ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33008.1—2016

工业自动化和控制系统网络安全 可编程序控制器(PLC) 第1部分:系统要求

Industrial automation and control system security—Programmable logic controller(PLC)—Part 1: System requirements

2016-10-13 发布　　2017-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 33009《工业自动化和控制系统网络安全　集散控制系统(DCS)》和GB/T 33008《工业自动化和控制系统网络安全　可编程序控制器(PLC)》等共同构成工业自动化和控制系统网络安全系列标准。

GB/T 33008《工业自动化和控制系统网络安全　可编程序控制器(PLC)》计划发布如下部分：

——第1部分：系统要求；

——第2部分：系统评测实施指南；

……

本部分为GB/T 33008的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)和全国信息安全标准化技术委员会(SAC/TC 260)归口。

本部分起草单位：北京和利时系统工程有限公司、机械工业仪器仪表综合技术经济研究所、中国电子技术标准化研究院、国网智能电网研究院、中国核电工程有限公司、上海自动化仪表股份有限公司、清华大学、西门子(中国)有限公司、施耐德电气(中国)有限公司、北京钢铁设计研究总院、华中科技大学、北京奥斯汀科技有限公司、罗克韦尔自动化(中国)有限公司、中国仪器仪表学会、工业和信息化部电子第五研究所、东土科技股份有限公司、北京海泰方圆科技有限公司、青岛多芬诺信息安全技术有限公司、北京国电智深控制技术有限公司、北京力控华康科技有限公司、重庆邮电大学、中国科学院沈阳自动化研究所、西南大学、中国石油天然气管道有限公司、北京匡恩网络科技有限责任公司、西南电力设计院、北京启明星辰信息安全技术有限公司、广东航宇卫星科技有限公司、华北电力设计院工程有限公司、华为技术有限公司、中国电子科技集团公司第三十研究所、深圳万讯自控股份有限公司、横河电机(中国)有限公司北京研发中心。

本部分主要起草人：王弢、王玉敏、范科峰、梁潇、孙静、冯冬芹、朱毅明、梅恪、王浩、徐皑冬、刘枫、王亦君、张建军、薛百华、许斌、陈小淙、华镕、高昆仑、王雪、周纯杰、张莉、刘杰、刘安正、田雨聪、魏钦志、马欣欣、王勇、杜佳琳、陈日罡、丁露、李锐、刘文龙、孟雅辉、刘利民、胡伯良、孔勇、黄敏、朱镜灵、张智、张建勋、兰昆、张晋宾、成继勋、尚文利、钟诚、梁猛、陈小枫、卜志军、李琳、杨应良、杨磊。

工业自动化和控制系统网络安全 可编程序控制器(PLC) 第1部分:系统要求

1 范围

GB/T 33008的本部分规定了可编程序控制器(PLC)系统的网络安全要求,包括PLC直接或间接与其他系统通信的网络安全要求。

本部分适用于工程设计方、设备生产商、系统集成商、用户以及评估认证机构等。

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/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

可编程序(逻辑)控制器 programmable (logic) controller;PLC

一种用于工业环境的数字式操作的电子系统。这种系统用可编程的存储器作面向用户指令的内部寄存器,完成规定的功能,如逻辑、顺序、定时、计数、运算等,通过数字或模拟的输入/输出,控制各种类型的机械或过程。可编程序控制器及其相关外围设备的设计,使它能够非常方便地集成到工业控制系统中,并能很容易地达到所期望的所有功能。

注:在本部分中使用缩写词PLC代表可编程序控制器(programmable controllers),这在自动化行业中已形成共识。原来曾用PC作为可编程序控制器的缩略语,它容易与个人计算机所使用的缩略语PC相混淆。

[GB/T 15969.1—2007,定义3.5]

3.1.2

可编程序控制器(PLC)系统 programmable controller system or PLC-system

用户根据所要完成的自动化系统要求而建立的由可编程序控制器及其相关外围设备组成的配置。其组成是一些由连接永久设施的电缆或插入部件,以及由连接便携式或可搬运外围设备的电缆或其他连接方式互连的单元。

[GB/T 15969.1—2007,定义3.6]

3.1.3

脆弱性 vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点,可被利用来危害系统的完整性或安全策略。

[GB/T 30976.1—2014,定义3.1.1]

3.1.4

识别　identify

对某一评估要素进行标识与辨别的过程。

[GB/T 30976.1—2014,定义 3.1.2]

3.1.5

验收　acceptance

风险评估活动中用于结束项目实施的一种方法,主要由被评估方组织机构,对评估活动进行逐项检验,以是否达到评估目标为接受标准。

[GB/T 30976.1—2014,定义 3.1.4]

3.1.6

风险处置　risk treatment

选择并且执行措施来更改风险的过程。

[GB/T 30976.1—2014,定义 3.1.5]

3.1.7

残余风险　residual risk

经过风险处置后遗留的风险。

[GB/T 30976.1—2014,定义 3.1.6]

3.1.8

风险分析　risk analysis

系统地使用信息来识别风险来源和估计风险。

[GB/T 30976.1—2014,定义 3.1.8]

3.1.9

风险评估　risk assessment

风险分析和风险评价的整个过程。

[GB/T 30976.1—2014,定义 3.1.9]

3.1.10

风险管理　risk management

指导和控制一个组织机构相关风险的协调活动。

[GB/T 30976.1—2014,定义 3.1.10]

3.1.11

(网络)安全　security

a) 保护系统所采取的措施;

b) 由建立和维护保护系统的措施而产生的系统状态;

c) 能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态;

d) 基于 PLC 系统的能力,能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统功能,同时保证授权人员和系统不被阻止;

e) 防止对 PLC 系统的非法或有害的入侵,或者干扰其正确和计划的操作。

注 1:措施可以是与物理(网络)安全(控制物理访问计算机的资产)或者逻辑(网络)安全(登录给定系统和应用的能力)相关的控制手段。

注 2:改写 GB/T 30976.1—2014,定义 3.1.14。

3.2　缩略语

下列缩略语适用于本文件。

PLC:可编程序控制器[Programmable (Logic) Controller]
FR:基本要求(Foundational Requirement)
SR:系统要求(System Requirement)
RE:增强要求(Requirement Enhancement)
PKI:公钥基础设施(Public Key Infrastructure)
CA:数字证书认证中心(Certificate Authority)
CL:能力等级(Capability Level)
USB:通用串行总线(Universal Serial Bus)
ID:身份标识号码(Identification)
API:应用程序编程接口(Application Programming Interface)

4 PLC 网络安全概述

4.1 总则

本部分只针对 PLC 系统的网络安全要求,主要描述风险内容及安全要求、安全管理、检测与验收几个环节,为 PLC 网络安全提供依据和守则。PLC 网络安全与工程设计、管理和环境条件等各种因素相关。PLC 系统网络安全应包括在系统生命周期内的设计开发、安装、运行维护、退出使用等各阶段与系统相关的所有活动。应认识到系统面临的风险在整个生命周期内会发生变化,应该通过技术和管理两个方面,把 PLC 系统网络安全风险降低到最低或可接受的范围内。

4.2 网络安全相关内容概述

4.2.1 危险源

危险源主要包括非安全设备、系统和网络的接入点。危险源可能来自 PLC 系统外部,也可能来自 PLC 系统内部。安全威胁通过危险引入点并利用传播途径可能对受体造成伤害。危险引入点归结为以下几类,但不限于:

a) 网络通信的连接点:

例如:开放的 PLC 系统网络连接、与 PLC 系统专网互联的其他网络连接、远程技术支持和访问点、无线接入点、因特网或物联网连接;

b) 移动媒体:

例如:USB 设备、光盘、移动硬盘等;

c) 不当操作:

例如:恶意攻击、无意识误操作等;

d) 第三方设备:

例如:受感染的工业控制系统以及其他现场设备。

4.2.2 传播途径

危险源可能通过传播途径对受体造成伤害。通常,可识别单一的传播途径,但在多数情况下,一个完整的传播途径是由若干单一类型的传播途径组合而成。传播途径一般分为以下几类,但不限于:

a) 外部公共网络,如因特网、无线;
b) 局域网络(环网、点对点、无线通信);
c) 移动存储装置。

4.2.3 环境条件

PLC 系统网络安全应考虑环境条件的制约因素，特别是针对在用工业自化控制系统，应考虑现场测试和引入安全技术措施对正常生产过程的影响。

4.2.4 系统能力等级(CL)

系统能力等级如下：

a) 能力等级 CL1 ：提供机制保护控制系统防范偶然的、轻度的攻击。

b) 能力等级 CL2 ：提供机制保护控制系统防范有意的、利用较少资源和一般技术的简单手段可能达到较小破坏后果的攻击。

c) 能力等级 CL3 ：提供机制保护控制系统防范恶意的、利用中等资源、PLC 特殊技术的复杂手段可能达到较大破坏后果的攻击。

d) 能力等级 CL4 ：提供机制保护控制系统防范恶意的、使用扩展资源、PLC 特殊技术的复杂手段与工具可能达到重大破坏后果的攻击。

4.3 PLC 系统典型结构

PLC 系统典型结构如图 1 所示。

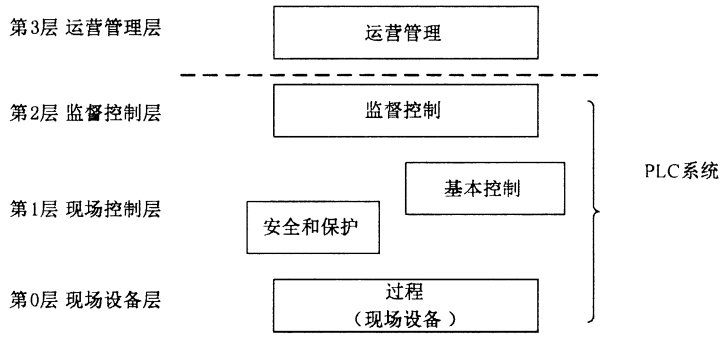

图 1 PLC 系统典型结构

第 3 层 运营管理层

包括管理生产所要求的最终产品的工作流程的功能。例子包括：生产调度、详细生产计划、可靠性保证和生产全现场控制优化。

第 2 层 监督控制层

包括监督和控制物理过程的功能。典型功能包括：操作员界面、工程师组态下装、历史数据存储、报警等。

第 1 层 现场控制层

包括感知和操作物理过程的功能。典型设备为 PLC 控制器及输入输出模块、安全和保护系统等。此层设备从传感器读取数据，必要时执行算法，并维护过程历史记录。安全和保护系统监视过程，并在超出安全限值时将过程自动返回安全状态。

第 0 层 现场设备层

包括直接连接到过程和过程设备的传感器和执行器。

4.4 PLC 系统网络安全总体要求

4.4.1 概述

工程设计方、设备生产商、系统集成商、用户以及评估认证机构(以下简称“组织”)宜识别、分析、评

价、管理、监视和评审组织所面临安全风险，建立并维护网络安全管理的要求，建立网络安全管理职责，分配和管理资源，运用过程方法实现 PLC 系统的正常运行，并采取有效的措施测量、分析和改进，以满足 PLC 系统网络安全管理的要求。

4.4.2 建立 PLC 系统网络安全管理要求

4.4.2.1 网络安全管理方针

依据业务要求和相关法律法规提供管理指导并支持网络安全。

网络安全管理要求由管理者组织、制定、批准、发布并传达给所有员工和外部相关方；网络安全方针文件应说明管理承诺，并提出组织机构的管理网络安全的方法。方针文件建议包括以下声明：

a) 网络安全、整体目标和范围的定义，以及在允许信息共享机制下安全的重要性；

b) 管理者意图的声明，以支持符合业务策略和目标的网络安全目标和原则；

c) 设置控制目标和控制措施的框架，包括风险评估和风险管理的结构；

d) 对组织机构特别重要的安全方针策略、原则、标准和符合性要求的简要说明，包括：

- 符合法律法规要求；
- 安全教育、培训和意识要求；
- 业务连续性管理；
- 违反网络安全方针的后果。

4.4.2.2 识别、分析和评价安全风险

组织应建立、维护 PLC 系统网络安全风险的识别、分析和评价的方法：

a) 确定风险评估方法：

- 识别适合 PLC 系统网络安全、已识别的业务网络安全和法律法规要求的风险评估方法；
- 制定接受风险的准则，识别可接受的风险级别；
- 选择的风险评估方法应确保风险评估产生可比较的和可再现的结果。

b) 定期识别风险，包括：

- 识别 PLC 系统网络安全管理范围内的资产及其责任人；
- 识别资产所面临的威胁；
- 识别可能被威胁利用的脆弱性；
- 识别丧失保密性、完整性和可用性可能对资产造成的影响。

c) 定期分析和评价风险，应：

- 在考虑丧失资产的保密性、完整性和可用性所造成的后果的情况下，评估安全失效可能造成的对组织的影响；
- 根据主要的威胁和脆弱性、对资产的影响以及当前所实施的控制措施，评估安全失效发生的可能性；
- 估计风险的级别；
- 确定风险是否可接受，或者是否需要使用接受风险的准则进行处理。

d) 识别和评价风险处置的可选措施，可能的措施包括：

- 采取适当的控制措施；
- 在明显满足组织方针策略和接受风险的准则的条件下，有意识地、客观地接受风险；
- 避免风险；
- 将相关业务风险转移到其他方，如：保险，供应商等。

4.4.2.3 确定安全管理目标

控制目标和控制措施应加以选择和实施，以满足风险评估和风险处置过程中所识别的要求。这种选择应考虑接受风险的准则以及法律法规的要求。

从 GB/T 22080—2008 附录 A 中选择控制目标和控制措施成为此过程的一部分，但并不是所有的控制目标和控制措施，组织宜按照设计、集成或应用的 PLC 系统网络安全技术等级要求，在其整体业务活动中且在所面临风险的环境下确定控制目标和控制措施。

获得管理者对建议的残余风险的批准。

4.4.3 实施和运行网络安全管理

4.4.3.1 管理职责

4.4.3.1.1 管理承诺

应通过清晰的说明、可证实的承诺、明确的网络安全职责分配及确认，来积极支持组织机构内的安全：

- 制定网络安全管理方针；
- 确保网络安全控制目标和计划得以制定；
- 建立网络安全的角色和职责；
- 为安全启动提供明确的方向和支持；
- 为网络安全提供所需的资源；
- 启动计划和程序来保持网络安全意识；
- 决定接受风险的准则和风险的可接受级别。

4.4.3.1.2 资源提供

应确定并提供所需的资源，以：

- 确保网络安全规程支持 PLC 系统业务要求；
- 通过正确实施所有的控制措施保持适当的安全；
- 必要时，进行评审，并适当响应评审的结果；
- 在需要时，改进网络安全管理的有效性。

4.4.3.1.3 培训、意识和能力

通过以下方式，确保所有被赋予网络安全管理职责的人员具有执行所要求的任务的能力：

- 确定从事影响 PLC 系统网络安全管理工作的人员所必要的能力；
- 提供培训或采取其他措施（如聘用有能力的人员）以满足这些需求；
- 评价所采取措施的有效性；
- 保持教育、培训、技能、经理和资格的记录。

确保所有相关人员意识到他们网络安全活动的相关性和重要性，以及如何为达到网络安全目标做出贡献。

4.4.3.2 风险处置计划、实施

组织应：

a) 为管理 PLC 系统网络安全风险制定处置计划，该计划应包含：适当的管理措施、资源、职责和优先顺序；

b) 实施风险处置计划以达到已识别的控制目标，包括资金安排、角色和职责的分配；
c) 实施所选择的控制措施，以满足控制目标；
d) 确定如何测量所选择的控制措施或控制措施集的有效性，并指明如何用这些测量措施来评估控制措施的有效性，以产生可比较的和可再现的结果；
e) 管理 PLC 系统网络安全相关的资源；
f) 实施能够迅速检测安全事态和响应安全事件的规程和其他控制措施。

4.4.4 监视和评审网络安全管理的有效性

组织应：
a) 执行监视评审规程和其他控制措施，以：
- 迅速检测过程运行结果中的错误；
- 迅速识别试图的和得逞的安全违规和事件；
- 使管理者能够确定分配给人员的安全活动或通过信息技术实施的安全活动是否按期望执行；
- 通过使用指示器，帮助检测安全事态并预防安全事件；
- 确定解决安全违规的措施是否有效。

b) 在考虑安全事件、有效性测量结果、所有相关方的建议和反馈的基础上，进行网络安全管理有效性的定期评审(包括满足网络安全管理方针和目标，以及安全控制措施的评审)。
c) 测量控制措施的有效性已验证安全要求是否被满足。
d) 按照计划时间间隔进行风险评估的评审，以及对残余风险和以确定的可接受的风险及级别进行评审，应考虑以下方面的变化：
- 组织；
- PLC 系统升级或更新；
- 业务目标和过程；已识别的威胁；
- 已实施的控制措施的有效性；
- 外部事态，如法律法规环境的变更、合同义务的变更和社会环境的变更。

e) 考虑监视评审活动的结果，以更新安全计划。
f) 记录可能影响 PLC 系统网络安全的有效性或执行情况的措施和事态。

4.4.5 保持和改进

组织应经常：
a) 实施易识别的网络安全管理改进；
b) 采取纠正和预防措施，从其他组织和组织自身的安全经验中吸取教训；
c) 向所有相关方沟通措施和改进情况，其详细程度与环境相适应，需要时，商定如何进行；
d) 确保改进达到了预期目标。

5 PLC 系统网络安全技术要求

5.1 网络安全技术要求说明

本部分关注从第 2 层到第 1 层的网络安全技术要求。

PLC 系统安全要求包括基本要求(FR)、系统要求(SR)和系统增强要求(RE)，每一项基本要求分为若干个系统要求(SR)，其中有些系统要求还包含了增强要求(RE)。其与能力等级(CL)的映射见附录 A。

本部分引用 GB/T 30976.1—2014 的部分内容，并针对 PLC 系统进行了裁剪和细化。为方便对照和使用，本部分 FR、SR、RE 的编号与 GB/T 30976.1—2014 保持一致。

5.2 对第 2 层和第 1 层的总体要求

5.2.1 FR 5：限制的数据流

5.2.1.1 SR 5.1：网络分区

应将 PLC 系统网络与非 PLC 系统网络进行逻辑分区，将关键 PLC 系统网络和其他 PLC 系统网络进行逻辑分区。

5.2.1.2 SR 5.1 RE (1)：物理网络分区

应将 PLC 系统网络与非 PLC 系统网络进行物理分区，将关键 PLC 系统网络和其他 PLC 系统网络进行物理分区。

5.2.1.3 SR 5.1 RE (2)：与非 PLC 系统网络的独立性

PLC 系统网络服务可独立运行，不依靠非 PLC 系统设备网络连接。

5.2.1.4 SR 5.1 RE (3)：关键网络的逻辑或物理隔离

关键 PLC 系统网络与其他 PLC 系统网络进行逻辑或物理隔离。

5.2.1.5 SR 5.2：区域边界防护

PLC 系统应提供监视和控制区域边界通信的能力：

a) 能监视区域边界的通信；

b) 能控制区域边界的通信。

5.2.1.6 SR 5.2 RE (1)：默认拒绝，例外允许

PLC 系统应提供默认拒绝所有网络流量、例外允许网络流量(也称为拒绝所有，允许例外)的能力。

5.2.1.7 SR 5.2 RE (2)：孤岛模型

PLC 系统应提供能力防止任何通过 PLC 系统边界的通信(也称为孤岛模型)。

5.2.1.8 SR 5.2 RE (3)：故障关闭

当边界防护机制出现操作故障时，PLC 系统应提供阻止所有 PLC 系统边界通信(也称为故障关闭)的能力。故障关闭功能的设计应不干扰功能安全系统或其他功能安全相关功能的运行。

5.2.1.9 SR 5.3：一般目的的内部节点间通信限制

PLC 系统应提供能力防止一般目的的内部节点间通信消息被 PLC 系统外部的用户或系统接收到。

5.2.1.10 SR 5.4：应用分离

PLC 系统应基于实现分区模型的关键程度提供对数据、应用和服务进行分离的能力。

5.2.1.11 SR 5.5：网络分层

应将 PLC 系统根据实际应用场景进行逻辑分层。

5.2.1.12 SR 5.5 RE (1):层间边界防护

PLC 系统应提供监视和控制第 2 层与第 1 层通信的能力。

5.3 对第 2 层的要求

5.3.1 FR 1: 标识和认证控制

5.3.1.1 SR 1.1:用户(人)的标识和认证

PLC 系统应提供标识和认证所有用户(人)的能力。这一能力应在访问 PLC 系统的所有访问接口上实施,以支持符合相应安全策略和规程的职责分离和最小特权原则。PLC 系统应使:

a) 用户标识符能在所有访问接口上被认证。

b) 无效用户标识符在所有访问接口上被拒绝。

5.3.1.2 SR 1.1 RE (1):唯一标识和认证

PLC 系统应对所有用户(人)提供唯一标识和认证的能力。

5.3.1.3 SR 1.1 RE (2):非可信网络的多因子认证

当人通过非可信网络访问(例如远程访问)PLC 系统时,PLC 系统应为其提供多因子认证的能力。对于经由非可信网络的远程访问的认证方法要求多于一种。

5.3.1.4 SR 1.2:软件进程的标识和认证

PLC 系统宜提供标识和认证所有软件进程的能力。这一能力应在访问 PLC 系统的所有访问接口上实施,以支持符合相应安全策略和规程的职责分离和最小特权原则。

5.3.1.5 SR 1.2 RE (1):唯一标识和认证

PLC 系统应对所有合法软件进程拥有唯一标识认证的能力。

5.3.1.6 SR1.3 :账号管理

PLC 系统应提供对所有账号的管理,包括创建、激活、修改、禁用和移除账号的能力,当一个或多个账号被修改或移除时,未被修改的账号保持激活和账号权限不变。

5.3.1.7 SR 1.3 RE(1):统一的账号管理

PLC 系统应提供能力支持统一的账号管理。

5.3.1.8 SR 1.4:标识符管理

PLC 系统应提供按照用户、组、角色和/或 PLC 系统接口管理标识符(例如用户 ID)的能力。

5.3.1.9 SR 1.5:认证码管理

PLC 系统应保护认证码存储和传输时不被未经授权的泄露和更改。

5.3.1.10 SR 1.5 RE (1):软件进程标识凭证的硬件安全

对于软件进程和设备用户,PLC 系统应提供使用硬件机制保护相关认证码的能力。

5.3.1.11 SR 1.6:无线访问管理

对参与无线通信的所有的用户,PLC 系统应提供标识和认证的能力。PLC 系统应使:

a) 合法用户标识符能在无线访问接口上被认证;

b) 无效用户标识符在无线访问接口上被拒绝。

5.3.1.12 SR 1.6 RE (1):唯一标识和认证

对参与无线通信的所有的用户,PLC 系统应提供唯一标识和认证的能力。

5.3.1.13 SR 1.7:口令认证

对于使用口令认证的 PLC 系统,PLC 系统应提供能力,实施可配置的基于最小长度和不同字符类型的口令强度。PLC 系统应:

a) 提供实施口令的最小长度的能力。验证小于最小长度的口令被拒绝用于认证。

b) 提供能力,实施口令中除字母字符外至少还要包含最小数目的特殊字符。验证不符合最小字符集的口令被拒绝用于认证。

5.3.1.14 SR 1.7 RE (1):对用户(人)的口令生成和口令有效期的限制

PLC 系统应为用户(人)提供口令重用次数、口令有效期可配置的能力,这些能力符合普遍接受的安全工业实践。

5.3.1.15 SR 1.8:公钥基础设施证书

当使用公钥基础设施 PKI 时,PLC 系统应提供能力按照普遍接受的最佳实践运行 PKI 或从现有 PKI 中获取公钥证书。

5.3.1.16 SR 1.9:公钥认证的加强

对于使用公钥认证的 PLC 系统,PLC 系统应提供以下能力:

a) 通过检查给定证书的签名的有效性来证实证书;

b) 通过可接受的证书认证机构(CA)证实证书,或在自签名证书情况下,以某种事先定义的方式证实证书;

c) 通过给定证书的撤销状态证实证书;

d) 建立用户对相应私钥的控制;

e) 将已认证的标识映射为用户。

5.3.1.17 SR 1.9 RE (1):公钥认证的硬件安全

PLC 系统应提供能力,按照普遍接受的安全工业实践和推荐,通过硬件机制保护相关的私钥。

5.3.1.18 SR 1.10:认证反馈

PLC 系统将认证信息的反馈模糊化,使得当一个或多个凭证无效时,失败的认证尝试不提供任何合法凭证有效性的信息(例如用户名和口令)。

5.3.1.19 SR 1.11:失败的登录尝试

PLC 系统应:

a) 对任何用户在可配置的时间周期内连续无效访问尝试的次数限制为一个可配置的数目;

b) 在可配置时间周期内未成功尝试次数超过上限时，在指定时间内拒绝访问直到由管理员解锁；

c) 不应允许关键服务或服务器运行的系统账号交互式登录。

5.3.1.20 SR 1.13：经由非可信网络的访问

PLC 系统应：

a) 能监视和控制所有经由不可信网络对控制系统的访问；

b) 拒绝来自不可信网络的访问，除非被指定角色批准。

5.3.1.21 SR 1.13 RE (1)：明确的对访问请求的批准

默认的，PLC 系统应提供能力拒绝来自不可信网络的访问，除非被指定角色批准，例如 限制未授权的 IP 地址接入。

5.3.2 FR 2：使用控制

5.3.2.1 SR 2.1：授权的执行

在所有接口上，PLC 系统应提供能力执行分配给所有用户(人)的授权，按照职责分离和最小特权来控制对 PLC 系统的使用。

PLC 系统应为资产所有者提供修改许可到角色的映射的能力。包括但不限于：

a) 浏览权限用户；

b) 操作员；

c) 控制应用工程师；

d) PLC 系统管理员；

e) 操作主管；

f) 仪表技术员。

5.3.2.2 SR 2.2：无线使用控制

PLC 系统应提供能力，对 PLC 系统的无线连接应依据普遍接受的安全工业实践进行授权、监视和限制使用。PLC 系统应：

a) 能授权、监视和限制对 PLC 系统的无线访问；

b) 能使用适当的认证机制保护无线访问。

5.3.2.3 SR 2.2 RE (1)：对未授权的无线设备进行识别和报告

PLC 系统应提供识别和报告未授权的与 PLC 系统相关的无线设备在 PLC 系统物理环境内发射信号的能力。

5.3.2.4 SR 2.3：对便携和移动设备的使用控制

对于便携和移动设备，PLC 系统应提供使用限制的能力，包括：

a) PLC 系统提供手段来禁用/控制便携或移动设备的使用；

b) PLC 系统监视和记录便携和移动设备的访问和使用；

c) PLC 系统安全手册提供了对便携和移动设备使用限制的列表。

5.3.2.5 SR 2.3 RE (1)：便携和移动设备的安全状态的实施

PLC 系统应提供能力，确保便携和移动设备连接到一个区域之前，其安全状态符合该区域的安全

策略和规程。包括：

a) PLC 系统提供在授权连接之前对便携和移动设备进行扫描；

b) PLC 系统监视和记录扫描结果；

c) PLC 系统安全手册提供对移动设备合规扫描进行配置的指示。

5.3.2.6 SR 2.4：移动代码

基于移动代码破坏控制系统的潜在可能性，控制系统应提供以下能力：对编辑、修改移动代码的人员进行权限管理和身份认证。

5.3.2.7 SR 2.4 RE(1)：移动代码的完整性检查

控制系统应提供能力，在允许代码执行之前验证移动代码的完整性。

5.3.2.8 SR 2.4 RE(2)：移动代码的使用限制

PLC 系统应：

a) 预防移动代码的执行；

b) 对代码源要求适当的认证和授权；

c) 限制移动代码传入/传出控制系统；

d) 监视移动代码的使用。

5.3.2.9 SR 2.7：并发连接控制

对任意给定用户，PLC 系统应提供将每个接口的并发连接的数目限制为一个可配置的数目的能力。

5.3.2.10 SR 2.8：可审计的事件

PLC 系统应提供为以下类别生成审计记录的能力：访问控制、请求错误、系统事件、备份和存储事件、配置变更、潜在的侦查行为和审计日志事件。

5.3.2.11 SR 2.8 RE (1)：中央管理的、系统范围的审计跟踪

PLC 系统应提供能力，对审计事件进行中央管理，并将来自整个 PLC 系统内多个部件的审计记录汇聚为系统范围的、时间相关的审计跟踪。PLC 系统应提供按照工业标准格式输出审计记录的能力，以便标准的商业日志分析工具对其分析。

5.3.2.12 SR 2.9：审计存储容量

PLC 系统应根据日志管理和系统配置普遍认可的推荐值来分配足够的审计记录存储容量。PLC 系统应提供审计机制减少超出该容量的可能性。

当分配的审计记录存储量达到最大审计记录存储容量的某个可配置比例时，PLC 系统应提供发出警告的能力。

5.3.2.13 SR 2.10：对审计流程失败时的响应

PLC 系统应：

a) 在审计流程失败时，提供向人员告警并防止技术服务和功能丢失的能力；

b) 当审计流程失败时，提供以下响应的能力：覆盖最老的审计记录、停止生成审计记录。

5.3.2.14 SR 2.11：时间戳

PLC 系统应提供时间戳用于生成审计记录。

5.3.2.15 SR 2.11 RE (1)：内部时间同步

PLC 系统应提供以可配置的频率同步内部系统时钟的能力。

5.3.2.16 SR 2.11 RE (2)：时间源的完整性的保护

时间源应被保护不受未授权的变更，其变更应触发审计事件。

5.3.2.17 SR 2.12：不可否认性

PLC 系统应提供对给定用户(人)是否实施了某个特定行为进行判定的能力。

5.3.2.18 SR 2.12 RE (1)：所有用户的不可否认性

PLC 系统应提供对所有用户是否执行了某个行为进行判定的能力。

5.3.3 FR 3：系统完整性

5.3.3.1 SR 3.1：通信完整性

PLC 系统应保护通信信道上传输的信息的完整性。

5.3.3.2 SR 3.1 RE (1)：基于密码技术的完整性保护

PLC 系统应提供能力采用密码学机制识别信息在通信过程中的变更，除非信息已被其他可替换的物理措施保护。

5.3.3.3 SR 3.2：恶意代码的防护

PLC 系统应提供能力，采用防护机制来防止、检测、报告和消减恶意代码或非授权软件的影响。PLC 系统应：

a) 采用一定的防护机制以防护恶意代码；
b) 配置、启用防护产品；
c) 更新防护产品到软件最新版本；
d) 提供防护产品防护的恶意代码类型的列表或说明。

5.3.3.4 SR 3.2 RE (1)：在入口和出口点防护恶意代码

PLC 系统应提供在所有入口和出口点上采用恶意代码防护机制的能力。PLC 系统应：

a) 在区域边界提供恶意代码的防护；
b) 配置和启用防护产品；
c) 更新防护产品到软件最新的版本；
d) 提供防护产品防护的恶意代码类型的列表或说明。

5.3.3.5 SR 3.2 RE(2)：恶意代码防护的集中管理和报告

PLC 系统应提供集中管理恶意代码防护机制的能力。

5.3.3.6 SR 3.4：软件和信息完整性

PLC 系统应提供能力检测、记录和保护软件和信息不受未经授权的变更。

5.3.3.7 SR 3.4 RE（1）：对破坏完整性进行自动通知

PLC 系统应提供能力，使用自动化工具在完整性验证期间发现不符时通知人员。

5.3.3.8 SR 3.5：输入验证

PLC 系统应验证任何输入的语法和内容，这些输入是作为工业过程控制输入或直接影响 PLC 系统行为的输入。

5.3.3.9 SR 3.6：确定性的输出

控制系统提供能力，在遭受攻击无法保持正常运行时能够将输出设为预先定义的状态。

这些状态包括：

a） 未上电状态；

b） 可知的最后的好值；

c） 由资产属主或应用确定的固定值。

5.3.3.10 SR 3.7：错误处理

PLC 系统识别和处理错误条件的方式应能够实施有效的补救，这一方式不能提供可能被敌人利用来攻击工业 PLC 系统的信息，除非泄露这一信息对于及时发现并修理问题是必须的。

PLC 系统能规定错误信息的适当的结构和内容，以提供及时有用的信息而不暴露潜在的有害信息。

5.3.3.11 SR 3.8：会话完整性

PLC 系统应提供保护通信会话完整性的机制，能为通信会话的每一端提供端对端身份和传输信息正确性的信任。

5.3.3.12 SR 3.8 RE（1）：会话终止后会话 ID 的失效

在用户登出或会话终止（包括浏览器会话）后，系统应提供使其会话标识失效的能力。

5.3.3.13 SR 3.8 RE（2）：唯一会话 ID 的产生和承认

系统应提供能力，为每个会话生成唯一的会话标识 ID，并且只认可系统生成的会话标识。

5.3.3.14 SR 3.8 RE（3）：会话 ID 的随机性

控制系统应提供使用普遍接受的随机源生成唯一的会话标识的能力。

5.3.3.15 SR 3.9：审计信息的保护

PLC 系统应保护审计信息和审计工具不被未授权地访问、修改和删除。

5.3.3.16 SR 3.9 RE（1）：一次性写入介质上的审计记录

PLC 系统应提供在基于硬件的、一次性写入介质上生成审计记录的能力。

5.3.4 FR 4：数据保密性

5.3.4.1 SR 4.1：信息保密性

PLC 系统应提供能力，对有读授权的信息在静态和传输中进行保密性保护。PLC 系统应：

a) 通过维护具有可控物理访问的可信网络来保护敏感信息的保密性（认证信息，例如用户名和口令应考虑保密）；
b) 识别敏感信息；
c) 对敏感信息的访问和传输进行控制，以防止窃听和篡改。

5.3.4.2 SR 4.1 RE（1）：静态和经由不可信网络传输的数据的保密性保护

PLC 系统应：

a) 提供能力保护静态信息和穿越不可信网络的远程访问连接的保密性；
b) 加密敏感的 PLC 系统信息，例如口令，在存储和穿过外部网络传输时是加密的。

5.3.4.3 SR 4.1 RE（2）：区域边界的机密性保护

PLC 系统应提供能力保护穿越所有区域边界的信息的机密性，敏感的 PLC 系统数据例如口令在存储和穿越区域边界时是加密的。

5.3.4.4 SR 4.2：信息存留

PLC 系统应提供退役能力，清除被在用服务所释放的部件中所有与安全相关的资料。

5.3.4.5 SR 4.2 RE（1）：共享内存资源的清除

PLC 系统应防止借助易失性存储资源进行的未经授权的和无意的信息传输，当易失性共享存储释放回 PLC 系统供不同用户使用时，所有的特有数据及特有数据的关联都应从资源中清除，从而使新用户对其不可见和不可访问。

5.3.4.6 SR 4.3：密码的使用

如果需要密码，PLC 系统应根据普遍接受的工业实践和推荐来使用密码算法、密钥长度以及密钥创建和管理机制。

5.3.5 FR 6：对事件的及时响应

5.3.5.1 SR 6.1：审计日志的可访问性

PLC 系统应为已授权的人和/或工具提供访问审计日志的能力。

5.3.5.2 SR 6.1 RE（1）：对审计日志的编程式访问

PLC 系统应使用应用编程接口 API 提供对审计记录的访问。

5.3.5.3 SR 6.2：持续监视

PLC 系统应使用普遍接受的安全工业实践和推荐来提供持续监视所有安全机制的性能的能力，以及时检测、特征化、削减和报告对安全的违背。

5.3.6 FR 7：资源可用性

5.3.6.1 SR 7.1：拒绝服务的防护

PLC 系统应对拒绝服务攻击有一定的防护能力。

5.3.6.2 SR 7.1 RE (1)：管理通信负荷

PLC 系统应提供管理通信负荷的能力(例如使用限速)来消减信息泛洪类的拒绝服务攻击事件。

5.3.6.3 SR 7.1 RE (2)：限制拒绝服务攻击对其他系统和网络的影响

PLC 系统应提供能力限制所有用户引发拒绝服务攻击事件的能力，这些事件可能影响其他 PLC 系统和网络。

5.3.6.4 SR 7.2：资源管理

PLC 系统应对资源的使用提供安全功能，防止资源耗尽。

5.3.6.5 SR 7.3：数据备份

系统应在不影响工厂正常运行情况下，支持识别和定位关键文件，并有能力执行用户级和系统级备份(包含系统状态信息)。控制系统应提供以可配置的频率自动实现上述功能的能力。

5.3.6.6 SR 7.3 RE (1)：备份验证

控制系统应提供验证备份机制的可靠性的能力。

5.3.6.7 SR 7.3 RE (2)：备份自动化

控制系统应提供按照可配置的频率自动备份的能力。

5.3.6.8 SR 7.4：PLC 系统恢复和重构

当遭受攻击而造成系统中断或故障，PLC 系统应提供恢复和重构到已知的安全状态的能力。

5.3.6.9 SR 7.5：紧急电源

PLC 系统应在不影响现有安全状态条件下提供与紧急电源之间进行切换的能力。

5.3.6.10 SR 7.6：网络和安全配置设置

PLC 系统应提供能力，按照 PLC 系统提供商规定的指南中描述的推荐网络和安全配置进行配置。PLC 系统应提供与现有部署网络和安全配置设置之间的一个接口。PLC 系统应：

a) 能为配置设置提供可调节的参数；
b) 能根据安全策略和规程对配置变更进行监视和控制。

5.3.6.11 SR 7.7：最小功能化

PLC 系统应提供必要的能力，明确禁止和/或限制对非必要的功能、端口、协议和/或服务的使用。

5.3.6.12 SR 7.8：PLC 系统部件清单

PLC 系统应提供报告当前已安装的部件及其关联属性的列表的能力。PLC 系统应：

a) 提供报告已安装部件及其关联属性的方法；
b) 确保已安装部件在系统部件清单目录中是正确的；
c) 在部件增加、移除或部件属性变更时，正确更新系统部件清单目录。

5.4 对第 1 层的要求

5.4.1 FR 1：标识和认证控制

5.4.1.1 SR 1.1：用户(人)的标识和认证

PLC 系统应提供标识和认证所有用户(人)的能力。这一能力应在访问控制器的所有访问接口上实施，以支持符合相应安全策略和规程的职责分离和最小特权原则。

5.4.1.2 SR 1.6：无线访问管理

对参与无线通信的所有的用户，控制器应提供标识和认证的能力。PLC 系统应：
a) 能在无线访问接口上验证合法用户标识符，认证为正确；
b) 能在无线访问接口上验证无效用户标识符，无效用户被拒绝。

5.4.1.3 SR 1.13：经由非可信网络的访问

PLC 系统应提供能力控制所有经由不可信网络对控制器的访问方法，例如可限制未授权的 IP 地址接入。

5.4.2 FR 2：使用控制

5.4.2.1 SR 2.1：授权的执行

在所有逻辑接口上，控制器应提供能力执行分配给所有用户(人)的授权，按照职责分离和最小特权来控制对控制系统的使用。

5.4.2.2 SR 2.2：无线使用控制

PLC 系统应提供能力，对控制系统的无线连接应依据普遍接受的安全工业实践进行授权、监视和限制使用。

5.4.2.3 SR 2.3：对便携和移动设备的使用控制

控制器应提供限制使用便携和移动存储介质的能力，包括：
a) 防止使用便携和移动存储介质；
b) 要求上下文特定的授权；
c) 限制代码、数据传入传出便携和移动存储介质。

5.4.2.4 SR 2.4：用户工程代码

PLC 系统应提供能力，限制用户工程代码传入/传出。

5.4.2.5 SR 2.7：连接过程要求

对任意给定用户，控制器应提供将每个接口的并发连接的数目限制为一个数目的能力。

5.4.2.6 SR 2.8：诊断能力

控制器应提供错误诊断能力。

5.4.2.7 SR 2.11：时间戳

控制器或对控制器的审计设备应提供时间戳用于生成审计记录。

5.4.2.8 SR 2.11 RE (1)：内部时间同步

PLC 系统具备同步内部系统时钟的能力。

5.4.3 FR 3：系统完整性

5.4.3.1 SR 3.1：通信信息完整性

PLC 系统应保护传输的信息的完整性。

5.4.3.2 SR 3.5：输入验证

PLC 系统应验证任何影响关键输出的输入，这些输入有可能来自上位机或其他控制器。

5.4.3.3 SR 3.6：确定性的输出

PLC 应提供能力，在遭受攻击无法保持正常运行时能够将输出设为预先定义的状态。

这些状态包括：

a) 未上电状态；

b) 可知的最后的好值；

c) 由资产所有者或应用确定的固定值。

5.4.3.4 SR 3.7：错误处理

PLC 应提供基本的错误处理的标识。

5.4.3.5 SR 3.8：连接完整性

PLC 系统应提供保护通信连接完整性的机制。

5.4.4 FR 4：数据保密性

5.4.4.1 SR 4.1：信息保密性

控制器应提供能力，对有读授权的信息在静态和传输中进行保密性保护，对敏感信息的访问和传输进行控制，以防止窃听和篡改。

5.4.4.2 SR 4.3：密码的使用

如果层间通信需要密码，控制器应采用符合国家和行业的相关法律、法规要求的密码算法、密钥长度以及密钥创建和管理机制。

5.4.5 FR 6：对事件的及时响应

5.4.5.1 SR 6.1：诊断记录的可访问性

控制器应提供访问错误诊断记录的能力。

5.4.6 FR 7：资源可用性

5.4.6.1 SR 7.1：管理通信负荷

控制器应提供管理通信负荷的能力(例如使用限速)来消减信息泛洪类的拒绝服务攻击事件。

5.4.6.2 SR 7.2：资源管理

控制器应提供对资源的使用的安全能力，防止资源耗尽。

5.4.6.3 SR 7.4：PLC 系统恢复和重构

当遭受攻击而造成系统中断或故障，系统应具有根据工艺要求，采用技术和管理手段维持已知安全状态的能力。

5.4.6.4 SR 7.5：紧急电源

应在不影响现有安全状态条件下提供与紧急电源之间进行切换的能力。

5.4.6.5 SR 7.6：网络和安全配置设置

控制系统应提供能力，按照控制系统提供商规定的指南中描述的推荐网络和安全配置进行配置。控制系统应提供与现有部署网络和安全配置设置之间的一个接口。

5.4.6.6 SR 7.7：最小功能化

控制器应明确禁止和/或限制对非必要的功能、端口、协议和/或服务的使用。

6 PLC 系统网络安全管理要求

6.1 总体要求

组织宜在其整体业务活动中按照 GB/T 30976.1—2014、本部分的附录 B 以及 6.2 要求执行，以满足 PLC 系统网络安全管理的要求。

6.2 PLC 系统设计、开发过程网络安全管理补充要求

组织宜针对拟提供的 PLC 系统的网络安全技术要求，建立管理职责、分配和管理资源，运用过程方法实现 PLC 系统的设计、开发、生产及交付，对产品实现过程予以测量、分析和改进，以满足 PLC 系统的网络安全要求。

对于 PLC 系统的设计、开发过程应满足系统网络安全管理要求，包括但不限于：

a) 在进行设计和开发策划时，组织应当针对 PLC 网络安全技术要求，研究安全性设计、可维护性设计等设计理念，并在适合时加以应用；
b) 产品应用后的网络安全风险应当作为设计和开发的输入；
c) 设计和开发的输出应包含满足 PLC 系统网络安全技术要求的内容；
d) 应证明对所有已识别的网络安全风险进行了设计和开发的验证及确认；
e) 对设计和开发更改的评审应包含网络安全风险的再确认。

附 录 A
（规范性附录）
系统要求和增强要求与安全等级的映射

系统要求和增强要求与安全等级的映射关系见表 A.1。

表 A.1 系统要求和增强要求与安全等级的映射

SR 和 RE	CL1	CL2	CL3	CL4
对第 2 层到第 1 层的总体要求				
FR 5：限制的数据流				
SR 5.1：网络分区	√	√	√	√
RE (1)：物理网络分区			√	√
RE (2)：与非 PLC 系统网络的独立性		√	√	√
RE (3)：关键网络的逻辑或物理隔离			√	√
SR 5.2：区域边界防护	√	√	√	√
RE (1)：默认拒绝，例外允许		√	√	√
RE (2)：孤岛模型			√	√
RE (3)：故障关闭			√	√
SR 5.3：一般目的的内部节点间通信限制	√	√	√	√
SR 5.4：应用分离	√	√	√	√
SR 5.5：网络分层	√	√	√	√
RE (1)：层间边界防护			√	√
对第 2 层的要求				
FR 1：标识和认证控制				
SR 1.1：用户(人)的标识和认证	√	√	√	√
RE(1)：唯一标识和认证		√	√	√
RE(2)：非可信网络的多因子认证			√	√
SR 1.2：软件进程的标识和认证		√	√	√
RE(1)：唯一标识和认证			√	√
SR 1.3：账号管理	√	√	√	√
RE(1)：统一的账号管理			√	√
SR 1.4：标识符管理	√	√	√	√
SR 1.5：认证码管理			√	√
RE(1)：软件进程身份凭证的硬件安全			√	√
SR 1.6：无线访问管理	√	√	√	√
RE (1)：唯一标识和认证		√	√	√
SR 1.7：口令认证	√	√	√	√

表 A.1（续）

SR 和 RE	CL1	CL2	CL3	CL4
RE (1)：用户(人)的口令生成和口令有效期限制			√	√
SR 1.8：公钥基础设施证书				√
SR 1.9：公钥认证的加强				√
RE (1)：公钥认证的硬件安全				√
SR 1.10：认证反馈	√	√	√	√
SR 1.11：失败的登录尝试	√	√	√	√
SR 1.13：经由非可信网络的访问	√	√	√	√
RE (1)：明确的对访问请求的批准		√	√	√
FR 2：使用控制				
SR 2.1：授权的执行	√	√	√	√
SR 2.2：无线使用控制	√	√	√	√
RE (1)：对未授权的无线设备进行识别和报告			√	√
SR 2.3：对便携和移动设备的使用控制	√	√	√	√
RE (1)：便携和移动设备的安全状态的实施			√	√
SR 2.4：移动代码	√	√	√	√
RE(1)：移动代码的完整性检查			√	√
RE(2)：移动代码的使用限制		√	√	√
SR 2.7：并发连接控制			√	√
SR 2.8：可审计的事件	√	√	√	√
RE (1)：中央管理的、系统范围的审计跟踪			√	√
SR 2.9：审计存储容量	√	√	√	√
SR 2.10：对审计流程失败时的响应	√	√	√	√
SR 2.11：时间戳		√	√	√
RE (1)：内部时间同步			√	√
RE (2)：时间源的完整性保护				√
SR 2.12：不可否认性			√	√
RE (1)：所有用户的不可否认性				√
FR 3：系统完整性				
SR 3.1：通信完整性	√	√	√	√
RE (1)：基于密码技术的完整性保护				√
SR 3.2：恶意代码的防护	√	√	√	√
RE (1)：在入口和出口点防护恶意代码		√	√	√
RE (2)：恶意代码防护的集中管理和报告			√	√
SR 3.4：软件和信息完整性		√	√	√

表 A.1（续）

SR 和 RE	CL1	CL2	CL3	CL4
RE (1)：对破坏完整性进行自动通知			√	√
SR 3.5：输入确认	√	√	√	√
SR 3.6：确定性的输出	√	√	√	√
SR 3.7：错误处理		√	√	√
SR 3.8：会话完整性		√	√	√
RE (1)：会话终止后会话 ID 的失效			√	√
RE (2)：唯一会话 ID 的产生和承认			√	√
RE (3)：会话 ID 的随机性				√
SR 3.9：审计信息的保护		√	√	√
RE (1)：一次性写入介质上的审计记录				√
FR 4：数据保密性				
SR 4.1：信息保密性	√	√	√	√
RE (1)：静止和经由不可信网络传输的数据的保密性保护			√	√
RE (2)：区域边界的保密性保护				√
SR 4.2：信息存留		√	√	√
RE (1)：共享内存资源的清除			√	√
SR 4.3：密码的使用	√	√	√	√
FR 6：对事件的及时响应				
SR 6.1：审计日志的可访问性	√	√	√	√
RE (1)：对审计日志的编程式访问			√	√
SR 6.2：持续监视		√	√	√
FR 7：资源可用性				
SR 7.1：拒绝服务的防护	√	√	√	√
RE (1)：管理通信负荷		√	√	√
RE (2)：限制拒绝服务攻击对其他系统和网络的影响			√	√
SR 7.2：资源管理	√	√	√	√
SR 7.3：数据备份	√	√	√	√
RE (1)：备份验证		√	√	√
RE(2)：备份自动化			√	√
SR 7.4：PLC 系统恢复和重构	√	√	√	√
SR 7.5：紧急电源	√	√	√	√
SR 7.6：网络和安全配置设置	√	√	√	√
SR 7.7：最小功能化	√	√	√	√
SR 7.8：PLC 系统部件清单		√	√	√

表 A.1（续）

SR 和 RE	CL1	CL2	CL3	CL4
对第 1 层的要求				
FR 1：标识和认证控制				
SR 1.1：用户（人）的标识和认证			√	√
SR 1.6：无线访问管理			√	√
SR 1.13：经由非可信网络的访问			√	√
FR 2：使用控制				
SR 2.1：授权的执行			√	√
SR 2.2：无线使用控制			√	√
SR 2.3：对便携和移动设备的使用控制			√	√
SR 2.4：用户工程代码		√	√	√
SR 2.7：连接过程要求			√	√
SR 2.8：诊断能力			√	√
SR 2.11：时间戳			√	√
RE（1）：内部时间同步			√	√
FR 3：系统完整性				
SR 3.1：通信信息完整性	√	√	√	√
SR 3.5：输入验证		√	√	√
SR 3.6：确定性的输出	√	√	√	√
SR 3.7：错误处理		√	√	√
SR 3.8：连接完整性			√	√
FR 4：数据保密性				
SR 4.1：信息保密性			√	√
SR 4.3：密码的使用				√
FR 6：对事件的及时响应				
SR 6.1：诊断记录的可访问性	√	√	√	√
FR 7：资源可用性				
SR 7.1：管理通信负荷		√	√	√
SR 7.2：资源管理		√	√	√
SR 7.4：PLC 系统恢复和重构		√	√	√
SR 7.5：紧急电源		√	√	√
SR 7.6：网络和安全配置设置	√	√	√	√
SR 7.7：最小功能化	√	√	√	√
注：如果以上技术要求存在互斥，同等级采用其中一种要求即可。				

附 录 B
（规范性附录）
网络安全管理评估列表

以下要求引用自 GB/T 30976.1—2014 附录 A，针对产品供应商、系统集成商、用户的特点与评估规范进行了对应。具体内容详见评估规范。针对 PLC 系统的网络安全管理评估列表见表 B.1。

表 B.1 网络安全评估列表

安全管理要素	产品供应商	系统集成商	用户
5.1 安全方针			
5.1.1 网络安全方针	√	√	√
要求：依据业务要求和相关法律法规提供管理指导并支持网络安全			
5.1.1.1 网络安全方针文件	√	√	√
5.1.1.2 网络安全方针的评审	√	√	√
5.2 网络安全组织机构			
5.2.1 内部组织机构	√	√	√
要求：管理组织机构范围内网络安全			
5.2.1.1 网络安全的承诺	√	√	√
5.2.1.2 网络安全协调	√	√	√
5.2.1.3 网络安全职责的分配	√	√	√
5.2.1.4 信息处理设施的授权过程	√	√	√
5.2.1.5 保密性协议	√	√	√
5.2.1.6 与政府部门的联系	√	√	√
5.2.1.7 网络安全的独立评审	√	√	√
5.2.2 外部方	√	√	√
要求：保持组织机构的被外部方访问、处理、管理或外部进行通信和信息处理设施的安全			
5.2.2.1 与外部方相关风险的识别	√	√	√
5.2.2.2 处理与顾客有关的安全问题	√	√	
5.2.2.3 处理第三方协议中的安全问题	√	√	√
5.3 资产管理			
5.3.1 对资产负责	√	√	√
要求：实现和保持对组织机构资产的适当保护			
5.3.1.1 资产清单	√	√	√
5.3.1.2 资产责任人	√	√	√
5.3.1.3 资产的可接受使用		√	√
5.3.2 资产信息分类		√	√
要求：确保信息受到适当级别的保护			

表 B.1（续）

安全管理要素	产品供应商	系统集成商	用户
5.3.2.1 分类指南		√	√
5.3.2.2 资产信息的标记和处理		√	√
5.4 人力资源安全			
5.4.1 任用之前	√	√	√
要求：确保雇员、承包方人员和第三方人员理解其职责、考虑对其承担的角色是适合的，以降低设施被窃取，欺诈和误用的风险			
5.4.1.1 角色和职责	√	√	√
5.4.1.2 审查	√	√	√
5.4.1.3 任用条款和条件	√	√	√
5.4.2 任用中	√	√	√
要求：确保所有的雇员、承包方人员和第三方人员知悉网络安全威胁和利害关系、他们的职责和义务，并准备好在其正常工作过程中支持组织机构的安全方针，以减少人为出错的风险			
5.4.2.1 管理职责	√	√	√
5.4.2.2 网络安全意识、教育和培训	√	√	√
5.4.2.3 纪律处理过程	√	√	√
5.4.3 任用的终止或变更	√	√	√
要求：确保所有的雇员、承包方人员和第三方人员以一个规范的方式退出一个组织机构或改变其任用关系			
5.4.3.1 终止职责	√	√	√
5.4.3.2 资产的归还	√	√	√
5.4.3.3 撤销访问权	√	√	√
5.5 物理和环境安全			
5.5.1 安全区域			√
要求：防止对组织机构场所和信息的未授权物理访问、损坏和干扰			
5.5.1.1 物理安全周边			√
5.5.1.2 物理入口控制			√
5.5.1.3 办公室、房间和设施的安全保护			√
5.5.1.4 外部和环境的安全防护			√
5.5.1.5 在安全区域工作			√
5.5.1.6 公共访问，交换区安全			√
5.5.2 设备安全			√
要求：防止资产的丢失、损坏、失窃或危及资产安全以及组织机构活动的中断			
5.5.2.1 设备安置和保护			√
5.5.2.2 支持性设施			√
5.5.2.3 布缆安全			√

表 B.1（续）

安全管理要素	产品供应商	系统集成商	用户
5.5.2.4 设备维护			√
5.5.2.5 组织机构场所外的设备安全			√
5.5.2.6 设备的安全处置或再利用			√
5.5.2.7 资产的移动			√
5.6 通信和操作管理			
5.6.1 操作规程和职责	√	√	√
要求：确保正确、安全的操作信息处理设施			
5.6.1.1 文件化的操作规程	√	√	√
5.6.1.2 变更管理	√	√	√
5.6.1.3 责任分割	√	√	√
5.6.1.4 测试和运行分离		√	√
5.6.2 第三方服务交付管理	√	√	√
要求：实施和保持符合第三方服务交付协议的网络安全和服务交付的适当水准			
5.6.2.1 服务交付	√	√	√
5.6.2.2 第三方服务的监视和评审	√	√	√
5.6.2.3 第三方服务的变更管理	√	√	√
5.6.3 系统规划和验收		√	√
要求：将系统失效的风险降至最小			
5.6.3.1 容量管理		√	√
5.6.3.2 系统验收		√	√
5.6.4 防范恶意和移动代码	√	√	√
要求：保护软件和信息的完整性			
5.6.4.1 控制恶意代码	√	√	√
5.6.5 备份	√	√	√
要求：保持信息和信息处理设施的完整性及可用性			
5.6.5.1 信息备份	√	√	√
5.6.6 网络安全管理	√		√
要求：确保网络中信息的安全性并保护支持性的基础设施			
5.6.6.1 网络控制	√		√
5.6.6.2 网络服务安全	√		√
5.6.7 介质处置		√	√
要求：防止资产遭受未授权泄露、修改、移动或销毁以及业务活动的中断			
5.6.7.1 可移动介质的管理		√	√
5.6.7.2 介质的处置		√	√

表 B.1（续）

安全管理要素	产品供应商	系统集成商	用户
5.6.7.3 信息处理规程		√	√
5.6.7.4 系统文件(文档)安全		√	√
5.6.8 信息的交换(传输)			√
要求：保持组织机构内以及与组织机构外信息和软件交换的安全			
5.6.8.1 信息交换策略和规程			√
5.6.8.2 交换协议			√
5.6.8.3 运输中的物理介质			√
5.6.8.4 电子消息发送			√
5.6.8.5 业务信息系统			√
5.6.9 监视			√
要求：检测未经授权的信息处理活动			
5.6.9.1 审计记录			√
5.6.9.2 监视系统的使用			√
5.6.9.3 日志信息的保护			√
5.6.9.4 管理员和操作日志			√
5.6.9.5 故障日志			√
5.6.9.6 时钟同步			√
5.7 访问控制			
5.7.1 访问控制的业务要求		√	√
要求：控制对信息的访问			
5.7.1.1 访问控制策略		√	√
5.7.2 用户访问控制		√	√
要求：确保授权用户访问信息系统，并防止未授权的访问			
5.7.2.1 用户注册		√	√
5.7.2.2 特殊权限管理		√	√
5.7.2.3 用户口令管理		√	√
5.7.2.4 用户访问权的复查		√	√
5.7.3 用户职责		√	√
要求：防止未授权用户对信息和信息处理设施的访问、损害和窃取			
5.7.3.1 口令使用		√	√
5.7.3.2 无人职守的用户设备		√	√
5.7.3.3 清空桌面和屏幕策略		√	√
5.7.4 网络访问控制		√	√
要求：防止对网络服务的未授权访问			

表 B.1（续）

安全管理要素	产品供应商	系统集成商	用户
5.7.4.1 使用网络服务的策略		√	√
5.7.4.2 外部连接的用户鉴别		√	√
5.7.4.3 网络上的设备标识		√	√
5.7.4.4 远程诊断和配置端口的保护		√	√
5.7.4.5 网络隔离		√	√
5.7.4.6 网络连接控制		√	√
5.7.4.7 网络路由控制		√	√
5.7.5 操作系统访问控制		√	√
要求：防止对操作系统的未授权访问			
5.7.5.1 安全登录规程		√	√
5.7.5.2 用户标识和鉴别		√	√
5.7.5.3 口令管理系统		√	√
5.7.5.4 系统实用工具的使用		√	√
5.7.5.5 会话超时		√	√
5.7.5.6 联机时间的限定		√	√
5.7.6 应用和信息访问控制		√	√
要求：防止对应用系统中信息的未授权访问			
5.7.6.1 信息访问控制		√	√
5.7.6.2 敏感系统隔离		√	√
5.7.7 移动计算和远程工作		√	√
要求：确保使用移动计算机和远程工作设施时的网络安全			
5.7.7.1 移动计算和通信		√	√
5.7.7.2 远程工作		√	√
5.8 信息系统获取，开发和维护			
5.8.1 信息系统的安全要求	√	√	√
要求：确保安全是信息系统的一个有机组成部分			
5.8.1.1 安全要求分析和说明	√	√	√
5.8.2 应用中的正确处理		√	√
要求：防止应用系统中的信息的差错、遗失、未授权的修改或误用			
5.8.2.1 输入数据确认		√	√
5.8.2.2 内部处理的控制		√	√
5.8.2.3 消息完整性		√	√
5.8.2.4 输出数据确认		√	√
5.8.3 密码控制			

表 B.1（续）

安全管理要素	产品供应商	系统集成商	用户
要求：通过密码方法保护信息的保密性、真实性或完整性			
5.8.3.1 使用密码控制的策略		√	√
5.8.3.2 密钥管理		√	√
5.8.4 系统文件的安全	√	√	√
要求：确保系统文件的安全			
5.8.4.1 运行软件的控制	√	√	√
5.8.4.2 系统测试数据的保护	√	√	√
5.8.4.3 对程序源代码的访问控制	√	√	√
5.8.5 开发和支持过程中的安全	√	√	√
要求：维护应用系统软件和信息的安全			
5.8.5.1 变更控制规程	√	√	√
5.8.5.2 操作系统变更后应用的技术评审	√	√	√
5.8.5.3 软件包变更的限制	√	√	√
5.8.5.4 信息泄露	√	√	√
5.8.5.5 外包软件开发	√	√	√
5.8.6 技术脆弱性管理	√	√	√
要求：降低利用公布的技术脆弱性导致的风险			
5.8.6.1 技术脆弱性的控制	√	√	√
5.9 网络安全事件管理			
5.9.1 报告网络安全事态和弱点	√	√	√
要求：确保与信息系统有关的网络安全事态和弱点能够以某种方式传达，以便及时采取纠正措施			
5.9.1.1 报告网络安全事态	√	√	√
5.9.1.2 报告安全弱点	√	√	√
5.9.2 网络安全事件和改进的管理	√	√	√
要求：确保采用一致和有效的方法对网络安全事件进行管理			
5.9.2.1 职责和规程	√	√	√
5.9.2.2 对网络安全事件的总结	√	√	√
5.9.2.3 证据的收集	√	√	√
5.10 业务连续性管理			
5.10.1 业务连续性管理的网络安全方面			√
要求：防止业务活动中断，保护关键业务过程免受信息系统重大失误或灾难的影响，并确保他们及时恢复			
5.10.1.1 在业务连续性管理过程中包含网络安全			√
5.10.1.2 业务连续性和风险评估			√
5.10.1.3 制定和实施包含网络安全的连续性计划			√

表 B.1（续）

安全管理要素	产品供应商	系统集成商	用户
5.10.1.4 业务连续性计划框架			√
5.10.1.5 测试、维护和再评估业务连续性计划			√
5.11 符合性			
5.11.1 符合法律要求	√	√	√
要求：避免违反任何法律，法令，法规或合同义务以及任何安全要求			
5.11.1.1 可用法律的识别	√	√	√
5.11.1.2 知识产权	√	√	√
5.11.1.3 保护组织机构的记录	√	√	√
5.11.1.4 数据保护和个人信息的隐私	√	√	√
5.11.1.5 防止滥用信息处理设施	√	√	√
5.11.1.6 密码控制措施的规则	√	√	√
5.11.2 符合安全策略和标准以及技术符合性	√	√	√
要求：确保系统符合组织机构的安全策略及标准			
5.11.2.1 符合安全策略和标准	√	√	√
5.11.2.2 技术符合性核查	√	√	√
5.11.3 信息系统审计考虑	√	√	√
要求：将信息系统审计过程的有效性最大化，干扰最小化			
5.11.3.1 信息系统审计控制措施	√	√	√
5.11.3.2 信息系统审计工具的保护	√	√	√

参 考 文 献

[1] GB/T 15851—1995 信息技术 安全技术 带消息恢复的数字签名方案

[2] GB/T 15969 可编程序控制器

[3] GB/T 17902—1999 信息技术 安全技术 带附录的数字签名

[4] GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则

[5] GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求

[6] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则

[7] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[8] GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

[9] ISO/IEC 9798-1:2010 信息技术 安全技术 实体鉴别

[10] IEC 62443-1-1 工业过程测量和控制安全 网络和系统安全 第1-1部分:术语、概述和模型

[11] IEC 62443-1-3 工业过程测量和控制安全 网络和系统安全 第1-3部分:系统的安全性符合指标

[12] IEC 62443-2-1 工业过程测量和控制安全 网络和系统安全 第2-1部分:建立工业自动化和PLC系统(IACS)安全程序

[13] IEC 62443-3-2 工业过程测量和控制安全 网络和系统安全 第3-2部分:用于区域和管道的安全保证等级(SAL)

[14] IEC 62443-3-3 工业过程测量和控制安全 网络和系统安全 第3-3部分:系统安全要求和安全等级

[15] IEC 62443-4-1 工业过程测量和控制安全 网络和系统安全 第4-1部分:用于工业自动化和PLC系统的产品开发要求

[16] IEC 62443-4-2 工业过程测量和控制安全 网络和系统安全 第4-2部分:用于工业自动化和PLC系统组件的技术的安全要求