ICS 91.140.60
P 41

DB33

浙 江 省 地 方 标 准

DB33/T 2051—2017

智慧供排水信息系统安全技术规范

Technical specification for intelligent water supply and drainage information system safety

2017－09－11 发布　　2017－10－11 实施

浙江省质量技术监督局　　发布

目　　次

前　言

本标准依据GB/T1.1-2009的规则起草。

本标准由浙江省住房和城乡建设厅提出并归口。

本标准主要起草单位：浙江省城市水业协会、宁波市供排水集团有限公司、浙江和达科技股份有限公司、太平洋水处理工程有限公司、宁波东海集团有限公司、杭州安信检测技术有限公司。

本标准主要起草人：柳成荫、陈爱朝、林好斌、刘青友、滕良方、郭军、曹滢锋、鲍建军、达云祥、张嘉伟、郭健。

智慧供排水信息系统安全技术规范

1 范围

本标准主要内容包括智慧供排水信息系统建设原则和目标、安全等级划分与保护、信息安全保护原则与保障体系、水厂与污水厂工控系统保护等。

本标准适用于浙江省智慧供排水信息系统安全建设、运行与管理。

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 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

3 术语和定义

下列术语和定义适用于本标准。

3.1

信息系统 information systems

用于采集、处理、存储、传输，分发和部署信息的整个基础设施、组织结构、人员和组件的总和。

3.2

信息系统安全 information systems security

通过使用合理的安全控制措施保护在存储、处理或传输等过程中的信息不被未授权用户访问，并保证授权用户能够正常使用系统。

3.3

安全保护能力 security protection ability

系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

3.4

授权 authentication

授予权限，包括允许基于访问权的访问。

3.5

安全策略 security policy

为信息系统安全管理制定的行动方针、路线、工作方式、指导原则或程序。

3.6

资产 asset

信息系统安全策略中所保护的信息或资源。

3.7

访问控制 access control

按确定的规则，对实体之间的访问活动进行控制的安全机制，能防止对资源的未授权使用。

3.8

风险 risk

威胁利用资产或一组资产的脆弱性对组织机构造成伤害的潜在可能。

3.9

攻击 attack

在信息系统中一种绕过安全控制的行为。攻击成功与否取决于信息系统的脆弱性以及现有对策的有效性。

3.10

服务集标识 Service Set Identifier （简称 SSID）

一个局域网的名称。

3.11

MAC 地址 Medium/Media Access Control

用来表示互联网上每一个站点的标识符，采用十六进制数表示，共六个字节（48 位）。

3.12

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

以计算机为基础的生产过程控制与调度自动化系统。

3.13

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

专门为在工业环境下应用而设计的数字运算操作电子系统。它采用一种可编程的存储器，在其内部存储执行逻辑运算、顺序控制、定时、计数和算术运算等操作的指令，通过数字式或模拟式的输入输出来控制各种类型的机械设备或生产过程。

3.14

虚拟专用网络 Virtual Private Network （简称 VPN）

一种在公用网络上建立的专用网络，并进行加密通讯。

3.15

敏感信息 sensitive information

企业商业机密信息或国家机密信息或未经授权被修改会对国家、企业造成不利影响的信息。

4 保护原则和目标

4.1 原则

4.1.1 保密性：保证非授权操作不能获取受保护的信息或计算机资源。
4.1.2 完整性：保证非授权操作不能修改数据。
4.1.3 有效性：保证非授权操作不能破坏信息或计算机资源。
4.1.4 可控性：对信息的传播及内容具有控制能力。
4.1.5 可用性：保证合法用户在需要时可访问到需要的信息
4.1.6 易操作：能够方便地部署各种安全策略。

4.2 目标

4.2.1 保证信息系统安全、可靠、稳定的运行。
4.2.2 保证信息系统中的信息的保密性、完整性、可用性和抗抵赖性。
4.2.3 保证信息系统中传播内容的合法性。

5 安全等级划分与保护

5.1 国家信息安全保护等级划分原则

信息系统的安全保护等级应根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素划分。

5.2 国家信息系统安全等级划分

根据 GB/T 22240-2008 的规定，信息系统安全保护等级分为以下五级：

a) 第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
b) 第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
c) 第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
d) 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
e) 第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

5.3 城镇供水信息系统安全等级划分

5.3.1 水厂工控系统

水厂工控系统安全等级划分应符合表 1 的规定。

表 1　水厂工控系统控制系统安全等级

日供水规模 X	有备用供水方案	无备用供水方案
X＜5 万 m^3/d	第一级	第一级
5 万 m^3/d≤X＜30 万 m^3/d	第一级	第二级
X≥30 万 m^3/d	第二级	第三级

5.3.2　生产调度系统

生产调度系统安全等级划分应符合表 2 的规定。

表 2　生产调度系统安全等级

总供水规模 X	只监测不能远程控制或设置运行参数	监测并且能远程控制或设置运行参数
X＜20 万 m^3/d	第一级	第一级
20 万 m^3/d≤X＜50 万 m^3/d	第一级	第二级
X≥50 万 m^3/d	第二级	第三级

5.3.3　管网地理信息系统

管网地理信息系统安全等级划分应符合表 3 的规定。

表 3　管网地理信息系统安全等级

总供水规模 X	地图不涉敏感信息	地图涉敏感信息
X＜50 万 m^3/d	第一级	第二级
X≥50 万 m^3/d	第二级	第三级

5.3.4　区域加压泵站或阀门监控系统

区域加压泵站或阀门监控系统安全等级划分应符合表 4 的规定。

表 4　区域加压泵站或阀门监控系统安全等级

日供水规模 X	只监测不远程控制	监测且需远程控制
X＜2 万 m^3/d	第一级	第一级
2 万 m^3/d≤X＜5 万 m^3/d	第一级	第二级
X≥5 万 m^3/d	第一级	第三级

5.3.5　二次供水集中管理系统

二次供水集中管理系统安全等级划分应符合表 5 的规定。

表 5　二次供水集中管理系统安全等级

泵房数量 X（座）	只监测不能远程控制或设置运行参数	监测并且能远程控制或设置运行参数
X＜100	第一级	第一级
100≤X＜500	第一级	第二级
X≥500	第二级	第三级

5.3.6　营业收费系统

用户数量小于 50 万的营业收费系统，应定为第一级，否则应定为第二级。

5.3.7　门户网站和办公自动化系统

县级市供水企业门户网站和办公自动化系统应定为第一级；地级市以上（含）供水企业门户网站和办公自动化系统为第二级。

5.3.8　安防系统

公司（厂区）、城区范围的安防系统摄像头总数小于 100 个，其信息系统安全等级应定为第一级，否则应定为第二级。

5.3.9　其它信息系统

其它信息系统安全等级划分应符合表 6 规定。

表 6　其它信息系统安全等级

总供水规模 X	不涉敏感信息	涉敏感信息
X＜50 万 m^3/d	第一级	第二级
X≥50 万 m^3/d	第二级	第二级

5.4　城镇排水信息系统安全等级划分

5.4.1　污水厂、泵站工控系统

污水处理厂规模小于 10 万 m^3/d、泵站规模小于 5 万 m^3/d，其信息系统安全等级应定为第一级，否则应定为第二级。

5.4.2　生产调度系统

排水实时生产调度系统能监测数据但不能实行控制，其信息系统安全等级应定为第一级，排水实时生产调度系统能监测数据且能实行控制，其信息系统应定为第二级。

5.4.3　地理信息系统

地下管网地理信息系统地图不涉敏感信息，其信息系统安全等级应定为第一级，否则应定为第二级。

5.4.4　门户网站和办公自动化系统

县级市及以下排水企业门户网站和办公自动化系统，其信息系统安全等级应定为第一级；地级市及以上（含）排水企业门户网站和办公自动化系统，其信息系统安全等级应定为第二级。

5.4.5　安防系统

公司（厂区）、城区范围的安防系统摄像头总数小于 100 个，其信息系统安全等级应定为第一级，否则应定为第二级。

5.4.6　其它信息系统

其它信息系统若不涉敏感信息，其信息系统安全等级应定为第一级，否则应定为第二级。

5.5　城镇供排水信息系统安全等级保护

5.5.1　城镇供排水信息系统应具备的基本安全保护能力

城镇供排水信息系统的安全保护等级属于1～3级。1～3级的信息系统应具备的基本安全保护能力见现行国家标准《信息安全技术 信息系统安全等级保护基本要求》 GB/T 22239-2008 中4.2。

5.5.2　城镇供排水信息系统安全保护能力的基本要求

5.5.2.1　第一级信息系统安全保护能力基本技术要求及管理要求见 GB/T 22239-2008 中第5章。

5.5.2.2　第二级信息系统安全保护能力基本技术要求及管理要求见 GB/T 22239-2008 中第6章。

5.5.2.3　第三级信息系统安全保护能力基本技术要求及管理要求见 GB/T 22239-2008 中第7章。

5.5.2.4 水厂、污水厂工控系统相应等级保护除应符合 GB/T 22239-2008 安全保护能力基本技术要求及管理要求外，尚应符合本规范第7章的规定。

6 信息安全保护原则与保障体系

6.1 保护原则

6.1.1 自主保护原则

信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

6.1.2 重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

6.1.3 同步建设原则

信息系统在新建、改建、扩建时应同步规划和设计安全方案，投入一定比例的资金建设与维护信息安全设施，保障信息安全与信息化建设相适应。

6.1.4 动态调整原则

应跟踪信息系统的变化情况，调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

6.2 保障体系

6.2.1 信息安全体系建设

信息安全体系建设应依据安全等级保护的基本要求，从物理安全、网络安全、主机安全、应用安全、数据安全以及安全管理等方面综合考虑，建设成可管理、可控制、可信任的并且融管理、运行和技术为一体的信息安全体系。

6.2.2 安全管理体系

信息安全管理架构应包括：安全组织架构、人员管理架构和安全管理制度架构。应通过建立安全管理机制、成立信息安全协调小组，明确安全管理责任人，落实安全责任制，部署安全防护措施。

6.2.3 安全运行体系

信息安全运行体系应成为技术体系和管理体系作为运行体系的支撑，可通过运行体系的运行情况分析出技术体系和管理体系所存在的不足，为后期进一步完善加强信息安全工作打下基础。信息安全运行体系应包括建设管理、运维管理、监督检查等。

6.2.4 安全技术体系

6.2.4.1 体系要求

信息安全技术体系是其安全管理体系和安全运行体系的交叉组成部分。安全技术体系应是整个信息安全体系框架的基础，应包括：数据安全、系统安全和基础设施安全。

6.2.4.2 数据安全

6.2.4.2.1 数据保密性

数据不得被非授权人员获取或被获取也不能被破解，采用数据访问控制、数据存储和传输加等技术措施实现。

6.2.4.2.2 数据完整性

数据不得被未授权的篡改或在篡改后能够被迅速发现，采用数据操作权限、数字签名、数据监控与审计等技术措施实现；

6.2.4.2.3 数据可用性

保证数据能被授权者正常使用，不得因为数据损坏而获取不到信息，采用数据备份、数据恢复、异地灾备等技术措施实现。

6.2.4.3 系统安全

6.2.4.3.1 应用安全

应用安全应保障应用程序使用过程和结果的安全，通过身份鉴别、访问控制、安全审计等功能和配置部署，达到安全防护目标。同时应用系统的程序缺陷、错误信息可能会导致严重的安全漏洞，可通过源代码安全审计来保证程序安全性。

6.2.4.3.2 平台安全

平台安全应支撑应用系统运行的各类平台的安全，包括操作系统、数据库、开发平台等。

6.2.4.4 基础设施安全

6.2.4.4.1 物理安全

物理安全应保护计算机网络设备、设施以及其他媒体免遭地震、火灾、水灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程，应包括机房安全、设施安全和动力安全等方面。

6.2.4.4.2 网络安全

网络安全应以网络安全架构为主体，并在此基础上结合相应的网络设备、安全设备和系统软硬件进行安全部署和配置，应包括安全区域划分、边界安全防护、网络访问控制等方面。

6.2.4.4.3 通信安全

通信安全应建立在信号层面的安全，不得涉及具体的数据信息内容，可为信息的正确、可靠传输提供了物理保障。应包括通信线路安全、通信完整性、通信保密性等内容。

7 工控系统安全保护

7.1 安全软件选择与管理

7.1.1 工业主机上应采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。

7.1.2 应建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备应采取病毒查杀等安全预防措施。
7.1.3 重大工控安全漏洞及补丁发布后，应及时采取补丁升级措施，在补丁安装前，应对补丁进行严格的安全评估和测试验证。

7.2 工控系统配置管理

7.2.1 工控系统应有详实的工控系统网络图，现场每个网络接入点应有明确的标识牌，与网络图一一对应，并即时更新。
7.2.2 应建立工控系统配置清单并定期进行配置审计，第一级系统不低于一年一次，第二级系统不低于半年一次，第三级系统不低于三个月一次。
7.2.3 对重大配置变更应制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。
7.2.4 严禁在工控系统服务器、工控机、计算机上安装非必须的软件，除软件自身通讯必须的网络端口外，其余的网络端口必须全部关闭。

7.3 边界安全防护

7.3.1 工控网络必须与其它网络分开组建，严禁与其它网络混合搭建。
7.3.2 工控网络必须通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。
7.3.3 第二级以上的工控网络采用技术手段进行物理隔离，必须做到其它任何网（包括办公网、互联网）都无法向工控网传送任何控制指令和数据。
7.3.4 第二级以上的系统要求分离工控系统的开发、测试和生产环境。
7.3.5 第三级以上的工控系统严禁使用无线通信技术。第一、二级工控系统确需使用无线通信技术的，应采取必要的安全措施。

7.4 物理和环境安全防护

7.4.1 核心工控软硬件所在区域应根据其安全等级按中心机房要求进行物理安全防护。
7.4.2 必须拆除或封闭工业主机上不必要的通用串行总线（USB）、光驱等接口。确需使用通用串行总线（USB）、光驱等接口的，应按信息系统三级等保要求使用通用串行总线（USB）、光驱等接口，使用结束后应立即拆除或封闭工业主机上不必要的USB、光驱等接口。

7.5 安全账户认证

7.5.1 在工业主机登录，应用服务资源访问、工业云平台访问等过程中应使用身份认证管理；对于关键设备、系统和平台的访问应采用多因素认证。
7.5.2 应合理分类设置账户权限，以最小特权原则分配账户极限。
7.5.3 工控设备、SCADA软件、工业通信设备等应用软件的登录账户及密码应避免使用默认口令或弱口令，并应定期更新口令，其中第一级系统不低于半年一次，第二级系统以上不低于三个月一次。
7.5.4 必须对PLC内下载程序进行加密，避免使用默认口令或弱口令；应定期更新口令，其中第一级系统不低于半年一次，第二级系统以上不低于三个月一次；必须通过配置关闭PLC的默认网页服务功能。
7.5.5 应加强对身份认证证书信息保护力度，除组态软件特殊要求，严禁任何网络文件共享。

7.6 远程访问安全

7.6.1 第三级以上的工控系统严禁任何远程访问。
7.6.2 严禁工控系统面向互联网开通通用网络服务。

7.6.3 第一、二级工控系统确需远程维护的，应采用临时虚拟专用网络(VPN)等远程接入方式进行，保留工业控制系统的相关访问日志，并对操作过程进行安全审计。维护完毕后，应及时关闭临时虚拟专用网络(VPN)通道。

7.7 安全监测及应急预案演练

7.7.1 工控网络应部署网络安全监测设备，及时发现、报告并处理网络攻击异常行为。
7.7.2 在重要工控设备前应部署具备工业协议深度包检测功能的防护设备，限制违法操作。
7.7.3 应制定工控安全事件应急响应预案，当遭受安全威胁导致工控系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并逐级报送至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证。
7.7.4 应定期对工控系统的应急响应预案演练，必要时对应急响应预案进行修订。演练第一级系统不应低于两年一次，第二级系统不应低于一年一次，第三级系统不应低于半年一次。

7.8 资产安全

7.8.1 应建立工控系统资产清单、资产使用及处置规则，明确资产责任人。
7.8.2 对关键主机设备、网络设备、控制组件等应进行冗余配置。

7.9 数据安全

7.9.1 应对采集、存储、传输、应用过程中的重要工业数据进行保护，并根据风险评估结果对数据信息进行分级分类管理。
7.9.2 应定期备份关键业务数据。
7.9.3 每次修改PLC等应用程序后，必须备份，并记录备份日志。
7.9.4 应对测试数据进行保护。

7.10 供应链管理

7.10.1 选择工控系统规划、设计、建设、运维或评估等服务商时，应优先选择具备工控安全防护能力的企事业单位，以合同等方式明确服务商应承担的信息安全责任和义务。
7.10.2 应以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄。