ICS 35.040
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1390.5—2017

信息安全技术　网络安全等级保护基本要求　第5部分:工业控制系统安全扩展要求

Information security technology—General requirements for classified protection of cyber security—Part 5:Special security requirements for industrial control system

2017-05-08 发布　　2017-05-08 实施

中华人民共和国公安部　　发布

目　　次

前　言

GA/T 1390《信息安全技术　网络安全等级保护基本要求》已经或计划发布以下部分：

——第 1 部分：安全通用要求；

——第 2 部分：云计算安全扩展要求；

——第 3 部分：移动互联安全扩展要求；

——第 4 部分：物联网安全扩展要求；

——第 5 部分：工业控制系统安全扩展要求；

——第 6 部分：大数据安全扩展要求。

本部分为 GA/T 1390 的第 5 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由公安部信息系统安全标准化技术委员会提出并归口。

本部分负责起草单位：浙江大学、浙江中控研究院有限公司、机械工业仪器仪表综合技术经济研究所、公安部第三研究所、杭州科技职业技术学院、北京启明星辰信息安全技术有限公司。

本部分参加起草单位：中国电力工程顾问集团西南电力设计院有限公司、北京国电智深控制技术有限公司、西门子(中国)有限公司、施耐德电气(中国)有限公司、工业和信息化部电子第五研究所、北京和利时系统工程公司、东方电气中央研究院、北京市轨道交通设计研究院有限公司、国家信息技术安全研究中心、中国软件测评中心、中石化齐鲁石化公司、中科院沈阳自动化所、中国电子科技集团公司第三十研究所、国家电力投资集团公司、中国电力工程顾问集团华北电力设计院有限公司、国核自仪系统工程有限公司、北京自来水集团。

本部分主要起草人：冯冬芹、刘之涛、贾驰千、陆耿虹、高梦州、梁耀、刘大龙、梅恪、王玉敏、赵艳领、任卫红、袁静、杨悦梅。

本部分参与起草人：张晋宾、朱镜灵、李锐、梁军、刘杰、刘太洪、赵军凯、袁晓舒、梅棋、肖衍、李冰、庞宁、周峰、刘利民、陈秀丽、王爱鹏、孟雅辉、方进社、卜志军、张晨艳、王戬、兰昆、王静、李忠生、王勇、刘志祥、罗安、尚文利、马欣欣、何彦君。

引　言

为了适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下信息安全等级保护工作的开展，需对 GB/T 22239—2008 进行修订，修订的思路和方法是针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域提出扩展的安全要求。

信息安全技术　网络安全等级保护基本要求　第5部分:工业控制系统安全扩展要求

1　范围

GA/T 1390的本部分规定了不同安全保护等级工业控制系统的安全扩展要求。

本部分适用于批量控制、连续控制、离散控制等工业控制系统,为工业控制系统网络安全等级保护措施的设计、落实、测试、评估等提供指导要求。

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 17859—1999　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　信息系统安全等级保护基本要求

GB/T 25069—2010　信息安全技术　术语

IEC 62443-1-1　工业通信网络　网络和系统安全　第1-1部分:术语、概念和模型

IEC 62443-3-2　工业通信网络　网络和系统安全　第3-2部分:区域和通道的安全保障等级

3　术语、定义和缩略语

3.1　术语和定义

GB 17859—1999、GB/T 25069—2010和IEC 62443-1-1界定的以及下列术语和定义适用于本文件。

3.1.1

工业控制系统　industrial control system

对工业生产过程安全、信息安全和可靠运行产生作用和影响的人员、硬件和软件的集合。

注:系统包括,但不限于:

1) 工业控制系统包括集散式控制系统(DCS)、可编程逻辑控制器(PLC)、智能电子设备(IED)、监视控制与数据采集(SCADA)系统,运动控制(MC)系统、网络电子传感和控制,监视和诊断系统[在本标准中,不论物理上是分开的还是集成的,过程控制系统(PCS)包括基本过程控制系统和安全仪表系统(SIS)];

2) 相关的信息系统,例如先进控制或多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、制造执行系统(MES);

3) 相关的部门、人员、网络或机器接口,为连续的、批处理、离散的和其他过程提供控制、安全和制造操作功能。

3.1.2

区域　area

站点内划分的物理的、地理的或逻辑的资源分组。

3.1.3

安全域　security zone

具有相同安全要求的逻辑资产或物理资产的集合。

3.1.4

边界 boundary

软件、硬件或者其他物理屏障，限制进入系统或者部分系统。

3.1.5

控制中心 control center

资产集合的运行中心。

3.1.6

控制网络 control network

用于连接控制物理过程设备的实时网络。

3.1.7

现场总线 fieldbus

将安装在工业过程现场的智能自动化仪表和装置与设置在控制室内的仪表和控制设备连接起来的一种数字化、串行、双向、多站的通信网络技术。

3.1.8

移动代码 mobile code

通过网络或者可移动媒介与可能是非可信的系统之间传递的程序，被不经显式安装在本地系统，会被自动执行或被接收者执行。

3.1.9

会话 session

在两个或者多个通信设备之间的半永久性、状态性或者交互式的信息交换。

3.1.10

会话 ID session ID

用于表明特定会话入口的标识符。

3.2 缩略语

下列缩略语适用于本文件。

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

DMZ：隔离区(Demilitarized Zone)

ERP：企业资源计划(Enterprise Resource Planning)

HMI：人机界面(Human Machine Interafce)

ICS：工业控制系统(Industrial Control System)

MES：制造执行系统(Manufactoring Execution System)

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

RTU：远程终端单元(Remote Terminal Unit)

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

VPN：虚拟专用网(Virtual Private Network)

4 概述

4.1 安全通用要求

信息安全技术网络安全等级保护基本要求的通用要求应符合 GB/T 22239。

4.2 工业控制系统概述提要

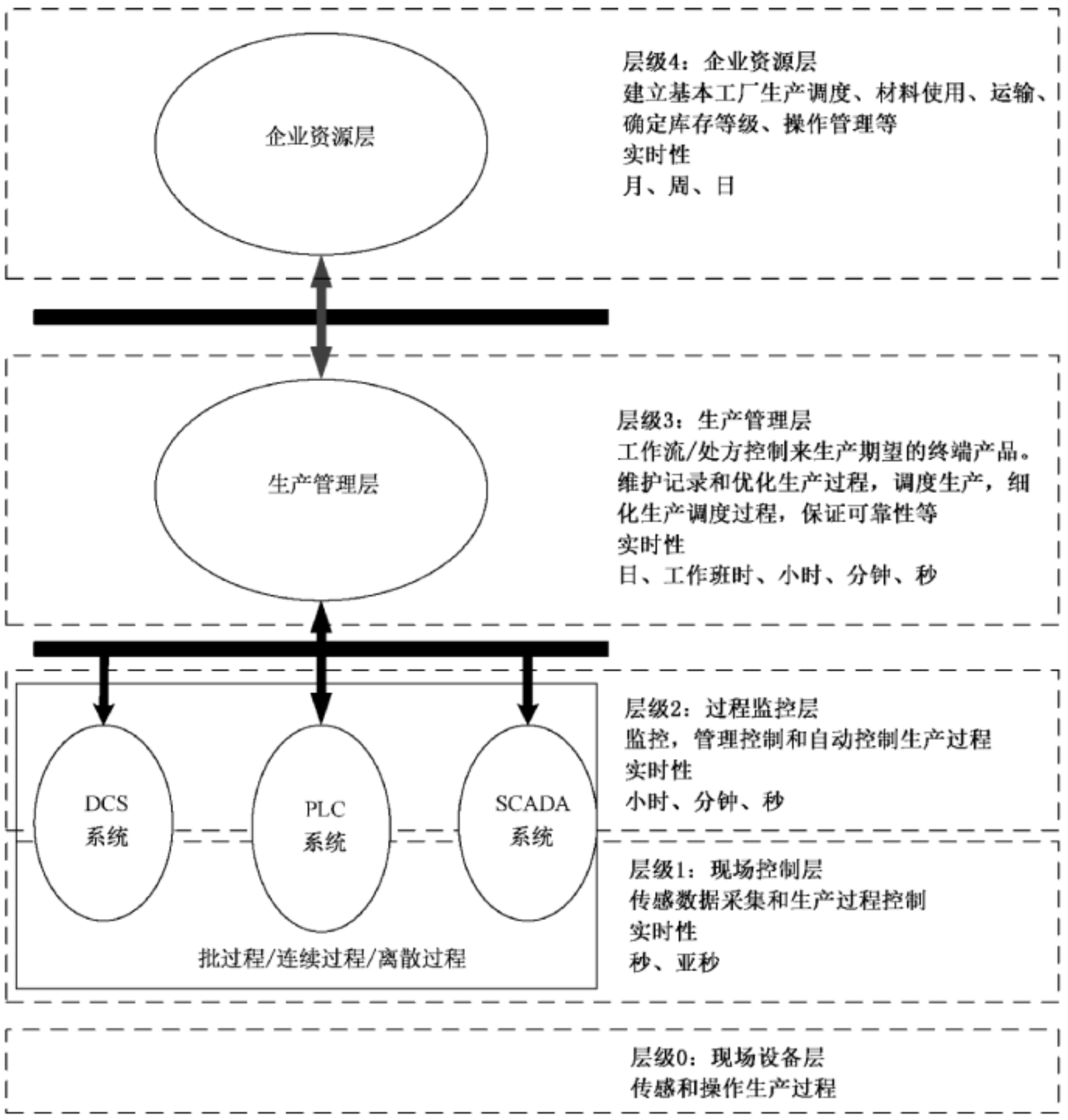
4.2.1 总则

工业控制系统(ICS)是几种类型控制系统的总称,包括数据采集与监视控制系统(SCADA)系统、集散控制系统(DCS)和其他控制系统,如在工业部门和关键基础设施中经常使用的可编程逻辑控制器(PLC)。对包括 SCADA 系统、PLC 系统、DCS 系统、RTU 系统在内的几种工业控制系统的概述与比较,可参见附录 A。ICS 通常用于诸如电力、水和污水处理、石油和天然气、化工、交通运输、制药、纸浆和造纸、食品和饮料以及离散制造(如汽车、航空航天和耐用品)等行业。在阅读、规定和实施第 5～8 章详述的控制系统的安全等级要求时,应遵循一些通用约束。本章和后续章节提供了必要的规范性材料,扩展现有的工业控制系统安全技术,支持工业控制系统所需的完整性和可用性要求。

4.2.2 层次模型

参考 IEC 62264-1 的层次结构模型划分,同时将 SCADA 系统、DCS 系统和 PLC 系统的模型的共性进行抽象,对通用工业企业采用层次模型进行说明。层次模型的内容包括:功能层次模型、功能单元映射模型、资产组件映射模型。

工业企业功能层次模型从上到下共分为 5 个层级,依次为企业资源层、生产管理层、过程监控层、现场控制层和现场设备层,不同层级的实时性要求不同。该层次结构的简要划分模型如图 1 所示。



注:该图为工业控制系统经典的功能层次模型,参考自 IEC 62264-1,但随着工业 4.0 和信息物理系统的发展,已不能完全适用,因此对于不同的行业企业实际发展情况,允许部分层级合并。

图 1 工业企业功能层次模型

图 1 描述并解释了功能层次模型的各个层级。在不同实时性下，各层级的具体分工见 IEC 62443-1-1。

根据图 1 的层次结构划分，各个层次在工业控制系统中发挥不同的功能。各层次功能单元映射模型如图 2 所示。

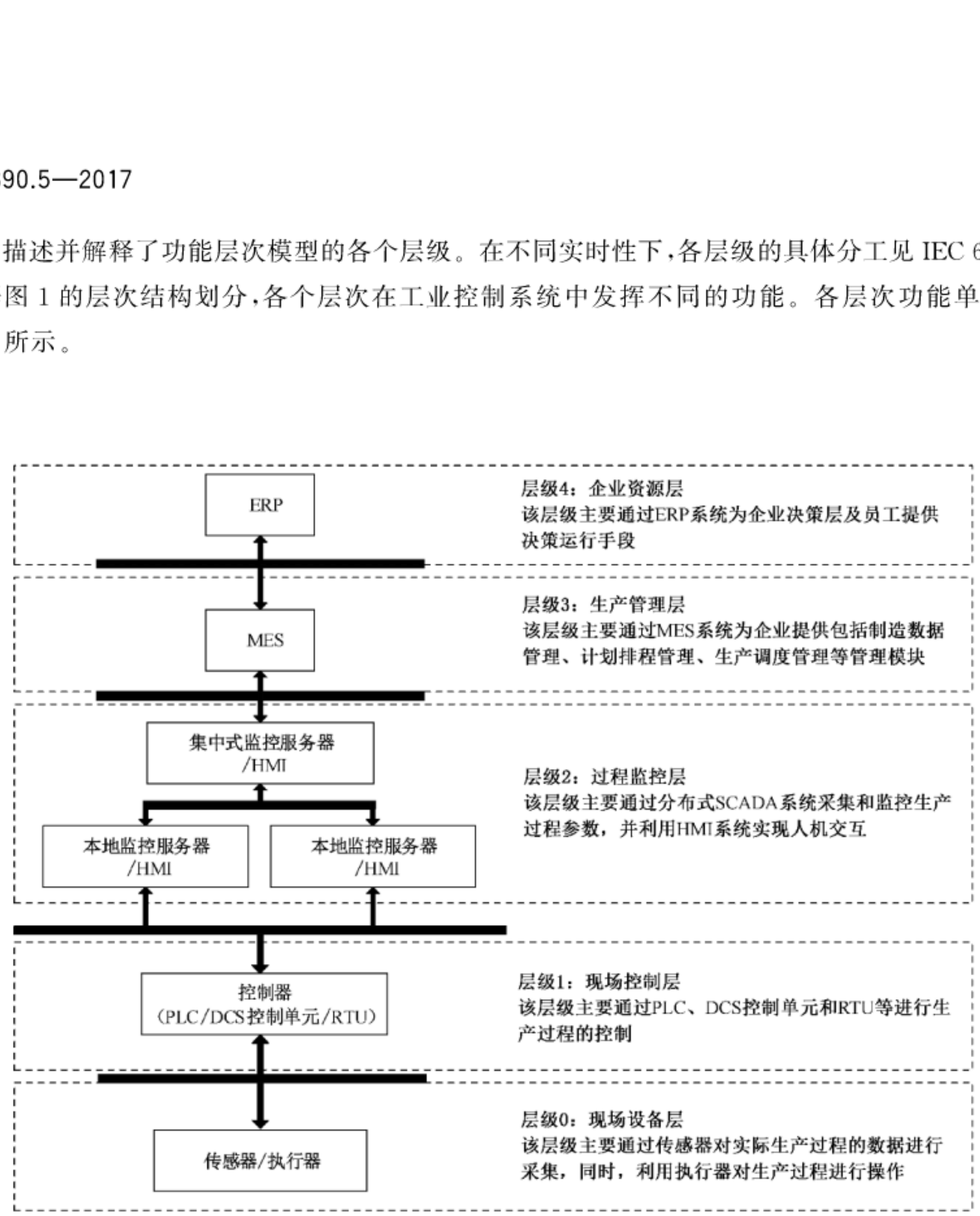


图 2　工业企业各层次功能单元映射模型

其中各个层次功能单元有：

a）　企业资源层：主要包括 ERP 系统功能单元，用于为企业决策层员工提供决策运行手段；

b）　生产管理层：主要包括 MES 系统功能单元，用于对生产过程进行管理，如制造数据管理、生产调度管理等；

c）　过程监控层：主要包括监控服务器与 HMI 系统功能单元，用于对生产过程数据进行采集与监控，并利用 HMI 系统实现人机交互；

d）　现场控制层：主要包括各类控制器单元，如 PLC、DCS 控制单元等，用于对各执行设备进行控制；

e）　现场设备层：主要包括各类过程传感设备与执行设备单元，用于对生产过程进行感知与操作。

工业企业的资产组件映射模型可用于明确各层次保护对象，为安全域划分提供依据；应能够根据各层次主要资产来构建，且与图 2 的各层级功能单元一一映射，如图 3 所示。

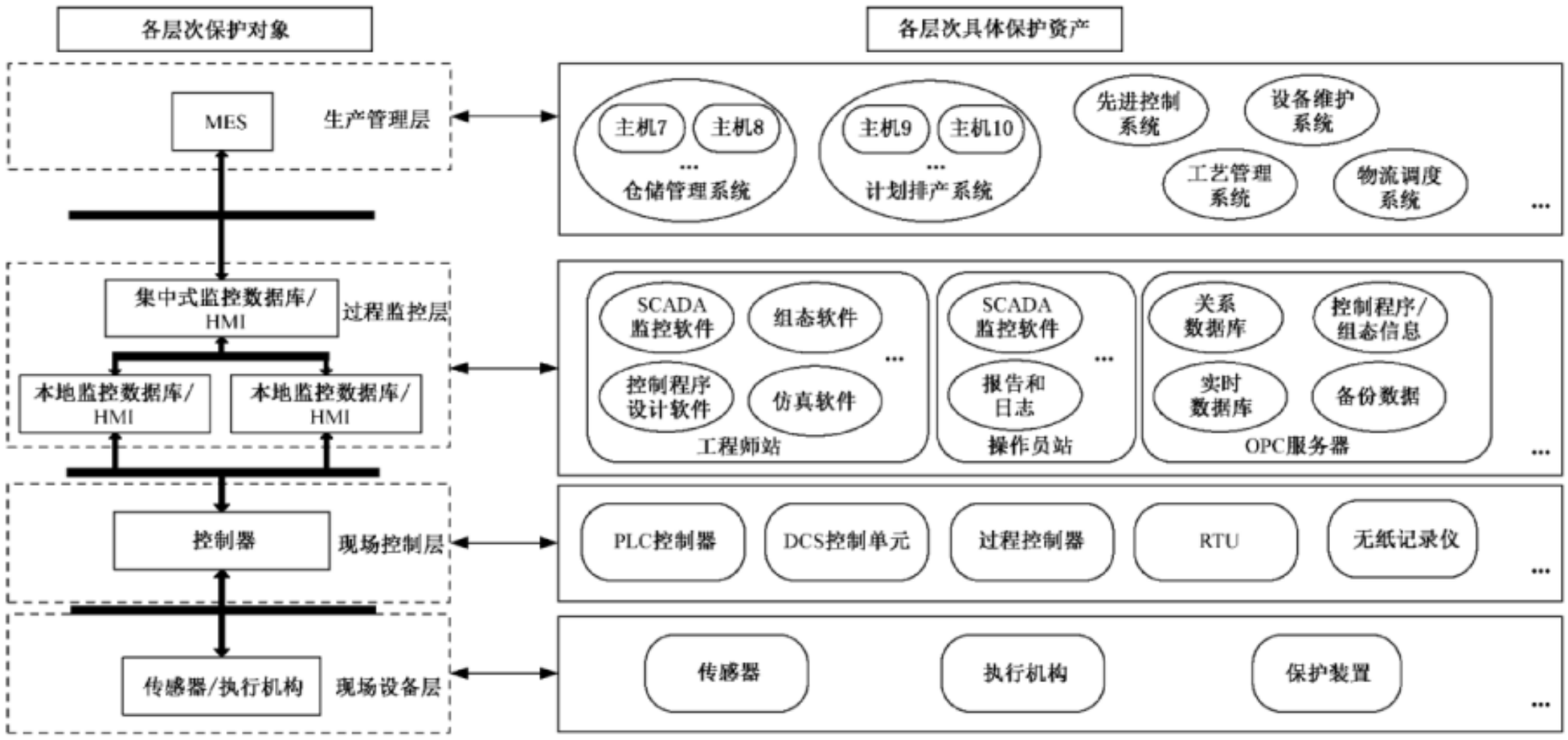


图 3　工业企业资产组件映射模型

其中各个层次具体应保护的资产有：

a）　企业资源层应保护与企业资源相关的财务管理、资产管理、人力管理等系统的软件和数据资产不被恶意窃取，硬件设施不遭到恶意破坏；

b）　生产管理层应保护与生产制造相关的仓储管理、先进控制、工艺管理等系统的软件和数据资产不被恶意窃取，硬件设施不遭到恶意破坏；

c）　过程监控层应保护各个操作员站、工程师站、OPC 服务器等物理资产不被恶意破坏，同时应保护运行在这些设备上的软件和数据资产，如组态信息、监控软件、控制程序/工艺配方等不被恶意篡改或窃取；

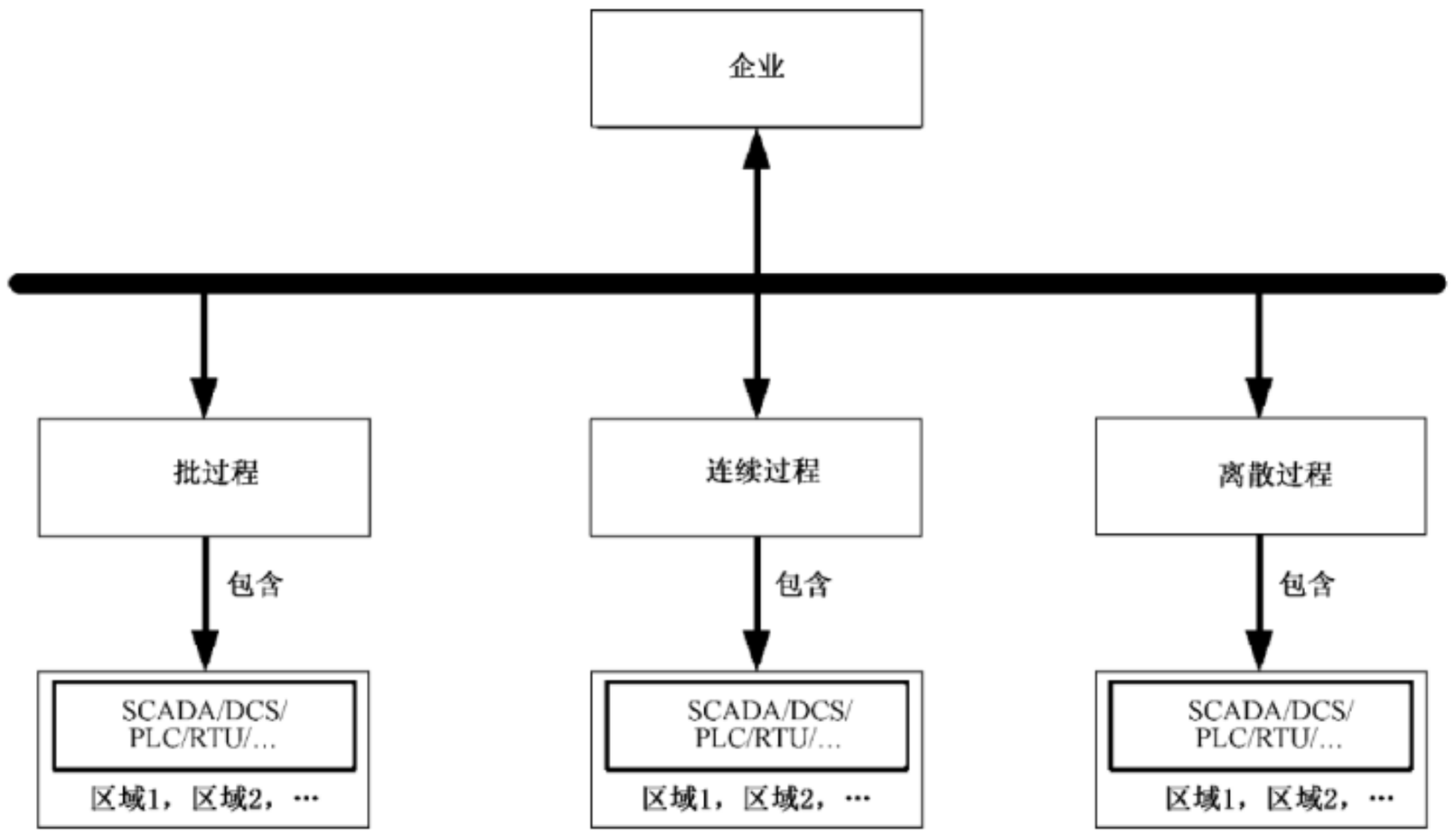
d）　现场控制层应保护各类控制器、控制单元、记录装置等不被恶意破坏或操控，同时应保护控制单元内的控制程序或组态信息不被恶意篡改；

e）　现场设备层应保护各类变送器、执行机构、保护装置等不被恶意破坏。

4.2.3　区域模型

区域是一些具备公有属性的独立资产构成的组群，或一些子区域构成的组群，或一些独立资产与子区域中具备公有属性的资产构成的组群。

区域模型是符合区域定义要求，辅助分析工业控制系统安全性的框架。它用于定义保护区域内资产所需的不同安全等级，分析安全政策和安全要求，评估通用风险、脆弱性及相应对策等。如图 4 所示，根据生产过程的不同，工控企业在各自的工厂或站点可以构建不同的区域模型。



注：批过程包括制药工业、食品工业、啤酒工业、造纸工业、轧钢工业等；连续过程包括能源工业、石油化工、化工、冶金、电力、天然气、水处理等；离散过程包括机械制造工业、汽车工业、仪器仪表工业、家电工业、机床等。

图 4　工业企业区域模型

4.2.4　安全域划分原则

在一个工业大系统或复杂系统中，对所有组件采取相同等级的安全措施是不实际或不必要的。在不同的实际情况下，资产的安全等级不同，因此提出使用安全域（或受保护的区域）的概念。

划分安全域时，应参考 IEC 62443-1-1 中安全域的划分方式，综合考虑资产价值、资产重要性、资产地理位置、系统功能、控制对象、生产厂商及资产被破坏时所造成的损失、社会影响程度等因素，将控制系统进行安全域划分。参照附录 B 中给出的 DCS 系统和 SCADA 系统安全域划分的参考模型。

4.3　工业控制系统等级保护原则和要求

4.3.1　总则

针对工业控制系统等级保护定义有总体原则、技术要求和管理要求共 3 类说明。其中，总体原则是针对工业控制系统整体提出的安全域保护原则；技术要求和管理要求是针对不同安全保护等级工业控制系统应该具有的基本安全保护能力提出的安全要求。

针对工业控制系统的软件、硬件、网络协议等的安全性，规定了需要保护的数据、指令、协议等要素，其具体实现方式（如可信性计算等）、防护手段应根据具体的工业控制系统品牌、配置、工程实际等确定。但应保证这些防护措施对系统的正常运行不产生危害或灾难性的生产停顿，应保证这些防护措施经过工业现场的工程实践验证，并获得用户认可。附录 C 中给出了基于可信计算技术的工业控制系统安全等级防护的要求与说明。

企业用户应结合自身行业特点和企业特点依照 GB/T 22239 和本部分的各级技术要求和管理要求部署实现各安全要点。

4.3.2　安全域保护原则

根据工业控制系统安全域模型的划分原则，将工业控制系统划分为若干安全域，再根据系统实际情况，对不同的安全域采取不同的安全保护措施：

a）　安全域划分：依据 4.2.4 提出的安全域划分原则，对系统进行安全域划分；

b) 安全域边界防护：在不影响各安全域工作的前提下，于各安全域边界处设置不同的安全隔离装置，确保各个安全域之间有清楚明晰的边界设定；

c) 各安全域保护措施：依据定级对象安全等级，结合各安全域实际情况，按照本部分中第一级至第四级基本要求（第5～8章内容），对照各层级要求，采取不同安全保护措施。

4.3.3 安全域保护措施实施说明

为了方便说明，图5仅作为一个示例，并不表示真实工业控制系统的安全域划分模型。当读者使用本部分时，需要根据特定的系统、安全和业务等需求进行安全域划分，然后参考以下两点说明来实施安全等级保护措施。

应参考以下两点说明来确定安全域安全措施与系统功能层次的关系：

a) 一个安全域只包含一个功能层次：如图5中安全域1、2、4、6、8、9、10所示，每个安全域只包含一个功能层次的设备。在确定安全域的安全要求后，安全域的所有设备根据安全要求，采取对应功能层次的安全保护措施，每一级具体保护措施见第5～8章；

b) 一个安全域包含多个功能层次：如图5中安全域3、5、7所示，每个安全域包含多个功能层次的设备。在确定安全域的安全要求后，安全域内的不同功能层次设备，应分别采取对应功能层次的安全等级保护措施，具体保护措施见第5～8章。

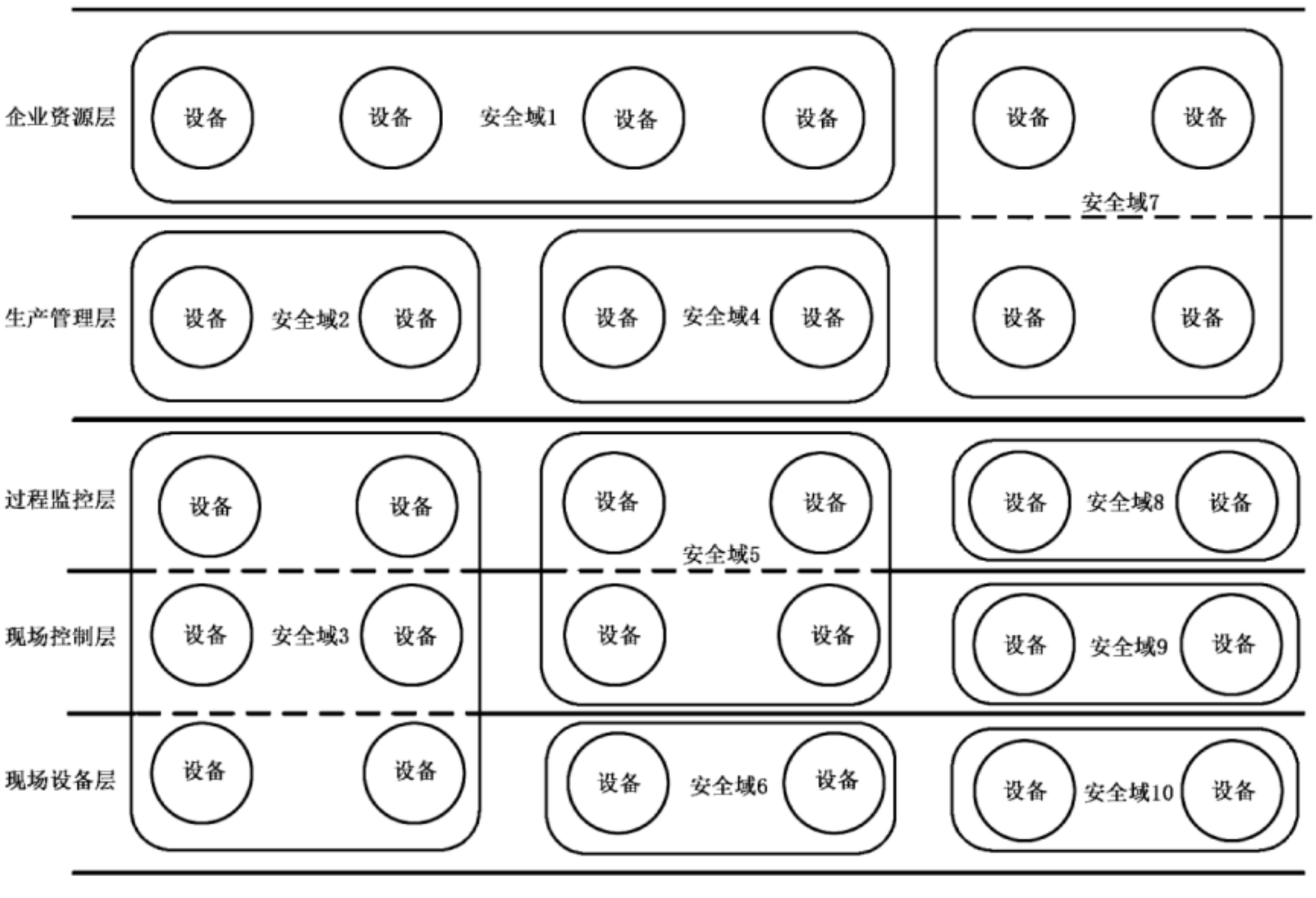


图5 安全域安全措施设定示意图

4.3.4 技术要求和管理要求

技术要求与工业控制系统提供的技术安全机制有关，主要通过在工业控制系统中部署软硬件并正确配置其安全功能来实现。管理要求与工业控制系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、标准、流程以及记录等方面作出规定来实现。技术要求和管理要求是确保工业控制系统安全不可分割的两个部分。

技术要求主要从物理安全、各层级安全提出，其中各层级安全要求从网络和通信安全、设备和计算安全、应用和数据安全3个方面提出；管理要求主要参照GB/T 22239中各个安全等级要求中的管理要求。

技术要求和管理要求从各个层面或方面提出了工业控制系统的每个组件应该满足的安全要求，工业控制系统具有的整体安全保护能力通过不同组件实现基本安全要求来保证。除了保证系统的每个组件满足安全要求外，还要考虑组件之间的相互关系，来保证系统的整体安全保护能力。

4.4 工业控制系统定级

本部分作为通用安全要求的扩展要求，只对层次模型的生产管理层、过程监控层、现场控制层、现场设备层进行等级保护说明，企业资源层不在本部分标准范围内。对控制系统的组件、要素提出安全防护要求，不具体限定安全防护技术或安全防护产品。但是，安全防护技术或产品的使用应该在工业现场的工程实践验证、用户认可的基础上进行，确保不会导致工业控制系统异常。

应根据工业控制系统业务对象、业务特点和业务范围等因素，综合确定工业控制系统等级保护对象。在对等级保护对象进行安全定级的基础上，可对定级对象进行安全域划分，各个安全域可根据工业控制系统实际情况，采用相应的安全保护措施。定级时应综合考虑以下因素，确定定级对象的安全等级：

a) 资产价值：物理资产、信息资产和生产产品的价值；
b) 生产对象：工艺生产对象的属性，如危险程度、人员密集程度；
c) 后果：遭到破坏后对国家安全、社会秩序、公共利益以及个人利益的危害程度。

4.5 工业控制系统等级保护通用约束条件

4.5.1 概述

实施第5～8章详述的安全等级保护要求时，应遵循以下通用约束，以满足工业控制系统对可用性的高要求。

4.5.2 基本功能支持

基本功能是一种“维护受控设备健康、安全、环境友好和可用性所必须的功能和能力”。当阅读、规定和实施本部分所描述的要求时，不应造成保护丧失、控制丧失、观察丧失或其他基本功能丧失。经过风险分析发现，一些装置可能决定特定类型的安全措施可能会终止其连续运行，而安全措施不应导致在健康、安全和环保(HSE)方面的保护丧失。一些具体的制约因素包括：

a) 除非有相应的风险评估，否则信息安全措施不应对高可用性的工业控制系统基本功能产生不利影响。
b) 不应妨碍基本功能的运行，尤其是：
   1) 用于基本功能的账户不应被锁定，即使是短暂的锁定也不允许；
   2) 验证和记录操作员的操作，加强抗抵赖性，但不应显著增加延迟而影响系统响应时间；
   3) 对于高可用性的控制系统，授权证书错误不应中断基本功能；
   4) 标识和鉴别，不应妨碍安全仪表功能触发。同样，适用于授权执行；
   5) 不正确的时间戳审计记录不应对基本功能产生不利影响。
c) 如果安全域边界保护进入故障关闭(阻止所有边界通信)和/或孤岛模式，应保持工业控制系统的基本功能。
d) 发生在控制系统或安全仪表系统网络中的拒绝服务事件，不应妨碍安全仪表功能的运作。

4.5.3 补偿措施

补偿措施应当遵循 IEC 62443-3-2。

控制系统应具备的安全等级要求相关措施可能由外部组件来执行。在这样的情况下，控制系统应向外部组件提供一个“接口程序”。

一些补偿措施的例子如下：

a） 口令强度加强弥补无法定期更换口令；

b） 在一个关键操作室中，操作员的紧急操作能力至关重要，因此即使没有鉴别与认证的功能，采用严格物理访问控制与监视也可以认为本部分的要求得到了补偿和满足。

5 第一级基本要求

5.1 技术要求

5.1.1 物理安全

5.1.1.1 物理位置选择

应符合所选用设备的物理和环境条件。

5.1.1.2 物理访问控制

进入安全区域边界有明确的防止非授权人员接触的提示标志。

5.1.1.3 防盗窃和防破坏

应将设备或主要部件进行固定。

5.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

5.1.1.5 防火

机房应设置灭火设备。

5.1.1.6 防水和防潮

应符合所选用设备的物理和环境条件。

5.1.1.7 防静电

本项要求包括：

a） 机房应安装防静电地板并采用必要的接地防静电措施；

b） 现场设备应符合各行业领域相关标准的要求。

5.1.1.8 温、湿度控制

本项要求包括：

a） 机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；

b） 现场设备应符合所选用设备的物理和环境条件。

5.1.1.9 电力供应

应在机房供电线路上配置稳压器和过电压防护设备。

5.1.1.10 电磁防护

现场设备应符合所选用设备的物理和环境条件。

5.1.2 边界防护

本项要求包括：

a) 应对控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，进行监视和控制区域边界通信；

b) 应能识别控制网络和非控制网络上的边界通讯入侵行为，并有效阻断。

5.1.3 生产管理层安全要求

5.1.3.1 网络和通信安全

5.1.3.1.1 无线使用控制

根据普遍接受的安全工业实践，应对无线连接的授权、监视以及执行使用进行限制。

5.1.3.1.2 访问控制

本项要求包括：

a) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

b) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话。

c) 应根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。

d) 应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。

5.1.3.1.3 安全审计

本项要求包括：

a) 应能生成安全相关审计记录，包括：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源(源设备、软件进程或人员用户账户)、分类、类型、事件 ID 和事件结果。

b) 根据一般公认的日志管理和系统配置的建议，系统应设置足够的审计记录存储容量。系统应提供审计机制来减少超出容量的可能性。

c) 在审计事件的处理失败时，系统能对人员进行警示并防止丧失基本服务和功能。根据普遍接受的工业实践和建议，系统应能在审计处理失败的情况下，采取恰当响应行动。

d) 授权人员和/或工具以只读方式访问审计日志。

5.1.3.2 设备和计算安全

5.1.3.2.1 身份鉴别

本项要求包括：

a) 应在所有接口上执行标识和鉴别。当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。
b) 应支持用户、组、角色或者接口的标识符管理功能。
c) 应能初始化鉴别器内容；系统一经安装完成，立即改变所有鉴别器的默认值；改变或者刷新所有的鉴别器；当存储或者传输的时候，要保护鉴别器免受未经授权的泄露和修改。
d) 对于使用设备的用户，应通过硬件机制保护相关鉴别器。
e) 对于使用口令鉴别机制的设备，设备应能通过设置最小长度和多种字符类型，实现强制配置口令强度。
f) 应能隐藏鉴别过程中的鉴别信息反馈。
g) 应针对任何用户（人员、软件进程或设备）在可配置时间周期内，对连续无效的访问尝试进行可配置次数限制。当限制次数超出后，应在规定的周期内拒绝访问或者直到管理员解锁。对于代表关键服务或者服务器运行的系统账户，不应允许交互式登录。
h) 在进行鉴别之前，应能显示系统提示信息。使用提示信息应可通过授权人进行配置。

5.1.3.2.2 访问控制

本项要求包括：

a) 应能支持授权用户管理所有账户，包括添加、激活、修改、禁用和删除账户；
b) 应限制默认账户的访问权限，重命名系统默认账户，修改默认口令；
c) 应及时删除多余的、过期的账户，避免共享账户的存在。

5.1.3.2.3 入侵防范

见 GB/T 22239 中的相关要求。

5.1.3.2.4 恶意代码防范

本项要求包括：

a) 应能对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出系统；监视移动代码的使用。
b) 应能应用保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响。应能更新防护机制。

5.1.3.2.5 资源控制

在不影响当前安全状态下，系统应能切换至和切换出应急电源的供应。

5.1.3.3 应用和数据安全

5.1.3.3.1 身份鉴别

见 GB/T 22239 中的相关要求。

5.1.3.3.2 访问控制

见 GB/T 22239 中的相关要求。

5.1.3.3.3 软件容错

见 GB/T 22239 中的相关要求。

5.1.3.3.4 数据完整性

见 GB/T 22239 中的相关要求。

5.1.3.3.5 数据保密性

本项要求包括：

a) 无论在信息存储或传输时，都应对有明确读权限的信息提供保密性保护；

b) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

5.1.3.3.6 数据备份恢复

见 GB/T 22239 中的相关要求。

5.1.4 过程监控层安全要求

5.1.4.1 网络和通信安全

5.1.4.1.1 网络架构

应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络和非关键控制系统网络进行逻辑分区。

5.1.4.1.2 无线使用控制

应对无线连接的授权、监视以及执行使用进行限制。

5.1.4.1.3 访问控制

本项要求包括：

a) 应提供在一个可配置的非活动时间周期后，或通过手动启动，通过启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

b) 应在根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。

c) 应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。

5.1.4.1.4 入侵防范

应在有效的补救条件下识别和处理错误状况，该过程不应泄露任何安全相关信息，除非及时排除故障会不可避免地泄露某些信息。

5.1.4.1.5 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) 根据一般公认的日志管理和系统配置的建议，应设置足够的审计记录存储容量，提供审计机制来减少超出容量的可能性。

c) 在审计事件的处理失败时，应警示人员采取恰当响应行动，防止丧失基本服务和功能。

d） 应授权人员和/或工具以只读方式访问审计日志。

5.1.4.2 设备和计算安全

5.1.4.2.1 身份鉴别

本项要求包括：

a） 对于使用口令鉴别机制的设备，设备应具有通过设置最小长度和多种字符类型，从而达到强制配置口令强度的能力；可能对实时性产生影响进而影响到系统正常操作的，应采用其他替代安全手段或通过管理手段弥补。

b） 应在可配置时间周期内，对连续无效的访问，尝试对可配置次数进行限制。

c） 应具有登录失败处理功能，应配置并启用结束会话、当登录连接超时自动退出等相关措施。

5.1.4.2.2 访问控制

本项要求包括：

a） 应支持授权用户管理所有账户，包括添加、激活、修改、禁用和删除账户；

b） 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话；

c） 对于所有接口，应根据职责分离和最小权限对特定用户（人员、软件进程或设备）实施控制系统的控制使用授权；

d） 在日常维护时，应支持安全功能操作的验证和报告异常事件；

e） 应重命名系统默认账户，修改默认口令，禁止在工程师站、操作员站、服务器使用默认账户；

f） 应及时删除多余的、过期的账户，避免共享账户的存在。

5.1.4.2.3 安全审计

本项要求包括：

a） 应生成安全相关审计记录，类别有：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b） 应授权人员和/或工具以只读方式访问审计日志。

5.1.4.2.4 入侵防范

本项要求包括：

a） 应自动执行可配置的使用限制，其中包括：防止使用便携式和移动设备；要求特定内容的授权；限制来自/写入便携式和移动设备的代码和数据传输。

b） 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

c） 所有主机设备操作系统采用最小化系统安装原则，除了必要的安全组件或软件外，只安装与自身业务相关的操作系统组件及应用软件，如工程师站、操作员站只安装组态软件、监控软件、编程软件、报表软件以及与此相关的操作系统组件，OPC 服务器、实时数据库服务器只安装数据库软件、服务器软件以及与此业务相关的操作系统组件。

5.1.4.2.5 恶意代码防范

本项要求包括：

a） 应对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出控制系统；监视移动代码的使用。
b） 应采取保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响，应更新防护机制。

5.1.4.2.6 资源控制

应参照供应商提供的指南，根据所推荐的网络和安全配置进行系统设置。

5.1.4.3 应用和数据安全

5.1.4.3.1 身份鉴别

本项要求包括：
a） 应唯一地标识和鉴别所有人员用户。应在所有接口上执行标识和鉴别。当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。
b） 应在可配置时间周期内，对连续无效的访问，尝试对可配置次数进行限制。
c） 应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

5.1.4.3.2 访问控制

本项要求包括：
a） 应支持授权用户来管理所有账户，包括添加、激活、修改、禁用和删除账户；
b） 对于所有接口，应根据职责分离和最小权限对所有用户实施控制使用授权；
c） 应重命名系统默认账户，修改默认口令，禁止在工程师站、操作员站、服务器使用默认账户；
d） 应及时删除多余的、过期的账户，避免共享账户的存在。

5.1.4.3.3 安全审计

本项要求包括：
a） 应生成安全相关审计记录，类别有：访问控制、请求错误、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。
b） 授权人员和/或工具应使用只读方式访问审计日志。

5.1.4.3.4 软件容错

应对数据有效性进行检验，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

5.1.4.3.5 资源控制

应对任何给定软件进程的每个接口限制并发会话数量。

5.1.4.3.6 数据完整性

本项要求包括：
a） 应保护传输信息完整性；
b） 应检测、记录、报告、防止对软件和信息的未经授权更改；
c） 应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

5.1.4.3.7 数据保密性

本项要求包括：

a) 无论在信息存储或传输时，都应对有明确读权限的信息提供保密性保护；
b) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

5.1.4.3.8 数据备份恢复

本项要求包括：

a) 应在不影响正常设备使用的前提下，识别和定位关键文件，以及备份用户级和系统级的信息（包括系统状态信息）；
b) 应定期记录一个安全状态，在系统受到破坏或发生失效后，应能够恢复和重构控制系统到一个已知的安全状态。

5.1.5 现场控制层安全要求

5.1.5.1 网络和通信安全

5.1.5.1.1 网络架构

应提供将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络和非关键控制系统网络进行逻辑分区的能力。

5.1.5.1.2 无线使用控制

本项要求包括：

a) 根据普遍接受的安全工业实践，对无线连接的授权、监视以及执行使用限制；
b) 应能够标识和鉴别所有参与无线通讯的用户（设备）。

5.1.5.1.3 访问控制

本项要求包括：

a) 应在根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信；
b) 应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。

5.1.5.1.4 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、操作系统事件、控制系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。
b) 根据一般公认的日志管理和系统配置的建议，控制系统应设置足够的审计记录存储容量。控制系统应提供审计机制来减少超出容量的可能性。
c) 在审计事件的处理失败时，控制系统应提供警示人员的能力和防止丧失基本服务和功能。根据普遍接受的工业实践和建议，控制系统应提供这样的能力，在审计处理失败的情况下，采取恰当响应行动。
d) 授权人员和/或工具以只读方式访问审计日志。

5.1.5.2 设备和计算安全安全审计

本项要求包括：

a) 应提供生成安全相关审计记录的能力，类别有：访问控制、请求错误、配置改变、潜在的侦察活

动和审计日志事件。单个审计记录应包括时间戳、来源(源设备、软件进程或人员用户账户)、分类、类型、事件 ID 和事件结果。

b) 授权人员和/或工具以只读方式访问审计日志。

5.1.5.3 应用和数据安全

5.1.5.3.1 数据完整性

应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

5.1.5.3.2 数据备份恢复

在受到破坏或发生失效后,应恢复和重构控制系统到一个已知的安全状态。

5.1.6 现场设备层安全要求

5.1.6.1 网络和通信安全无线使用控制

对于采用网络(工业无线/现场总线)通讯的联网设备,应确保无线空中接口安全。

5.1.6.2 应用和数据安全

5.1.6.2.1 数据完整性

本项要求包括:

a) 对于采用网络(工业无线/现场总线)通讯的联网设备,应保护传输信息完整性;

b) 对于采用网络(工业无线/现场总线)通讯的联网设备,应防止对软件和信息的未授权更改;

c) 对于采用网络(工业无线/现场总线)通讯的联网设备,应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

5.1.6.2.2 数据备份恢复

本项要求包括:

a) 对于采用网络(工业无线/现场总线)通讯的联网设备,应在不影响正常设备使用的前提下,提供关键文件的识别和定位,包括设备状态信息的能力;

b) 对于采用网络(工业无线/现场总线)通讯的联网设备,在受到破坏或发生失效后,应能够恢复和重构设备到一个已知的安全状态。

5.2 管理要求

5.2.1 安全管理机构和人员

5.2.1.1 岗位设置

应设立工控系统管理员、工控网络管理员、工控安全管理员等岗位,并定义各个工作岗位的职责。

5.2.1.2 人员配备

应配备一定数量的工控系统管理员、工控网络管理员、工控安全管理员等。

5.2.2 安全运维管理漏洞和风险管理

本项要求包括:

a） 应定期开展安全测评，形成安全测评报告，提出整改建议和计划；
b） 应采取必要的措施识别安全漏洞和隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；或评估可能的影响后采取必要的补救措施，补救措施宜在系统维护期间开展。

6 第二级基本要求

6.1 技术要求

6.1.1 物理和环境安全

6.1.1.1 物理位置选择

应符合所选用设备的物理和环境条件。

6.1.1.2 物理访问控制

本项要求包括：
a） 进入安全区域边界有明确的防止非授权人员接触的提示标志；
b） **有防止非授权人员进入的物理措施**（如栅栏）。

6.1.1.3 防盗窃和防破坏

应将设备或主要部件进行固定。

6.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

6.1.1.5 防火

本项要求包括：
a） 机房应设置灭火设备；
b） **机房应设置火灾报警消防系统，能够检测火情、报警，并灭火**。

6.1.1.6 防水和防潮

应符合所选用设备的物理和环境条件。

6.1.1.7 防静电

本项要求包括：
a） 机房应安装防静电地板并采用必要的接地防静电措施；
b） 现场设备应符合各行业领域相关标准的要求。

6.1.1.8 温、湿度控制

本项要求包括：
a） 机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；
b） 现场设备应符合所选用设备的物理和环境条件。

6.1.1.9 电力供应

应在机房供电线路上配置稳压器和过电压防护设备。

6.1.1.10 电磁防护

现场设备应符合所选用设备的物理和环境条件。

6.1.2 边界防护

本项要求包括：

a) 应对控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，进行监视和控制区域边界通信；

b) **应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，默认拒绝所有非必要的网络数据流，允许例外网络数据流；**

c) 应能识别控制网络和非控制网络上的边界通讯入侵行为，并有效阻止。

6.1.3 生产管理层安全要求

6.1.3.1 网络和通信安全

6.1.3.1.1 网络架构

见 GB/T 22239 中的相关要求。

6.1.3.1.2 通信传输

应利用会话完整性机制，保证会话完整性。

6.1.3.1.3 无线使用控制

本项要求包括：

a) 根据普遍接受的安全工业实践，应对无线连接的授权、监视以及执行使用进行限制；

b) **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。**

6.1.3.1.4 访问控制

本项要求包括：

a) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

b) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话。

c) 应**在网络边界或安全域之间**根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。

d) 应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。

6.1.3.1.5 入侵防范

应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用以攻击信息安全管理系统的信息，除非透露这一信息对于及时排除故障是必要的。

6.1.3.1.6 安全审计

本项要求包括：

a) 应能生成安全相关审计记录，包括：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) 根据一般公认的日志管理和系统配置的建议，系统应设置足够的审计记录存储容量。系统应提供审计机制来减少超出容量的可能性。

c) 在审计事件的处理失败时，系统能对人员进行警示并防止丧失基本服务和功能。根据普遍接受的工业实践和建议，系统应能在审计处理失败的情况下，采取恰当响应行动。

d) **在审计记录生成时，系统应提供时间戳。**

e) **应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。**

f) 授权人员和/或工具以只读方式访问审计日志。

6.1.3.2 设备和计算安全

6.1.3.2.1 身份鉴别

本项要求包括：

a) **应能唯一地鉴别和认证全部人员用户。**应在所有接口上执行标识和鉴别。当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。

b) **应在进行系统访问时，使所有接口根据适用的安全策略和规程支持最小权限，实施标识和鉴别。**

c) 应支持用户、组、角色或者接口的标识符管理功能。

d) 应能初始化鉴别器内容；系统一经安装完成，立即改变所有鉴别器的默认值；改变或者刷新所有的鉴别器；当存储或者传输的时候，要保护鉴别器免受未经授权的泄露和修改。

e) 对于使用设备的用户，应通过硬件机制保护相关鉴别器。

f) 对于使用口令鉴别机制的设备，设备应能通过设置最小长度和多种字符类型，实现强制配置口令强度。

g) 应能隐藏鉴别过程中的鉴别信息反馈。

h) 应针对任何用户（人员、软件进程或设备）在可配置时间周期内，对连续无效的访问尝试进行可配置次数限制。当限制次数超出后，应在规定的周期内拒绝访问或者直到管理员解锁。对于代表关键服务或者服务器运行的系统账户，不应允许交互式登录。

i) 在进行鉴别之前，应能显示系统提示信息。使用提示信息应可通过授权人进行配置。

j) **当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。**

6.1.3.2.2 访问控制

本项要求包括：

a) 应能支持授权用户管理所有账户，包括添加、激活、修改、禁用和删除账户；

b) **应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话；**

c) **对于所有接口，应根据职责分离和最小权限对特定用户（人员、软件进程或设备）实施控制系统的控制使用授权；**

d) **应能使授权用户或角色，对所有人员用户的许可到角色映射进行规定和修改；**

e) **应能在日常维护时，进行安全功能操作的验证和报告异常事件；**

f) 应限制默认账户的访问权限，重命名系统默认账户，修改默认口令；

g) 应及时删除多余的、过期的账户，避免共享账户的存在。

6.1.3.2.3 安全审计

见 GB/T 22239 中的相关要求。

6.1.3.2.4 入侵防范

见 GB/T 22239 中的相关要求。

6.1.3.2.5 恶意代码防范

本项要求包括：

a) 应能对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出系统；监视移动代码的使用。

b) 应能应用保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响。应能更新防护机制。

c) 应在所有入口和出口提供恶意代码防护机制。

6.1.3.2.6 资源控制

在不影响当前安全状态下，系统应能切换至和切换出应急电源的供应。

6.1.3.3 应用和数据安全

6.1.3.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

6.1.3.3.2 身份鉴别

见 GB/T 22239 中的相关要求。

6.1.3.3.3 访问控制

见 GB/T 22239 中的相关要求。

6.1.3.3.4 安全审计

见 GB/T 22239 中的相关要求。

6.1.3.3.5 软件容错

见 GB/T 22239 中的相关要求。

6.1.3.3.6 资源控制

见 GB/T 22239 中的相关要求。

6.1.3.3.7 数据完整性

见 GB/T 22239 中的相关要求。

6.1.3.3.8 数据保密性

本项要求包括：

a) 无论在信息存储或传输时，都应对有明确读权限的信息提供保密性保护；

b) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

6.1.3.3.9 数据备份恢复

见 GB/T 22239 中的相关要求。

6.1.3.3.10 剩余信息保护

见 GB/T 22239 中的相关要求。

6.1.4 过程监控层安全要求

6.1.4.1 网络和通信安全

6.1.4.1.1 网络架构

本项要求包括：

a) 应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络非关键控制系统网络进行逻辑分区；

b) **应将控制系统网络与非控制系统网络进行物理分段，将关键控制系统网络和非关键控制系统网络进行物理分段。**

6.1.4.1.2 通信传输

应保护会话完整性的能力，应拒绝任何非法会话 ID 的使用。

6.1.4.1.3 无线使用控制

本项要求包括：

a) **应对所有参与无线通信的用户(设备)提供唯一性标识和鉴别；**

b) 应对无线连接的授权、监视以及执行使用进行限制。

6.1.4.1.4 访问控制

本项要求包括：

a) 应提供在一个可配置的非活动时间周期后，或通过手动启动，通过启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

b) **应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话。**

c) 应**在网络边界或安全域之间**根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。

d) 应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。

6.1.4.1.5 入侵防范

应在有效的补救条件下识别和处理错误状况，该过程不应泄露任何安全相关信息，除非及时排除故

障会不可避免地泄露某些信息。

6.1.4.1.6 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) 根据一般公认的日志管理和系统配置的建议，应设置足够的审计记录存储容量，提供审计机制来减少超出容量的可能性。

c) **在审计事件的处理失败时，应警示人员采取恰当响应行动，防止丧失基本服务和功能。**

d) **在审计记录生成时，控制系统应提供时间戳。**

e) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。

f) 应授权人员和/或工具以只读方式访问审计日志。

6.1.4.2 设备和计算安全

6.1.4.2.1 身份鉴别

本项要求包括：

a) **应支持用户、组、角色或者接口的标识符管理功能；应在所有人机接口上执行标识和鉴别，当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。**

b) 对于使用口令鉴别机制的设备，设备应具有通过设置最小长度和多种字符类型，从而达到强制配置口令强度的能力；可能对实时性产生影响进而影响到系统正常操作的，应采用其他替代安全手段或通过管理手段弥补。

c) 应在可配置时间周期内，对连续无效的访问进行可配置次数限制。

d) **当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。**

e) 应具有登录失败处理功能，应配置并启用结束会话、**限制非法登录次数和**当登录连接超时自动退出等相关措施。

6.1.4.2.2 访问控制

本项要求包括：

a) 应支持授权用户管理所有账户，包括添加、激活、修改、禁用和删除账户；

b) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话；

c) 对于所有接口，应根据职责分离和最小权限对特定用户（人员、软件进程或设备）实施控制系统的控制使用授权；

d) **应授权用户或角色对所有人员用户的访问权限进行规定和修改；**

e) 在日常维护时，应支持安全功能操作的验证和报告异常事件；

f) 应重命名系统默认账户，修改默认口令，禁止在工程师站、操作员站、服务器使用默认账户；

g) 应及时删除多余的、过期的账户，避免共享账户的存在。

6.1.4.2.3 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账

户)、分类、类型、事件 ID 和事件结果。

b) **在审计记录生成时,设备应提供时间戳。**

c) **应保护审计信息和审计工具(如有),防止其在未授权情况下被获取、修改和删除。**

d) 应授权人员和/或工具以只读方式访问审计日志。

6.1.4.2.4 入侵防范

本项要求包括:

a) 应自动执行可配置的使用限制,其中包括:防止使用便携式和移动设备;要求特定内容的授权;限制来自/写入便携式和移动设备的代码和数据传输。

b) 应通过手动或在一个可配置非活动周期后,系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效,直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

c) **应在有效的补救条件下识别和处理错误状况,该过程不应泄露任何安全相关信息,除非及时排除故障会不可避免地泄露某些信息。**

d) 所有主机设备操作系统采用最小化系统安装原则,除了必要的安全组件或软件外,只安装与自身业务相关的操作系统组件及应用软件,如工程师站、操作员站只安装组态软件、监控软件、编程软件、报表软件以及与此相关的操作系统组件,OPC 服务器、实时数据库服务器只安装数据库软件、服务器软件以及与此业务相关的操作系统组件。

6.1.4.2.5 恶意代码防范

本项要求包括:

a) 应对可能造成损害的移动代码技术执行使用限制,包括:防止移动代码的执行;对于代码的来源要求适当的鉴别和授权;限制移动代码传入/传出控制系统;监视移动代码的使用;

b) 应采取保护机制,防止、检测、报告和减轻恶意代码或未经授权软件的影响,应更新防护机制。

6.1.4.2.6 资源控制

应参照供应商提供的指南,根据所推荐的网络和安全配置进行系统设置。

6.1.4.3 应用和数据安全

6.1.4.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

6.1.4.3.2 身份鉴别

本项要求包括:

a) 应唯一地标识和鉴别所有人员用户。应在所有接口上执行标识和鉴别。当有人员用户访问时,应根据适用的安全策略和规程实施职责分离和最小权限。

b) **对于使用口令鉴别机制的应用,应具有通过设置最小长度和多种字符类型,从而达到强制配置口令强度的能力;可能对实时性产生影响进而影响到系统正常操作的,应采用其他替代安全手段或通过管理手段弥补。**

c) 应在可配置时间周期内,对连续无效的访问,尝试对可配置次数进行限制。

d) **当进行远程管理时,应采取必要措施,防止鉴别信息在网络传输过程中被窃听。**

e) 应提供并启用登录失败处理功能,多次登录失败后应采取必要的保护措施。

6.1.4.3.3 访问控制

本项要求包括：

a) 应支持授权用户来管理所有账户，包括添加、激活、修改、禁用和删除账户。

b) **应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。**

c) 对于所有接口，应根据职责分离和最小权限对所有用户实施控制使用授权。

d) **应为授权用户或角色提供这样的能力，即对所有人员的访问权限进行规定和修改。**

e) 应重命名系统默认账户，修改默认口令，禁止在工程师站、操作员站、服务器使用默认账户。

f) 应及时删除多余的、过期的账户，避免共享账户的存在。

6.1.4.3.4 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) **在审计记录生成时，设备应提供时间戳。**

c) **应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。**

d) 授权人员和/或工具应使用只读方式访问审计日志。

6.1.4.3.5 软件容错

本项要求包括：

a) 应对数据有效性进行检验，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

b) **在故障发生时，应能够继续提供基本功能，确保能够实施必要的措施。**

6.1.4.3.6 资源控制

本项要求包括：

a) 应对任何给定软件进程的每个接口限制并发会话数量；

b) **当应用系统中的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。**

6.1.4.3.7 数据完整性

本项要求包括：

a) 应保护传输信息完整性；

b) 应检测、记录、报告、防止对软件和信息的未经授权更改；

c) 应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

6.1.4.3.8 数据保密性

本项要求包括：

a) 无论在信息存储或传输时，都应对有明确读权限的信息提供保密性保护；

b) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

6.1.4.3.9 数据备份恢复

本项要求包括：

a) 应在不影响正常设备使用的前提下，识别和定位关键文件，以及备份用户级和系统级的信息（包括系统状态信息）；

b) **应验证备份机制可靠性；**

c) 应定期记录一个安全状态，在系统受到破坏或发生失效后，应能够恢复和重构控制系统到一个已知的安全状态。

6.1.4.3.10 剩余信息保护

本项要求包括：

a) **清除不再使用的和/或退役组件上的具有显式读权限访问的信息；**

b) **应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。**

6.1.5 现场控制层安全要求

6.1.5.1 网络和通信安全

6.1.5.1.1 网络架构

本项要求包括：

a) 应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络和非关键控制系统网络进行逻辑分区；

b) **应将控制系统网络与非控制系统网络进行物理分段，将关键控制系统网络和非关键控制系统网络进行物理分段。**

6.1.5.1.2 通信传输

应保护会话完整性。控制系统应拒绝任何非法会话 ID 的使用。

6.1.5.1.3 无线使用控制

本项要求包括：

a) 应对所有参与无线通信的用户（设备）提供**唯一性**标识和鉴别；

b) 根据普遍接受的安全工业实践，对无线连接的授权、监视以及执行使用限制。

6.1.5.1.4 访问控制

本项要求包括：

a) 应**在网络边界或安全域之间**根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信；

b) 应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。

6.1.5.1.5 入侵防范

本项要求包括：

a) **应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用的信息安全管理系统的信息，除非排除故障过程中应透露这一信息。**

b) **应在关键网络节点处监视网络攻击行为。**

6.1.5.1.6 恶意代码防范

本项要求包括：

a) **应提供对可能造成损害的移动代码技术执行使用限制的能力，包括：限制移动代码传入/传出控制系统；监视移动代码的使用；**

b) **应在所有入口和出口提供恶意代码防护机制。**

6.1.5.1.7 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、操作系统事件、控制系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) 根据一般公认的日志管理和系统配置的建议，控制系统应设置足够的审计记录存储容量。控制系统应提供审计机制来减少超出容量的可能性。

c) 在审计事件的处理失败时，控制系统应提供警示人员的能力和防止丧失基本服务和功能。根据普遍接受的工业实践和建议，控制系统应提供这样的能力，在审计处理失败的情况下，采取恰当响应行动。

d) **在审计记录生成时，控制系统应提供时间戳。**

e) **应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。**

f) 授权人员和/或工具以只读方式访问审计日志。

g) **应在网络边界、重要网络节点进行安全审计，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。**

6.1.5.2 设备和计算安全

6.1.5.2.1 安全审计

本项要求包括：

a) 应提供生成安全相关审计记录的能力，类别有：访问控制、请求错误、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) **在审计记录生成时，设备应提供时间戳。**

c) **应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。**

d) 授权人员和/或工具以只读方式访问审计日志。

e) **应启用安全审计功能，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。**

6.1.5.2.2 入侵防范

本项要求包括：

a) **应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用的信息安全管理系统的信息，除非排除故障过程中应透露这一信息。**

b) **应遵循最小安装的原则，仅安装需要的组件和应用程序。**

c) **应关闭不需要的系统服务、默认共享和高危端口。**

d) **停机维护期间，应能发现可能存在的漏洞，并在充分测试评估后，及时修补漏洞。**

6.1.5.3 应用和数据安全

6.1.5.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

6.1.5.3.2 数据完整性

本项要求包括:

a) 应保护传输信息完整性;

b) 应防止对软件和信息的未授权更改;

c) 应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

6.1.5.3.3 数据保密性

本项要求包括:

a) 在信息传输时,应对有明确读权限的信息进行保密性保护;

b) 在进行加密时,应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

6.1.5.3.4 数据备份恢复

本项要求包括:

a) 应在不影响正常设备使用的前提下进行对关键文件的识别和定位,以及用户级和系统级的信息备份(包括系统状态信息);

b) 应验证备份机制可靠性;

c) 在受到破坏或发生失效后,应能够恢复和重构控制系统到一个已知的安全状态。

6.1.6 现场设备层安全要求

6.1.6.1 网络和通信安全无线使用控制

对于采用网络(工业无线/现场总线)通讯的联网设备,应确保无线空中接口安全。

6.1.6.2 应用和数据安全

6.1.6.2.1 数据完整性

本项要求包括:

a) 对于采用网络(工业无线/现场总线)通讯的联网设备,应保护传输信息完整性;

b) 对于采用网络(工业无线/现场总线)通讯的联网设备,应防止对软件和信息的未授权更改;

c) 对于采用网络(工业无线/现场总线)通讯的联网设备,应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

6.1.6.2.2 数据备份恢复

本项要求包括:

a) 对于采用网络(工业无线/现场总线)通讯的联网设备,应在不影响正常设备使用的前提下,提供关键文件的识别和定位,包括设备状态信息的能力;

b) 对于采用网络(工业无线/现场总线)通讯的联网设备,应提供验证备份机制可靠性的能力;

c) 对于采用网络(工业无线/现场总线)通讯的联网设备,在受到破坏或发生失效后,应能够恢复和重构设备到一个已知的安全状态。

6.2 管理要求

6.2.1 安全管理机构和人员

6.2.1.1 岗位设置

本项要求包括:

a) **应设立信息安全管理工作的职能部门,设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责;**

b) 应设立工控系统管理员、工控网络管理员、工控安全管理员等岗位,并定义部门及各个工作岗位的职责。

6.2.1.2 人员配备

应配备一定数量的工控系统管理员、工控网络管理员、工控安全管理员等;

6.2.2 安全运维管理漏洞和风险管理

本项要求包括:

a) 应定期开展安全测评,形成安全测评报告,提出整改建议和计划;

b) 应采取必要的措施识别安全漏洞和隐患,并根据风险分析的后果,对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补;或评估可能的影响后采取必要的补救措施,补救措施宜在系统维护期间开展。

7 第三级基本要求

7.1 技术要求

7.1.1 物理和环境安全

7.1.1.1 物理位置选择

应符合所选用设备的物理和环境条件。

7.1.1.2 物理访问控制

本项要求包括:

a) 进入安全区域边界有明确的防止非授权人员接触的提示标志;

b) 有防止非授权人员进入的物理措施(如栅栏);

c) **有身份识别机制手段(如门禁、视频监视等)或专人值守。**

7.1.1.3 防盗窃和防破坏

本项要求包括:

a) 应将设备或主要部件进行固定;

b) **对通信线缆实施防护,如可铺设在地下或管道中。**

7.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

7.1.1.5 防火

本项要求包括：

a） 机房应设置灭火设备；

b） 机房应设置火灾报警消防系统，能够检测火情、报警，并灭火。

7.1.1.6 防水和防潮

应符合所选用设备的物理和环境条件。

7.1.1.7 防静电

本项要求包括：

a） 机房应安装防静电地板并采用必要的接地防静电措施；

b） 现场设备应符合各行业领域相关标准的要求。

7.1.1.8 温、湿度控制

本项要求包括：

a） 机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；

b） 现场设备应符合所选用设备的物理和环境条件。

7.1.1.9 电力供应

本项要求包括：

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） **应为机房提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。**

7.1.1.10 电磁防护

现场设备应符合所选用设备的物理和环境条件。

7.1.2 边界防护

本项要求包括：

a） 应对控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，进行监视和控制区域边界通信；

b） 应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，默认拒绝所有非必要的网络数据流，允许例外网络数据流；

c） **应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界上，阻止任何通过的非必要通信；**

d） **应在控制网络和非控制网络的边界防护机制失效时，能阻止所有边界通信（也称故障关闭）；但故障关闭功能的设计不应干扰安全相关功能的运行；**

e） **应在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，并保障不影响关键设备通讯；**

f） **应确保无线网络通过受控的控制网络和非控制网络的边界，以及控制系统内安全域和安全域**

之间的边界时，边界防护设备接入（有线）网络；

g） 应能识别控制网络和非控制网络上的边界通讯入侵行为，并有效阻断。

7.1.3 集中管控

见 GB/T 22239 中的相关要求。

7.1.4 生产管理层安全要求

7.1.4.1 网络和通信安全

7.1.4.1.1 网络架构

见 GB/T 22239 中的相关要求。

7.1.4.1.2 通信传输

应利用会话完整性机制，保证会话完整性。

7.1.4.1.3 无线使用控制

本项要求包括：

a） 根据普遍接受的安全工业实践，应对无线连接的授权、监视以及执行使用进行限制；

b） 应对所有参与无线通信的用户（设备）提供唯一性标识和鉴别。

7.1.4.1.4 访问控制

本项要求包括：

a） 对一个可配置的时间或事件序列，应支持主管手动超驰当前人员用户授权。

b） 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

c） 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话。

d） 应在网络边界或安全域之间根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。

e） 应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。

7.1.4.1.5 入侵防范

本项要求包括：

a） 应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用以攻击信息安全管理系统的信息，除非透露这一信息对于及时排除故障是必要的。

b） 应禁止传输、接收私人消息。

c） 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。

d） 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。

e） 应采取技术措施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。

f） 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。

7.1.4.1.6 恶意代码防范

本项要求包括：

a) **应在关键网络节点处对恶意代码进行检测和清除，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。**

7.1.4.1.7 安全审计

本项要求包括：

a) 应能生成安全相关审计记录，包括：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) **应能集中管理审计事件并从系统多个组件收集审计记录，系统范围（逻辑或物理）的时间相关审计踪迹。应能按照工业标准格式输出这些审计记录，用于商业日志分析工具进行分析，例如，安全信息和事件管理。**

c) 根据一般公认的日志管理和系统配置的建议，系统应设置足够的审计记录存储容量。系统应提供审计机制来减少超出容量的可能性。

d) **当分配审计记录存储值达到最大审计记录存储容量的配置比例时，系统应能发出警告；当容量超出时，支持覆盖。**

e) 在审计事件的处理失败时，系统能对人员进行警示并防止丧失基本服务和功能。根据普遍接受的工业实践和建议，系统应能在审计处理失败的情况下，采取恰当响应行动。

f) 在审计记录生成时，系统应提供时间戳。

g) **应在可配置的频率下，对系统时钟进行同步。**

h) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。

i) 授权人员和/或工具以只读方式访问审计日志。

j) **应提供编程访问审计记录的能力。**

7.1.4.2 设备和计算安全

7.1.4.2.1 身份鉴别

本项要求包括：

a) 应能唯一地鉴别和认证全部人员用户。应在所有接口上执行标识和鉴别。当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。

b) **应能对所有使用人员用户实施多因子鉴别。**

c) **应能对所有设备提供唯一性标识和鉴别。**应在进行系统访问时，使所有接口根据适用的安全策略和规程支持最小权限，实施标识和鉴别。

d) 应支持用户、组、角色或者接口的标识符管理功能。

e) 应能初始化鉴别器内容；系统一经安装完成，立即改变所有鉴别器的默认值；改变或者刷新所有的鉴别器；当存储或者传输的时候，要保护鉴别器免受未经授权的泄露和修改。

f) 对于使用设备的用户，应通过硬件机制保护相关鉴别器。

g) 对于使用口令鉴别机制的设备，设备应能通过设置最小长度和多种字符类型，实现强制配置口令强度。

h) **设备应防止任何已有的用户账户重复使用同一批口令。此外，设备应加强用户口令的最大和最小有效期的使用。这些能力应符合一般公认的安全产业实践要求。**

i) **应根据通用的可以接受的安全行业实践和建议，通过硬件机制来保护相关的私钥。**

j) 应能隐藏鉴别过程中的鉴别信息反馈。

k) 应针对任何用户（人员、软件进程或设备）在可配置时间周期内，对连续无效的访问尝试进行可配置次数限制。当限制次数超出后，应在规定的周期内拒绝访问或者直到管理员解锁。对于代表关键服务或者服务器运行的系统账户，不应允许交互式登录。

l) 在进行鉴别之前，应能显示系统提示信息。使用提示信息应可通过授权人进行配置。

m) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

7.1.4.2.2 访问控制

本项要求包括：

a) 应能支持授权用户管理所有账户，包括添加、激活、修改、禁用和删除账户；

b) **应能支持统一账户管理；**

c) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话；

d) 对于所有接口，应根据职责分离和最小权限对特定用户（人员、软件进程或设备）实施控制系统的控制使用授权；

e) 应能使授权用户或角色，对所有人员用户的许可到角色映射进行规定和修改；

f) 应能在日常维护时，进行安全功能操作的验证和报告异常事件；

g) 应限制默认账户的访问权限，重命名系统默认账户，修改默认口令；

h) 应及时删除多余的、过期的账户，避免共享账户的存在。

7.1.4.2.3 安全审计

见 GB/T 22239 中的相关要求。

7.1.4.2.4 入侵防范

见 GB/T 22239 中的相关要求。

7.1.4.2.5 恶意代码防范

本项要求包括：

a) 应能对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出系统；监视移动代码的使用。

b) **应能允许代码执行之前验证移动代码完整性。**

c) 应能应用保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响。应能更新防护机制。

d) 应在所有入口和出口提供恶意代码防护机制。

e) **应能管理恶意代码防护机制。**

f) **可采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。**

7.1.4.2.6 资源控制

本项要求包括：

a) 在不影响当前安全状态下，系统应能切换至和切换出应急电源的供应；

b) **应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；**

c) **应能对重要节点的服务水平降低到预先规定的最小值进行检测和报警。**

7.1.4.3 应用和数据安全

7.1.4.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

7.1.4.3.2 身份鉴别

见 GB/T 22239 中的相关要求。

7.1.4.3.3 访问控制

见 GB/T 22239 中的相关要求。

7.1.4.3.4 安全审计

见 GB/T 22239 中的相关要求。

7.1.4.3.5 软件容错

见 GB/T 22239 中的相关要求。

7.1.4.3.6 资源控制

见 GB/T 22239 中的相关要求。

7.1.4.3.7 数据完整性

见 GB/T 22239 中的相关要求。

7.1.4.3.8 数据保密性

本项要求包括:

a) 无论在信息存储或传输时,都应对有明确读权限的信息提供保密性保护;

b) 在进行加密时,应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制;

c) **应支持国家密码管理主管部门批准使用的密码算法,使用国家密码管理主管部门认证核准的密码产品,遵循相关密码国家标准和行业标准。**

7.1.4.3.9 数据备份恢复

见 GB/T 22239 中的相关要求。

7.1.4.3.10 剩余信息保护

见 GB/T 22239 中的相关要求。

7.1.5 过程监控层安全要求

7.1.5.1 网络和通信安全

7.1.5.1.1 网络架构

本项要求包括:

a) 应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络与非关键控制系统网络进行逻辑分区；
b) 应将控制系统网络与非控制系统网络进行物理分段，将关键控制系统网络与非关键控制系统网络进行物理分段；
c) **应在不与非控制系统网络相连的情况下，能为关键或非关键控制系统网络提供网络服务。**

7.1.5.1.2 通信传输

本项要求包括：

a) 应保护会话完整性，拒绝任何非法会话 ID 的使用；
b) **应在用户退出或其他会话结束（包括浏览器会话）后使会话 ID 失效；**
c) **应为每一个会话生成唯一的会话 ID 并处理非期望的会话 ID 为非法 ID。**

7.1.5.1.3 无线使用控制

本项要求包括：

a) 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；
b) 应对无线连接的授权、监视以及执行使用进行限制；
c) **应识别未经授权的无线设备在控制系统物理环境中发射，及报告对系统造成的影响。**

7.1.5.1.4 访问控制

本项要求包括：

a) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。
b) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话。
c) 应在网络边界或安全域之间根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。
d) 应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。

7.1.5.1.5 入侵防范

本项要求包括：

a) 应在有效的补救条件下识别和处理错误状况，该过程不应泄露任何安全相关信息，除非及时排除故障会不可避免地泄露某些信息；
b) **应禁止传输、接收私人消息；**
c) **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；**
d) **应禁止未经授权的数据传输；**
e) **应采取技术措施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；**
f) **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。**

7.1.5.1.6 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、潜在的侦察活动和审计日志事件。单

个审计记录应包括时间戳、来源(源设备、软件进程或人员用户账户)、分类、类型、事件 ID 和事件结果。

b) **应能集中管理审计事件,对来自系统范围(包括逻辑或物理)内的多个组件进行审计记录收集,并能集中管理时间相关的审计踪迹。应按照工业标准格式输出这些审计记录,用日志分析工具进行分析,例如,安全信息和事件管理。**

c) 根据一般公认的日志管理和系统配置的建议,应设置足够的审计记录存储容量,提供审计机制来减少超出容量的可能性。

d) **当分配审计记录存储值达到最大审计记录存储容量的配置比例时,应发出警告。**

e) 在审计事件的处理失败时,应警示人员采取恰当响应行动,防止丧失基本服务和功能。

f) 在审计记录生成时,应提供时间戳。

g) **应在可配置的频率下,对系统时钟进行同步。**

h) 应保护审计信息和审计工具(如有),防止其在未授权情况下被获取、修改和删除。

i) 应向授权人员和/或工具提供以只读的方式访问审计日志。

j) **应提供编程访问审计记录的能力。**

7.1.5.2 设备和计算安全

7.1.5.2.1 身份鉴别

本项要求包括:

a) 应支持用户、组、角色或者接口的标识符管理功能;应在所有人机接口上执行标识和鉴别,当有人员用户访问时,应根据适用的安全策略和规程实施职责分离和最小权限。

b) 对于使用口令鉴别机制的设备,设备应具有通过设置最小长度和多种字符类型,从而达到强制配置口令强度的能力;可能对实时性产生影响进而影响到系统正常操作的,应采用其他替代安全手段或通过管理手段弥补。

c) **应防止任何已有的用户账户重复使用同一批口令,并加强用户口令的最大和最小有效期的使用,以符合公认的安全产业实践要求。**

d) 应在可配置时间周期内,对连续无效的访问进行可配置次数限制;**当访问次数超出限制后,应进行报警;对于代表关键服务或者服务器运行的系统账户,应不允许交互式登录。**

e) **不允许进行远程管理。**

f) 应具有登录失败处理功能,应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

7.1.5.2.2 访问控制

本项要求包括:

a) 应支持授权用户管理所有账户,包括添加、激活、修改、禁用和删除账户;

b) 应在一个可配置非活动时间周期后自动地,或由发起会话的用户手动地终止远程会话;

c) 对于所有接口,应根据职责分离和最小权限对特定用户(人员、软件进程或设备)实施控制系统的控制使用授权;

d) 应授权用户或角色对所有人员用户的访问权限进行规定和修改;

e) 在日常维护时,应支持安全功能操作的验证和报告异常事件;

f) 应重命名系统默认账户,修改默认口令,禁止在工程师站、操作员站、服务器使用默认账户;

g) 应及时删除多余的、过期的账户,避免共享账户的存在。

7.1.5.2.3 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、控制系统事件、备份和恢复事件、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) **设备应能够为集中审计管理提供接口，将自身生成的审计记录上传。**

c) 在审计记录生成时，设备应提供时间戳。

d) **应具备以可配置频率的，与系统时钟同步的能力。**

e) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。

f) 应向授权人员和/或工具提供以只读的方式访问审计日志。

g) **应提供编程访问审计记录的能力。**

7.1.5.2.4 入侵防范

本项要求包括：

a) 应自动执行可配置的使用限制，其中包括：防止使用便携式和移动设备；要求特定内容的授权；限制来自/写入便携式和移动设备的代码和数据传输。

b) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

c) 应在有效的补救条件下识别和处理错误状况，该过程不应泄露任何安全相关信息，除非及时排除故障会不可避免地泄露某些信息。

d) 所有主机设备操作系统采用最小化系统安装原则，除了必要的安全组件或软件外，只安装与自身业务相关的操作系统组件及应用软件，如工程师站、操作员站只安装组态软件、监控软件、编程软件、报表软件以及与此相关的操作系统组件，OPC 服务器、实时数据库服务器只安装数据库软件、服务器软件以及与此业务相关的操作系统组件。

7.1.5.2.5 恶意代码防范

本项要求包括：

a) 应对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出控制系统；监视移动代码的使用。

b) **应允许代码执行之前验证移动代码完整性。**

c) 应采取保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响，应更新防护机制。

7.1.5.2.6 资源控制

本项要求包括：

a) **应对于任何给定设备的每个接口限制并发会话数量；**

b) 应参照供应商提供的指南，根据所推荐的网络和安全配置进行系统设置；

c) **应把当前的安全配置设置生成一个设备可读的报告列表；**

d) **应对工程师站、操作员站、服务器等系统运行资源进行监视，包括 CPU、硬盘、内存、网络等资源的使用情况；设置预警限值并在触发时预警。**

7.1.5.3 应用和数据安全

7.1.5.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

7.1.5.3.2 身份鉴别

本项要求包括：

a) 应唯一地标识和鉴别所有人员用户。应在所有接口上执行标识和鉴别。当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。

b) 对于使用口令鉴别机制的应用，应具有通过设置最小长度和多种字符类型，从而达到强制配置口令强度的能力；可能对实时性产生影响进而影响到系统正常操作的，应采用其他替代安全手段或通过管理手段弥补。

c) **应防止任何已有的用户账户重复使用同一批口令，并加强用户口令的最大和最小有效期的使用，以符合一般公认的安全产业实践要求。**

d) 应在可配置时间周期内，对连续无效的访问，尝试对可配置次数进行限制；**当访问次数超出限制后，应进行报警；对于代表关键服务或者服务器运行的系统账户，应不允许交互式登录。**

e) 应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

7.1.5.3.3 访问控制

本项要求包括：

a) 应支持授权用户来管理所有账户，包括添加、激活、修改、禁用和删除账户。

b) **应支持统一账户管理。**

c) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

d) 对于所有接口，应根据职责分离和最小权限对所有用户实施控制使用授权。

e) 应为授权用户或角色提供这样的能力，对所有人员的访问权限进行规定和修改。

f) 应重命名系统默认账户，修改默认口令，禁止在工程师站、操作员站、服务器使用默认账户。

g) 应及时删除多余的、过期的账户，避免共享账户的存在。

7.1.5.3.4 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、配置改变和审计日志事件。单个审计记录应包括时间戳、来源(源设备、软件进程或人员用户账户)、分类、类型、事件 ID 和事件结果。

b) 应能够为集中审计管理提供接口，将自身生成的审计记录上传。

c) 在审计记录生成时，应提供时间戳。

d) **应具备以可配置频率的，与系统时钟同步的能力。**

e) 应保护审计信息和审计工具(如有)，防止其在未授权情况下被获取、修改和删除。

f) 授权人员和/或工具应使用只读方式访问审计日志。

g) **应对审计进程进行保护，防止未经授权的中断。**

7.1.5.3.5 软件容错

本项要求包括：

a) 应对数据有效性进行检验，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

b) 在故障发生时，应能够继续提供基本功能，确保能够实施必要的措施。

7.1.5.3.6 资源控制

本项要求包括：

a) 应对任何给定软件进程的每个接口限制并发会话数量；

b) 当应用系统中的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

7.1.5.3.7 数据完整性

本项要求包括：

a) 应保护传输信息完整性；

b) 应检测、记录、报告、防止对软件和信息的未经授权更改；

c) **在完整性验证过程中发现差异时，应提供自动化工具通知给一组可配置的接收者；**

d) 应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验；

e) **应采用校验码技术或加解密技术或同等安全性的技术手段保证重要数据在存储过程中的完整性。**

7.1.5.3.8 数据保密性

本项要求包括：

a) 无论在信息存储或传输时，应对有明确读权限的信息提供保密性保护；

b) **当信息穿过任何安全域边界时，应保护其保密性；**

c) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

7.1.5.3.9 数据备份恢复

本项要求包括：

a) 应在不影响正常设备使用的前提下，识别和定位关键文件，以及备份用户级和系统级的信息（包括系统状态信息）；

b) 应验证备份机制可靠性；

c) **应在可配置的频率下，自动进行备份；**

d) 应定期记录一个安全状态，在系统受到破坏或发生失效后，应能够恢复和重构控制系统到一个已知的安全状态。

7.1.5.3.10 剩余信息保护

本项要求包括：

a) 清除不再使用的和/或退役组件上的具有显式读权限访问的信息；

b) **应防止通过易失性共享内存资源未授权地和无意地传输信息；**

c) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

d) **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。**

7.1.6 现场控制层安全要求

7.1.6.1 网络和通信安全

7.1.6.1.1 网络架构

本项要求包括：

a) 应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络和非关键控制系统网络进行逻辑分区；

b) 应将控制系统网络与非控制系统网络进行物理分段，将关键控制系统网络和非关键控制系统网络进行物理分段；

c) 应在不与非控制系统网络相连的情况下，能为关键或非关键控制系统网络提供网络服务。

7.1.6.1.2 通信传输

本项要求包括：

a) 应保护会话完整性。控制系统应拒绝任何非法会话 ID 的使用；

b) **应在用户退出或其他会话结束（包括浏览器会话）后使会话 ID 失效；**

c) **应为每一个会话生成唯一的会话 ID，并将非期望的会话 ID 处理为非法 ID。**

7.1.6.1.3 无线使用控制

本项要求包括：

a) 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；

b) 根据普遍接受的安全工业实践，对无线连接的授权、监视以及执行使用限制；

c) **识别在控制系统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行为。**

7.1.6.1.4 访问控制

本项要求包括：

a) 应在网络边界或安全域之间根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信；

b) 应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。

7.1.6.1.5 入侵防范

本项要求包括：

a) 应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用的信息安全管理系统的信息，除非排除故障过程中应透露这一信息。

b) 应在关键网络节点处检测从外部发起的网络攻击行为。

c) 应在关键网络节点处检测从内部发起的网络攻击行为。

d) 应采取技术措施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。

e) 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。

f) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

7.1.6.1.6 恶意代码防范

本项要求包括：

a) 应提供对可能造成损害的移动代码技术执行使用限制的能力，包括：限制移动代码传入/传出控制系统；监视移动代码的使用。

b) 应在所有入口和出口提供恶意代码防护机制。

7.1.6.1.7 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、操作系统事件、控制系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) 根据一般公认的日志管理和系统配置的建议，控制系统应设置足够的审计记录存储容量。控制系统应提供审计机制来减少超出容量的可能性。

c) **当分配审计记录存储值达到最大审计记录存储容量的配置比例时，控制系统应发出警告。**

d) 在审计事件的处理失败时，控制系统应警示人员和防止丧失基本服务和功能。根据普遍接受的工业实践和建议，控制系统应提供这样的能力，在审计处理失败的情况下，采取恰当响应行动。

e) 在审计记录生成时，控制系统应提供时间戳。

f) **应在可配置的频率下，对系统时钟进行同步。**

g) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。

h) 授权人员和/或工具以只读方式访问审计日志。

i) **应提供编程访问审计记录的能力。**

j) 应在网络边界、重要网络节点进行安全审计，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。

7.1.6.2 设备和计算安全

7.1.6.2.1 身份鉴别

本项要求包括：

a) **应对设备的远程管理、组态文件下装等重要操作进行身份鉴别，设备自身不具备识别能力的应采用其他技术方法或管理手段。**

b) **禁止使用默认账户和口令，口令应有复杂度要求，口令长度和特征应足够强壮，以防止通过如猜测或暴力破解等手段通过验证。若安全性不够，应使用其他手段；口令应设定有效期限，并定期更换。**

c) **应具有鉴别失败处理功能，应配置并启用结束会话、限制非法登录次数并报警，当登录连接超时自动退出等相关措施。**

d) **应采取必要的措施，防止鉴别信息在传输过程中被窃听。**

7.1.6.2.2 安全审计

本项要求包括：

a) 应提供生成安全相关审计记录的能力，类别有：访问控制、请求错误、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、

分类、类型、事件 ID 和事件结果。

b) 在审计记录生成时，设备应提供时间戳。

c) **应具备以可配置频率的，与系统时钟同步的能力**。

d) 应保护审计信息和审计工具(如有)，防止其在未授权情况下被获取、修改和删除。

e) 授权人员和/或工具以只读方式访问审计日志。

f) 应启用安全审计功能，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。

7.1.6.2.3 入侵防范

本项要求包括：

a) 应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用的信息安全管理系统的信息，除非排除故障过程中应透露这一信息。

b) 应遵循最小安装的原则，仅安装需要的组件和应用程序。

c) 应关闭不需要的系统服务、默认共享和高危端口。

d) 停机维护期间，应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。

7.1.6.2.4 资源控制

本项要求包括：

a) **应提供重要节点设备的硬件冗余，保证系统的可用性**；

b) **应能实时监控设备的运行和通信状态，并及时发现异常情况给予报警**。

7.1.6.3 应用和数据安全

7.1.6.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

7.1.6.3.2 数据完整性

本项要求包括：

a) 应保护传输信息完整性；

b) 应防止对软件和信息的未授权更改；

c) 应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验；

d) **应采用校验码技术、加解密技术或同等安全性的技术手段保证重要数据在存储过程中的完整性**。

7.1.6.3.3 数据保密性

本项要求包括：

a) 在信息传输时，应对有明确读权限的信息进行保密性保护；

b) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

7.1.6.3.4 数据备份恢复

本项要求包括：

a) 应在不影响正常设备使用的前提下进行对关键文件的识别和定位，以及用户级和系统级的信息备份(包括系统状态信息)；

b) 应验证备份机制可靠性；

c) 在受到破坏或发生失效后，应能够恢复和重构控制系统到一个已知的安全状态。

7.1.7 现场设备层安全要求

7.1.7.1 网络和通信安全无线使用控制

对于采用网络（工业无线/现场总线）通讯的联网设备，应确保无线空中接口安全。

7.1.7.2 应用和数据安全

7.1.7.2.1 数据完整性

本项要求包括：

a) 对于采用网络（工业无线/现场总线）通讯的联网设备，应保护传输信息完整性；

b) **对于采用网络（工业无线/现场总线）通讯的联网设备，应能使用密码学机制识别信息在通信过程中是否被篡改；**

c) 对于采用网络（工业无线/现场总线）通讯的联网设备，应防止对软件和信息的未授权更改；

d) **对于采用网络（工业无线/现场总线）通讯的联网设备，在完整性验证过程中发现差异时，应提供自动化工具通知给一组可配置的接收者；**

e) 对于采用网络（工业无线/现场总线）通讯的联网设备，应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

7.1.7.2.2 数据备份恢复

本项要求包括：

a) 对于采用网络（工业无线/现场总线）通讯的联网设备，应在不影响正常设备使用的前提下，提供关键文件的识别和定位，包括设备状态信息的能力；

b) 对于采用网络（工业无线/现场总线）通讯的联网设备，应提供验证备份机制可靠性的能力；

c) 对于采用网络（工业无线/现场总线）通讯的联网设备，在受到破坏或发生失效后，应能够恢复和重构设备到一个已知的安全状态。

7.2 管理要求

7.2.1 安全策略和管理制度

应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

7.2.2 安全管理机构和人员

7.2.2.1 岗位设置

本项要求包括：

a) **应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；**

b) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c) 应设立工控系统管理员、工控网络管理员、工控安全管理员等岗位，并定义部门及各个工作岗位的职责。

7.2.2.2 人员配备

本项要求包括：

a） 应配备一定数量的工控系统管理员、工控网络管理员、工控安全管理员等；

b） 应配备专职安全管理员，不可兼任。

7.2.3 安全建设管理外包软件开发

本项要求包括：

a） **应在软件交付前检测软件质量和其中可能存在的恶意代码；**

b） **应要求开发单位提供软件设计文档和使用指南；**

c） **应要求进行黑盒，并审查软件中可能存在的后门和隐蔽信道。**

7.2.4 安全运维管理漏洞和风险管理

本项要求包括：

a） 应定期开展安全测评，形成安全测评报告，提出整改建议和计划。

b） 应采取必要的措施识别安全漏洞和隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；或评估可能的影响后采取必要的补救措施，补救措施宜在系统维护期间开展。

c） **应对所用工控设备的版本号及每个版本对应的漏洞信息进行统一管理。**

8 第四级基本要求

8.1 技术要求

8.1.1 物理和环境安全

8.1.1.1 物理位置选择

应符合所选用设备的物理和环境条件。

8.1.1.2 物理访问控制

本项要求包括：

a） 进入安全区域边界有明确的防止非授权人员接触的提示标志；

b） 有防止非授权人员进入的物理措施（如栅栏）；

c） 有身份识别机制手段（如门禁、视频监视等）或专人值守；

d） **重要区域至少配置双重身份识别。**

8.1.1.3 防盗和防破坏

本项要求包括：

a） 应将设备或主要部件进行固定；

b） 对通信线缆实施防护，如可铺设在地下或管道中；

c） **应设置防盗报警系统或设置有专人值守的视频监控系统。**

8.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

8.1.1.5 防火

本项要求包括：

a） 机房应设置灭火设备；

b） 机房应设置火灾报警消防系统，能够检测火情、报警，并灭火；

c） **机房应采用具有耐火等级的建筑材料**。

8.1.1.6 防水和防潮

应符合所选用设备的物理和环境条件。

8.1.1.7 防静电

本项要求包括：

a） 机房应安装防静电地板并采用必要的接地防静电措施；

b） 现场设备应符合各行业领域相关标准的要求。

8.1.1.8 温、湿度控制

本项要求包括：

a） 机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；

b） 现场设备应符合所选用设备的物理和环境条件。

8.1.1.9 电力供应

本项要求包括：

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应为机房提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求(3 级)；

c） **应为机房设置冗余或并行的电力电缆线路为系统供电**；

d） **应为机房提供应急供电设施**。

8.1.1.10 电磁防护

本项要求包括：

a） 现场设备应符合所选用设备的物理和环境条件；

b） **应对关键设备或关键区域实施电磁屏蔽**。

8.1.2 边界防护

本项要求包括：

a） 应对控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，进行监视和控制安全域边界通信；

b） 应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，默认拒绝所有非必要的网络数据流，允许例外网络数据流；

c） 应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界上，阻止任何通过的非必要通信；

d） 应在控制网络和非控制网络的边界防护机制失效时，能阻止所有边界通信(也称故障关闭)；但故障关闭功能的设计不应干扰安全相关功能的运行；

e） 应在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，并保障不影响关

键设备通讯；

f) **应能对连接到内部网络的设备进行可信验证，确保接入网络的设备真实可信；**

g) 应确保无线网络通过受控的控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界时，边界防护设备接入（有线）网络；

h) 应能识别控制网络和非控制网络上的边界通讯入侵行为，并有效阻断。

8.1.3 集中管控

见 GB/T 22239 中的相关要求。

8.1.4 生产管理层安全要求

8.1.4.1 网络和通信安全

8.1.4.1.1 网络架构

见 GB/T 22239 中的相关要求。

8.1.4.1.2 通信传输

本项要求包括：

a) 应利用会话完整性机制，保证会话完整性；

b) **应在通信前对通信的双方进行验证或认证。**

8.1.4.1.3 无线使用控制

本项要求包括：

a) 根据普遍接受的安全工业实践，应对无线连接的授权、监视以及执行使用进行限制；

b) 应对所有参与无线通信的用户（设备）提供唯一性标识和鉴别；

c) **应识别和报告系统内部存在的未经授权的无线设备。**

8.1.4.1.4 访问控制

本项要求包括：

a) 对一个可配置的时间或事件序列，应支持主管手动超驰当前人员用户授权。

b) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

c) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话。

d) 应在网络边界或安全域之间根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。

e) 应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。

8.1.4.1.5 入侵防范

本项要求包括：

a) 应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用以攻击信息安全管理系统的信息，除非透露这一信息对于及时排除故障是必要的。

b) 应禁止传输、接收私人消息。

c) 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。

d) 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。
e) 应采取技术措施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。
f) 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。

8.1.4.1.6 恶意代码防范

本项要求包括：

a) 应在关键网络节点处对恶意代码进行检测和清除，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。

8.1.4.1.7 安全审计

本项要求包括：

a) 应能生成安全相关审计记录，包括：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。
b) 应能集中管理审计事件并从系统多个组件收集审计记录，系统范围（逻辑或物理）的时间相关审计踪迹。应能按照工业标准格式输出这些审计记录，用于商业日志分析工具进行分析，例如，安全信息和事件管理。
c) 根据一般公认的日志管理和系统配置的建议，系统应设置足够的审计记录存储容量。系统应提供审计机制来减少超出容量的可能性。
d) 当分配审计记录存储值达到最大审计记录存储容量的配置比例时，系统应能发出警告；当容量超出时，支持覆盖。
e) 在审计事件的处理失败时，系统能对人员进行警示并防止丧失基本服务和功能。根据普遍接受的工业实践和建议，系统应能在审计处理失败的情况下，采取恰当响应行动。
f) 在审计记录生成时，系统应提供时间戳。
g) 应在可配置的频率下，对系统时钟进行同步。
h) **应防止时间源被非授权改动，一旦改动则生成审计事件**。
i) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。
j) **系统应把审计记录写入一次性硬件介质**。
k) 授权人员和/或工具以只读方式访问审计日志。
l) **应使用应用编程接口**，能利用编程进行审计记录访问。

8.1.4.2 设备和计算安全

8.1.4.2.1 身份鉴别

本项要求包括：

a) 应能唯一地鉴别和认证全部人员用户。应在所有接口上执行标识和鉴别。当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。
b) 应能对所有使用人员用户实施多因子鉴别。
c) 应能对所有设备提供唯一性标识和鉴别。应在进行系统访问时，使所有接口根据适用的安全策略和规程支持最小权限，实施标识和鉴别。
d) 应支持用户、组、角色或者接口的标识符管理功能。

e) 应能初始化鉴别器内容；系统一经安装完成，立即改变所有鉴别器的默认值；改变或者刷新所有的鉴别器；当存储或者传输的时候，要保护鉴别器免受未经授权的泄露和修改。

f) 对于使用设备的用户，应通过硬件机制保护相关鉴别器。

g) 对于使用口令鉴别机制的设备，设备应能通过设置最小长度和多种字符类型，实现强制配置口令强度。

h) 设备应防止任何已有的用户账户重复使用同一批口令。此外，设备应加强用户口令的最大和最小有效期的使用。这些能力应符合一般公认的安全产业实践要求。

i) **设备应能提供用户口令的最大和最小有效期的限制**。

j) 应根据通用的可以接受的安全行业实践和建议，通过硬件机制来保护相关的私钥。

k) 应能隐藏鉴别过程中的鉴别信息反馈。

l) 应针对任何用户(人员、软件进程或设备)在可配置时间周期内，对连续无效的访问尝试进行可配置次数限制。当限制次数超出后，应在规定的周期内拒绝访问或者直到管理员解锁。对于代表关键服务或者服务器运行的系统账户，不应允许交互式登录。

m) 在进行鉴别之前，应能显示系统提示信息。使用提示信息应可通过授权人进行配置。

n) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

8.1.4.2.2 访问控制

本项要求包括：

a) 应能支持授权用户管理所有账户，包括添加、激活、修改、禁用和删除账户；

b) 应能支持统一账户管理；

c) 应能在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话；

d) 对于所有接口，应根据职责分离和最小权限对特定用户(人员、软件进程或设备)实施控制系统的控制使用授权；

e) 应能使授权用户或角色可对所有人员用户的许可到角色映射进行规定和修改；

f) 应能在日常维护时，进行安全功能操作的验证和报告异常事件；

g) 应限制默认账户的访问权限，重命名系统默认账户，修改默认口令；

h) 应及时删除多余的、过期的账户，避免共享账户的存在。

8.1.4.2.3 安全审计

见 GB/T 22239 中的相关要求。

8.1.4.2.4 入侵防范

见 GB/T 22239 中的相关要求。

8.1.4.2.5 恶意代码防范

本项要求包括：

a) 应能对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出系统；监视移动代码的使用。

b) 应能允许代码执行之前验证移动代码完整性。

c) 应能应用保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响；应能更新防护机制。

d) 应在所有入口和出口提供恶意代码防护机制。

e) **可采用可信计算技术或其他有效机制**管理恶意代码防护机制。

f) 可采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。

8.1.4.2.6 资源控制

本项要求包括：

a) 在不影响当前安全状态下，系统应能切换至和切换出应急电源的供应；

b) 应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；

c) 应能对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

8.1.4.3 应用和数据安全

8.1.4.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

8.1.4.3.2 身份鉴别

见 GB/T 22239 中的相关要求。

8.1.4.3.3 访问控制

见 GB/T 22239 中的相关要求。

8.1.4.3.4 安全审计

见 GB/T 22239 中的相关要求。

8.1.4.3.5 软件容错

见 GB/T 22239 中的相关要求。

8.1.4.3.6 资源控制

见 GB/T 22239 中的相关要求。

8.1.4.3.7 数据完整性

见 GB/T 22239 中的相关要求。

8.1.4.3.8 数据保密性

本项要求包括：

a) 无论在信息存储或传输时，都应对有明确读权限的信息提供保密性保护；

b) **应提供信息在穿过任何安全域边界时，保护其保密性的能力；**

c) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制；

d) **应对重要数据传输提供专用通信协议或安全通信协议，避免来自基于通用通信协议的攻击破坏数据保密性；**

e) 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。

8.1.4.3.9 数据备份恢复

见 GB/T 22239 中的相关要求。

8.1.4.3.10 剩余信息保护

见 GB/T 22239 中的相关要求。

8.1.5 过程监控层安全要求

8.1.5.1 网络和通信安全

8.1.5.1.1 网络架构

本项要求包括：

a) 应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络和非关键控制系统网络进行逻辑分区；

b) 应将控制系统网络与非控制系统网络进行物理分段，将关键控制系统网络和非关键控制系统网络进行物理分段；

c) 应在不与非控制系统网络相连的情况下，能为关键或非关键控制系统网络提供网络服务；

d) **应通过逻辑的和物理的方式，将关键控制系统网络与非关键控制系统网络隔离**。

8.1.5.1.2 通信传输

本项要求包括：

a) 应保护会话完整性，拒绝任何非法会话 ID 的使用；

b) 应在用户退出或其他会话结束(包括浏览器会话)后使会话 ID 失效；

c) 应为每一个会话生成唯一的会话 ID，并将非期望的会话 ID 处理为非法 ID。

8.1.5.1.3 无线使用控制

本项要求包括：

a) 应对所有参与无线通信的用户(设备)提供唯一性标识和鉴别；

b) 应对无线连接的授权、监视以及执行使用进行限制；

c) 应识别在控制系统物理环境中发射的未经授权的无线设备，**并对其进行有效阻断**，以及报告对系统造成的影响。

8.1.5.1.4 访问控制

本项要求包括：

a) 应通过手动的方式或在一个可配置非活动周期后系统自动的方式，启动会话锁定，以阻止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

b) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话。

c) 应在网络边界或安全域之间根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信。

d) 应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。

8.1.5.1.5 入侵防范

本项要求包括：

a) 应在有效的补救条件下识别和处理错误状况，该过程不应泄露任何安全相关信息，除非及时排除故障会不可避免地泄露某些信息；
b) 应禁止传输、接收私人消息；
c) 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；
d) 应禁止未经授权的数据传输；
e) 应采取技术措施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；
f) 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。

8.1.5.1.6 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。
b) 应能集中管理审计事件，对来自系统范围（包括逻辑或物理）内的多个组件进行审计记录的收集，并能集中管理时间相关的审计踪迹。应按照工业标准格式输出这些审计记录，用日志分析工具进行分析，例如，安全信息和事件管理。
c) 根据一般公认的日志管理和系统配置的建议，应　置足够的审计记录存储容量，提供审计机制来减少超出容量的可能性。
d) 当分配审计记录存储值达到最大审计记录存储容量的配置比例时，应发出警告。
e) 在审计事件的处理失败时，应警示人员采取恰当的响应行动，防止丧失基本服务和功能。
f) 在审计记录生成时应提供时间戳。
g) 应在可配置的频率下，对系统时钟进行同步。
h) **应防止时间源被非授权改动，一旦改动则生成审计事件**。
i) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。
j) **应把审计记录写入一次性硬件介质**。
k) 应授权人员和/或工具以只读方式访问审计日志。
l) **应使用应用编程接口**，提供编程访问审计记录的能力。

8.1.5.2 设备和计算安全

8.1.5.2.1 身份鉴别

本项要求包括：

a) 应支持用户、组、角色或者接口的标识符管理功能；应在所有人机接口上执行标识和鉴别，当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。
b) 对于使用口令鉴别机制的设备，设备应具有通过设置最小长度和多种字符类型，从而达到强制配置口令强度的能力；可能对实时性产生影响进而影响到系统正常操作的，应采用其他替代安全手段或通过管理手段弥补。
c) 应防止任何已有的用户账户重复使用同一批口令，并加强用户口令的最大和最小有效期的使用，以符合公认的安全产业实践要求。
d) **应对用户口令的最大和最小有效期进行限制**。
e) 应在可配置时间周期内，对连续无效的访问进行可配置次数限制；当访问次数超出限制后，应

进行报警;对于代表关键服务或者服务器运行的系统账户,应不允许交互式登录。

f) 不允许进行远程管理。

g) 应具有登录失败处理功能,应配置并启用结束会话、当登录连接超时自动退出等相关措施。

8.1.5.2.2 访问控制

本项要求包括:

a) 应支持授权用户管理所有账户,包括添加、激活、修改、禁用和删除账户;

b) 应在一个可配置非活动时间周期后自动地,或由发起会话的用户手动地终止远程会话;

c) 对于所有接口,应根据职责分离和最小权限对特定用户(人员、软件进程或设备)实施控制系统的控制使用授权;

d) 应授权用户或角色对所有人员用户的访问权限进行规定和修改;

e) 在日常维护时,应支持安全功能操作的验证和报告异常事件;

f) 应重命名系统默认账户,修改默认口令,禁止在工程师站、操作员站、服务器使用默认账户;

g) 应及时删除多余的、过期的账户,避免共享账户的存在。

8.1.5.2.3 安全审计

本项要求包括:

a) 应生成安全相关审计记录,类别有:访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变和审计日志事件。单个审计记录应包括时间戳、来源(源设备、软件进程或人员用户账户)、分类、类型、事件 ID 和事件结果。

b) 设备应能够为集中审计管理提供接口,将自身生成的审计记录上传。

c) 在审计记录生成时,设备应提供时间戳。

d) 应具备以可配置频率的,与系统时钟同步的能力。

e) 应保护审计信息和审计工具(如有),防止其在未授权情况下被获取、修改和删除。

f) 应向授权人员和/或工具提供以只读的方式访问审计日志。

g) **应使用应用编程接口**,提供编程访问审计记录的能力。

8.1.5.2.4 入侵防范

本项要求包括:

a) 应自动执行可配置的使用限制,其中包括:防止使用便携式和移动设备;要求特定内容的授权;限制来自/写入便携式和移动设备的代码和数据传输。

b) **应验证便携式或移动设备对设备的连接是否符合该安全域安全要求**。

c) 应通过手动或在一个可配置非活动周期后系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效,直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。

d) 应在有效的补救条件下,识别和处理错误状况。该过程不应暴露任何可能被攻击者利用于攻击信息安全管理系统的信息,除非透露这一信息对于及时排除故障是必要的。

e) 所有主机设备操作系统采用最小化系统安装原则,除了必要的安全组件或软件外,只安装与自身业务相关的操作系统组件及应用软件,如工程师站、操作员站只安装组态软件、监控软件、编程软件、报表软件以及与此相关的操作系统组件,OPC 服务器、实时数据库服务器只安装数据库软件、服务器软件以及与此业务相关的操作系统组件。

8.1.5.2.5 恶意代码防范

本项要求包括:

a) 应对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出控制系统；监视移动代码的使用。
b) 应允许代码执行之前验证移动代码完整性。
c) 应采取保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响，应提供更新防护机制的能力。
d) **可采用可信计算技术或其他有效机制管理恶意代码防护机制**。

8.1.5.2.6 资源控制

本项要求包括：

a) 应对于任何给定设备的每个接口限制并发会话数量；
b) 应参照供应商提供的指南，根据所推荐的网络和安全配置进行系统设置；
c) 应对工程师站、操作员站、服务器等系统运行资源进行监视，包括 CPU、硬盘、内存、网络等资源的使用情况；设置预警限值并在触发时预警。

8.1.5.3 应用和数据安全

8.1.5.3.1 无线使用控制

应对所有参与无线通信的用户(人员和软件进程)提供唯一性标识和鉴别。

8.1.5.3.2 身份鉴别

本项要求包括：

a) 应唯一地标识和鉴别所有人员用户。应在所有接口上执行标识和鉴别。当有人员用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限。
b) 对于使用口令鉴别机制的应用，应具有通过设置最小长度和多种字符类型，从而达到强制配置口令强度的能力；可能对实时性产生影响进而影响到系统正常操作的，应采用其他替代安全手段或通过管理手段弥补。
c) 应防止任何已有的用户账户重复使用同一批口令，并加强用户口令的最大和最小有效期的使用，以符合一般公认的安全产业实践要求。
d) **应对用户口令的最大和最小有效期进行限制**。
e) 应在可配置时间周期内，对连续无效的访问进行可配置次数限制；当访问次数超出限制后，应进行报警；对于代表关键服务或者服务器运行的系统账户，应不允许交互式登录。
f) **不允许进行远程管理**。
g) 应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

8.1.5.3.3 访问控制

本项要求包括：

a) 应支持授权用户来管理所有账户，包括添加、激活、修改、禁用和删除账户。
b) 应支持统一账户管理。
c) 应通过手动或系统在一个可配置非活动周期后自动启动会话锁定防止进一步访问。会话锁定应一直保持有效，直到拥有会话的人员用户或其他授权的人员用户使用适当的身份标识和鉴别规程重新建立访问。
d) 对于所有接口，应根据职责分离和最小权限对所有用户实施控制使用授权。
e) 应为授权用户或角色提供这样的能力，即对所有人员的访问权限进行规定和修改。

f) **为一个可配置的时间或事件序列，应支持主管手动超驰当前人员用户授权。**

g) 应重命名系统默认账户，修改默认口令，禁止在工程师站、操作员站、服务器使用默认账户。

h) 应及时删除多余的、过期的账户，避免共享账户的存在。

8.1.5.3.4 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、配置改变、审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) 应能够为集中审计管理提供接口，将自身生成的审计记录上传。

c) 在审计记录生成时，应提供时间戳。

d) 应具备以可配置频率的，与系统时钟同步的能力。

e) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。

f) 授权人员和/或工具应使用只读方式访问审计日志。

g) 应对审计进程进行保护，防止未经授权的中断。

8.1.5.3.5 软件容错

本项要求包括：

a) 应对数据有效性进行检验，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

b) 在故障发生时，应能够继续提供基本功能，确保能够实施必要的措施。

8.1.5.3.6 资源控制

本项要求包括：

a) 应对任何给定软件进程的每个接口限制并发会话数量；

b) 当应用系统中的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

8.1.5.3.7 数据完整性

本项要求包括：

a) 应保护传输信息完整性；

b) **应使用密码学机制识别通信过程中信息修改；**

c) 应检测、记录、报告、防止对软件和信息的未经授权更改；

d) 在完整性验证过程中发现差异时，应提供自动化工具通知给一组可配置的接收者；

e) 应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行验证；

f) 应采用校验码技术、加解密技术或同等安全性的技术手段保证重要数据在存储过程中的完整性。

8.1.5.3.8 数据保密性

本项要求包括：

a) 无论在信息存储或传输时，应对有明确读权限的信息提供保密性保护；

b) 当信息穿过任何安全域边界时，应保护其保密性；

c) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

8.1.5.3.9 数据备份恢复

本项要求包括：

a) 应在不影响正常设备使用的前提下，识别和定位关键文件，以及备份用户级和系统级的信息（包括系统状态信息）；

b) 应验证备份机制可靠性；

c) 应在可配置的频率下，自动进行备份；

d) 应定期记录一个安全状态，在系统受到破坏或发生失效后，应能够恢复和重构控制系统到一个已知的安全状态。

8.1.5.3.10 剩余信息保护

本项要求包括：

a) 清除不再使用的和/或退役组件上的具有显式读权限访问的信息；

b) 应防止通过易失性共享内存资源未授权地和无意地传输信息；

c) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

d) 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。

8.1.6 现场控制层安全要求

8.1.6.1 网络和通信安全

8.1.6.1.1 网络架构

本项要求包括：

a) 应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络和非关键控制系统网络进行逻辑分区；

b) 应将控制系统网络与非控制系统网络进行物理分段，将关键控制系统网络与非关键控制系统网络进行物理分段；

c) 应在不与非控制系统网络相连的情况下，能为关键或非关键控制系统网络提供网络服务。

8.1.6.1.2 通信传输

本项要求包括：

a) 应保护会话完整性。控制系统应拒绝任何非法会话 ID 的使用。

b) 应在用户退出或其他会话结束（包括浏览器会话）后使会话 ID 失效。

c) 应为每一个会话生成唯一的会话 ID，并将非期望的会话 ID 处理为非法 ID。

8.1.6.1.3 无线使用控制

本项要求包括：

a) 应对所有参与无线通信的用户（设备）提供唯一性标识和鉴别；

b) 根据普遍接受的安全工业实践，对无线连接的授权、监视以及执行使用限制；

c) 识别在控制系统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行为。

8.1.6.1.4 访问控制

本项要求包括：

a) 应在网络边界或安全域之间根据访问控制策略设置访问控制规则，默认情况下，受控接口拒绝所有非允许的通信；
b) 应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。

8.1.6.1.5 入侵防范

本项要求包括：

a) 应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用的信息安全管理系统的信息，除非排除故障过程中应透露这一信息；
b) 应在关键网络节点处检测从外部发起的网络攻击行为；
c) 应在关键网络节点处检测从内部发起的网络攻击行为；
d) 应采取技术措施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；
e) 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；
f) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

8.1.6.1.6 恶意代码防范

本项要求包括：

a) 应提供对可能造成损害的移动代码技术执行使用限制的能力，包括：限制移动代码传入/传出控制系统；监视移动代码的使用。
b) 应在所有入口和出口提供恶意代码防护机制。
c) **可采用可信计算技术或其他有效机制管理恶意代码防护机制。**

8.1.6.1.7 安全审计

本项要求包括：

a) 应生成安全相关审计记录，类别有：访问控制、请求错误、操作系统事件、控制系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。
b) 根据一般公认的日志管理和系统配置的建议，控制系统应设置足够的审计记录存储容量。控制系统应提供审计机制来减少超出容量的可能性。
c) 当分配审计记录存储值达到最大审计记录存储容量的配置比例时，控制系统应发出警告。
d) 在审计事件的处理失败时，控制系统应提供警示人员的能力，应防止丧失基本服务和功能。根据普遍接受的工业实践和建议，控制系统应提供这样的能力，在审计处理失败的情况下，采取恰当的响应行动。
e) 在审计记录生成时，控制系统应提供时间戳。
f) 应在可配置的频率下，对系统时钟进行同步。
g) **应防止时间源被非授权改动，一旦改动则生成审计事件。**
h) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。
i) **应把审计记录写入一次性硬件介质。**
j) 授权人员和/或工具以只读方式访问审计日志。
k) 应提供编程访问审计记录的能力。
l) 应在网络边界、重要网络节点进行安全审计，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。

8.1.6.2 设备和计算安全

8.1.6.2.1 身份鉴别

本项要求包括：

a) 应对所有操作进行身份识别，身份标识具有唯一性，设备自身不具备识别能力的应采用其他技术方法或管理手段。

b) 禁止使用默认账户和口令，口令应有复杂度要求，口令长度和特征应足够强壮，以防止通过如猜测或暴力破解等手段通过验证。若安全性不够，应使用其他手段；口令应设定有效期限，并定期更换。

c) 应具有鉴别失败处理功能，应配置并启用结束会话、限制非法登录次数并报警，当登录连接超时自动退出等相关措施。

d) 应采取必要的措施，防止鉴别信息在传输过程中被窃听。

8.1.6.2.2 安全审计

本项要求包括：

a) 应提供生成安全相关审计记录的能力，类别有：访问控制、请求错误、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户账户）、分类、类型、事件 ID 和事件结果。

b) 在审计记录生成时，设备应提供时间戳。

c) 应具备以可配置频率的，与系统时钟同步的能力。

d) 应保护审计信息和审计工具（如有），防止其在未授权情况下被获取、修改和删除。

e) **应提供把审计记录写入一次性硬件介质的能力。**

f) 授权人员和/或工具以只读方式访问审计日志。

g) 应启用安全审计功能，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。

8.1.6.2.3 入侵防范

本项要求包括：

a) 应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用的信息安全管理系统的信息，除非排除故障过程中应透露这一信息。

b) 应遵循最小安装的原则，仅安装需要的组件和应用程序。

c) 应关闭不需要的系统服务、默认共享和高危端口。

d) 停机维护期间，应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。

8.1.6.2.4 资源控制

本项要求包括：

a) 应提供重要节点设备的硬件冗余，保证系统的可用性；

b) 应能实时监控设备的运行和通信状态，并及时发现异常情况给予报警。

8.1.6.3 应用和数据安全

8.1.6.3.1 无线使用控制

应对所有参与无线通信的用户（人员和软件进程）提供唯一性标识和鉴别。

8.1.6.3.2 数据完整性

本项要求包括：

a） 应保护传输信息完整性；

b） 应保护防止对软件和信息的未经授权更改；

c） 应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行验证；

d） 应采用校验码技术、加解密技术或同等安全性的技术手段保证重要数据在存储过程中的完整性。

8.1.6.3.3 数据保密性

本项要求包括：

a） 在信息传输时，应对有明确读权限的信息进行保密性保护；

b） **信息在穿过任何安全域边界时，应保护其保密性；**

c） 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和密钥管理机制。

8.1.6.3.4 数据备份恢复

本项要求包括：

a） 应在不影响正常设备使用的前提下进行对关键文件的识别和定位，以及用户级和系统级的信息备份(包括系统状态信息)；

b） 应验证备份机制可靠性；

c） 在受到破坏或发生失效后，应能够恢复和重构控制系统到一个已知的安全状态。

8.1.7 现场设备层安全要求

8.1.7.1 网络和通信安全

8.1.7.1.1 恶意代码防范

本项要求包括：

a） **对于采用网络(工业无线/现场总线)通讯的联网设备，应对可能造成损害的移动代码技术执行使用限制，包括：限制移动代码传入/传出控制系统；监视移动代码的使用。**

b） **对于采用网络(工业无线/现场总线)通讯的关键联网设备，应在所有入口和出口施加恶意代码防护机制。**

c） **可采用可信计算技术或其他有效机制管理恶意代码防护机制。**

8.1.7.1.2 无线使用控制

对于采用网络(工业无线)通讯的联网设备，应确保无线空中接口安全。

8.1.7.2 应用和数据安全

8.1.7.2.1 数据完整性

本项要求包括：

a） 对于采用网络(工业无线/现场总线)通讯的联网设备，应保护传输信息完整性；

b） 对于采用网络(工业无线/现场总线)通讯的联网设备，应能使用密码学机制识别信息在通信过

程中是否被篡改；

c) 对于采用网络(工业无线/现场总线)通讯的联网设备，应防止对软件和信息的未授权更改；

d) 对于采用网络(工业无线/现场总线)通讯的联网设备，在完整性验证过程中发现差异时，应提供自动化工具通知给一组可配置的接收者；

e) 对于采用网络(工业无线/现场总线)通讯的联网设备，应对工业过程控制输入或直接影响控制系统动作的输入内容和语法的合法性进行校验；

f) **对于采用网络(工业无线/现场总线)通讯的联网设备，应采用校验码技术或加解密技术保证重要数据在存储过程中的完整性。**

8.1.7.2.2 数据备份恢复

本项要求包括：

a) 对于采用网络(工业无线/现场总线)通讯的联网设备，应在不影响正常设备使用的前提下，提供关键文件的识别和定位，包括设备状态信息的能力；

b) 对于采用网络(工业无线/现场总线)通讯的联网设备，应提供验证备份机制可靠性的能力；

c) 对于采用网络(工业无线/现场总线)通讯的联网设备，在受到破坏或发生失效后，应能够恢复和重构设备到一个已知的安全状态。

8.2 管理要求

8.2.1 安全策略和管理制度安全策略

应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

8.2.2 安全管理机构和人员

8.2.2.1 岗位设置

本项要求包括：

a) 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；

b) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c) 应设立工控系统管理员、工控网络管理员、工控安全管理员等岗位，并定义部门及各个工作岗位的职责。

8.2.2.2 人员配备

本项要求包括：

a) 应配备一定数量的工控系统管理员、工控网络管理员、工控安全管理员等；

b) 应配备专职安全管理员，不可兼任；

c) **关键事务岗位应配备多人共同管理。**

8.2.3 安全管理建设外包软件开发

本项要求包括：

a) 应在软件交付前检测软件质量和其中可能存在的恶意代码；

b) 应要求开发单位提供软件设计文档和使用指南；

c） **应要求开发单位提供软件源代码**，并审查软件中可能存在的后门和隐蔽信道。

8.2.4 安全运维管理漏洞和风险管理

本项要求包括：

a） 应定期开展安全测评，形成安全测评报告，提出整改建议和计划。

b） 应采取必要的措施识别安全漏洞和隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；或评估可能的影响后采取必要的补救措施，补救措施宜在系统维护期间开展。

c） 应对所用工控设备的版本号及每个版本对应的漏洞信息进行统一管理。

附　录　A
（资料性附录）
工业控制系统概述详解

A.1　概述

工业控制系统包括了用于制造业和流程工业的控制系统、楼宇控制系统、地理上分散的操作诸如公共设施(例如,电力、天然气和自来水)、管道和石油生产及分配设施、其他工业和应用如交通运输网络,那些使用自动化或远程被控制或监视的资产。

工业控制系统主要由过程级、操作级以及各级之间和内部的通信网络构成,对于大规模的控制系统,也包括管理级。过程级包括被控对象、现场控制设备和测量仪表等,操作级包括工程师和操作员站、人机界面和组态软件、控制服务器等,管理级包括生产管理系统和企业资源系统等,通信网络包括商用以太网、工业以太网、现场总线等。

A.2　SCADA 系统

SCADA 是数据采集与监视控制系统的简称,SCADA 系统是用于控制地理上资产高度分散的大规模分布式系统,往往分散数千平方公里,其中集中的数据采集和控制功能是 SCADA 系统运行的关键。SCADA 系统主要采用远程通信技术,如广域网、广播、卫星、电话线等技术,对跨地区的远程站点执行集中的监视和控制。控制中心根据从远程站点收到的信息,自动或操作员手动产生监督指令,再传送到远程站点的控制装置上,即现场设备。现场设备控制本地操作,如打开和关闭阀门和断路器,从传感器系统收集数据,以及监测本地环境的报警条件。

SCADA 系统主要由区域控制中心、主控制中心、冗余控制中心和多个远程站点构成。控制中心和所有远程站点之间采用远程通信技术进行点对点连接,区域控制中心提供比主控制中心更高级别的监督控制,企业管理网络可以通过广域网访问所有控制中心,并且站点也可以被远程访问以进行故障排除和维护操作。图 A.1 是 SCADA 系统的实施示意图,参考 NIST SP800-82 Revision 2,24。

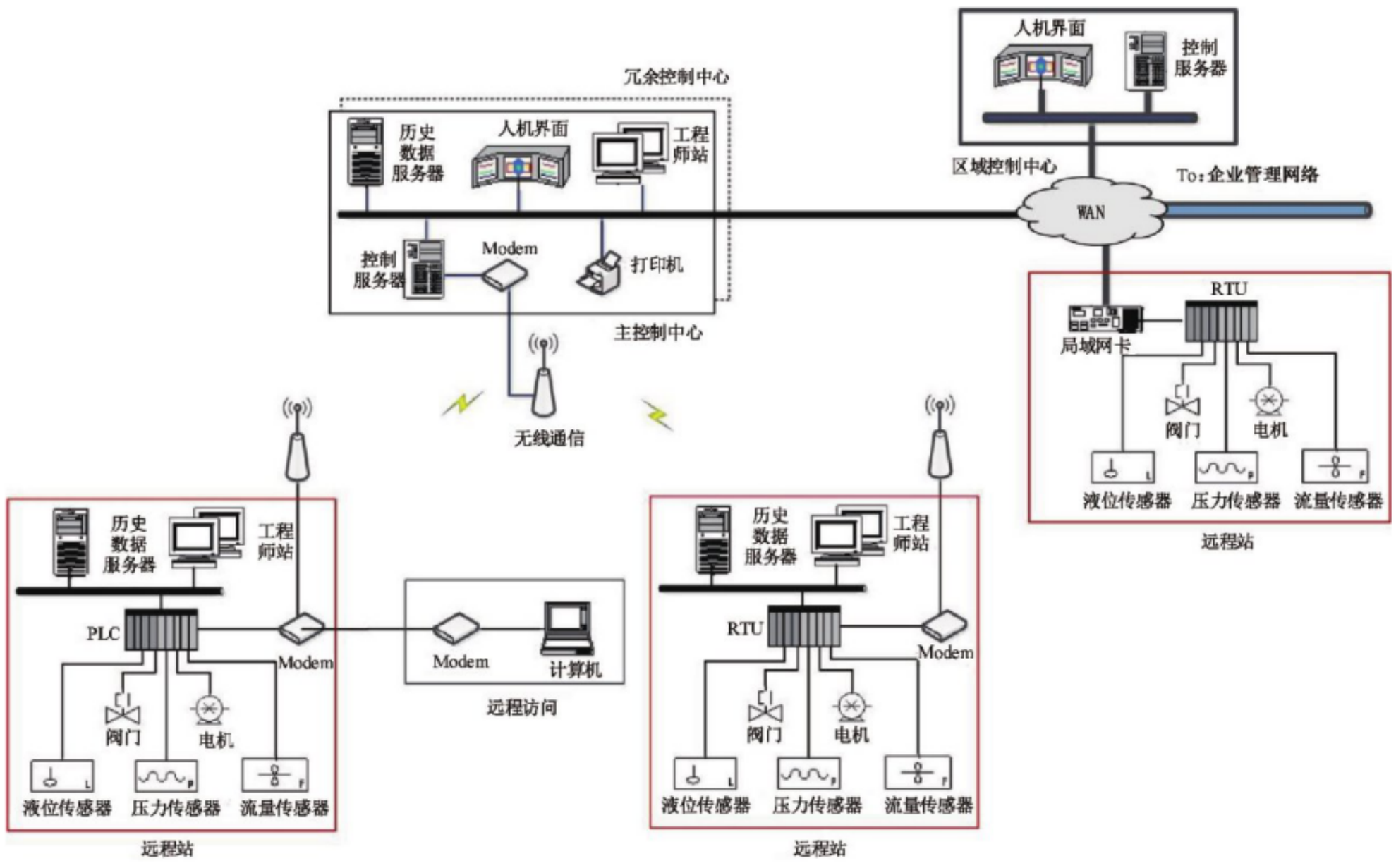


图 A.1 SCADA 系统实施示意图

SCADA 系统的主要特点是利用远程通信技术将地理位置分散的远程测控站点进行集中监控，主要应用在石油和天然气管道、电力电网以及轨道交通等行业。

A.3 DCS 系统

DCS 是集散控制系统的简称，DCS 是用于控制资产设备处于同一地理位置的规模化生产系统。DCS 主要采用局域网技术进行通信，对通信速率和实时性要求高。DCS 采用集中监控的方式协调本地控制器以执行整个生产过程，本地控制器可以包括多种类型，如 PLC、过程控制器和单回路控制器可同时作为控制器应用在 DCS 中。产品和过程控制通常通过部署反馈或前馈控制回路实现，关键产品或过程条件自动保持在一个所需的设定点范围内。

DCS 系统主要由过程级、操作级和管理级构成。过程级主要包括分布式控制器、过程仪表、执行机构、I/O 单元等；操作级主要包括操作员站、工程师站、控制服务器等；管理级主要包括生产管理系统等。图 A.2 是 DCS 实施示意图，参考 NIST SP800-82 Revision 2，27。

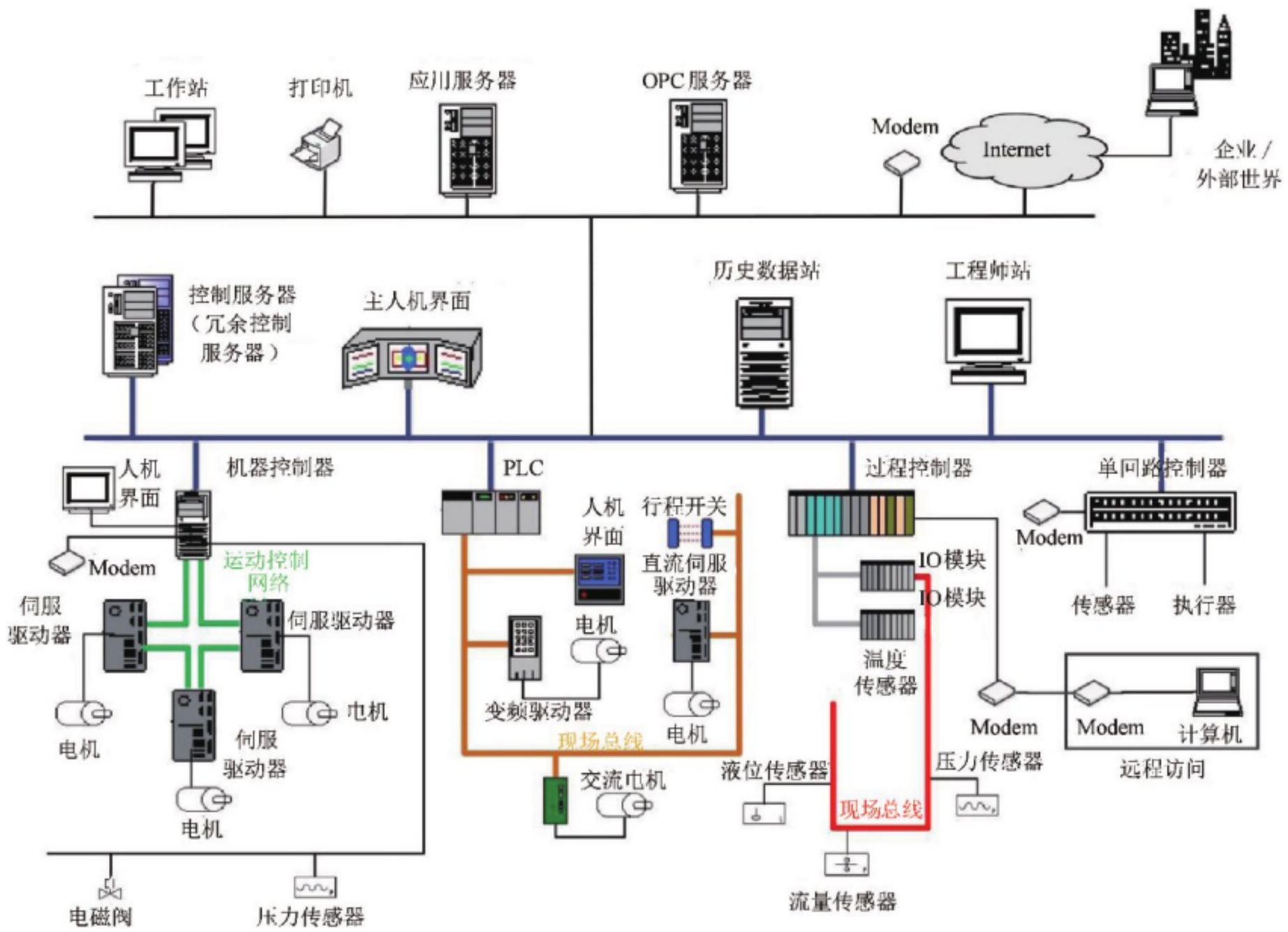


图 A.2　DCS 系统实施示意图

DCS 主要的特点是利用局域网对控制回路进行集中监视和分散控制，主要应用于过程控制行业，如发电厂、炼油厂、水和废水处理、食品和医药加工等。

A.4　PLC 系统

PLC 是可编程逻辑控制器的简称，广泛应用于几乎所有的工业生产过程中。PLC 需要配合工程师站和组态软件运行，主要采用局域网技术进行通信，传输速率高，可靠性好。

PLC 系统主要由工程师站、历史数据站、PLC 控制器、现场设备和局域网络构成。PLC 由工程师站上的编程接口访问，通过局域网控制现场设备，数据存储在历史数据库中。图 A.3 是 PLC 系统实施示意图，参考 NIST SP800-82 Revision 2，28。

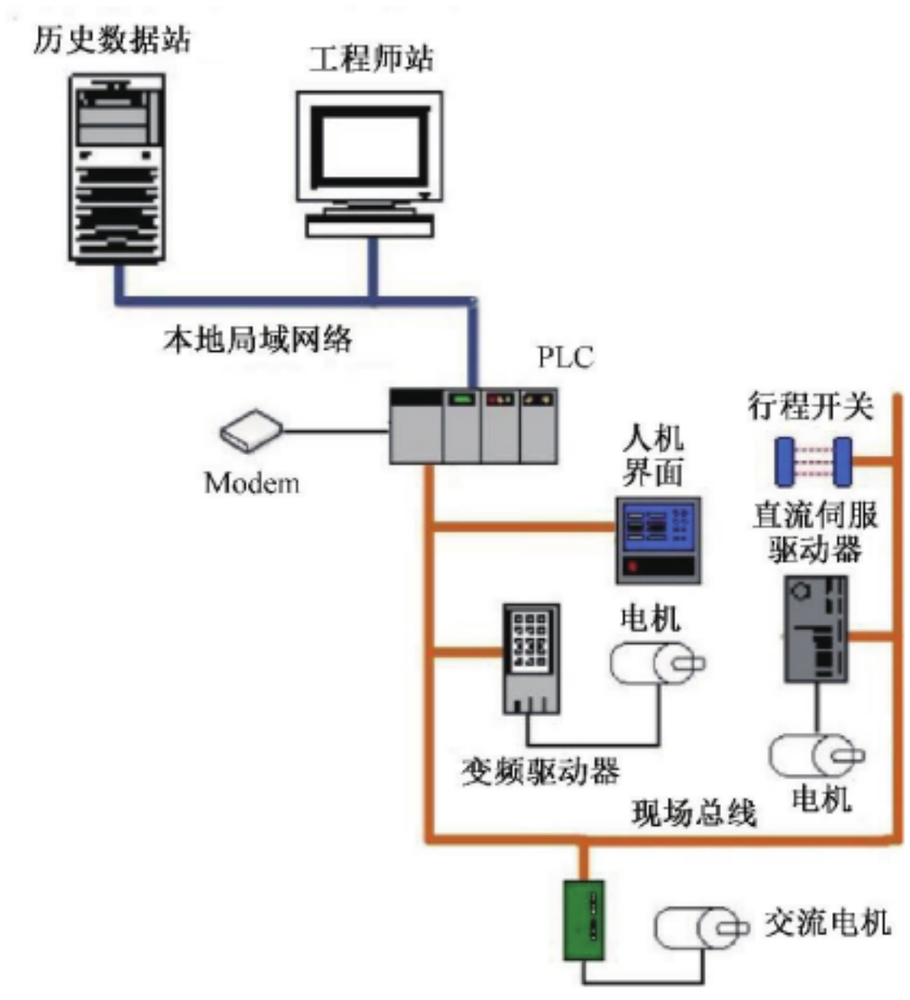


图 A.3　PLC 系统实施示意图

PLC 的主要特点是逻辑控制功能强，同时具有性能稳定、可靠性高、技术成熟的特点，使其被广泛用于工厂自动化行业中。

A.5　RTU 系统

RTU 是远程终端单元的简称，是 SCADA 系统中远程站点使用的专用数据采集和控制单元。RTU 主要具备两种功能，数据采集和处理、数据传输（网络通信），许多 RTU 兼具 PID 控制和逻辑控制功能等。

RTU 的主要特点是能对远程站点的现场数据测量，作为 SCADA 系统中的基本组成单元，主要应用在石油和天然气、电力等行业中。RTU 系统的组成部分与 PLC 系统类似，需要配合工程师站和组态软件运行，区别在于 RTU 系统使用的控制组件是 RTU，而 PLC 系统使用控制组件的是 PLC。

A.6　SCADA 系统、DCS 系统、PLC 系统、RTU 系统的区别

表 A.1 说明了 SCADA 系统、DCS 系统、PLC 系统和 RTU 系统各方面的区别。

表 A.1　SCADA 系统、DCS 系统、PLC 系统、RTU 系统的区别

	SCADA 系统	DCS 系统	PLC 系统	RTU 系统
主要特点	利用远程通信技术将地理位置分散的远程测控站点进行集中监控	利用局域网对控制回路进行集中监视和分散控制，用于连续变量、多回路的复杂控制	逻辑控制功能强，用于数字量、开关量的控制	对远程站点的现场数据测量功能强
地理范围	地理位置高度分散	地理位置集中（如工厂或以工厂为中心的区域）	地理位置集中	危险、恶劣的远程生产现场

表 A.1（续）

	SCADA 系统	DCS 系统	PLC 系统	RTU 系统
应用领域	远程监控行业[如石油和天然气管道、电力电网、轨道交通运输系统（含铁路运输系统与城市轨道交通系统）]	过程控制行业（如发电、炼油、食品和化工等）	工业自动化（如生产线等）	远程监控行业
通信技术	广域网、广播、卫星和电话或电话网等远程通信技术	局域网技术	局域网技术	远程通信技术
规模大小	大规模系统，现场站点多	控制回路复杂，测控点数多	—	作为 SCADA 系统的组成部分

特定的工业控制系统具有特定的安全要求，为了确保提出的安全等级保护基本要求具备通用性，本部分将以通用工业控制系统作为叙述对象。实施本部分时，需要根据特定的系统、安全和业务等需求对各级基本要求进行修改与补充。本部分所提出的不同安全防护安全域划分方法及具体安全要求仍有待扩展。

附 录 B
（资料性附录）
安全域划分示例

DCS 系统示例如图 B.1 所示。

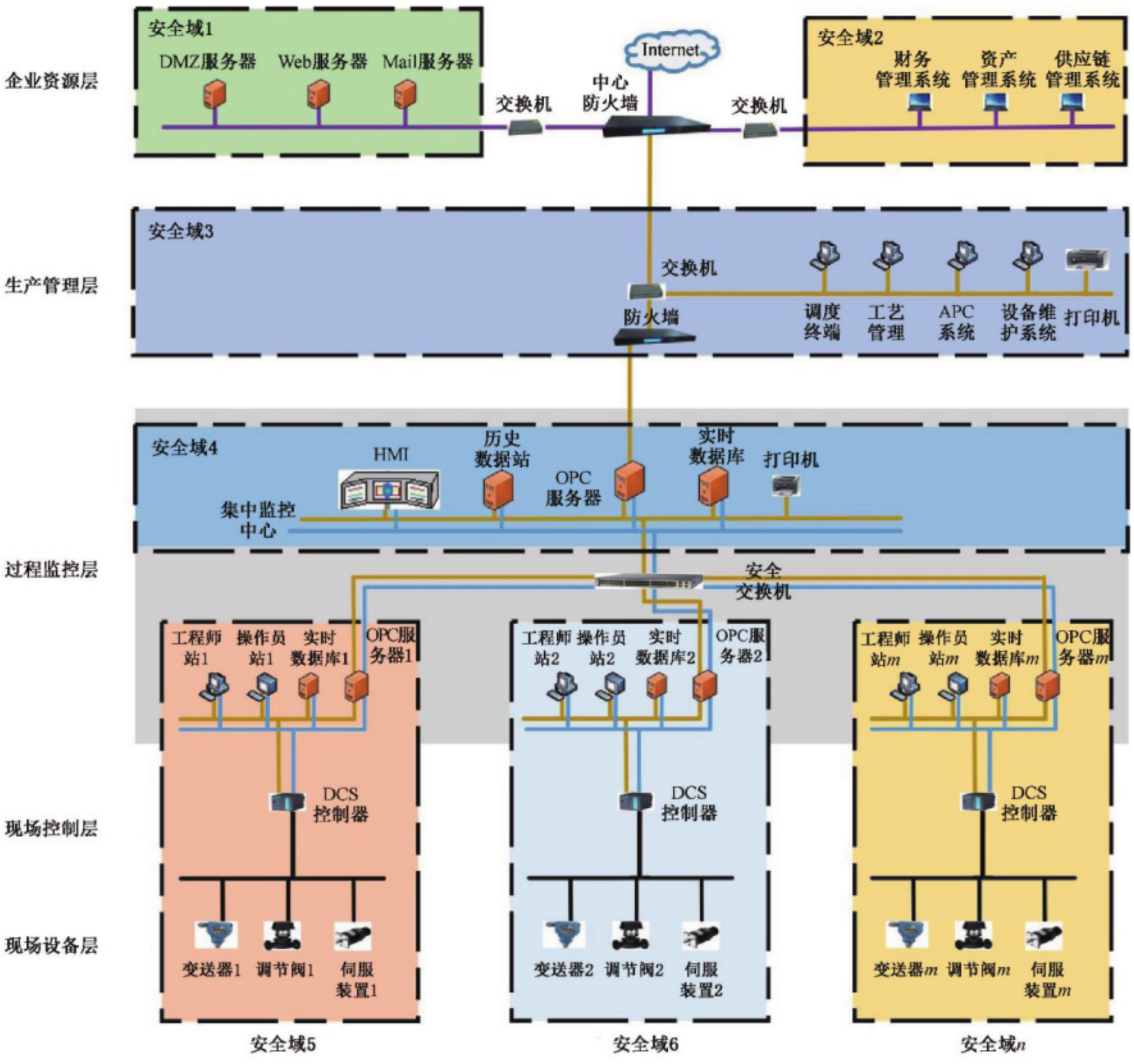


图 B.1 DCS 系统示例

考虑系统功能及资产地理位置因素。在本例中，企业资源层分为安全域 1 和安全域 2。安全域 1 为 DMZ 区域，由部分提供对外服务的服务器主机组成的一个特定子网，将企业内部网络与外部网络的隔离，实现对外部入侵的防护；安全域 2 为企业运营资源区域，包括各类企业运营系统与设备；将生产管理层单独划分为安全域 3，该区资产包括各类生产管理系统与设备；将过程监控层的集中过程监控部分划分为安全域 4，该区资产包括各类过程监控系统与设备。

考虑生产厂商和控制对象因素，将包含不同被控装置的本地过程监控部分，现场控制层及现场设备层划分为不同的安全域 5、安全域 6、……、安全域 n。以安全域 4 为例，该区覆盖 3 个功能层，包含了过程监控层的资产、现场控制层的资产和现场设备层的资产。

应明确各安全域边界，在本例中采用隔离技术对安全域 1 和安全域 2 进行隔离，对安全域 2 和安全域 3 进行隔离，对安全域 3、安全域 4、安全域 5、……、安全域 n 进行隔离。

SCADA 系统安全域划分示例如图 B.2 所示。

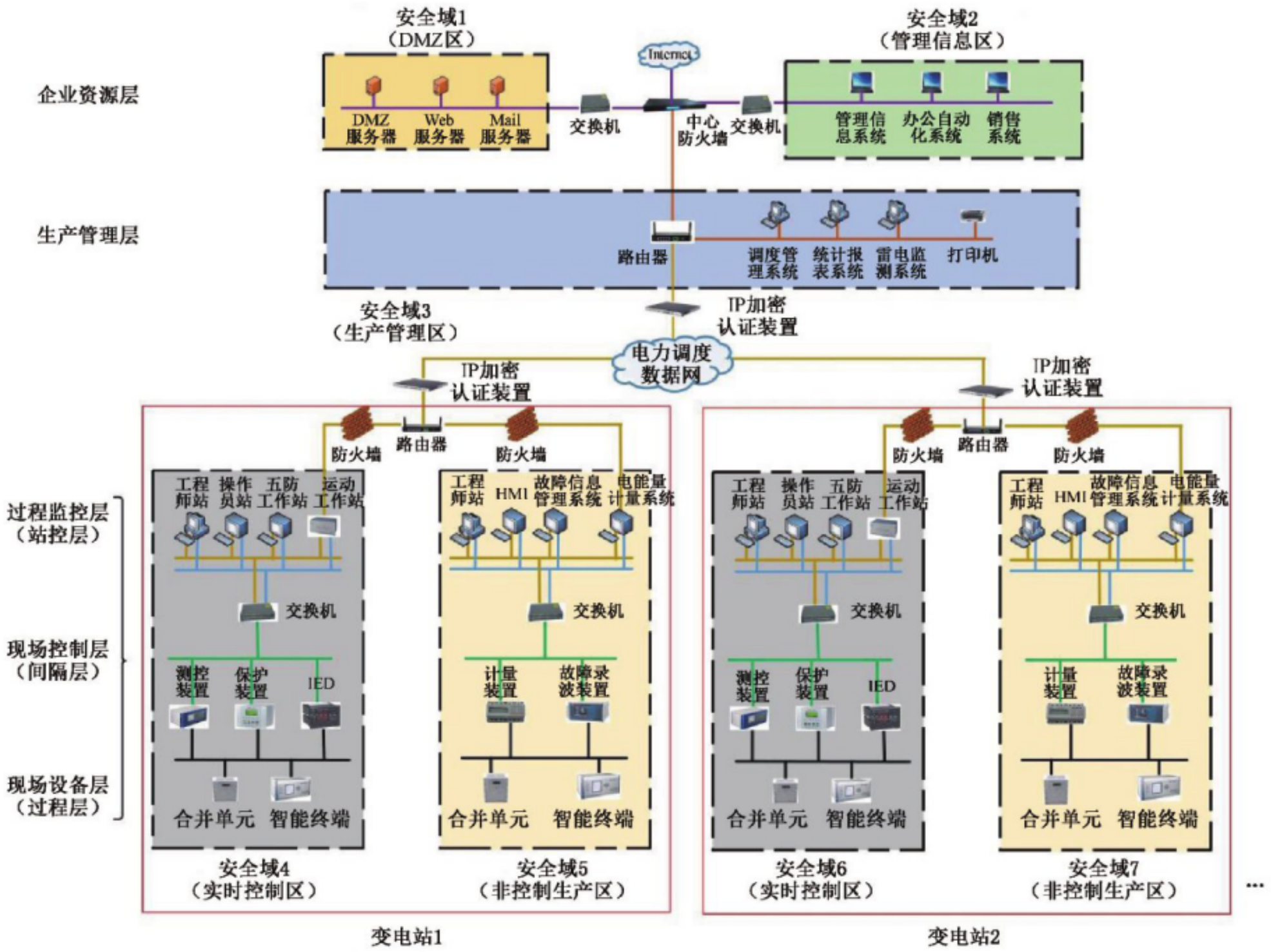


图 B.2　SCADA 系统安全域划分示例

考虑系统功能因素，企业资源层分为安全域 1 和安全域 2。安全域 1 为 DMZ 区域，由部分提供对外服务的服务器主机组成的一个特定子网，将企业内部网络与外部网络的隔离，实现对外部入侵的防护；安全域 2 为管理信息区域，包括各类企业运营系统与设备；将生产管理层单独划分为安全域 3，该区资产包括各类生产管理系统与设备。

考虑控制对象因素，以变电站 1 为例，可将实时控制区和非控制生产区分别划分为安全域 4、安全域 5。安全域 4 覆盖了 3 个功能层，包含了过程监控层的资产、现场控制层的资产和现场设备层的资产。安全域 5 覆盖了 3 个功能层，包含了过程监控层的资产、现场控制层的资产和现场设备层的资产。

应明确各安全域边界，在本例中采用隔离技术对各个安全域进行隔离，采用 IP 加密认证装置对利用远程通信技术的双方双向身份认证和数据加密。

附 录 C
（资料性附录）
基于可信计算技术的工业控制系统安全等级防护

C.1 基本要求

在进行工业控制系统网络安全等级防护时，应逐步应用可信保障的三重防御多级互联技术框架。重要工业控制系统应在有条件时逐步推广应用可信计算技术。可信保障的三重防御多级互联技术框架主要适用于新建或新开发的重要工业控制系统，在运系统具备升级改造条件时可参照执行，不具备升级改造条件的应强化安全管理和安全应急措施。

本部分针对工业控制系统的软件、硬件、网络协议等的安全性，规定了需要保护的数据、指令、协议等要素，在使用可信保障的三重防御多级互联技术框架对工控系统进行等级保护时，应结合具体的工业控制系统品牌、配置、工程实际等实际情况，保证这些可信计算的采用对系统的正常运行不产生危害或灾难性的生产停顿，应保证在采用该框架时，经过工业现场的工程实践验证，并获得用户认可。

C.2 可信保障的三重防御多级互联技术框架

由于工业控制系统存在总线协议复杂多样、实时性要求强、节点计算资源有限、设备可靠性要求高、故障恢复时间短、安全机制不能影响实时性、工控设备不易更换等特点，传统的“封堵查杀”安全防护技术难以解决工控系统安全，因此推荐使用可信保障的安全管理中心支持下的计算环境、区域边界、通信网络三重防御多级互联技术框架，该框架融合了专网专用，分区隔离的思想，以实现可信、可控、可管的系统安全互联、区域边界安全防护和计算环境安全。

利用图 C.1 对工业控制系统信息安全三重防御多级互联技术框架进行举例说明：

a) 可信计算环境：由可信计算节点组成，使应用系统在可信计算资源支持下安全运行，图中分为企业管理计算环境、生产监控计算环境、现场控制计算环境，以确保现场控制、生产监控调度、企业管理过程的安全。每个计算环境有其对应的二级安全管理中心。

b) 应用区域边界可信：区域边界子系统通过对进入和流出计算环境的信息流进行可信度量和安全检查，确保不会有违背系统安全策略的信息流经过边界。将每个计算环境和边界组成的系统作为一个定级对象处理（例如，在图 C.1 中将工控整体划分为 3 个定级系统）。

c) 通信网络可信：通信网络子系统通过对通信对象的可信验证，并对通信数据包的保密性和完整性进行保护，确保其在传输过程中不会被非授权窃听和篡改，使得数据在传输过程中的安全得到了保障，与区域边界结合，实现可信接入。

d) 可信/安全管理中心：对工控系统的安全策略以及计算环境、应用区域边界和通信网络上的安全机制实现统一管理的平台。在安全管理中心内部又分为系统资源管理、安全控制和审计 3 部分。可信管理对关键资源信息度量策略和基准库进行管理。在一级可信/安全管理中心实现了多级互联。

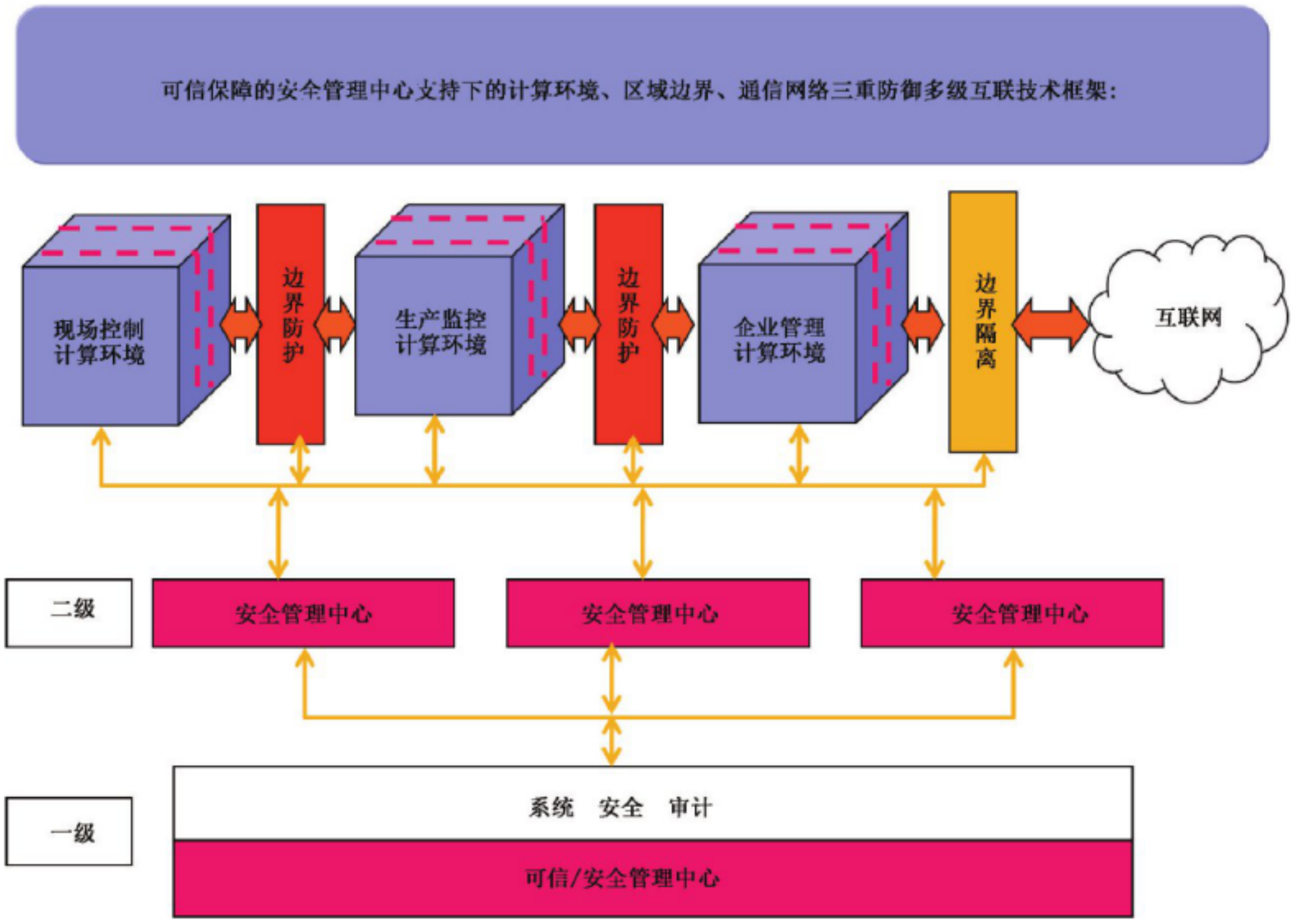


图 C.1 工业控制系统信息安全三重防御多级互联技术框架

C.3 计算节点可信架构

图 C.2 所示为计算节点可信架构示意图。在不改变应用进程的前提下，采用可信基础软件进行防护：

a) 可信基础软件中的控制机制对工控系统的应用进行(主体)进行监视；

b) 通过协作机制将审计上传到安全管理中心的审计子系统，且安全管理中心可将策略下发至可信基础软件；

c) 可信基础软件利用可信协作处理多个节点(或部件)；

d) 通过信任管理与访问控制机制相结合。

在采用可信基础软件时，应确保不与原有的安全机制发生冲突，不影响工控系统的应用进程。

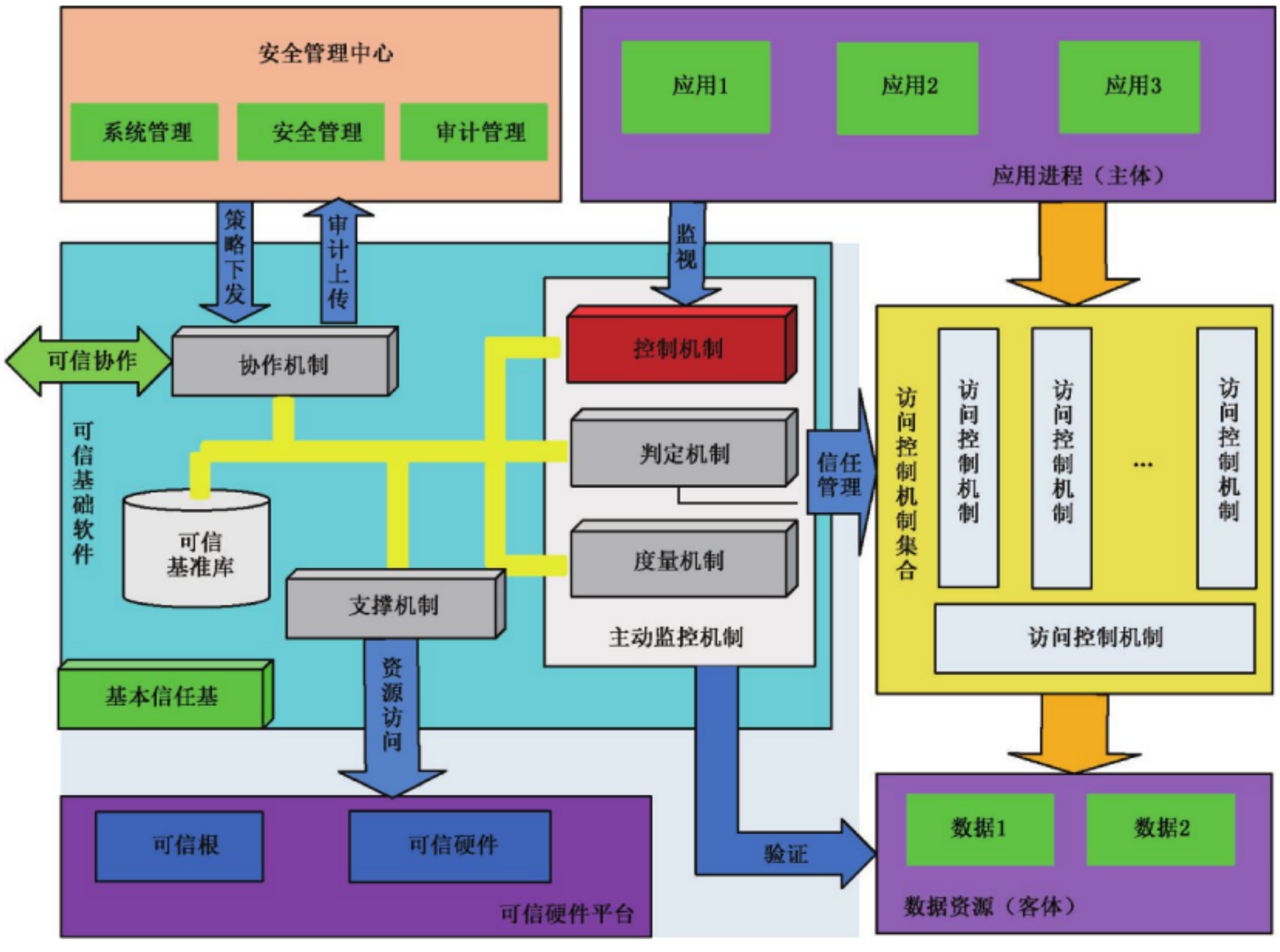


图 C.2　计算节点可信架构示意图

C.4　可信接入

在对工控系统的边界设备进行防护时，推荐采用可信策略进行边界防护。如图 C.3 所示为可信接入示意图。

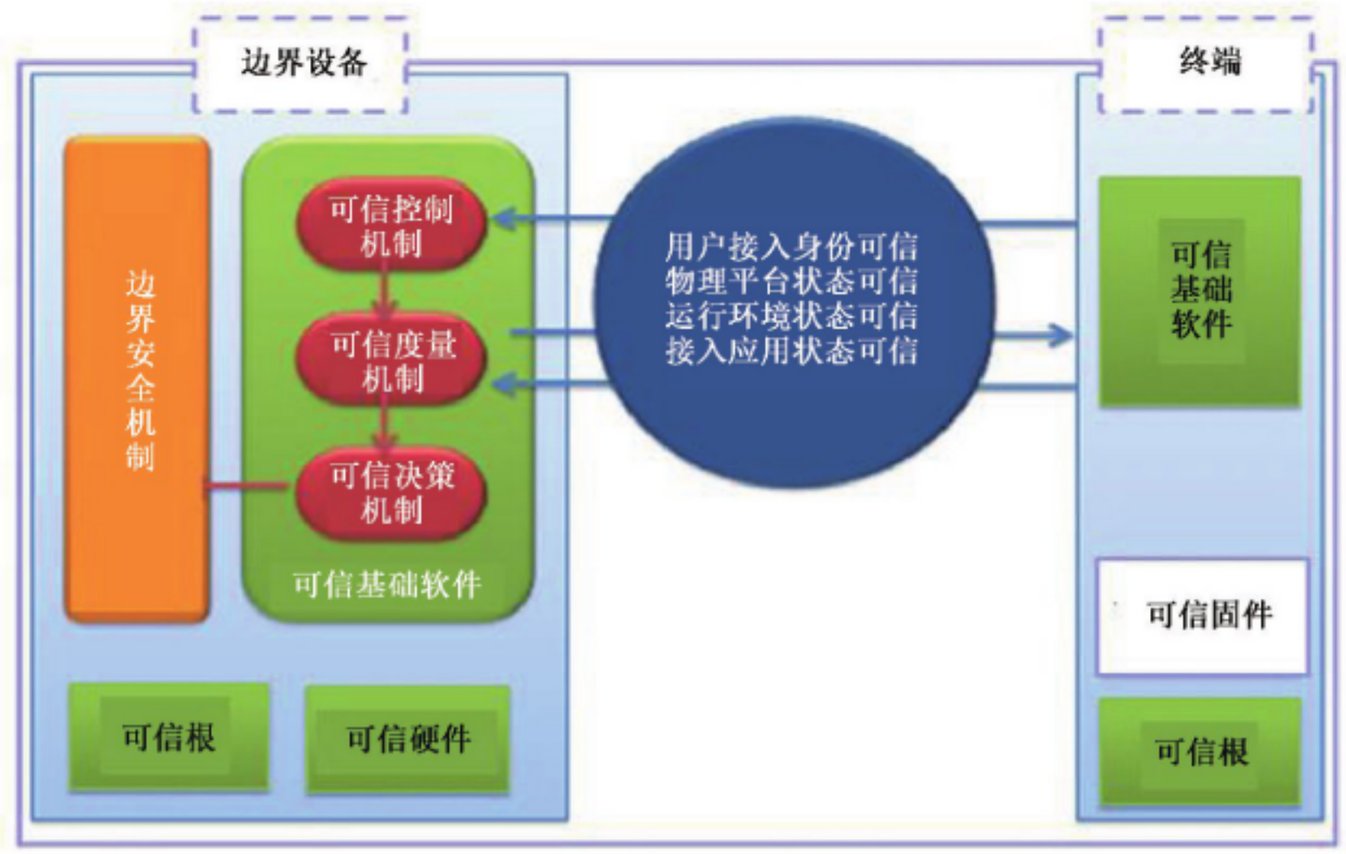


图 C.3　可信接入示意图

C.5 工业控制系统可信安全免疫技术

C.5.1 基本要求

在构成工业控制系统网络安全防护体系的各个模块内部，应逐步采用基于可信计算的安全免疫防护技术，形成对病毒木马等恶意代码的自动免疫。重要工业控制系统应在有条件时逐步推广应用以密码硬件为核心的可信计算技术，用于实现计算环境和网络环境安全免疫，免疫未知恶意代码，防范有组织的、高级别的恶意攻击。安全免疫的相关要求主要适用于新建或新开发的重要工业控制系统，在运系统具备升级改造条件时可参照执行，不具备升级改造条件的应强化安全管理和安全应急措施。

C.5.2 强制版本管理

重要工业控制系统关键控制软件应采用基于可信计算的强制版本管理措施，操作系统和监控软件的全部可执行代码，在开发或升级后应由生产厂商采用数字证书对其签名并送检，通过检测的控制软件程序应由检测机构用其数字证书对其签名，各安全域应禁止未包含生产厂商和检测机构签名版本的可执行代码启动运行。

C.5.3 静态安全免疫

重要工业控制系统应采用基于可信计算的静态安全启动机制。服务器加电至操作系统启动前应对系统内核等对象执行静态度量，业务应用、系统内核模块等对象在启动时应对其执行静态度量，确保被度量对象未被篡改且不存在未知代码，未经度量的对象应无法启动或执行。

C.5.4 动态安全免疫

重要工业控制系统应采用基于可信计算的动态安全防护机制，对系统进程、数据、代码段进行动态度量，不同进程之间不应存在未经许可的相互调用，禁止向内存代码段与数据段直接注入代码的执行。

重要工业控制系统应对业务网络进行动态度量，业务连接请求与接收端的主机设备应可以向对端证明当前本机身份和状态的可信性，不应在无法证明任意一端身份和状态可信的情况下建立业务连接。

参 考 文 献

[1] GB 17859—1999 计算机信息系统安全保护等级划分准则

[2] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型

[3] GB/T 18336.2—2015 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能组件

[4] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保障组件

[5] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[6] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

[7] GB/Z 24364—2009 信息安全技术 信息安全风险管理指南

[8] GB/T 25069—2010 信息安全技术 术语

[9] GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

[10] GB/T 30976.2—2014 工业控制系统信息安全 第2部分:验收规范

[11] GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

[12] IEC 62264-1 Enterprise-control system integration—Part 1:Models and terminology

[13] IEC 62443-3-3 Industrial communication networks—Network and system security—Part 3-3:System security requirements and security levels

[14] NIST SP800-82—2011 Guide to Industrial Control Systems(ICS) Security

[15] NIST SP800-41—2009 Guidelines on Firewalls and Firewall Policy

GA/T 1390.5—2017

中华人民共和国公共安全
行　业　标　准
信息安全技术　网络安全等级保护基本要求　第5部分：工业控制系统安全扩展要求
GA/T 1390.5—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2018年1月第一版
*
书号：155066·2-31893

GA/T 1390.5-2017