 11

5.3 技术架构 13

6　安全纵深防御能力建设要求 **14**

6.1 安全物理环境 14

6.2 安全通信网络 17

6.3 安全区域边界 18

6.4 安全计算环境 22

6.5 工控系统扩展安全 27

7　监测预警能力建设要求 **32**

7.1 安全信息采集 32

7.2 威胁感知 35

7.3 工控系统扩展要求 35

7.4 关键信息基础设施扩展要求 36

8 安全应急响应能力建设要求 36

8.1 应急决策与指挥系统建设 36

8.2 安全集中管控 39

8.3 应急预案 39

8.4 应急演练 40

8.5 应急资源 41

8.6 应急灾备能力 41

9 安全运营能力建设要求 42

9.1 基本要求 42

9.2 运营要素 43

10 安全监督检查要求 46

10.1 监督检查方法 46

10.2 监督检查原则 46

10.3 监督检查流程 47

10.4 关键信息基础设施增强要求 51

附录 1 建设示例 53

1.1 信息系统建设示例 53

1.2 工控系统建设示例 55

前　言

本标准是水利技术标准体系中的水利信息化标准之一。根据水利部水利行业标准制定计划，按照《标准化工作导则 第1部分：标准的结构和编写》（GB/T 1.1-2009）的要求编制。

本标准共10章，其主要技术内容包括：

—总体要求；

—安全技术体系框架；

—安全纵深防御建设要求；

—安全监测预警能力建设要求；

—安全应急响应能力建设要求；

—安全运营能力建设要求；

—安全监督检查要求。

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：**水利部海河水利委员会水利信息网络中心**

本标准出版单位：

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：

本标准体例格式审查人：

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。

水利网络与信息安全建设技术规范

1 范围

本标准规定了水利网络与信息安全建设技术总体要求、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、安全运营能力建设要求和安全监督检查要求。

本标准适用于水利信息系统(包括水利关键信息基础设施）网络安全技术体系规划、设计、建设、运行管理和监督检查。

2 规范性引用文件

下列文件对于本标准的引用是必不可少的。凡是注日期的引用文件，注明日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 25070 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 信息安全技术 网络安全等级保护测评要求

GB/T 28449 信息安全技术 网络安全等级保护测评过程指南

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 32919 信息安全技术 工业控制系统安全控制应用指南

3 术语与缩略语

GB/T 32919、GB/T 25069 界定的下列术语和定义适用于本标准

3.1

水利网络安全保护对象

由计算机或者其他信息终端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。

注：水利网络安全保护对象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。

3.2

水利关键信息基础设施 water conservancy 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。

注：水利关键信息基础设施可以是大型水利枢纽、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。

3.3

工业控制系统 industrial control system

工业控制系统(ICS) 是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统(SCADA)、分布式控制系统(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。

3.4

安全保护能力 security protection ability

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程度。

3.5

安全计算环境 Secure 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。安全计算环境按照保护能力划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。

3.6

安全区域边界 safe 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。安全区域边界按照保护能力划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。

3.7

安全通信网络 secure 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。安全通信网络按照保护能力划分第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。

3.8

安全管理中心 security operation 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。第二级及第二级以上的定级系统安全保护环境需要设置安全管理中心，称为第二级安全管理中心、第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。

3.9

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。

3.10

漏洞/脆弱性 vulnerability

在信息系统、系统安全程序、管理控制、物理设计、内部控制或实现中的，可能被攻击者利用来获得未授权的信息或破坏关键处理的弱点。

3.11

风险评估 risk assessment

一个评估过程，针对安全性以及对安全和可靠操作的连续性造成风险的安全问题。

3.12

安全等级保护测评 evaluation for security classified protection

安全等级保护测评（以下简称“等级测评”）是指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和计算标准，对未涉及国家秘密的等级保护对象进行安全等级保护状况进行检测评估的活动。等级测评是标准符合性评判活动，即依据信息安全等级保护的国家标准或行业标准，按照特定方法对等级保护对象的安全保护能力进行科学公正的综合评判过程。

3.13

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

是指基于威胁情报态势感知的不同层级信息进行应急响应。这包括应急决策指挥、综合展示和集中管理控制平台等内容。

下列缩略语适用于本标准。

DDoS: 拒绝服务(Distributed Denial of Service)

ICS: 工业控制系统(Industrial Control System)

PLC: 可编程逻辑控制器(P rogrammable L ogic Controller)

USB: 通用串行总线(Universal Serial Bus)

4 总体要求

4.1 一般要求

4.1.1 使用约定

本标准只是对水利网络安全体系框架和基本技术要求进行约定，而不是完整的水利网络安全体系建设方案。各单位在进行网络安全建设时，应依据本标准要求，结合各自信息

系统等级等实际情况，进行网络安全体系的规划、设计、建设及运行维护。

4.1.2 合规完整

在依照本标准进行水利网络安全建设时，应同时满足相关法律法规和国家标准的要求，按照网络安全等级保护标准要求，进行定级、备案、测评、整改等工作，网络安全体系架构应结构完整，全面覆盖所有安全要素。

4.1.3 适当调整

根据具体网络支撑环境和信息系统的特点，可适当调整部分安全要素要求。

4.1.4 持续更新

网络安全体系建设是一个逐步完善的过程，各单位应依据本标准进行统一规划，在建设时可根据本单位实际逐步建设、逐步完善。

4.1.5 自主可控

在水利网络安全建设过程中，在满足合规合法基本上，应优先采用成熟和自主可控产品，提高信息化基础设施的安全防护能力。

4.1.6 密码应用

在水利网络安全建设过程中，应充分考虑使用密码技术对数据传输存储等过程进行保护。

4.2 同步要求

4.2.1 全过程贯穿

网络安全建设应该贯穿于水利信息系统建设的全过程，确保网络安全与信息化建设项目同步规划、同步建设、同步运行。

4.2.2 规划设计

在水利网络安全建设中要分析水利信息系统的网络安全需求，参照本标准进行相关规划与设计。

4.2.3 建设验收

在水利信息系统建设完成后，应将网络安全作为水利关键信息基础设施验收的重要内容。

4.2.4 安全运行

在水利信息系统运行期间要切实将网络安全内容同步运行，全面及时的对信息系统运行进行防护，在信息系统及其运行环境发生明显变化时，评估其风险，及时对安全设施进行变更管理。

4.3 通用要求

4.3.1 计算设备安全

应优先选用自主可控的服务器、可编程逻辑控制器 PLC、嵌入式控制器 MCU、终端等计算设备，并根据需要进行计算设备安全评估。

4.3.2 计算软件安全

应优先选用自主可控的操作系统、PLC 系统、组态软件、应用软件等计算设备，并根据需要进行计算软件安全评估。

4.3.3 加密保护

对关键软硬件设备应采用密码技术进行加密保护。

4.3.4 安全服务

应与软硬件设备提供者签订安全保密协议并约定其为产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

4.3.5 容灾备份

系统和数据应具备容灾备份措施，定期进行备份恢复演练。

4.4 水利关键信息基础设施增强通用要求

4.4.1 计算设备安全

应优先选用自主可控的服务器、可编程逻辑控制器 PLC、嵌入式控制器 MCU、终端等计算设备，并对重要计算设备进行安全评估。

4.4.2 计算软件安全

应优先选用自主可控的操作系统、PLC 系统、组态软件、应用软件等计算设备，并对重要计算软件安全评估。

4.4.3 可信验证

应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入的网络设备真实可信。

4.4.4 协议安全

应采用具备安全加密校验机制的通信协议，禁止采用全透明或开放式协议。

4.4.5 认证检测

关键设备和安全专用产品应当按照相关国家标准的强制性要求，采用安全认证合格或者安全检测的产品。

所有硬件产品应采用符合运行环境要求的产品，采用相应级别产品或进行检测验证。

4.4.6 基础环境

一般应按不低于第三级系统安全保护环境进行设计实施，严格安全计算环境、安全区域边界、安全通信网络。

4.4.7 容灾备份

系统和数据应具备异地容灾备份措施，定期进行备份恢复演练。

5 安全技术体系框架

5.1 建设要求

5.1.1 体系组成

以智慧水利涉及的信息系统与关键信息基础设施为安全防护对象，开展行业网络安全纵深防御基础能力、网络安全监测预警能力、网络安全应急响应能力建设。建立行业各层级网络安全运营体系，实现闭环网络安全运营。

各级水利单位在网络安全体系建设中的重点不同。市县级水行政部门和中小型工程单位主要应做好本单位内部或辖区范围内的三层基础防护；流域机构、省级水行政部门、大型（重要）中型水利工程单位应在为流域省区工程单位区域网络提供统一安全服务的基础上做好网内数据分析，构建流域省级的威胁感知预警和应急决策指挥平台；水利部应在做好部本级的网络安全保护环境基础上，构建行业级的威胁感知预警和应急决策指挥平台，形成行业级网络安全运行管理中心。

5.1.2 水利部体系

水利部应建设网络安全情报服务、本地异地灾备服务、统一密码服务、统一身份认证

服务，提供给本级单位及各级行业单位共享使用。

水利部应以不低于三级等保要求开展安全计算环境、安全区域边界、安全通信网络等方面的安全保护环境达标建设，并对关键信息基础设施采取措施进行重点保护。

水利部应建设网络安全数据采集与处理分析系统，对本级单位及下级单位的关键网络安全数据进行统一分析。

水利部应在网络安全数据处理分析系统的基础上建设威胁感知预警平台，及时发现网络安全威胁。

水利部应建设网络安全应急决策指挥平台，对本级和行业内重要安全事件进行全流程跟踪处置。

水利部应建设以数据为核心，网络安全资源管理为支撑，涵盖威胁预测、威胁防护、持续检测、响应处置的闭环安全运营体系。

5.1.3 流域机构、省级水行政部门、大型（重要中型）水利工程单位体系

流域机构、省级水行政部门、大型（重要中型）水利工程单位可在水利部网络安全服务基础上建设区域级网络安全情报服务；在水利部异地灾备服务基础上建设区域级本地异地灾备服务；在水利部统一密码服务基础上建设区域级统一密码服务；在水利部统一身份认证基础上建设区域级统一身份认证服务，提供给本级单位及各级行业单位共享使用。

大型（重要中型）水利工程单位可根据水利工控系统实际情况建设工控专用的本地灾备服务、工控专用的统一密码服务、工控专用的身份认证服务。

流域机构、省级水行政部门、大型（重要中型）水利工程单位如无网内没有三级及以上信息系统等特殊情况外应以不低于三级等保要求开展安全计算环境、安全区域边界、安全通信网络等方面的安全保护环境达标建设，并对关键信息基础设施采取措施进行重点保护。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应建设网络安全数据采集与处理分析系统，对本级单位及下级单位的关键网络安全数据进行统一分析。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应在网络安全数据处理分析系统的基础上建设威胁感知预警平台，及时发现网络安全威胁，并与水利部威胁感知

预警平台进行数据共享。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应建设网络安全应急决策指挥平台，对本级和区域内重要安全事件进行全流程跟踪处置，并与水利部威胁感知预警平台进行数据共享。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应建设以数据为核心，网络安全资源管理为支撑，涵盖威胁预测、威胁防护、持续检测、响应处置的闭环安全运营体系。

5.1.4 市县级水行政部门、中小型水利工程单位体系

市县级水行政部门、中小型水利工程单位应以不低于二级等保要求开展安全计算环境、安全区域边界、安全通信网络等方面的安全保护环境达标建设。

市县级水行政部门、中小型水利工程单位应建设网络安全数据采集系统，并将数据上送上级单位的威胁感知预警平台。

市县级水行政部门、中小型水利工程单位应在上级单位指导下建设以数据为核心，网络安全资源管理为支撑，涵盖威胁预测、威胁防护、持续检测、响应处置的闭环安全运营体系。

5.2 体系结构

水利行业网络安全整体体系结构如图 1 所示，在各级单位网络安全建设中要充分利用行业和区域级网络安全统一资源，实现整合共享和能力一致性提升。

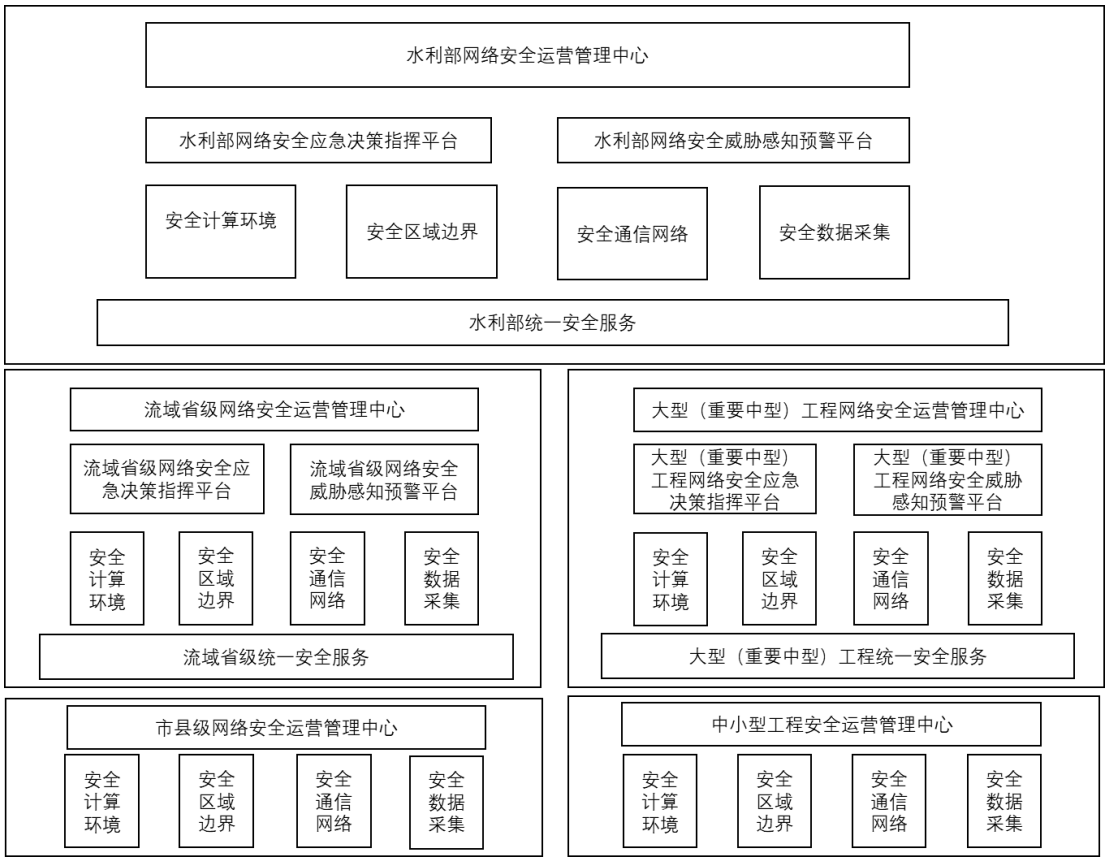

图 1 水利网络安全建设技术框架图-水利行业

5.2.1 统一安全服务

水利部应建设行业级完整统一网络安全服务体系，并对情报服务、灾备服务、密码服务、认证服务等服务建设标准规范。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应在共享使用行业统一安全服务的基础上，建设流域省区网、工程控制网内的区域级统一安全服务。

市县级水行政部门、中小型水利工程单位在网络安全建设中应共享使用上级单位的网络安全情报服务、灾备服务、统一密码服务、统一身份认证服务。

5.2.2 威胁感知预警平台

水利部应建设行业级网络安全大数据平台，建立数据采集标准规范，对部本级网络安全数据和流域机构、省级水行政部门、大型（重要中型）水利工程单位的关键网络安全数据进行威胁分析，及时发现网络安全威胁预警。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应建设区域级网络安全

数据平台，对本级网络安全数据和下级关键网络安全数据进行威胁分析。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应充分利用水利部网络安全大数据平台强化区域级网络安全威胁感知预警平台能力。

流域机构、省级水行政部门、大型（重要中型）水利工程单位威胁感知预警平台应建设共享交换机制，与水利部网络安全威胁感知预警平台实现关键流量数据、网络安全预警等数据交互。

市县级水行政部门、中小型水利工程单位应共享使用上级单位威胁感知预警平台，及时发现网络安全威胁。

5.2.3 应急决策指挥平台

水利部应急决策指挥平台应建设网络安全事件相关数据规范标准。

流域机构、省级水行政部门、大型（重要中型）水利工程单位应急决策指挥平台应遵照水利部网络安全事件相关数据标准与水利部应急决策指挥平台进行数据共享。

市县级水行政部门、中小型水利工程单位应共享使用上级单位网络安全应急决策指挥平台，对重要安全事件进行全流程跟踪处置。

5.3 技术架构

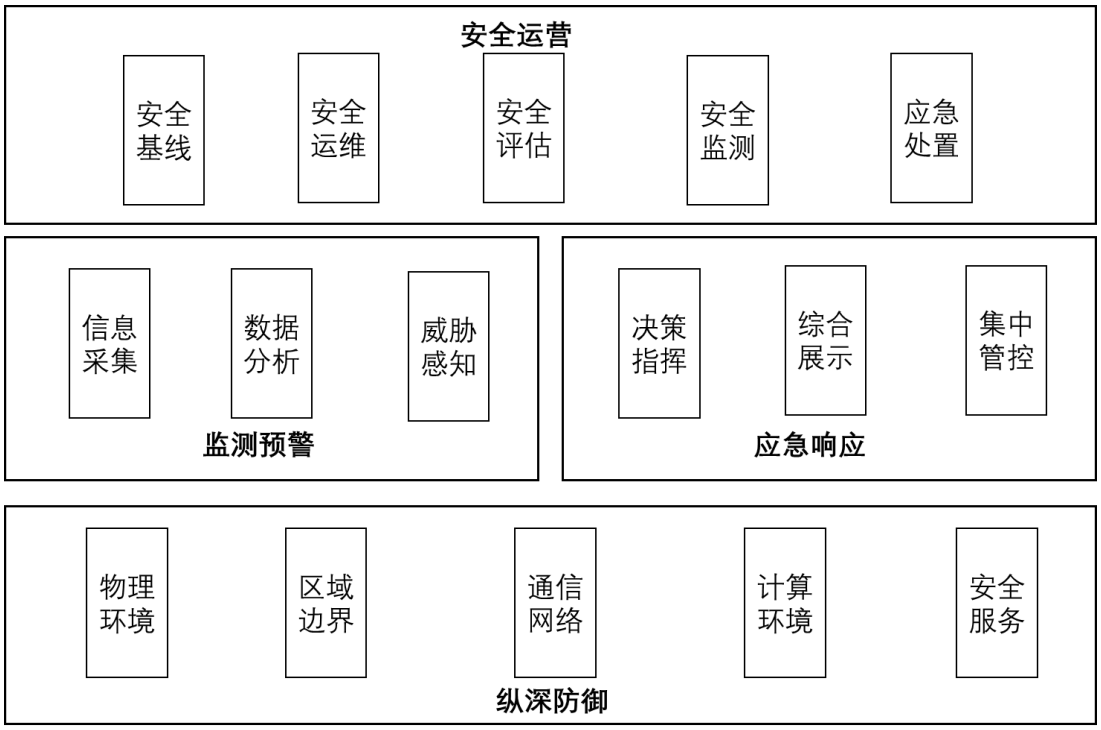

图 2 水利网络安全建设技术框架图-建设运营单位

以充分共享的情报服务、灾备服务、密码服务、认证服务等四项安全服务为支撑，落实安全计算环境、安全区域边界、安全通信网络的三层基础防护，构建网络安全威胁感知预警和网络安全应急决策指挥平台，形成贯穿所有安全活动的一个安全运营管理中心。

完整的水利网络技术架构应涵盖以上描述的四项服务、三层防护、两个平台、一个中心，从而构建纵深防御能力、监测预警能力、应急响应能力三大网络安全能力，如图 2 所示。

5.3.1 纵深防御

对于公共的安全技术形成统一的安全服务，包括统一身份认证服务、统一密码服务、统一灾备服务、统一安全情报服务等四项服务。应建立完善合规的计算环境、区域边界、通信网络防护。

5.3.2 监测预警

应根据实际，建立采集流量数据、各类设备日志、各类主机日志、应用系统日志的数据采集基础。

对于采集的数据进行数据分析，发现潜在的威胁和发生的安全事件，并进行风险预警。

5.3.3 决策指挥

应建设网络安全决策指挥系统，可管理网内网络安全资源，对网络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。

5.3.4 安全运营

应在纵深防御、监测预警、应急指挥等各类安全设备（系统）的支撑下，建立完善的安全运营体系，实时保证网络安全态势控制和不断优化。

6　安全纵深防御能力建设要求

6.1 安全物理环境

6.1.1 第二级安全要求

安全物理环境第二级安全要求适用于承载最高网络安全保护等级为第二级的保护对

象，机房物理环境建设应满足《数据中心设计规范》（GB 50174-2017）C 级标准，同时满足国家网络安全等级保护标准《信息安全技术网络安全等级保护基本要求》（GB 22239-2019）第二级的安全要求，包括物理位置选择、物理访问控制、防盗窃、防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等相关要求。

6.1.2 第三级安全要求

安全物理环境第三级安全要求适用于承载最高网络安全保护等级为第三级的保护对象，机房物理环境建设应满足《数据中心设计规范》（GB 50174-2017）B 级标准，同时满足国家网络安全等级保护标准《信息安全技术网络安全等级保护基本要求》（GB 22239-2019）第三级的安全要求，在第二级的基础上增强如下控制要求:

a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；

b）应设置机房防盗报警系统或设置有专人值守的视频监控系统；

c）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等；

d）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施；

e）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；

f）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环；

g）应设置冗余或并行的电力电缆线路为计算机系统供电；

h）应对关键设备实施电磁屏蔽。

6.1.3 关键信息基础设施安全要求

6.1.3.1 概述

关键信息基础设施安全在满足上述网络安全保护等级第三级的安全要求基础上，对机房环境安全、安全分域、电力安全、监控审计、设备设施安全和灾难备份中心提出增强要求。

6.1.3.2 机房环境安全

满足如下要求：

应配备人员加强关键信息基础设施机房周边环境的边界安全控制。

6.1.3.3 安全分域

满足如下要求：

a）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、设备类型等进一步划分子区域；

b）可配置第二道电子门禁系统，控制、鉴别和记录进入关键信息基础设施的人员。

6.1.3.4 电力安全

满足如下要求：

应提供关键信息基础设施专用备用电力供应，至少满足设备在断电情况下的正常运行要求。

6.1.3.5 监控审计

满足如下要求：

a）应对关键设备实施设置有专人值守的视频监控系统；

b）应定期对监控系统的记录进行审计。

6.1.3.6 设备设施安全

满足如下要求：

a）关键信息基础设备设施应配置冗余的设备设施，满足设备在设备故障情况下的正常运行要求。

b）关键信息基础设备设施均应设置电磁屏蔽措施。

6.1.3.7 灾难备份中心

满足如下要求：

a）应依据 GB/T 20988-2007《信息系统灾难恢复规范》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）应为灾难备份中心提供与主场所同等的网络安全措施；

c）灾难备份中心应位于中国境内；

d）应制定并实施业务连续性计划，确保关键信息基础设施对本单位职能和业务的核心支撑能力在重大信息安全事件中不受到明显影响，支持业务稳定、持续运行。

6.2 安全通信网络

6.2.1 第二级安全要求

安全通信网络第二级安全要求应满足国家网络安全等级保护标准《信息安全技术网络安全等级保护基本要求》（GB 22239-2019）第二级的安全要求，包括网络架构和通信传输相关要求。

6.2.2 第三级安全要求

安全通信网络第三级安全要求满足国家网络安全等级保护标准《信息安全技术网络安全等级保护基本要求》（GB 22239-2019）第三级的安全要求，包括网络架构和通信传输相关，在第二级的基础上增强如下控制要求:

a）应保证网络设备的业务处理能力满足业务高峰期需要；

b）应保证网络各个部分的带宽满足业务高峰期需要；

c）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性；

d)应根据业务属性的不同划分不同的安全区域，至少包括内部业务区、安全管理区、前置交换区和公众服务区等；

e）应采用校验技术或密码技术保证通信过程中数据的完整性；

f）应采用密码技术保证通信过程中数据的保密性；

g）可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

6.2.3 关键信息基础设施安全要求

6.2.3.1 概述

关键信息基础设施安全在满足上述网络安全保护等级第三级的安全要求基础上，对网络架构、传输加密提出增强要求。

6.2.3.2 网络架构

满足如下要求：

b)应对关键信息基础设施信息系统设置独立的网络区域，并与其他网络区域之间设置技术隔离手段；

c)应充分利用第三方网络、自建或专线租用的方式与业务相关单位实现互联互通和数据共享；

d)应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

6.2.3.3 传输加密

满足如下要求：

a)通信信道应保证能够满足关键业务处理需求，避免因信道容量不足引起的关键业务延误、中断等现象；

b)应采用密码技术对关键数据传输过程中的信道加密，确保信息在通信过程中不被监听、劫持、篡改及破译；

c)应对关键数据进行校验，保证通信信息的完整性、可用性。

6.3 安全区域边界

6.3.1 第二级安全要求

6.3.1.1 通用安全要求

安全区域边界第二级安全要求应满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第二级的安全要求，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相关要求。

6.3.1.2 内部边界安全

满足如下要求：

a） 应根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信，删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

b） 应对存放集权类设备系统、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安全事件进行审计。

6.3.1.3 互联网边界安全

满足如下要求：

a）应在互联网网络边界进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d）应能够检测到互联网网络边界的攻击行为，并进行告警。

6.3.1.4 骨干网边界安全

满足如下要求：

a）应满足接入骨干网相应等级的安全接入要求；

b）根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信，删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

6.3.1.5 外联网边界安全

a）根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信，删除多余或无效的访问控制规则，优化访问控制列表，并保证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，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

6.3.2 第三级安全要求

6.3.2.1 通用安全要求

安全区域边界第三级安全要求满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第三级的安全要求，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相关要求，在第二级的

基础上增强如下控制要求：

a）应能够对非授权设备私自联到内部网络的行为进行检查或限制；

b）应能够对内部用户非授权联到外部网络的行为进行检查或限制；

c）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；

d）应对进出网络边界的数据流实现基于应用协议和应用内容的访问控制；

e）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提供报警；

h）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；

i）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

6.3.2.2 内部边界安全

在第二级的基础上满足如下要求：

a）应对区域边界数据流实现基于应用协议和应用内容的访问控制；

b）应对区域边界进行安全审计，审计覆盖到每个用户，对用户行为和安全事件进行审计；

c）应能够将审计数据发送至安全管理中心进行统一分析。

6.3.2.3 互联网边界安全

在第二级的基础上满足如下要求：

a）应在关键网络节点处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）应能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）应能够将攻击监测数据和审计数据发送至安全管理中心进行统一分析。

6.3.2.4 骨干网边界安全

在第二级的基础上满足如下要求：

a）应能够对网络攻击行为进行监测、告警和阻断；

b）应能够将攻击监测数据和审计数据发送至安全管理中心进行统一分析。

6.3.2.5 外联网边界安全

在第二级的基础上满足如下要求：

a）应能够对网络攻击行为进行监测、告警和阻断；

b）应能够将攻击监测数据和审计数据发送至安全管理中心进行统一分析。

6.3.3 关键信息基础设施安全要求

6.3.3.1 概述

关键信息基础设施安全在满足上述网络安全保护等级第三级的安全要求基础上，针对内部边界、互联网边界、骨干网边界、外联网边界提出增强要求。

6.3.3.2 内部边界安全

满足如下要求：

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。

6.3.3.3 互联网边界安全

满足如下要求：

a）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。

b）应采用严格的接入控制措施，保证系统和设备接入的可信性。

c）应在网络边界限制网络最大流量数及网络连接数，优先保证关键信息基础设施的网络系统运行。

d）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；

e）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。

f）应在区域边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为标准格式，上报安全管理中心。

6.3.3.4 骨干网边界安全

满足如下要求：

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

b）应在关键网络节点处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的新型网络攻击的检测和分析；当检测到攻击行为时，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。

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）应在区域边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为标准格式，上报安全管理中心。

6.3.3.5 外联网边界安全

满足如下要求：

a）应在区域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；

c）应在关键网络节点处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的新型网络攻击的检测和分析；当检测到攻击行为时，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。

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）应在区域边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。

6.4 安全计算环境

6.4.1 第二级安全要求

6.4.1.1 通用安全要求

安全计算环境第二级安全要求应满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第二级的安全要求，包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人信息保护等相关要求。

6.4.1.2 云与虚拟化安全

云与虚拟化安全要求满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第二级的云计算安全扩展要求。

6.4.1.3 移动互联安全

移动互联安全要求满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第二级的移动互联安全扩展要求。

6.4.2 第三级安全要求

6.4.2.1 通用安全要求

安全计算环境第三级安全要求满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第三级的安全要求，包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人信息保护等相关要求，在第二级的基础上增强如下控制要求：

a）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；

b）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

c）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

d）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问；

e）应对审计进程进行保护，防止未经授权的中断；

f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；

g）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序

等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

h）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、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；

i）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、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。

j）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

k）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

l）应提供重要数据处理系统的热冗余，保证系统的高可用性。

m）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

6.4.2.2 云与虚拟化安全

满足如下要求：

a）当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制；

b）应能检测虚拟机之间的资源隔离失效，并进行告警；

c）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

d）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

6.4.2.3 移动互联安全

满足如下要求：

a）应保证移动终端安装、注册并运行终端管理客户端软件；

b）移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：

远程锁定、远程擦除等。

c）应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

6.4.3 关键信息基础设施安全要求

6.4.3.1 概述

关键信息基础设施安全在满足上述网络安全保护等级第三级的安全要求基础上，针对基础信息资源、云与虚拟化、应用和数据方面提出增强安全要求。

6.4.3.2 基础信息资源安全

满足如下要求：

a)应对关键信息基础设施操作系统进行统一安全配置，进行安全加固，遵循最小安装的原则，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)应采用受安全管理中心控制的口令、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的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)应采用统一的身份认证服务、统一的密码服务和统一的灾备服务，与水利部基础服务设施进行对接；

d)应对关键信息基础设施服务器操作系统部署统一的防病毒、防入侵和主机审计措施，能够发现漏洞、入侵行为和高级网络威胁，并在发生攻击事件时进行告警；

e)应采用统一的加密技术实现对关键数据的存储加密；

f)应对关键基础设施的基础信息资源部署数据灾备措施。

6.4.3.3 云与虚拟化安全

满足如下要求：

a）应采用集成身份认证服务、访问控制、权限控制实现云平台自身的安全功能；

b）应对东西向流量进行流量监控和访问控制；

c）可通过安全资源池实现对云平台的安全防护；

d）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，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；

e）应采用安全措施实现虚机主机防护、虚机隔离和安全补丁加固等措施。

6.4.3.4 应用安全

满足如下要求：

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）应通过应用攻击防护、网页防篡改、安全漏洞检测、访问控制等方面加强应用自身网络安全防护；

c）应对应用系统的安全性、可用性进行实时安全监测，监测内容篡改、挂马、可用性以及网络攻击等；

d）应实现关键信息基础设施核心应用的应用级灾备建设；

e）必要时关键信息基础设施有能力应用备用通信协议以保障业务连续性。

6.4.3.5 数据安全

满足如下要求：

a）应在数据规划和创建阶段实现数据的分级分类，明确数据的重要性和敏感程度；

b）应采用校验码技术或密码技术保证重要数据在传输、存储过程中的完整性，包括但不限于鉴别数据、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，根据实际情况与水利密码基础设施对接；

c）应采用密码技术保证重要数据在传输、存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等，根据实际情况与水利密码基础设施对接；

d）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；

e）应采用数据防泄漏技术实现对主机数据、网络数据、存储数据的防泄漏；

f）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；

g）应确保个人信息的收集、存储、使用、传输、披露符合 GB/T 35273-2017《信息安全技术 个人信息安全规范》，应确保境内运营中收集和产生的个人信息和重要数据在境内存储。

6.5 工控系统扩展安全

6.5.1 第二级安全要求

工控系统扩展要求第二级应满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第二级的安全要求。主要包括：

a）室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；

b）室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

c）工业控制系统与其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段；

d）工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；

e）涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离。

f）在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

g）应在工业控制系统与其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；

h）应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

i）工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，

并采取用户身份鉴别和访问控制等措施；

j）应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别，进行授权以及执行使用进行限制；

k）控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

l）应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作。

6.5.2 第三级安全要求

工控系统扩展要求第三级安全要求满足国家网络安全等级保护标准《信息安全技术 网络安全等级保护基本要求》（GB 22239-2019）第三级的安全要求，在第二级的基础上增强如下控制要求：

a）拨号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）应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

c）对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。

d）应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；

e）应使用专用设备和专用软件对控制设备进行更新；

f）应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。

6.5.3 关键信息基础设施安全要求

6.5.3.1 安全分区原则

水利工控系统应满足保护核心、有效隔离的原则进行分区分域，根据业务系统或其功能模块的实时性、使用者、主要功能、设备使用场所、各业务系统的相互关系、广域网通

信方式以及对生产的影响程度等，应按照以下规则将业务系统置于相应的安全区：

a）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应置于控制区，其他置于非控制区。

b）应尽可能将业务系统完整置于一个安全区内。当业务系统的某些功能模块与此业务系统不属于同一个安全分区内时，可以将其功能模块分置于相应的安全区中，经过安全区之间的安全隔离设施进行通信。

c）不允许把应属于高安全等级区域的业务系统或其功能模块迁移到低安全等级区域，但允许把属于低安全等级区域的业务系统或其功能模块放置于高安全等级区域。

d）对不存在外部网络联系的孤立业务系统，其安全分区无特殊要求，但需遵守所在安全区的防护要求。

e）现场控制区、过程监控区和水利业务网之间功能独立，严禁网络混用， 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，并按照便于管理和控制的原则为各子网、网段分配地址段。

6.5.3.2 安全区域边界

满足如下要求：

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的安全可靠的设备实现逻辑隔离、报文过滤、访问控制等功能。所选设备的功能、性能、电磁兼容性必须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部署工控单向隔离装置进行隔离，隔离强度应达到或接近物理隔离。

c）控制区中的业务系统如与环保、安全等政府部门进行数据传输，其边界防护应部署经国家指定部门检测认证的单向安全隔离装置。

d）过程监控区和水利业务网边界应部署网络入侵检测系统，合理设置检测规则，检测规则应包含工控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) 禁止其他设备生产厂商或其它外部单位远程连接控制区中的业务系统及设备。

f) 对于内部远程访问业务系统的情况，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。

6.5.3.3 安全通信网络

满足如下要求：

a）数据采集和通信应符合逐级通信原则，避免或越级进行数据采集和通信。

b）现场控制区与上级网络连接应使用独立的网络设备进行组网，与其他网络之间应当进行安全隔离。

c）过程监控区系统与上级集控中心进行远程通信时，应采用认证、加密、访问控制等技术措施实现数据的远程安全传输以及纵向边界的安全防护。

6.5.3.4 工控设备本体安全

满足如下要求：

a）应采用通过国家有关机构安全检测认证的工控设备和系统；

b）系统的可信技术应具备自主知识产权，或采用自主可控的安全技术机制；

c）应支持硬件级部件（安全芯片或安全固件）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）可采取加密技术对 PLC 通信数据进行安全加密,新建的工程控制系统可采用具有通信数据加密功能的 PLC 设施。

e）应采用应用程序白名单技术，对工业主机内必要的的业务组件、系统组件安全软件等执行程序进行保护；

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。

6.5.3.5 工控主机安全防护

满足如下要求：

a）应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的必须通过相关的技术措施实施严格的监控管理；

b）应使用专用设备和专用软件对控制设备进行更新；