ICS 25.040
N 10

中华人民共和国国家标准

GB/T 35673—2017/IEC 62443-3-3:2013

工业通信网络　网络和系统安全
系统安全要求和安全等级

Industrial communication networks—Network and system security—System security requirements and security levels

(IEC 62443-3-3:2013,Industrial communication networks—Network and system security—Part 3-3:System security requirements and security levels,IDT)

2017-12-29 发布　　2018-07-01 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

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 IEC 62443-3-3:2013《工业通信网络　网络和系统安全　第 3-3 部分：系统安全要求和安全等级》及其修正案 corrigendum1。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 33007—2016　工业通信网络　网络和系统安全　建立工业自动化和控制系统安全程序(IEC 62443-2-1:2010,IDT)

为了使用方便，本标准做了下列编辑性修改：

——标准名称修改为“工业通信网络　网络和系统安全　系统安全要求和安全等级”；

——纳入了技术勘误 1 的内容，这些技术勘误涉及的条款已通过在其外侧页边空白位置的垂直双线(‖)进行了标示；

——对 5.7.1 中错误的序列号进行了修正。

本标准由中国机械工业联合会提出。

本标准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)归口。

本标准起草单位：北京匡恩网络科技有限责任公司、机械工业仪器仪表综合技术经济研究所、中国核电工程有限公司、北京和利时系统工程有限公司、西南电力设计院有限公司、东土科技股份有限公司、全球能源互联网研究院、北京市自来水集团有限责任公司、浙江大学、华中科技大学、西南大学、重庆邮电大学、中国软件测评中心、西门子(中国)有限公司、施耐德电气(中国)有限公司、罗克韦尔自动化(中国)有限公司、中国科学院沈阳自动化研究所、北京启明星辰信息安全技术有限公司、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、华北电力设计院工程有限公司、深圳万讯自控股份有限公司、中国电子科技集团公司第三十研究所、上海自动化仪表研究院、工业和信息化部电子第五研究所、横河电机(中国)有限公司北京研发中心。

本标准主要起草人：王春霞、张大江、王玉敏、梅恪、梁猛、芦宁、徐岩、王亦君、王戬、罗安、张晋宾、薛百华、梁潇、冯冬芹、刘枫、周纯杰、李锐、陈小淙、华镕、张晨艳、朱镜灵、刘安正、马欣欣、周峰、魏旻、刘杰、成继勋、赵军凯、兰昆、王英、张东旗、董黎芳、刘广庆、宋秀娟、杨泓彬、徐近升、刘畅、尚文利、潘东波、刘志祥、钱大涛。

引　言

0.1　概述

注：本标准是涉及工业自动化和控制系统(IACS)信息安全系列标准的一部分。是由 ISA99 委员会第四工作组的第 2 任务组与 IEC TC 65/WG 10 一起合作制定的。本标准描述了在 IEC 62443-1-1 中定义的与控制系统信息安全要求相关的七个基本要求，并对待评估系统(SuC)分配了系统安全等级。

工业自动化和控制系统(IACS)的组织越来越多地使用商用网络设备成品，因为价格低廉、性能高效和高度自动化。出于商业目的，控制系统也越来越多地与非 IACS 网络相互连接。这些设备采用开放的网络技术和持续增加的网络连接，为针对控制系统硬件和软件的网络攻击提供了机会。这个弱点可能导致所部署的系统产生健康、安全和环境(HSE)、财务或声誉问题。

部署商用信息网络安全解决方案来应对 IACS 安全的组织，可能无法完全理解采用这一措施的后果。尽管许多商业 IT 应用和安全解决方案可应用于 IACS，但是它们需要以合适的方式来应用，以避免因疏忽造成的后果。因此，需要结合功能要求和风险评估，通常也包括对运营问题的意识，来定义系统要求。

IACS 安全措施不宜具有引起基本服务和功能(包括应急程序)丢失的隐患。(经常部署的 IT 安全措施，确实有这种潜在弱点。)IACS 安全目标集中在控制系统的可用性、工厂保护、工厂运行(即使在降级模式)和时间关键(time-critical)的系统响应。IT 安全目标往往对这些因素有不同程度的重视；他们可能更关心的是保护信息，而非有形资产。无论工厂集成的实现程度如何，这些不同的目标需要明确地表述为安全目标。根据 IEC 62443-2-1 要求，风险评估中的关键一步是识别出哪些服务和功能对运行是必不可少的。(例如，在一些设施中，工程支持可能被判定为非基本的服务或功能。)在某些情况下，安全性的动作引起非基本的服务或功能的暂时丧失是可以接受的，但是基本服务或功能不宜受到不利影响。

本标准假定系统已经按照 IEC 62443-2-1 规定建立并运行了安全程序。进一步假定通过利用本标准描述的适当的控制系统要求及增强要求，实现了符合 IEC/TR 62443-2-3[5] 所建议的补丁管理。此外，IEC 62443-3-2[8] 描述了怎样对项目定义基于风险的安全等级(SL)，并用于选择符合本标准中详述的适当技术安全能力的产品。本标准的主要参考标准包括 ISO/IEC 27002[15] 和 NIST SP 800-53 第 3 版[24](见第 2 章和参考文献)。

IEC 62443 系列标准的主要目的是提供一种灵活的框架，以应对 IACS 当前和未来的脆弱性，并采用系统化的防御方式，实施必要的缓解方法。IEC 62443 系列标准的目的是扩展企业安全性，使之适应业务 IT 系统的要求，并与 IACS 独特的高可用性需求相结合。

0.2　目的和本标准的使用者

本标准在 IACS 领域的使用者包括资产所有者、系统集成商、产品供应商、服务供应商、合规性管理机构。合规性管理机构包括具有法定权力、根据法律法规进行合规性审计的政府机构和监管部门。

系统集成商、产品供应商和服务提供商将使用本标准来评价其产品和服务是否能够提供满足资产所有者目标安全等级(SL-T)要求的安全能力。对于 SL-T 的分配，单个控制系统的要求(SR)和增强要求(RE)的适用性将基于资产所有者的安全策略、规程和基于具体场所的风险评估。值得注意的是，某些 SR 存在允许例外的特定条件，例如当满足 SR 将违反控制系统的基本操作要求时(这可能需要增加补偿对抗措施)。

当设计控制系统为满足特定 SL-T 相关的一系列 SR 时，不必要求该控制系统的每个组件都满足本标准强制级别的每项系统要求。补偿对抗措施可以用来提供其他子系统所需的功能，在控制系统级，全部的 SL-T 要求都得到满足。在设计阶段宜考虑包括补偿措施，并附有详尽的文档，这样所达到的控制系统 SL、SL-A(控制系统)，充分体现了安全能力的设计预期。同样，为满足整个控制系统的 SL，在认证测试和/或安装后的审计时，可以应用补偿措施并做文件记录。

本标准未提供设计和建立集成安全架构的详细内容。这需要额外的系统级分析和 IEC 62443 系列的其他标准(见 0)衍生的要求。需要注意的是，本标准的目标不是提供详细的规范来建立一个安全架构。本标准的目标是定义一个通用的最低限度要求，逐步达到更严格的信息安全等级。符合这些要求的架构实际设计是系统集成商和产品供应商的工作。在此工作中，他们可以自由选择，从而支持竞争和创新。因此，本标准仅严格地明确功能要求，并不涉及这些功能要求应如何满足。

0.3 本标准在 IEC 62443 系列标准的应用

图 1 给出了本标准撰写时 IEC 62443 系列标准的构成。

IEC 62443-3-2 使用 SR 和 RE 作为一个检查清单。在待评估系统(SuC)使用区域和管道术语进行描述，以及相应的目标 SL 分配给这些区域和管道之后，本标准定义的 SR 和 RE，以及它们与安全能力等级 SL(SL-C)的映射关系，汇集成控制系统设计需要满足的要求列表。一个给定的控制系统设计就可以 SL-A 为条件，进行完整性检查。

图 1 IEC 62443 系列标准的结构

IEC/TS 62443-1-3[2]将基本要求(FR)，SR，RE 和 SL-C 的映射作为检查表来测试量化指标规范的完整性。量化的安全符合性指标基于特定的上下文。结合 IEC 62443-3-2，资产所有者的 SL-T 的任务要求转换成量化指标，用来支持系统的分析和设计权衡研究，以及开发安全体系结构。

IEC 62443-4-1[9]提出产品开发过程中的总体要求。例如，IEC 62443-4-1 的规定内容都是围绕产品

供应商。产品安全性的要求都源于本标准中规定的基线要求列表和 RE。开发这些产品的功能时，将使用 IEC 62443-4-1 质量规范。

IEC 62443-4-2[10]包含一系列派生要求，提供了详细的本标准 SR 到子系统和 SuC 组件的映射。在本标准撰写的时候，IEC 62443-4-2 涉及的组件类别分别为：嵌入式设备、主机设备、网络设备和应用程序。同样，IEC 62443-4-2 主要以供应商（产品供应商和服务供应商）为中心。产品安全性的要求，首先来自本标准中规定的基本要求和 RE 列表。IEC 62443-3-2 和 IEC/TS 62443-1-3 的安全要求和度量被用来完善这些规范性派生需求。

工业通信网络　网络和系统安全
系统安全要求和安全等级

1　范围

本标准规定了与 IEC 62443-1-1 中所描述的 7 个基本要求(FR)相关的详细的技术类控制系统要求(SR),包括定义了控制系统安全能力等级(SL-C)要求。当为特定资产开发适用的控制系统目标 SL,即 SL-T(控制系统)时,对于待评估系统(SuC),工业自动化和控制系统(IACS)的各方可以将这些要求和明确的安全区域及管道一同采用。

根据 IEC 62443-1-1 定义,7 个基本要求(FR)如下:

a)　标识和鉴别控制(IAC);

b)　使用控制(UC);

c)　系统完整性(SI);

d)　数据保密性(DC);

e)　受限的数据流(RDF);

f)　对事件的及时响应(TRE);

g)　资源可用性(RA)。

这 7 项要求是控制系统能力 SL(SL-C)的基础。本标准的目标及目的在于确定控制系统级的安全能力等级。目标 SL(SL-T)或如何实现 SL(SL-A),不在本标准规定的范围。

全面实现控制系统的 SL 目标,还需参见 IEC 62443-2-1 规定的一系列非技术性、程序相关的 SR 能力要求。

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。

IEC 62443-1-1:2009　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(Industrial communication networks—Network and system security—Part 1-1:Terminology,concepts and models)

IEC 62443-2-1　工业通信网络　网络和系统安全　第 2-1 部分:建立工业自动化和控制系统安全程序(Industrial communication networks—Network and system security—Part 2-1:Establishing an industrial automation and control system sercurity program)

3　术语、定义、缩略语和约定

3.1　术语和定义

IEC 62443-1-1 和 IEC 62443-2-1 界定的以及下列术语和定义适用于本文件。

注:下列术语和定义多数是基于国际标准化组织(ISO)、国际电工委员会(IEC)或美国标准技术研究院(NIST)的标准,为适用于控制系统信息安全要求,有时会做少量修正以增强实用性。

3.1.1

资产　asset

对 IACS 具有潜在或实际价值的物理对象或逻辑对象。

注：本标准中，资产可以是 IACS 信息安全管理系统中任何受保护的对象。

3.1.2

资产所有者　asset owner

拥有一个或多个 IACS 的个人或者公司。

注 1：术语“资产所有者”用于代替通用术语“终端用户”而使用，并以示区别。

注 2：这个定义包括组成 IACS 的组件。

注 3：在本标准中，资产所有者也包括 IACS 的运营者。

3.1.3

攻击　attack

来自智能威胁对系统发起的袭击。

注 1：例如，企图躲避系统安全服务和违反系统安全策略的故意行为。

注 2：一般公认的攻击类别有：

- 主动发起的攻击行为：企图改变系统资源或者影响系统运行；
- 被动攻击行为：企图学习或者利用系统信息，但是不影响系统资源；
- 内部攻击：在安全边界内部的一个实体发起的攻击，例如，一个被授权可以访问系统资源的实体未按所授权的方式使用系统资源；
- 外部攻击：指在安全边界外部由系统未授权或者不合法的使用者发起的攻击（包括内部人员从安全边界外部发起的攻击），潜在的外部攻击者包括恶作剧者、有组织的罪犯、国际恐怖分子和敌对政府。

3.1.4

鉴别　authentication

身份所声明特征正确性的保证行为。

注：在一个控制系统中，鉴别是允许访问系统资源的先决条件。

3.1.5

鉴别器　authenticator

确认使用者（人、软件进程或设备）身份的手段。

注：例如，口令或者权标可以作为鉴别器使用。

3.1.6

真实性　authenticity

实体与其所声明属性符合的特性。

注：真实性一词通常用于说明一个实体身份的可信度，或传输、报文或报文发生器的正确性。

3.1.7

自动　automatic

在特定条件下，过程或者设备自行运行，无人工干预。

3.1.8

可用性　availability

确保及时和可靠访问或使用控制系统信息和功能的属性。

3.1.9

通信信道　communication channel

资产之间特定的逻辑或者物理通信链路。

注：信道帮助建立连接。

3.1.10

补偿对抗措施　compensating countermeasure

用于替代或增加固有安全能力，以满足一个或者多个安全要求而采取的措施。

注：例如，

- （组件级）：使用加锁的机柜，对没有充分的网络访问控制措施的控制器进行防护；
- （控制系统/区域级）：物理出入口控制（门卫、门闸、枪）用来保护一个控制室，只允许对某一已知人员群体的访问，以此来补偿 IACS 对人员鉴别的技术要求；
- （组件级）：设备供应商提供的可编程逻辑控制器（PLC）不具备满足终端用户进行访问控制的能力要求，因此，设备供应商在 PLC 前端设置一个防火墙，并将其作为一个整体进行售卖。

3.1.11

合规性管理机构　compliance authority

具有对政府文件中明确规定的安全评估、实施和有效性进行充分性判定的法定管理机构。

3.1.12

管道　conduit

连接两个及以上区域、满足共同安全要求的通信信道的逻辑分组。

注：管道允许穿过某个区域，只要该区域不影响管道内的信道安全。

3.1.13

保密性　confidentiality

对信息访问和信息公开保留授权限制，包括保护个人隐私和所有者信息的手段。

注：对于 IACS 来说，这个术语主要指保护的 IACS 数据和信息不受非授权访问。

3.1.14

连接　connection

两个或多个端点之间建立起来的联系，用来支持一个会话的建立。

3.1.15

后果　consequence

事件发生后，逻辑地或自然地产生的状况或状态。

3.1.16

控制系统　control system

IACS 的硬件和软件组件。

3.1.17

对抗措施　countermeasure

用来降低威胁、脆弱性或者攻击而采取的行动、装置、过程或者技术措施，主要通过采取消除或者阻止措施或者最大程度降低危害程度或者通过发现、报告攻击，并采取的纠正行动。

注：术语“控制”也用来描述相似的概念。但在本标准文本中，使用“对抗措施”一词，以避免与“过程控制”中“控制”一词相混淆。

3.1.18

降级模式　degraded mode

在控制系统设计中，预期的故障出现时所采取的操作模式。

注：在降级模式下，尽管一个或多个系统元件缺失，控制系统仍能继续提供基本的功能。例如，控制设备出现故障或者运行中断，通信中断或者发现可疑的子系统故障而刻意采取的系统隔离。

3.1.19

非军事区域　demilitarized zone

通用的服务器受限网络，连接两个或者多个区域，用于控制区域之间的数据流。

注：非军事区域主要用于避免不同区域之间的直接连接。

3.1.20

设备　device

集成一个或多个处理器的资产，具有数据收发和控制或者受控于另一资产的功能。

注：典型设备类型有：控制器、人-机界面(HMI)、PLC、远程终端单元(RTU)、变送器、执行器、阀门、网络交换机等。

3.1.21

环境　environment

可能影响 IACS 行为和/或被 IACS 影响的周围对象、区域或者事件。

3.1.22

基本功能　essential function

为维持健康、安全、环境和受控设备的可用性所要求的功能或能力。

注：基本功能包括但不限于，安全仪表功能，控制功能，操作员观察和操作受控设备的控制职责和能力。基本功能的失去通常被定义为失去保护、失去控制或失去观察。在一些工业领域，附加的功能可以被看作是重要功能，比如历史记录。

3.1.23

事件　event

特定情况的发生或者改变。

注：在 IACS 中，事件可能是授权或者未授权的个人行为、正常的或者异常的控制系统变化或者来源于正常的或异常的控制系统本身的自动响应。

3.1.24

应急响应　firecall

紧急情况时接入安全控制系统的方法。

注：在紧急情况下，非特权使用者能够获得授权访问关键系统来纠正问题。在应急响应的情况下，通常会设置一个检查的过程，确保授权恰当使用来纠正问题。这些方法通常包括提供一次性使用者标识符(ID)或者一次性使用的口令。

3.1.25

标识符　identifier

用于识别、指示或者命名一个实体所声称的身份符号，在安全域具有唯一性。

3.1.26

标识　identify

身份的声明。

3.1.27

影响　impact

某个特定事件的评估结果。

3.1.28

事故　incident

一个系统或服务发生非预期操作事件，造成或可能造成系统所提供的服务质量的中断或降低。

3.1.29

工业自动化和控制系统　industrial automation and control system

包括人员、硬件、软件和工业过程操作的策略，其中策略可能影响工业过程的安全、信息安全和可靠性操作。

3.1.30

完整性　integrity

保护资产的准确性和完备性的属性。

3.1.31

最小权限　least privilege

维持使用者(人员、软件进程或设备)在其职责和作用之内被授予最小权限的基本原则。

注：最小权限通常通过 IACS 中的一组角色来实现。

3.1.32

移动代码　mobile code

通过网络或者可移动媒介与远程的、可能“不可信的”系统之间传递的程序，不经显式安装、在本地系统未加改变的执行，或者被接收者执行。

注：移动代码典型例子包括 JavaScript、VBScript、Java 小型应用程序、ActiveX 控件、Flash 动画、Shockwave movies 和微软 office 宏命令。

3.1.33

抗抵赖　non-repudiation

证明一个声明的事件或行为的发生和其来源实体的能力。

注：抗抵赖的目的是为了解决关于事件是否发生、事件中的行为、接介入事件的实体等纠纷。

3.1.34

产品供应商　product supplier

硬件和/或软件产品的制造者。

注：这个术语用来代替通用词语“供应商”使用，以示区别。

3.1.35

远程访问　remote access

从区域边界外部，任何使用者(人员、软件进程或设备)对控制系统的寻址访问。

3.1.36

角色　role

在 IACS 中，与所有使用者(人员、软件进程或设备)相关的行为、权限和职责的集合。

注：执行特定操作的权限被授予特定的角色。

3.1.37

安全仪表系统　safety instrumented system

用于执行一个或者多个安全相关功能的系统。

3.1.38

信息安全等级　security level

IACS 不受脆弱性影响并按预期方式工作的置信度。

注：脆弱性可能在 IACS 生命周期的任何时间因为设计因素而引入，或者由不断变化的威胁所导致。因为设计导致的脆弱性有可能在 IACS 初始部署之后很长时间才能被发现，例如，一项加密技术被破解，或者不恰当的账户管理策略，如旧的使用者账户没有被移除。引入型脆弱性可能是打补丁引起的或者是策略改变导致的新脆弱性。

3.1.39

服务提供商　service provider

按照协议承诺，为提供指定的支持服务承担职责，并按规定，获得经费的组织(内部或者外部组织、厂商)。

注：这个术语在代替通用词语“供应商”而使用，以示区别。

3.1.40

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。

注：通常明确定义了起始过程和结束过程。

3.1.41

会话标识符　session ID

用于表明特定会话入口的标识符。

3.1.42

设定值　set point

在控制系统中定义的目标值，用于在控制系统内部控制一个或者多个动作。

3.1.43

系统集成商　system integrator

专业做组件子系统集成的个人或者公司，有能力确保这些子系统性能达到项目规范要求。

3.1.44

威胁　threat

通过非授权访问、破坏、披露、数据修改和/或拒绝服务方式，对运行（包括任务、功能、图像或者名誉）、资产、控制系统或者个人具有潜在不利影响的环境或者事件。

3.1.45

信任　trust

相信操作、数据交易源、网络或软件进程的行为如预期是可依靠的。

注1：通常，当第一个实体认为第二个实体的行为符合第一个实体预期时，第一个实体就可以称为“信任”第二个实体。

注2：这种信任仅用于某些特定的功能中。

3.1.46

非可信　untrusted

不满足预先定义的可信要求。

注：一个实体可能被简单地声明为不可信。

3.1.47

区域　zone

共享相同信息安全要求的逻辑资产或物理资产的集合。

注：区域具有清晰的边界。一个信息安全区域的信息安全策略在其内部和边界都要强制执行。

3.2　缩略语

下列缩略语适用于本文件。

AES	高级加密标准	Advanced encryption standard
API	应用编程接口	Application programming interface
ASLR	地址空间布局随机化	Address space layout randomization
BPCS	基本过程控制系统	Basic process control system
CA	认证机构	Certification authority
CIP	关键基础设施保护	Critical infrastructure protection
COTS	商用现货	Commercial off the shelf
CRL	证书撤销列表	Certificate revocation list
DC	数据保密性	Data confidentiality
DEP	数据执行保护	Data execution prevention
DHCP	动态主机配置协议	Dynamic host configuration protocol
DMZ	非军事区	Demilitarized zone
DNS	域名服务	Domain name service

DoS	拒绝服务	Denial of service
EICAR	欧洲计算机防病毒研究所	European Institute for Computer Antivirus Research
EMI	电磁干扰	Electromagnetic interference
FAT	出厂验收测试	Factory acceptance testing
FIPS	美国联邦信息处理标准	Federal Information Processing Standard
FR	基本要求	Foundational requirement
FS-PLC	功能安全 PLC	Functional safety PLC
FTP	文件传输协议	File transfer protocol
GLONASS	全球导航卫星系统	Global Navigation Satellite System
GPS	全球定位系统	Global Positioning System
HMI	人机界面	Human-machine interface
HSE	健康、安全和环境	Health, safety and environmental
HTTP	超文本传输协议	Hypertext transfer protocol
HTTPS	安全超文本传输协议	HTTP secure
IAC	标识和鉴别控制	Identification and authentication control
IACS	工业自动化和控制系统	Industrial automation and control system(s)
IAMS	仪表资产管理系统	Instrument asset management system
ID	标识符	Identifier
IDS	入侵检测系统	Intrusion detection system
IEC	国际电工委员会	International Electrotechnical Commission
IEEE	电气与电子工程师协会	Institute of Electrical and Electronics Engineers
IETF	互联网工程任务组	Internet Engineering Task Force
IM	即时通讯	Instant messaging
IP	互联网协议	Internet Protocol
IPS	入侵防护系统	Intrusion prevention system
ISA	国际自动化协会	International Society of Automation
ISO	国际标准化组织	International Organization for Standardization
IT	信息技术	Information technology
MES	制造执行系统	Manufacturing execution system
NERC	北美电力可靠性公司	North American Electric Reliability Corporation
NIST	美国国家标准技术研究所	U.S.National Institute of Standards and Technology
NX	不执行	No Execute
OCSP	在线证书状态协议	Online certificate status protocol
OWASP	开放式 Web 应用程序安全项目	Open Web Application Security Project
PDF	便携文档格式	Portable document format
PKI	公钥基础设施	Public key infrastructure
PLC	可编程逻辑控制器	Programmable logic controller
RA	资源可用性	Resource availability
RAM	随机存取存储器	Random access memory
RDF	受限的数据流	Restricted data flow
RE	增强要求	Requirement enhancement
RFC	请求评议	Request for Comment
RJ	已注册插座	Registered jack

RTU	远程终端单元	Remote terminal unit
SAT	现场验收测试	Site acceptance testing
SHA	安全哈希算法	Secure hash algorithm
SI	系统完整性	System integrity
SIEM	安全信息和事件管理	Security Information and Event Management
SIF	安全仪表功能	Safety instrumented function
SIL	安全完整性等级	Safety integrity level
SIS	安全仪表系统	Safety instrumented system
SL	信息安全等级	Security level
SL-A	实现的安全等级	Achieved security level
SL-C	能力安全等级	Capability security level
SL-T	目标安全等级	Target security level
SP	美国 NIST 特种出版物	Special Publication
SR	系统要求	System requirement
SSH	安全套接字程序	Secure socket shell
SuC	被考虑的系统	System under consideration
TCP	传输控制协议	Transmission Control Protocol
TPM	可信平台模块	Trusted platform module
TRE	事件及时响应	Timely response to events
UC	使用控制	Use control
USB	通用串行总线	Universal serial bus
VoIP	因特网语音协议	Voice over internet protocol
WEP	有线等效加密	Wired equivalent privacy
WLAN	无线局域网络	Wireless local area network

3.3 约定

本标准将 IEC 62443-1-1 中定义的 7 个 FR 扩展成一系列 SR，每个 SR 包含一个基线要求以及零个或几个加强安全性的增强要求(RE)。为使读者清晰理解，每一个基线要求以及相关的 RE 都提供原由和附加指南。每个基线要求和 RE(如果存在的话)，随后会被映射到对应的控制系统的能力安全等级 SL-C(FR，控制系统)1 级至 4 级。

所有 7 个 FR 都有一组四个 SL 定义。控制系统安全等级 0 为特殊 FR，意味着没有任何要求。例如，第 8 章的目的陈述，FR 4——数据保密性：

确保通信信道和数据存储中的信息保密性，以防止未经授权的泄露。

相关四个 SL 定义如下：

SL 1——防止窃听或不经意的暴露导致的未经授权的信息披露。

SL 2——防止未经授权地将信息泄露给通过少量资源、通用技能和低动机的简单手段主动进行信息搜索的实体。

SL 3——防止未经授权地将信息泄露给通过一般资源、IACS 特殊技能和一般动机的复杂手段主动进行信息搜索的实体。

SL 4——防止未经授权地将信息泄露给通过扩展资源、IACS 特殊技能和高动机的复杂手段主动进行信息搜索的实体。

每个 FR、SR 和 RE 在控制系统信息安全体系的分配基于逐步递增原则。

本标准中所使用的 SL-C(控制系统)，表示一个规定的 FR 需要达到指定的 SL 能力。SL 矢量概念

的完整描述参见附录 A。

4 控制系统通用信息安全约束

4.1 概述

在阅读、规定和实施本标准第 5 章～第 11 章详述的控制系统的 SR 时，应遵循一些通用约束。本标准的引言提供了一些编制本标准的背景和资料信息。本章和后续的 FR 章节提供了必要的规范性材料，以扩展现有的企业信息安全，支持 IACS 所需的严格的完整性和可用性的要求。

注：这一条款内容最终将被纳入 IEC 62443-1-1。

4.2 基本功能支持

如 3.1.22 所述，基本功能是一种“维护受控设备健康、安全、环境和可用性所必需的功能和能力。”

- 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 IACS 基本功能产生不利影响。

注：参见 IEC 62443-2-1 关于风险评估要求的相关文件和例证，信息安全措施可能会影响基本功能。

当阅读、规定和实施本标准所描述的 SR 时，落实信息安全措施不应造成保护丧失、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，某些设施可能会导致特定安全措施终止生产连续运行，但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：

- 访问控制(IAC 和 UC)不应妨碍基本功能的运行，尤其是：
  ——用于基本功能的账户不应被锁定，甚至短暂的锁定也不行(见 5.5，SR 1.3——账户管理，5.6，SR 1.4——标识符管理，5.13，SR 1.11——未成功的登陆尝试和 6.7，SR 2.5——会话锁定)。
  ——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。
  ——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(见 5.10，SR 1.8——公钥基础设施(PKI)证书)。
  ——标识和鉴别，不应妨碍 SIF 触发(见 5.3，SR 1.1——人员标识和鉴别，5.4，SR 1.2——软件进程和设备识别认证)。同样，适用于授权执行(见 6.3，SR 2.1——授权执行)。
  ——不正确的时间戳审计记录(见 6.10，SR 2.8——审计事件及 6.13，SR 2.11——时间戳)不应对基本功能产生不利影响。
- 如果区域边界保护进入故障关闭和/或孤岛模式，应保持 IACS 的基本功能(见 9.4，SR 5.2——区域边界保护)。
- 发生在控制系统或安全仪表系统网络(SIS)中的拒绝服务事件(DoS)，不应妨碍 SIF 的动作(见 11.3，SR 7.1——拒绝服务保护)。

4.3 补偿对抗措施

本标准中使用的补偿对抗措施，应当遵循 IEC 62443-3-2 指南。

在本标准中，SR 的规范性语言以“控制系统应提供……的能力”，来表述支持某些特定的信息安全需求。该控制系统应提供的能力可能由外部组件来执行。在这样的情况下，控制系统应提供一个“接口”给外部组件。一些补偿对抗措施的例子包括使用者识别(包括集中式与分布式)，加强口令强度，签名有效性检查，安全事件关联和设备退役(信息长期保存)。

注 1：本标准详述的控制系统信息安全要求适用于控制系统的所有技术功能相关的工具和应用软件。然而，如这里所指出，其中的一些功能可以由外部资源来处理。

注 2：在一些高资源可用性的应用程序[高 SL-T(RA，控制系统)]中，控制系统外部的补偿对抗措施(如附加的物理安全性措施和/或增强人员背景调查)是必要的。在这些情况下，在较低的 IAC SL 1 或 IAC SL 2 等级评定中，可

能看到一个高资源可用性 SL 控制系统，这取决于补偿对抗措施。对于高可用性 SL 控制系统，安全措施引起的锁定或控制丧失是增加的，而不是减少。因此，即使成本不是重要因素，较高的 SL 并不总是“更好”。

4.4 最小权限

应提供通过权限的粒度以及映射这些权限到众多支持角色的灵活性来实施最小权限概念的能力。必要时宜责任到人。

5 FR 1——标识和鉴别控制

5.1 目的和 SL-C(IAC)描述

在允许访问控制系统之前标识和鉴别所有使用者(人员，软件进程和设备)。

SL 1——通过防止未经认证实体不经意的或巧合的访问的机制，标识和鉴别所有使用者(人员，软件进程和设备)。

SL 2——通过防止实体采用少量资源、通用方法、低动机的简单方式进行的未经鉴别的蓄意访问机制，标识和鉴别所有使用者(人员，软件进程和设备)。

SL 3——通过防止实体采用一般资源、IACS 特殊技能、中度动机的复杂方式进行的未经鉴别的蓄意访问机制，标识和鉴别所有使用者(人员，软件进程和设备)。

SL 4——通过防止实体采用扩展资源、IACS 特殊技能、高度动机进行的未经鉴别的蓄意访问机制，标识和鉴别所有使用者(人员，软件进程和设备)。

5.2 原由

资产所有者应该制定所有使用者列表(人员，软件进程和设备)，并确定每个控制系统组件所要求的 IAC 保护等级。IAC 的目标是在通信前通过对任何请求访问该控制系统的使用者进行身份验证来保护控制系统，任何请求访问该控制系统的使用者，应该在验证身份后才能激活通信。建议和指导原则宜包括运行在混合模式下的机制。例如，一些控制系统组件需要强的 IAC，比如强的鉴别机制，另外一些则不需要。

5.3 SR 1.1——人员标识和鉴别

5.3.1 要求

控制系统应提供标识和鉴别所有人员的能力。这种能力应在控制系统的所有接口上执行标识和鉴别。当人员访问控制系统时，根据适用的安全策略和规程实施职责分离和最小权限。

5.3.2 原由和附加指南

所有人员对控制系统的所有访问都需要标识和鉴别。这些使用者的身份认证宜通过如下方法完成，如口令、权标、生物特征，或上述方法的组合的多因子鉴别。人员的地理位置也可以用作鉴别过程的一部分。此要求宜适用于本地和远程访问控制系统。除了在控制系统层标识和鉴别所有人员(例如，在系统登录)外，标识和鉴别机制也经常在应用层使用。

人员作为一个单独组(如控制室操作员)，使用者标识和鉴别可以是基于角色或基于组。对于一些控制系统，操作员之间的紧急交互动作的能力至关重要。关键的一点是，本地紧急操作以及控制系统的基本功能不应受到标识或鉴别需求的阻碍(更多内容见第 4 章)，对这些系统访问可以采用适当的物理安全机制加以限制 IEC 62443-2-1。例如，对于一个关键操作室，这些物理安全机制包括严格物理访问控制与监视，一组使用者轮流倒班。这些使用者使用相同的使用者标识符。此外，宜鉴别操作员工作站

的客户端(见 5.4,SR 1.2——软件进程和设备的标识和鉴别)或该共享账户宜被限制在控制室受限的环境内使用。

为了支持 IAC 策略,根据 IEC 62443-2-1 中定义,第一步,该控制系统鉴别所有人员身份。第二步,强制将权限分配给所标识的人员(见 6.3,SR 2.1——授权执法)。

5.3.3 增强要求

5.3.3.1 SR 1.1 RE 1——唯一标识和鉴别

控制系统应提供唯一地鉴别和认证全部人员的能力。

5.3.3.2 SR 1.1 RE 2——对于非可信的网络的多因子身份鉴别

当人员通过非可信的网络访问控制系统时,控制系统应具有多因子身份鉴别的能力(见 5.15,SR 1.13——经由非可信的网络访问)。

注:见.5.7.3.1,SR 1.5——鉴别器管理,RE 5.7.3.1 增强软件进程的鉴别器管理。

5.3.3.3 SR 1.1 RE 3——对于所有网络的多因子鉴别

控制系统应具备对所有人员的访问实施多因子鉴别的能力。

5.3.4 信息安全等级

与 SR 1.1——人员标识和鉴别相关的四个 SL 等级要求如下:

- SL-C(IAC,控制系统)1:SR 1.1
- SL-C(IAC,控制系统)2:SR 1.1(1)
- SL-C(IAC,控制系统)3:SR 1.1(1)(2)
- SL-C(IAC,控制系统)4:SR 1.1(1)(2)(3)

5.4 SR 1.2——软件进程及设备的标识和鉴别

5.4.1 要求

控制系统应具备标识和鉴别所有软件进程和设备的能力。这种能力应在访问控制系统时,强制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。

5.4.2 原由和附加指南

标识和鉴别功能就是将一个 ID 映射到一个未知软件进程或设备(本章条以下称实体),在允许数据交换之前将该未知实体变成已知。允许非授权实体发送和接收控制系统的特定数据将会导致合法控制系统产生有害行为。

所有实体对控制系统的所有访问都需要标识和鉴别。此类实体的身份鉴别采用这样一些方法,例如口令、权标或位置信息(物理的或逻辑的)。这项要求宜适用于对控制系统的本地和远程访问。然而,在某些情况下,单个实体常被连接到不同的目标系统(例如,远程供应商支持),在技术上不可能让一个实体具有多个标识。在这些情况下,应采取补偿对抗措施。

所有实体的标识和鉴别机制都要防止诸如中间人或消息欺诈等的攻击。在某些情况下,这些机制可能涉及在同一物理服务器上运行的多个软件进程,每一个都有自己的标识。在其他情况下,标识可以和物理设备绑定,例如某个给定 PLC 上运行的所有进程。

在标识和鉴别便携式和移动设备时需要特别注意。众所周知,此类设备是向控制系统,包括隔离网络,引进非预期的网络数据流、恶意软件和/或信息泄露的途径。

当实体作为单个组时，标识和鉴别可以基于角色、组或实体。必要的是，标识和鉴别的要求不能妨碍本地应急处理和控制系统基本功能(详见第4章)。例如，在公共防护和控制机制中，一组设备共同执行防护功能以及与该组中的其他设备之间通过多播消息通信。在这些情况下，通常使用基于共享账户或共享对称密钥的组鉴别。

为支持IEC 62443-2-1中定义的标识和鉴别控制策略，第一步，控制系统验证所有实体的标识。第二步，执行权限分配给所标识的实体(见6.3，SR 2.1——授权执行)。

5.4.3 增强要求

5.4.3.1 SR 1.2 RE 1——唯一性标识和鉴别

控制系统应具有对所有软件进程和设备提供唯一性标识和鉴别的能力。

5.4.3.2 空白

5.4.4 信息安全等级

与SR 1.2——软件进程和设备标识和鉴别相关的四个SL等级要求如下：

- SL-C(IAC，控制系统)1：不选择
- SL-C(IAC，控制系统)2：SR 1.2
- SL-C(IAC，控制系统)3：SR 1.2(1)
- SL-C(IAC，控制系统)4：SR 1.2(1)

5.5 SR 1.3——账户管理

5.5.1 要求

控制系统应具有支持授权使用者管理所有账户的能力，包括添加、激活、修改、禁用和删除账户。

5.5.2 原由和附加指南

账户管理可以包括账户分组(例如，个人，基于角色，基于设备和控制系统)，规定组员条件和分配相关授权。在某些IACS场合，从风险分析和/或监管方面来看，个人账户被确定为不必要的；而共享账户是可接受的，只要适当的补偿对抗措施(如受限的物理访问或待批准的组织措施)已经实施和文档化。

非人员账户(有时称为服务账户)被用于软件进程到进程间通信(例如，控制服务器到历史数据库服务器和PLC到控制服务器)，通常需要与人员账户不同的安全策略和规程。为了提高安全性，在本地控制系统相关组件中，账户管理宜按照统一策略开展。用于系统初始安装的未使用的默认系统账户宜可删除。增强安全在于账户管理的简化和一致性。

5.5.3 增强要求

5.5.3.1 SR 1.3 RE 1——统一账户管理

控制系统应具有支持统一账户管理的能力。

5.5.3.2 空白

5.5.4 信息安全等级

与SR 1.3——账户管理相关的四个SL等级要求如下：

- SL-C(IAC，控制系统)1：SR 1.3

- SL-C(IAC,控制系统)2:SR 1.3
- SL-C(IAC,控制系统)3:SR 1.3(1)
- SL-C(IAC,控制系统)4:SR 1.3(1)

5.6 SR 1.4——标识符管理

5.6.1 要求

控制系统应提供使用者、组、角色或者控制系统接口的标识符管理的能力。

5.6.2 原由和附加指南

标识符不同于权限,一个实体可以在一个特定的控制系统的控制域或区域执行权限(见 6.3,SR 2.1——授权执行)。在这些域或区域内,将人员作为一个单独组(例如控制室操作员),使用者标识可以是基于角色、组或设备的。对于一些控制系统,即时的操作交互是至关重要的。本地控制系统的应急措施不宜受到身份鉴别要求的阻碍。适当的补偿对抗措施可以用来限制这样的系统访问。标识符可应用于控制系统的一部分而没必要用于整个控制系统。例如,无线设备通常需要标识符,而有线设备可能不需要。

标识符管理将通过符合 IEC 62443-2-1 规定的本地策略和规程来确定。

5.6.3 增强要求

无。

5.6.4 信息安全等级

与 SR 1.4——标识符管理相关的 4 个 SL 等级的要求是:

- SL-C(IAC,控制系统)1:SR 1.4
- SL-C(IAC,控制系统)2:SR 1.4
- SL-C(IAC,控制系统)3:SR 1.4
- SL-C(IAC,控制系统)4:SR 1.4

5.7 SR 1.5——鉴别器管理

5.7.1 要求

控制系统应提供如下能力:

a) 初始化鉴别器内容;

b) 控制系统一经安装完成,立即改变所有鉴别器的默认值;

c) 改变或者刷新所有的鉴别器;

d) 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。

5.7.2 原由和附加指南

除了标识符(见 5.6,SR 1.4——标识符管理)还需要鉴别器来证明身份,控制系统的鉴别器包括但不局限于令牌、对称密钥、私钥(公/私密钥对的一部分)、生物特征识别、口令、物理钥匙和门卡。人员宜采取合理的措施来保管鉴别器,包括持有个人鉴别器,不借出或不与他人共享鉴别器,鉴别器丢失或者受损后立即报告。

鉴别器是有生命周期的。当自动建立一个账户的时候,就需要创建一个新的鉴别器,以便能鉴别账户拥有者。例如,在一个基于口令的系统里,该账户拥有与之相关联的口令。初始鉴别器内容的定义可

以被解释为管理员定义的初始口令，这些初始口令是账户管理系统为新账户使用所设置的。在创建账户和账户第一次使用之间，能够配置这些初始值使得攻击者很难去猜测这些口令(涉及到账户拥有者设置新口令)。一些控制系统采用无人值守的安装，就会创建口令为缺省值的账户，一些嵌入式操作系统采用出厂时的缺省值口令。随着时间的推移，这些口令就会成为常识并被记录在因特网上。修改缺省口令能够保护系统，防范未授权使用者利用缺省口令进入系统。口令可以通过网络认证并通过存储或传输获得。可以通过加密、哈希、或握手协议等密码学防护手段来增加口令复杂度，使用握手协议根本不需要传输口令。当然，口令可能会受到攻击，例如暴力猜测或者在传输或者存储时破解加密保护。通过周期性的修改或者刷新口令可以减少被攻击的机会。类似的考虑可以应用于基于密钥的认证系统，通过使用硬件安全机制可以增强保护，例如可信平台模块(TPM)。

在适用的安全策略和规程中，宜明确鉴别器管理，例如，限制修改默认鉴别器、刷新周期，鉴别器保护规范或者应急响应(firecall)(见 3.1.24)规程。

不能接受由于安全措施导致的控制系统锁定或者失控。如果控制系统需要有高可用性，就需要采取措施来保证这个高可用性(例如补偿物理对抗措施、重复键或监督覆盖)。

在本需求中除了鉴别器管理的能力，鉴别机制的强度取决于所选择的鉴别器强度(例如口令的复杂性或公钥鉴别的密钥长度)和在鉴别过程中的鉴别器验证策略(例如多长的口令是有效的或者对验证公钥证书进行哪类检查)，最常用的鉴别机制是基于口令和公钥认证，进一步要求见 5.9，SR 1.7——基于口令鉴别的强度，5.10，SR 1.8——公钥基础设施(PKI)证书和 5.11，SR 1.9——公钥鉴别强度。

5.7.3 增强要求

5.7.3.1 SR 1.5 RE 1——软件进程身份证书的硬件安全

对于软件进程和设备使用者，控制系统应能够通过硬件机制保护相关鉴别器。

5.7.3.2 空白

5.7.4 信息安全等级

与 SR 1.5——鉴别器管理相关的 4 个 SL 等级要求如下：

- SL-C(IAC，控制系统)1：SR 1.5
- SL-C(IAC，控制系统)2：SR 1.5
- SL-C(IAC，控制系统)3：SR 1.5(1)
- SL-C(IAC，控制系统)4：SR 1.5(1)

5.8 SR 1.6——无线访问管理

5.8.1 要求

控制系统应能够标识和鉴别所有参与无线通讯的使用者(人员、软件进程或设备)。

5.8.2 原由和附加指南

任何无线技术能够，且在多数情况下宜被当作另外一种通讯协议选项，因而应遵循相同的 IACS 信息安全要求，如同 IACS 使用的任何其他的通信类型一样。然而从安全角度考虑，有线和无线通信至少有一个显著差异：使用无线时，物理安全对抗措施通常低效。对于这个以及其他可能的原因(例如监管差异)，在同样的案例中，与使用有线协议相比，无线通讯的风险分析结果可能导致更高的目标安全等级。

无线技术包括但不限于微波、卫星、分组无线电、IEEE 802.11x、IEEE 802.15.4(ZigBee、

IEC 62591—*Wireless*HART®,ISA-100.11a)、IEEE 802.15.1(BlueTooth)、WLAN 移动路由器、移动电话网络共享和各种红外技术。

5.8.3 增强要求

5.8.3.1 SR 1.6 RE 1——唯一性标识和鉴别

控制系统应提供对所有参与无线通信的使用者(人员、软件进程或者设备)提供唯一性标识和鉴别的能力。

5.8.3.2 空白

5.8.4 信息安全等级

与 SR 1.6——无线访问管理相关的 4 个 SL 等级要求是:

- SL-C(IAC,控制系统)1:SR 1.6
- SL-C(IAC,控制系统)2:SR 1.6(1)
- SL-C(IAC,控制系统)3:SR 1.6(1)
- SL-C(IAC,控制系统)4:SR 1.6(1)

5.9 SR 1.7——基于口令的鉴别强度

5.9.1 要求

对于使用口令鉴别机制的控制系统,控制系统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。

5.9.2 原由和附加指南

基于用户名和口令进行鉴别是一种很常用的机制,对于这样的机制很多攻击者聚焦于口令猜测(例如,字典攻击或有针对性的社会工程)或破解存储口令表征的密码保护(例如,使用彩虹表或暴力哈希碰撞)。

通过增加允许的字符的数量来增大有效口令集,使得这样的攻击会更加复杂。但前提是的确使用了增大的口令集。(一般使用者认为不好记住,所以不倾向于在口令中加入特殊字符)。限制口令的有效期会违反给定口令的保密性,但是可以减少黑客攻击的机会。为了防止使用者绕过这个控制,在修改他们的口令为新口令时,立刻改回到原始口令,需要强制使用口令最小有效期。在口令到期之前通知使用者,则使用者可以在方便的时候参照操作流程来修改口令。

这种保护可以通过限制口令重复使用而得到进一步提高(防止一系列的口令交替使用),这个可以进一步减少易破解口令的使用。基于口令的防护机制可以延伸到使用多因子鉴别(见 5.3,SR 1.1——人员标识和鉴别,和 5.4,SR 1.2——软件进程及设备标识和鉴别)。

5.9.3 增强要求

5.9.3.1 SR 1.7 RE 1——人员口令的生成及使用有效期限制

控制系统应提供防止任何已有的人员账户重复使用同一批口令的能力。此外,控制系统应加强人员口令的最大和最小有效期的使用。这些能力应符合普遍接受的安全产业实践要求。

注:普遍接受的好的实践办法是,在口令过期之前的一段可配置时间,提示使用者修改口令。

5.9.3.2 SR 1.7 RE 2——所有使用者口令的有效期限制

控制系统应提供使用者口令的最大和最小有效期的限制。

5.9.4 信息安全等级

与 SR 1.7——基于口令鉴别强度相关的 4 个 SL 等级的要求如下：

- SL-C(IAC,控制系统)1:SR 1.7
- SL-C(IAC,控制系统)2:SR 1.7
- SL-C(IAC,控制系统)3:SR 1.7(1)
- SL-C(IAC,控制系统)4:SR 1.7(1)(2)

5.10 SR 1.8——公钥基础设施(PKI)证书

5.10.1 要求

使用 PKI 时,控制系统应根据普遍接受的最佳实践来提供操作 PKI 或者从已有的 PKI 中获得公钥证书的能力。

5.10.2 原由和附加指南

注册获得公钥证书需要由主管或相关负责人通过使用安全的过程来授权,这个过程将会验证该证书持有者的身份,确保证书颁发给了预期方。使用公钥证书引起的延迟不应该降低控制系统的运行性能。

选择合适的 PKI 宜考虑组织的证书策略,该策略宜基于受保护信息的保密性泄露所导致的风险。可以在普遍接受的标准和指南中找到策略定义指导,例如因特网工程任务组(IETF)RFC 3647[29] 基于 X.509 的 PKI。例如,CA 的合适位置,无论是在控制系统内还是在 Internet 上,以及可信 CA 列表,宜在策略中加以考虑,而且取决于网络架构(见 IEC 62443-2-1)。

5.10.3 增强要求

无。

5.10.4 信息安全等级

与 SR 1.8——公钥基础设施证书相关的 4 个 SL 等级要求是：

- SL-C(IAC,控制系统)1:不选择
- SL-C(IAC,控制系统)2:SR 1.8
- SL-C(IAC,控制系统)3:SR 1.8
- SL-C(IAC,控制系统)4:SR 1.8

5.11 SR 1.9——公钥鉴别强度

5.11.1 要求

控制系统使用公钥鉴别时,应提供以下能力：

a) 通过检查给定证书的签名有效性,对证书有效性进行验证；

b) 通过构建一个到可信任的 CA 的认证路径,或者在自签名证书情况下,通过给所有与证书签发者通信的主机部署叶证书,对证书有效性进行验证；

c) 通过检查一个给定证书撤销状态,对证书有效性进行验证；

d) 建立与私钥相关的使用者(人员、软件进程或设备)控制；

e) 给使用者(人员、软件进程或设备)映射身份鉴别。

5.11.2 原由和附加指南

公/私钥加密在很大程度上取决于一个给定对象的私钥保密性和对信任关系的恰当处理。基于公钥认证去验证两个实体之间的信任关系时,有必要去追溯公钥证书到一个可信任的实体。在证书验证时,一个常见的错误是只检查证书签名的有效性而非检查信任签名本身。在一个 PKI 设置中,如果签名是由一个可信任的认证机构签发或者由一个可信任的机构授权颁发的证书,则是可以信任的。因此,所有的验证需要追溯提交他们的证书到一个可信任的认证机构。如果不能建立可信任认证机构的信任链,则提交的证书是不可信任的。当使用自签名的证书取代 PKI 时,证书主体本身签署了证书,则就不存在可信任的第三方机构或者认证机构。这可通过部署自签名公钥证书给所有对等实体进行补偿,使用其他安全机制(例如,在可信任环境中,对所有对等实体进行配置)进行验证。可信证书应该通过安全的通道分发给所有对等实体。在验证过程中,如果自签名证书已经出现在可信证书列表中则是可信的。可信证书集宜被配置为最小必要集。

在两种情况下,验证还需要考虑证书撤销的可能性。在 PKI 设置中,典型的做法是维护证书撤销列表(CRL)或者运行在线证书状态协议(OCSP)服务器。当由于控制系统的约束导致撤销检查不可用时,证书短期有效期机制可以补偿即时的撤销消息缺失。需要注意的是,短有效期证书有时会造成重大的控制系统操作问题。

5.11.3 增强要求

5.11.3.1 SR 1.9 RE 1——公钥鉴别的硬件安全

控制系统应提供根据普遍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的能力。

5.11.3.2 空白

5.11.4 信息安全等级

与 SR 1.9——公钥鉴别强度相关的 4 个 SL 等级要求如下:

- SL-C(IAC,控制系统)1:不选择
- SL-C(IAC,控制系统)2:SR 1.9
- SL-C(IAC,控制系统)3:SR 1.9(1)
- SL-C(IAC,控制系统)4:SR 1.9(1)

5.12 SR 1.10——鉴别器反馈

5.12.1 要求

控制系统应提供鉴别过程中隐藏鉴别信息反馈的能力。

5.12.2 原由和附加指南

隐藏反馈可以保护信息被未经授权的个人所利用,例如,当人员在使用口令时显示星号或者另外的随机字符就可以隐藏鉴别信息的反馈。其他例子包括有线等效加密(WEP)密钥、安全套接字程序(SSH)、权标和 RSA 一次性口令。鉴别实体不宜提供任何有关鉴别失败原因的提示,例如“未知使用者名”。

5.12.3 增强要求

无。

5.12.4 信息安全等级

与 SR 1.10——鉴别器反馈相关的 4 个 SL 等级要求是：

- SL-C(IAC,控制系统)1:SR 1.10
- SL-C(IAC,控制系统)2:SR 1.10
- SL-C(IAC,控制系统)3:SR 1.10
- SL-C(IAC,控制系统)4:SR 1.10

5.13 SR 1.11——失败的登录尝试

5.13.1 要求

控制系统应提供针对任何使用者(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的能力。当限制次数超出后,控制系统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,控制系统应提供不允许交互式登录的能力。

5.13.2 原由和附加指南

由于潜在的拒绝服务,连续无效的访问次数可能被限制。如果允许,在适用的安全策略和规程所确定的预定时间周期内,经过一定数量的访问尝试后,控制系统可以自动复位访问尝试数目为 0。将尝试访问重置为 0,可以允许拥有正确的登录标识的使用者(人员、软件进程或设备)访问。当应急情况下需要操作员快速响应的时候,对于控制系统操作员站或节点不宜使用自动拒绝访问。所有的锁定机制宜考虑连续运行的功能要求,以减轻由于操作不当造成的系统故障或者对人员的伤害。允许关键服务账户进行交互式登录可能会提供潜在的拒绝服务或其他滥用情况。

5.13.3 增强要求

无。

5.13.4 信息安全等级

与 SR 1.11——失败的登录尝试相关的 4 个 SL 等级要求如下：

- SL-C(IAC,控制系统)1:SR 1.11
- SL-C(IAC,控制系统)2:SR 1.11
- SL-C(IAC,控制系统)3:SR 1.11
- SL-C(IAC,控制系统)4:SR 1.11

5.14 SR 1.12——系统使用提示

5.14.1 要求

在进行鉴别之前,控制系统应提供显示系统提示信息的能力。系统使用提示信息应可通过授权人进行配置。

5.14.2 原由和附加指南

隐私、安全策略和规程需要符合适用的法律、指令、政策、法规、标准和指南的相关要求。通常这一要求主要用于对违规者的法律起诉和提供蓄意破坏证明。该能力是支持策略要求必要的,但并不能提高 IACS 安全性。当个人登录到控制系统的时候,系统提示消息可以以警告标语形式来出现。在控制系统设施中使用警告提示标语不能防护远程登录问题。系统使用的提示信息内容示例有：

a) 个人正访问一个特定的控制系统；
b) 系统使用可能被监控、记录和审计；
c) 禁止未经授权使用系统，否则将会受到刑事和/或民事处罚；
d) 系统的使用表明同意被监控和记录。

5.14.3 增强要求

无。

5.14.4 信息安全等级

与 SR 1.12——系统使用提示相关的四个 SL 等级要求如下：

- SL-C(IAC,控制系统)1:SR 1.12
- SL-C(IAC,控制系统)2:SR 1.12
- SL-C(IAC,控制系统)3:SR 1.12
- SL-C(IAC,控制系统)4:SR 1.12

5.15 SR 1.13——通过不可信网络的访问

5.15.1 要求

控制系统应提供对通过不可信网络途径访问控制系统的所有方式进行监视和控制的能力。

5.15.2 原由与附加指南

通过不可信的网络访问控制系统通常包括远程访问方法(如拨号、宽带和无线)以及从一个公司办公室(非控制性系统)网络的连接。控制系统宜限制通过拨号连接的访问(例如,基于请求源的限制拨号访问)或者防止未授权的连接或授权连接的破坏(例如,使用虚拟专用网技术)。通过不可信网络访问在地理上远程的控制系统组件位置(例如,控制中心和现场位置)宜仅在必要和已鉴别的情况下。对于远程使用者访问控制系统,安全策略和规程可能要求多因子鉴别。

5.15.3 增强要求

5.15.3.1 SR 1.13 RE 1——显式访问请求批准

控制系统应提供拒绝来自不可信网络访问请求的能力,除非被一个指定的角色允许。

5.15.3.2 空白

5.15.4 信息安全等级

与 SR 1.13——通过不可信网络访问相关的四个 SL 等级要求如下：

- SL-C(IAC,控制系统)1:SR 1.13
- SL-C(IAC,控制系统)2:SR 1.13(1)
- SL-C(IAC,控制系统)3:SR 1.13(1)
- SL-C(IAC,控制系统)4:SR 1.13(1)

6 FR 2——使用控制

6.1 目的和 SL-C(UC)描述

对已鉴权的使用者(人员、软件进程或设备),强制指定权限以在 IACS 中执行所需动作,并监视这

些权限的使用。

SL 1——根据指定的权限限制 IACS 的使用，以防止不经意的或巧合的滥用。

SL 2——根据指定的权限限制 IACS 的使用，以防止实体采用少量资源、通用技能以及低动机这样简单的规避手段。

SL 3——根据指定的权限限制 IACS 的使用，以防止实体采用一般资源、IACS 特殊技能以及一般动机这样复杂的规避手段。

SL 4——根据指定的权限限制 IACS 的使用，以防止实体采用扩展资源、IACS 特殊技能以及高动机这样复杂的规避手段。

6.2 原由

一旦使用者被标识和鉴别，对于控制系统的授权使用，控制系统应该限制所允许的操作。资产所有者和系统集成商将应该为每一个使用者（人员、软件进程或设备）、组、角色等分配 IACS 的授权使用权限。（详见 5.6，SR 1.4——标识符管理）使用控制的目标是在使用者执行操作之前，验证准予其必要的权限，保护控制系统资源免受未经授权的操作。操作的例子为读或写数据，下载程序和设置配置。建议和指南宜包括在混合模式下的操作机制。例如，某些控制系统资源，要求较强的使用控制保护，比如受限权限，而其他部分没有。推而广之，使用控制要求需要扩展到静态数据。使用者权限可能会根据时间/日期、位置和访问方式而有所不同。

6.3 SR 2.1——授权执行

6.3.1 要求

对于所有接口，控制系统应提供对所有人员用户强制授权的能力，用于控制系统的使用控制，以支持职责分离和最小权限。

6.3.2 原由与附加指南

使用控制策略（例如，基于身份的策略，基于角色的策略和基于规则的策略）和相应的读写访问执行机制（如访问控制列表、访问控制矩阵和加密）用于控制使用者（人员、软件进程和设备）对资产（如设备、文件、记录、软件进程、规程和域）的使用。

在控制系统验证使用者的身份之后（人员、软件进程或设备）（见 5.3，SR 1.1——人员标识与鉴别和 5.4，SR 1.2——软件进程和设备标识与鉴别），根据定义的安全策略及步骤还应该验证所请求的操作是被实际允许的。例如，基于角色的访问控制策略，控制系统会检查哪些角色分配给已验证的使用者或资产，哪些权限分配给这些角色——如果请求的操作在权限内，那么将会被执行，否则拒绝。这允许执行职责分离和最小权限。执行机制的使用不允许严重影响控制系统的操作性能。

计划或非计划的更改控制系统组件会显著影响控制系统的整体安全性。因此，为了发起变更，只有具备资质和被授权的个体宜获得控制系统组件的使用权限，包括升级和修改。

6.3.3 增强要求

6.3.3.1 SR 2.1 RE 1——所有使用者的授权执行

对于所有接口，控制系统应提供对所有使用者（人员、软件进程或设备）强制授权的能力，用于控制系统的控制使用，以支持职责分离和最小权限。

6.3.3.2 SR 2.1 RE 2——许可到角色映射

控制系统应为授权使用者或角色提供这样的能力，即可对所有人员的许可到角色映射进行规定和

修改。

注 1：这是一个普遍接受的最佳实践，不将角色限制在固定的嵌套式层次中，即高级别角色的权限是低级别角色的超集。例如，系统管理员通常并不一定具备操作员权限。

注 2：这个 RE 也适用于软件进程和设备。

6.3.3.3 SR 2.1 RE 3——主管超驰(Supervisor override)

为一个可配置的时间或事件序列，控制系统应支持主管手动超驰当前人员授权。

注：实现控制，审计和手动覆盖自动化机制在发生突发事件或其他严重事件时通常是必要的。这允许主管能够使操作员对不寻常的状况快速做出反应，即使在没有关闭当前会话和作为一个更高权限人员建立一个新的会话情况下。

6.3.3.4 SR 2.1 RE 4——双重确认

控制系统应支持对工业过程造成严重影响的动作执行双重批准。

注：当需要很高级别可靠性和正确性执行的操作时，限制双重确认是一个普遍接受的良好实践。要求双重批准强调正确操作失败所导致后果的严重性。例如，需要双重确认的一种情况是关键工业过程的设定值改变。为防止出现严重 HSE 后果，有必要采用及时响应的情况下，不采用双重确认机制是普遍接受的良好实践，例如，工业生产过程的紧急关停。

6.3.4 信息安全等级

与 SR 2.1——授权执行相关的四个 SL 等级要求如下：

- SL-C(UC，控制系统)1：SR 2.1
- SL-C(UC，控制系统)2：SR 2.1(1)(2)
- SL-C(UC，控制系统)3：SR 2.1(1)(2)(3)
- SL-C(UC，控制系统)4：SR 2.1(1)(2)(3)(4)

6.4 SR 2.2——无线使用控制

6.4.1 要求

根据普遍接受的安全行业实践，控制系统应提供与控制系统的无线连接的授权、监视以及执行使用限制的能力。

6.4.2 原由与附加指南

任何无线技术可以，且在大多数情况下宜被视为只是一种通信协议的选择，因此应与 IACS 所使用的任何其他通信类型具有相同的 IACS 安全要求。然而，对于相同的用例和 SL-T，风险分析可能会要求无线 IACS 组件支持使用控制能力高于有线系统的典型要求。监管差异也会导致在有线与无线通信之间所需不同的能力要求。

如在 5.8，SR 1.6——无线访问管理中所述，无线技术包括但不限于微波、卫星、分组无线电、IEEE 802.11x、IEEE 802.15.4(ZigBee、IEC 62591—*Wireless*HART®，ISA-100.11a)、IEEE 802.15.1(BlueTooth)、无线 LAN 移动路由器、移动电话网络共享和各种红外技术。

6.4.3 增强要求

6.4.3.1 SR 2.2 RE 1——识别并报告非授权的无线设备

控制系统应提供识别和报告未经授权的无线设备在控制系统物理环境中发射的能力。

6.4.3.2 空白

6.4.4 信息安全等级

与 SR 2.2——无线使用控制相关的四个 SL 等级要求如下：

- SL-C(UC,控制系统)1:SR 2.2
- SL-C(UC,控制系统)2:SR 2.2
- SL-C(UC,控制系统)3:SR 2.2(1)
- SL-C(UC,控制系统)4:SR 2.2(1)

6.5 SR 2.3——便携式和移动设备使用控制

6.5.1 要求

控制系统应提供自动执行可配置的使用限制的能力,其中包括：

a) 防止使用便携式和移动设备；

b) 要求特定内容的授权；

c) 限制到/来自便携式和移动设备的代码和数据传输。

6.5.2 原由与附加指南

便携式和移动设备可能会引入非预期的网络数据流、恶意软件和/或信息泄露。因此在典型控制系统环境中,宜明确这些设备的使用控制。安全策略和规程可能不允许通过便携式和/或移动设备执行某些功能或活动。请参考 IEC 62443-2-1 何时何地宜允许使用便携式和移动设备的指导。

保护存储在便携和移动设备上的信息(例如,使用加密机制在存储和在控制区域外传输时提供保密性和完整性保护),使其在其他地方也能得到有效保护(见第 8 章,FR 4——数据保密性)。

6.5.3 增强要求

6.5.3.1 SR 2.3 RE 1——便携式和移动设备安全状态的加强

控制系统应提供对试图连接到一个区域的便携式或移动设备进行验证以符合该区域安全要求的能力。

6.5.3.2 空白

6.5.4 信息安全等级

与 SR 2.3——便携式和移动设备使用控制相关的四个 SL 等级要求如下：

- SL-C(UC,控制系统)1:SR 2.3
- SL-C(UC,控制系统)2:SR 2.3
- SL-C(UC,控制系统)3:SR 2.3(1)
- SL-C(UC,控制系统)4:SR 2.3(1)

6.6 SR 2.4——移动代码

6.6.1 要求

控制系统应提供对可能造成控制系统损害的移动代码技术执行使用限制的能力,包括：

a) 防止移动代码的执行；

b) 对于代码的来源要求适当的鉴别和授权；

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。

6.6.2 原由与附加指南

移动代码技术包括但不限于 Java、JavaScript、ActiveX、便携文档格式(PDF)、Postscript、Shockwave movies、Flash 动画和 VBScript。使用限制适用于移动代码的选择和使用，包括安装在服务器上或在个人工作站上载、下载并执行的移动代码。控制规程宜防止开发、获取或引入控制系统不可接受的移动代码。例如，不允许移动代码直接与控制系统进行交换，但在一个由 IACS 人员维护的受控的相邻环境中可能被允许进行。

6.6.3 增强要求

6.6.3.1 SR 2.4 RE 1——移动代码完整性检查

控制系统应提供在允许代码执行之前验证移动代码完整性的能力。

6.6.3.2 空白

6.6.4 信息安全等级

与 SR 2.4——移动代码相关的四级 SL 等级要求如下：

- SL-C(UC，控制系统)1：SR 2.4
- SL-C(UC，控制系统)2：SR 2.4
- SL-C(UC，控制系统)3：SR 2.4(1)
- SL-C(UC，控制系统)4：SR 2.4(1)

6.7 SR 2.5——会话锁定

6.7.1 要求

控制系统应提供在可配置的非活动时间周期后启动或通过手动启动会话锁定以阻止人员继续访问的能力。会话锁定应一直保持有效，直到拥有会话的人员或其他授权的人员使用适当的身份标识和鉴别规程重新建立访问。

6.7.2 原由与附加指南

负责控制系统的实体宜使用会话锁定去阻止对特定工作站和节点的访问。控制系统宜在一个配置的时间周期后，为工作站或节点自动激活会话锁定机制。在某些情况下，不建议对控制系统操作员工作站或节点会话加以锁定(例如，在紧急情况下当前的操作员响应所需的会话)。会话锁定不能代替控制系统注销。在控制系统不支持会话锁定的情况下，责任实体宜采取适当的补偿对抗措施(例如，提供增加物理安全、人员安全和审计措施)。

6.7.3 增强要求

无。

6.7.4 信息安全等级

与 SR 2.5——会话锁定相关的四个 SL 等级要求如下：

- SL-C(UC,控制系统)1:SR 2.5
- SL-C(UC,控制系统)2:SR 2.5
- SL-C(UC,控制系统)3:SR 2.5
- SL-C(UC,控制系统)4:SR 2.5

6.8 SR 2.6——远程会话终止

6.8.1 要求

控制系统应提供在可配置的非活动时间周期后自动终止或由发起会话的使用者手动终止远程会话的能力。

6.8.2 原由与附加指南

在通过区域边界访问控制系统时,一个远程会话会被启动,该区域是资产所有者根据他们的风险评估进行定义的。基于控制系统的风险评估和安全策略和规程,这个要求可能仅限于控制系统的监视和维护活动(非关键操作)会话。一些控制系统或组件可能不允许会话终止。

6.8.3 增强要求

无。

6.8.4 信息安全等级

与 SR 2.6——远程会话终止相关的四个 SL 等级要求如下:

- SL-C(UC,控制系统)1:不选择
- SL-C(UC,控制系统)2:SR 2.6
- SL-C(UC,控制系统)3:SR 2.6
- SL-C(UC,控制系统)4:SR 2.6

6.9 SR 2.7——并发会话控制

6.9.1 要求

控制系统应提供对于任何给定使用者(人员、软件进程或设备)的每个接口限制并发会话数量的能力,并且会话数量可配置。

6.9.2 原由与附加指南

如果不设限制,可能发生导致资源耗尽的 DoS。在控制系统资源缺乏情况下,应该在可能锁定一个特定的使用者和锁定所有使用者和服务之间有一个权衡。产品供应商和/或系统集成商的指南很可能需要提供关于会话数量该如何赋值的充分信息。

6.9.3 增强要求

无。

6.9.4 信息安全等级

与 SR 2.7——并发会话控制相关的四个 SL 等级要求如下:

- SL-C(UC,控制系统)1:不选择
- SL-C(UC,控制系统)2:不选择

- SL-C(UC,控制系统)3:SR 2.7
- SL-C(UC,控制系统)4:SR 2.7

6.10 SR 2.8——审计事件

6.10.1 要求

控制系统应为下述类型的事件提供生成安全相关审计记录的能力,事件类型包括: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、配置变更、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、软件进程或人员账户)、分类、类型、事件 ID 和事件结果。

6.10.2 原由与附加指南

这一要求的目的是记录重要事件的发生,对控制系统信息安全重要或相关的事件需要被审计。审计活动会影响控制系统的性能。安全审计功能通常与不同区域的网络健康和状态监控功能相协调。当编译可审计事件列表时,宜考虑通常公认和被接受的清单和配置指南。信息安全策略和规程宜定义可审计事件,它可充分支持安全事故的事后调查。另外,审计记录宜能充分地监视安全机制的有效性和恰当操作,以满足本标准要求。

应该指出的是,在给定的系统功能,特别是给定系统安全要求为特定等级时,事件记录要求是适用的。例如,鉴别事件的记录要求(在访问控制类别中),根据第 5 章要求,针对 SL 1 系统鉴别功能要求仅适用于 SL 1 的鉴别功能要求。事件可能发生在任何控制系统组件(例如登录事件)或应该被专用监视器所观测。例如,端口扫描可能被入侵检测系统(IDS)或入侵防护系统(IPS)检测。

6.10.3 增强要求

6.10.3.1 SR 2.8 RE 1——集中管理,系统范围的审计踪迹

控制系统应提供集中管理审计事件的能力和从控制系统多个组件汇编审计记录形成系统范围(逻辑或物理)的、时间相关的审计追踪。控制系统应提供按照工业标准格式输出这些审计记录的能力,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(SIEM)。

6.10.3.2 空白

6.10.4 信息安全等级

与 SR 2.8——审计事件相关的四个 SL 等级要求如下:

- SL-C(UC,控制系统)1:SR 2.8
- SL-C(UC,控制系统)2:SR 2.8
- SL-C(UC,控制系统)3:SR 2.8(1)
- SL-C(UC,控制系统)4:SR 2.8(1)

6.11 SR 2.9——审计存储容量

6.11.1 要求

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。

6.11.2 原由与附加指南

控制系统宜提供足够的审计存储容量,考虑保留策略,执行审计和在线审计处理要求。参考指南包

括 NIST SP800-92[27]。根据适用策略、法规或商业要求的时间周期内，审计存储容量宜能够足以保留日志。

6.11.3 增强要求

6.11.3.1 SR 2.9 RE 1——当审计记录存储容量达到临界值时，要求告警

当分配的审计记录存储容量达到最大审计记录存储容量的一个可设定的比例时，控制系统应提供发出告警的能力。

6.11.3.2 空白

6.11.4 信息安全等级

与 SR 2.9——审计存储容量相关的四个 SL 等级要求如下：

- SL-C(UC，控制系统)1：SR 2.9
- SL-C(UC，控制系统)2：SR 2.9
- SL-C(UC，控制系统)3：SR 2.9(1)
- SL-C(UC，控制系统)4：SR 2.9(1)

6.12 SR 2.10——审计处理失败响应

6.12.1 要求

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，采取恰当的响应行动。

6.12.2 原由与附加指南

审计生成通常发生在事件源。审计处理涉及传输、可能的添加(例如增加一个时间戳)和持续审计记录存储。审计处理失败包括，例如，软件或硬件出错，审计捕获机制失败和审计存储容量饱和或溢出。用于设计合适的响应行动的参考指南包括 NIST SP800-92。应该指出的是，通过覆盖日期最早的审计记录或停止审计日志生成可应对审计存储容量溢出问题，但也意味着潜在的基本取证信息的丢失。

6.12.3 增强要求

无。

6.12.4 信息安全等级

与 SR 2.10——对审计处理失败响应相关的四个 SL 等级要求如下：

- SL-C(UC，控制系统)1：SR 2.10
- SL-C(UC，控制系统)2：SR 2.10
- SL-C(UC，控制系统)3：SR 2.10
- SL-C(UC，控制系统)4：SR 2.10

6.13 SR 2.11——时间戳

6.13.1 要求

在审计记录生成时，控制系统应提供时间戳。

6.13.2 原由与附加指南

审计记录时间戳(包括日期和时间)的生成宜使用内部系统时钟。如果整个系统时钟不同步(在很多装置中常常如此),需要已知时间偏移量来支持事件序列分析。另外,同步内部生成的外部事件审计记录,需要与公认的外部时间源同步[例如全球定位系统(GPS),全球导航卫星系统(GLONASS),伽利略定位系统(Galileo)]。时间源宜防止未经授权的变更。

6.13.3 增强要求

6.13.3.1 SR 2.11 RE 1——内部时间同步

控制系统应提供按可配置频率同步内部系统时钟的能力。

6.13.3.2 SR 2.11 RE 2——时间源完整性保护

应保护时间源防止非授权改动,一旦改动则生成审计事件。

6.13.4 信息安全等级

与 SR 2.11——时间戳相关的四个 SL 等级要求如下:

- SL-C(UC,控制系统)1:不选择
- SL-C(UC,控制系统)2:SR 2.11
- SL-C(UC,控制系统)3:SR 2.11(1)
- SL-C(UC,控制系统)4:SR 2.11(1)(2)

6.14 SR 2.12——抗抵赖

6.14.1 要求

控制系统应提供判断给定人员是否实施特定行动的能力。

6.14.2 原由与附加指南

使用者特定行动实例包括执行操作动作,改变控制系统配置,创建信息,发送消息,批准信息(例如表示赞同)和接收消息。针对未采取特殊行动的使用者,没有制作特定文档的作者,没有传输信息的发送者,没有收到消息的接收者,或是没有签署文件的签名者,抗抵赖保护防止事后虚假声明。抗抵赖服务可用于确定信息是否来源于使用者,使用者是否采取特定行为(例如,发送电子邮件和批准工作命令)或接收到特定信息。抗抵赖服务是通过采用各种技术或机制(例如,数字签名、数字信息收条和时间戳)实现的。

6.14.3 增强要求

6.14.3.1 SR 2.12 RE 1——针对所有使用者的抗抵赖

控制系统应提供判断一个特定使用者(人员、软件进程或设备)是否实施特定行动的能力。

6.14.3.2 空白

6.14.4 信息安全等级

与 SR 2.12——抗抵赖相关的四个 SL 等级要求如下:

- SL-C(UC,控制系统)1:不选择

- SL-C(UC,控制系统)2:不选择
- SL-C(UC,控制系统)3:SR 2.12
- SL-C(UC,控制系统)4:SR 2.12(1)

7 FR 3——系统完整性

7.1 目的与 SL-C(SI)描述

确保 IACS 的完整性,防止非授权操控。

SL 1——保护 IACS 完整性,防止不经意的或巧合的操控。

SL 2——保护 IACS 完整性,防止某些人利用较少量资源、通用技能和低动机的简单手段进行操控。

SL 3——保护 IACS 完整性,防止某些人利用一般资源、IACS 特定技能和一般动机的复杂手段进行操控。

SL 4——保护 IACS 完整性,防止某些人利用扩展资源、IACS 特殊技能和高动机的复杂手段进行操控。

7.2 原由

IACS 往往会经历多个测试周期[单元测试、出厂验收测试(FAT)、现场验收测试(SAT)、认证、调试等],在它们开始生产之前,确认系统性能达到预期。一旦运行,资产所有者有责任保持 IACS 的完整性。使用他们的风险评估方法,资产所有者可分配不同等级的完整性保护给不同系统、通信信道和 IACS 中的信息。在运行和非运行状态下都宜保持物理资产的完整性,例如在生产过程中,在存储时或设备维护关闭时。在运输和静止时,例如通过网络传输或在数据库存储时,都宜保持逻辑资产完整性。

7.3 SR 3.1——通信完整性

7.3.1 要求

控制系统应提供保护传输信息完整性的能力。

7.3.2 原由和附加指南

许多常见的网络攻击基于对传输中的数据进行操纵,例如操纵网络数据包。交换网络或路由网络给攻击者提供了更大的机会操纵数据包,这是因为通常容易对这些网络进行未被发现的访问,同时,攻击者也会操纵交换和路由机制本身以获取对传输信息的更多访问。控制系统环境下的内容篡改包括改变从传感器到接收器的测量值,变更控制应用到执行器的命令参数。

根据上下文(例如在局域网段的传输和通过不可信网络的传输)和传输使用的网络类型[例如传输控制协议(TCP)/因特网协议(IP)和本地串行链路],可行的和适当的机制会有所不同。在一个直接连接(点对点)的小型网络中,如果端点完整性得到保护(见 7.6,SR 3.4——软件和信息的完整性),在较低 SL 的情况下,针对所有节点的物理访问保护就已足够。然而当网络分布在员工经常出现的区域或在一个广域网时,可能无法执行物理访问保护。如果一个商业服务被用作通信服务,作为一种商品项目而不是一个完全专用的服务(例如专线和 T1 链路),可能更难以获得实现通信完整性安全控制(例如由于法律的限制)所需的必要保证。当满足必要的安全需求不可行或不切实际时,应采用合适的补偿对抗措施,或者明确承认额外风险。

工业设备往往受到环境条件影响,会导致完整性问题和/或误报事件,很多时候环境因素包含微粒、液体、振动、气体、辐射或电磁干扰(EMI),这些可能会影响通信线路和信号的完整性。网络基础设施设

计宜减少这些物理/环境因素对通信完整性的影响。例如，当微粒、液体和/或气体是一个影响因素，它应该需要使用一个密封的 RJ-45 或 M12 接头代替商业级的 RJ-45 线路接头。电缆本身可使用不同保护层来应对微粒、液体和/或气体。当振动是影响因素时，可能有必要使用 M12 连接器以防止 RJ-45 连接器在使用中失去连接。当辐射和/或电磁干扰 EMI 是影响因素时，可能有必要使用屏蔽双绞线或光缆，防止对通信信号产生的影响。如果计划使用无线网络，则可能有必要做无线频谱分析以证明这是一个可行的解决方案。

7.3.3 增强要求

7.3.3.1 SR 3.1 RE 1——加密完整性保护

控制系统应提供使用密码学机制识别通信过程中信息被修改的能力。

注：这是一个普遍接受的最佳实践，经过仔细考虑信息安全需求、潜在系统性能、从系统故障中的恢复能力，确定使用适当的密码学机制用于信息认证和完整性。

7.3.3.2 空白

7.3.4 信息安全等级

与 SR 3.1——通信完整性相关的四个 SL 等级如下：

- SL-C(SI,控制系统)1:SR 3.1
- SL-C(SI,控制系统)2:SR 3.1
- SL-C(SI,控制系统)3:SR 3.1(1)
- SL-C(SI,控制系统)4:SR 3.1(1)

7.4 SR 3.2——恶意代码防护

7.4.1 要求

控制系统应提供应用保护机制的能力，以预防、检测、报告和减缓恶意代码或未经授权软件的影响。控制系统应提供更新防护机制的能力。

7.4.2 原由和附加指南

控制系统宜使用防护机制来预防、检测、减缓和报告检测到的恶意代码(例如，病毒、蠕虫、木马、后门)，这些恶意代码是通过电子邮件、电子邮件附件、因特网接入、移动介质[例如，通用串行总线(USB)设备、磁盘或光盘]、PDF 文档、Web 服务、网络连接和被感染的电脑或其他通用手段传播的。

检测机制宜能够检测应用程序二进制文件和数据文件的完整性是否被破坏。检测技术可以包括但不仅限于，二进制文件完整性和属性监测、哈希和签名技术。减缓技术可以包括但不限于，文件清理、隔离、文件删除、主机通信限制和 IPS。

预防技术可以包括但不限于，黑名单和白名单技术、可移动媒质控制、沙箱技术和特殊的计算平台机制，如：受限的固件更新功能，禁止执行位(NX)，数据执行保护(DEP)，地址空间布局随机化(ASLR)，堆栈溢出检测和强制访问控制。见 10.4，SR 6.2——连续监测，涉及控制系统监测工具和技术相关的要求。

预防和减缓机制可能包括基于主机(如计算机和服务器)的机制、基于网络的机制(如 IDS 和 IPS)和那些专注于控制系统特定组件的机制(如 PLC 和 HMI)。

7.4.3 增强要求

7.4.3.1 SR 3.2 RE 1——入口和出口的恶意代码防护

控制系统应具有在所有入口和出口提供恶意代码防护机制的能力。

注：这些机制通常在可移动介质、防火墙、单向网关、网络服务器、代理服务器或远程访问服务器上提供。

7.4.3.2 SR 3.2 RE 2——恶意代码保护集中管理和报告

控制系统应具有提供管理恶意代码防护机制的能力。

注：这些机制是通过终端基础设施的集中式管理或 SIEM 解决方案提供。

7.4.4 信息安全等级

与 SR 3.2——恶意代码防护相关的四个 SL 等级如下：

- SL-C(SI,控制系统)1:SR 3.2
- SL-C(SI,控制系统)2:SR 3.2(1)
- SL-C(SI,控制系统)3:SR 3.2(1)(2)
- SL-C(SI,控制系统)4:SR 3.2(1)(2)

7.5 SR 3.3——信息安全功能验证

7.5.1 要求

控制系统应提供在 FAT、SAT 及日常维护时，支持安全功能操作的验证和报告异常事件的能力。这些安全功能应包括支持本标准中规定的安全要求的所有必要内容。

7.5.2 原由和附加指南

产品供应商或系统集成商宜提供关于如何测试其设计的信息安全控制的指南。资产所有者需要意识到在正常运行期间运行这些验证测试的可能影响。这些验证的执行细节需要仔细考虑连续运行的要求(例如，日程安排或事先通知)。

信息安全功能验证的例子包括：

- 通过欧洲计算机防病毒研究协会(EICAR)的控制系统的文件系统测试，进行防病毒措施验证。防病毒软件宜进行此检测并触发适当的事故处理规程。
- 验证标识与鉴别及对未授权账户尝试访问的使用控制措施(对于某些功能，这可能是自动的)。
- 验证 IDS 安全控制，包含对不规则流量触发 IDS 规则，此流量已知为非恶意数据流。测试可通过通信量触发这个规则以及合适的 IDS 监控和事故处理规程来实现。
- 确认审计日志记录按照所要求的安全策略和规程执行，没有被内部或外部实体禁止。

7.5.3 增强要求

7.5.3.1 SR 3.3 RE 1——信息安全功能验证的自动化机制

控制系统应提供在 FAT、SAT 和定期维护过程中，应用自动化机制来管理信息安全验证的能力。

7.5.3.2 SR 3.3 RE 2——正常操作过程中的信息安全功能验证

控制系统应提供在正常操作期间对信息安全功能的预期操作进行验证的能力。

注：由于可能导致严重影响，谨慎地执行这个要求是一个最佳实践。在安全系统中，经常没有被恰当考虑。

7.5.4 信息安全等级

与 SR 3.3——信息安全功能验证相关的四个 SL 等级要求如下：

- SL-C(SI,控制系统)1:SR 3.3
- SL-C(SI,控制系统)2:SR 3.3

- SL-C(SI,控制系统)3:SR 3.3(1)
- SL-C(SI,控制系统)4:SR 3.3(1)(2)

7.6 SR 3.4——软件和信息完整性

7.6.1 要求

控制系统应提供对软件和信息的未经授权的更改的检测、记录、报告和防范的能力。

7.6.2 原由和附加指南

未经授权的更改是指试图发起更改的实体不具备所要求的权限。这个 SR 补充了 FR 1 和 2 中相关联的 SR。FR 1 和 2 涉及执行的角色、权限和所设计的使用模式。如果其他的保护机制(如授权执行)已经被规避,完整性验证方法被用来检测、记录、报告和防范可能发生的软件和信息被篡改。控制系统宜采用正规的或推荐的完整性机制(如哈希加密)。例如,这些机制可以用来监视现场设备最新配置信息,以此检测破坏安全的行为(包括未授权更改)。

7.6.3 增强要求

7.6.3.1 SR 3.4 RE 1——完整性破坏的自动通知

在完整性验证过程中发现差异时,控制系统应具有自动通知一组可配置的接收者的能力。

7.6.3.2 空白

7.6.4 信息安全等级

与 SR 3.4——软件和信息完整性相关的四个 SL 等级要求如下:

- SL-C(SI,控制系统)1:不选择
- SL-C(SI,控制系统)2:SR 3.4
- SL-C(SI,控制系统)3:SR 3.4(1)
- SL-C(SI,控制系统)4:SR 3.4(1)

7.7 SR 3.5——输入检验

7.7.1 要求

控制系统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。

7.7.2 原由和附加指南

宜设置控制系统输入的有效语法的检查规则,例如设置检查点,在输入信息时验证此信息未被篡改并符合规范。传递给解释器的输入宜预先筛选,以防止被无意地解析为命令。注意,这是一个安全 SR,因此没有涉及人为错误,例如,提供超出预期范围的合法整数。

普遍接受的工业实践是输入数据验证,包括预定义字段值超出范围、数据字段的无效字符、缺失或不完整的数据和缓冲区溢出。更多关于无效的输入导致系统安全问题的例子包括 SQL 注入攻击,跨站脚本或畸形数据包(通常由协议模糊器生成)。要考虑的指导原则可能包括开放 Web 应用安全项目(OWASP)[31]代码审查指南。

7.7.3 增强要求

无。

7.7.4 信息安全等级

与 SR 3.5——输入合法性相关的四个 SL 等级要求如下：

- SL-C(SI,控制系统)1:SR 3.5
- SL-C(SI,控制系统)2:SR 3.5
- SL-C(SI,控制系统)3:SR 3.5
- SL-C(SI,控制系统)4:SR 3.5

7.8 SR 3.6——确定性输出

7.8.1 要求

控制系统应提供在受到攻击后正常的操作不能保持时，设定输出为预定义状态的能力。

7.8.2 原由和附加指南

针对控制系统威胁行为的确定性输出是保证正常操作完整性的重要特征。理想情况下，控制系统在受到攻击时，操作继续保持正常，但如果控制系统不能维持正常运作，则控制系统输出为预设的失败状态。适当的控制系统预定义状态输出依赖于应用，并可以是下列使用者可配置的选项之一：

失能——输出失效至无动力状态

保持——输出失效至最后已知的正常值

固定——输出失效至由资产所有者或者应用程序确定的固定值

7.8.3 增强要求

无。

7.8.4 信息安全等级

与 SR 3.6——确定性输出相关的四个 SL 等级要求如下：

- SL-C(SI,控制系统)1:SR 3.6
- SL-C(SI,控制系统)2:SR 3.6
- SL-C(SI,控制系统)3:SR 3.6
- SL-C(SI,控制系统)4:SR 3.6

7.9 SR 3.7——出错处理

7.9.1 要求

控制系统应在有效的补救条件下，识别和处理错误状况。这一行为不应暴露可能被对手利用来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。

7.9.2 原由和附加指南

出错信息的结构和内容宜由产品供应商和/或系统集成商仔细考虑。由控制系统生成的出错信息宜提供及时和有用的信息，而不会暴露出可以被对手利用来攻击 IACS 的潜在有害的信息。因为不清楚是否因信息安全事件产生特定出错情况，所以可能需要在事件响应过程中很方便地获得所有的出错信息。是否披露这些信息宜取决于出错情况及时解决的必要性。要考虑的指导原则可能包括 OWASP 代码审查指南[31]。

7.9.3 增强要求

无。

7.9.4 信息安全等级

与 SR 3.6——出错处理相关的四个 SL 等级要求如下：

- SL-C(SI,控制系统)1:不选择
- SL-C(SI,控制系统)2:SR 3.7
- SL-C(SI,控制系统)3:SR 3.7
- SL-C(SI,控制系统)4:SR 3.7

7.10 SR 3.8——会话完整性

7.10.1 要求

控制系统应提供保护会话完整性的能力。控制系统应拒绝任何非法会话 ID 的使用。

7.10.2 原由和附加指南

这种控制的重点是会话层次的通信保护,包括数据包。这种控制的目的是通信会话两端之间建立对另一方当前身份和传输信息的有效性的信任的基础。例如,这种控制应对中间人攻击,包括会话劫持,将虚假信息插入会话或重放攻击。会话完整性机制的使用将显著增加系统开销,因此它们的使用宜考虑通信实时性要求。

7.10.3 增强要求

7.10.3.1 SR 3.8 RE 1——会话结束后使会话 ID 失效

控制系统应提供在使用者退出或其他会话结束(包括浏览器会话)后使会话 ID 失效的能力。

7.10.3.2 SR 3.8 RE 2——唯一性会话 ID 生成

控制系统应提供为每一个会话生成唯一的会话 ID 和将所有非期望的会话 ID 视为非法 ID 的能力。

7.10.3.3 SR 3.8 RE 3——会话 ID 的随机性

控制系统应根据常用的可接受的随机源,提供产生唯一性会话 ID 的能力。

注：会话劫持和中间人攻击或者错误信息注入经常利用容易猜测的会话 ID(口令或者其他共享密钥)或者会话结束后没有适时地使会话 ID 失效。因此会话权限的合法性检验需要和会话生命周期紧密关联。使用随机方式生成唯一的未来会话 ID,有助于阻止暴力攻击。

7.10.4 信息安全等级

与 SR 3.6——会话完整性相关的四个 SL 等级要求如下：

- SL-C(SI,控制系统)1:不选择
- SL-C(SI,控制系统)2:SR 3.8
- SL-C(SI,控制系统)3:SR 3.8(1)(2)
- SL-C(SI,控制系统)4:SR 3.8(1)(2)(3)

7.11 SR 3.9——审计信息保护

7.11.1 要求

控制系统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。

7.11.2 原由和附加指南

审计信息包含所有需要成功审计控制系统活动的信息(例如,审计记录、审计设置和审计报告)。审计信息对错误纠正、安全破坏恢复、调查和相关工作是重要的。防止修改和删除等增强保护机制包括把审计信息存储在一次性写入的硬件介质中。

7.11.3 增强要求

7.11.3.1 SR 3.9 RE 1——一次性写入介质的审计记录

控制系统应提供把审计记录写入一次性硬件介质的能力。

7.11.3.2 空白

7.11.4 信息安全等级

与 SR 3.6——审计信息保护相关的四个 SL 等级要求如下:

- SL-C(SI,控制系统)1:不选择
- SL-C(SI,控制系统)2:SR 3.9
- SL-C(SI,控制系统)3:SR 3.9
- SL-C(SI,控制系统)4:SR 3.9(1)

8 FR 4——数据保密性

8.1 目的和 SL-C(DC)描述

确保通信信道和数据仓库的信息保密性,防止未经授权的披露。

SL 1——防止窃听或不经意的暴露导致的未经授权的信息披露。

SL 2——防止未经授权地将信息泄露给通过少量资源、通用技能和低动机的简单手段主动进行信息搜索的实体。

SL 3——防止未经授权地将信息泄露给通过一般资源、IACS 特殊技能和一般动机的复杂手段主动进行信息搜索的实体。

SL 4——防止未经授权地将信息泄露给通过扩展资源、IACS 特殊技能和高动机的复杂手段主动进行信息搜索的实体。

8.2 原由

一些控制系统生成的信息,无论是静态还是传输状态,都具有保密性或敏感性。因此,需要保护相关通信信道和数据存储以防止窃听和未经授权访问。

8.3 SR 4.1——信息保密性

8.3.1 要求

在信息存储或传输时,控制系统应具有通过明确的读授权来提供信息保密性的能力。

8.3.2 原由与附加指南

信息存储或传输时,均可通过物理手段、数据分段或数据加密的技术手段,来对信息进行保护。所选的技术关键要考虑到对控制系统性能的潜在影响和系统从故障或攻击中恢复的能力。

是否对一段信息进行保密性防护取决于此信息的内容，而非产品设计之初就能确定。事实上通过明确的授权访问配置来限制对信息的访问，表明组织认为该信息是保密的。因此，需要控制系统分配明确的读授权的所有信息，宜被认为是保密的，因此控制系统宜提供保护能力。

不同的组织和行业可以根据信息的敏感性、行业标准和指导要求，针对不同类别的信息采取不同级别的加密强度等级(见 8.5，SR 4.3——使用加密技术)。在一些场景中，可认为在交换机、路由器中保存和处理的网络配置信息需要保密。

含有明文信息传输的通信很有可能受到窃听或篡改。如果控制系统依赖于外部的通信服务供应商，就可能更难获得对通信保密性实施信息安全所要求的必要保障。在此情况下，应用补偿对抗措施是合适的，否则将接受额外的风险。

使用便携式设备、移动设备(例如，工程用笔记本电脑和 U 盘)时，实体也宜注意信息保密性。

如“5.7，SR 1.5——鉴别器管理”所要求的，鉴别信息，例如口令等，应视为保密信息，且绝不以明文形式进行发送。

8.3.3 增强要求

8.3.3.1 SR 4.1 RE 1——静态或通过不可信网络传输的保密性保护

控制系统应提供保护静态信息和通过不可信网络的远程访问的会话信息的保密性的能力。

注：加密是常用的机制，以保证信息保密性。

8.3.3.2 SR 4.1 RE 2——跨区域边界的保密性保护

当信息穿过任何区域边界时，控制系统应提供保护其保密性的能力。

8.3.4 信息安全等级

与 SR 4.1——信息保密性相关的 4 个 SL 等级要求如下：

- SL-C(DC，控制系统)1：SR 4.1
- SL-C(DC，控制系统)2：SR 4.1(1)
- SL-C(DC，控制系统)3：SR 4.1(1)
- SL-C(DC，控制系统)4：SR 4.1(1)(2)

8.4 SR 4.2——剩余信息

8.4.1 要求

控制系统应提供这样的能力，清除不再使用的和/或退役组件上的具有明确读授权访问的信息。

8.4.2 原由和附加指南

移除控制系统现役组件时，宜避免具有明确读授权访问的信息不经意的泄露。例如，储存在非易失性存储器内的“加入密钥”(用于无线现场设备)或其他可能促成未授权活动或恶意活动的密码信息。

由使用者或角色的行为(或代表一个使用者或角色的软件进程的行为)所产生的信息不宜以不受控的方式泄露给不同的使用者或角色。对控制系统信息或剩余数据的控制，可防止共享资源释放回控制系统后存储在共享资源中的信息不经意的泄露。

8.4.3 增强要求

8.4.3.1 SR 4.2 RE 1——共享内存资源的清除

控制系统应提供防止通过易失性共享内存资源未授权地和不经意地传输信息的能力。

注：易失性存储资源在被释放到内存管理后不再保留信息。但是，针对随机存取存储器(RAM)的攻击有能力在其被复写前提取关键资料或其他保密数据。因此，一种普遍接受的实践是，当易失性共享内存释放回工业控制系统由不同使用者使用时，从内存中清除所有独特的数据及其相关信息，这样，这些数据对新使用者而言就是不可见或不可访问的了。

8.4.3.2 空白

8.4.4 信息安全等级

与 SR 4.2——信息留存有关的四个 SL 等级要求是：

- SL-C(DC，控制系统)1：不选择
- SL-C(DC，控制系统)2：SR 4.2
- SL-C(DC，控制系统)3：SR 4.2(1)
- SL-C(DC，控制系统)4：SR 4.2(1)

8.5 SR 4.3——加密的使用

8.5.1 要求

若控制系统要求使用加密，应按照公认的安全行业实践和建议采用合适的加密算法、密钥长度和机制进行密钥的建立与管理。

8.5.2 原由和附加指南

加密保护的选择宜与被保护信息的价值、信息保密性被破坏的后果、信息保密和控制系统操作受限的时间周期相匹配。这可能涉及信息存储、传输或两者兼而有之。需要注意的是，备份也是存储信息的一个例子，宜被认为是数据保密性评估过程的一部分。控制系统产品的供应商宜记录密钥建立和管理的实践和规程。控制系统宜根据指定的标准使用经过测试的加密算法和哈希算法，例如高级加密标准(AES)和安全哈希算法(SHA)系列，和密钥长度。密钥生成需要使用有效的随机数发生器来执行。密钥管理的信息安全策略和规程需要按照规定的标准处理密钥的周期性变化、密钥的消除、密钥的分配和加密密钥的备份。可以在 NIST SP800-57[25] 中找到通用可接受的实践和推荐。可以在例如 ISO/IEC 19790[12] 中找到实施要求。

当满足本标准中定义的许多其他要求时，这个 SR 与 5.10，SR 1.8-公钥基础设施(PKI)证书都可以适用。

8.5.3 增强要求

无。

8.5.4 信息安全等级

与 SR 4.3——加密的使用有关的四个 SL 等级要求如下：

- SL-C(DC，控制系统)1：SR 4.3
- SL-C(DC，控制系统)2：SR 4.3
- SL-C(DC，控制系统)3：SR 4.3
- SL-C(DC，控制系统)4：SR 4.3

9 FR 5——受限的数据流

9.1 目的和 SL-C(RDF)描述

通过区域与管道划分，对控制系统进行分段来限制非必需的数据流。

SL 1——防止不经意地、或巧合地规避区域与管道划分措施。

SL 2——防止实体采用少量资源、通用技能、低动机的简单方法来有意规避区域与管道划分措施。

SL 3——防止实体采用一般资源、IACS 特殊技能、一般动机的复杂方法来有意规避区域与管道划分措施。

SL 4——防止实体采用扩展资源、IACS 特殊技能、高动机的复杂方法来有意规避区域与管道划分措施。

9.2 原由

资产所有者需要使用风险评估的方法来确定必要的信息流量限制，进而确定传递信息的管道配置。衍生的规范性建议和指南宜包含从断开控制系统网络与业务或公共网络的连接，到使用单向网关、基于状态检测的防火墙和 DMZ 等手段，以管理信息流。

9.3 SR 5.1——网络分段

9.3.1 要求

控制系统应提供将控制系统网络与非控制系统网络进行逻辑分段，将关键控制系统网络和其他控制系统网络进行逻辑分段的能力。

9.3.2 原由和附加指南

网络分段可用于多种目的，包括网络安全。网络分段的主要原因是降低流入控制系统网络数据的量或暴露程度，以及降低流出控制系统网络数据的量或传播广度。网络分段可以提高整个系统的响应性和可靠性，并提供一种网络安全保护措施。同时，在控制系统中允许不同的网络分段，包括为了提高安全等级，对关键控制系统和安全相关系统与其他系统进行分段。

从控制系统到万维网的访问宜根据控制系统的运行需求进行明确的界定。

控制系统网络分段和它提供的保护等级将很大程度上取决于资产所有者、甚至系统集成商使用的整体网络架构。基于功能的网络逻辑分段提供了某些防护手段，但仍可能因一个设备的失效而导致单点故障；网络物理分段通过排除单点故障来提供另一个层面上的保护，但会导致网络设计更复杂、成本更高。在网络设计的过程中，需要综合评估折衷的方案(见 IEC 62443-2-1)。

对一个事件的响应，可能需要切断不同网络分段之间的连接。在这种情况下，支持基本操作的服务宜保持在这样一个状态，使设备能连续操作和/或以有序的方式正确地进行关停操作。这就要求控制系统网络中的某些服务器需要备份服务器以支持一些常用的网络功能，例如动态主机配置协议(DHCP)、域名服务(DNS)或本地的认证机构(CA)。这也意味着，一些关键控制系统和安全相关系统的设计，需要从一开始就与其他网络完全隔离。

9.3.3 增强要求

9.3.3.1 SR 5.1 RE 1——物理网络分段

控制系统应提供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其他非关键控制系统网络进行物理分段的能力。

9.3.3.2 SR 5.1 RE 2——与非控制系统网络的独立

控制系统应提供在不与非控制系统网络相连的情况下，无论关键与否，向控制系统网络提供网络服务的能力。

9.3.3.3 SR 5.1 RE 3——关键网络的逻辑和物理隔离

控制系统应提供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的能力。

9.3.4 信息安全等级

与 SR 5.1——网络分段相关的四个 SL 等级要求是:

- SL-C(RDF,控制系统)1:SR 5.1
- SL-C(RDF,控制系统)2:SR 5.1(1)
- SL-C(RDF,控制系统)3:SR 5.1(1)(2)
- SL-C(RDF,控制系统)4:SR 5.1(1)(2)(3)

9.4 SR 5.2——区域边界防护

9.4.1 要求

控制系统应提供监视和控制区域边界通信的能力,以实现基于风险的区域和管道模型定义的划分。

9.4.2 原由和附加指南

任何与外部网络或其他控制系统的连接宜通过可管理的接口,接口由适当的边界防护设备组成(例如代理、网关、路由器、防火墙、单向网关、防护装置和加密通道),并设置成有效的体系架构(例如保护应用网关的防火墙应位于 DMZ 区)。任何备用站点控制系统的边界保护也宜提供与主站同等的防护等级。

作为纵深防御战略的一部分,有更大影响的控制系统宜被划分成不同的单独区域,按照安全策略、规程或风险评估结果使用管道来限制或禁止网络访问。SL-T(系统)分类可指导选择合适的区域划分方式(见 IEC 62443-3-2[8])。

9.4.3 增强要求

9.4.3.1 SR 5.2 RE 1——默认拒绝,例外允许

控制系统应提供默认拒绝所有网络数据流,例外允许网络数据流(也称为拒绝所有,允许例外)的能力。

9.4.3.2 SR 5.2 RE 2——孤岛模式

控制系统应提供阻止任何通过控制系统边界通信的能力(也称为孤岛模式)。

注:何时应用这种能力的例子包括,在控制系统内部检测到安全事件或者安全攻击正在企业级网络发生时(见 4.2,基本功能支持)。

9.4.3.3 SR 5.2 RE 3——失效关闭

当边界防护机制出现操作失效时,控制系统应提供阻止所有控制系统边界通信的能力(也称为失效关闭)。失效关闭功能的设计不应干扰 SIS 或其他安全相关功能的运行。

注:何时应用这种能力的例子包括掉电、硬件故障所导致的边界防护设备功能降级或完全失效(见 4.2,基本功能支持)。

9.4.4 信息安全等级

与 SR 5.2——区域边界防护有关的四个 SL 等级要求是:

- SL-C(RDF,控制系统)1:SR 5.2
- SL-C(RDF,控制系统)2:SR 5.2(1)
- SL-C(RDF,控制系统)3:SR 5.2(1)(2)(3)
- SL-C(RDF,控制系统)4:SR 5.2(1)(2)(3)

9.5 SR 5.3——普通目的的个人间通信限制

9.5.1 要求

控制系统应提供阻止接收来自控制系统外的使用者或系统的普通意图的个人间通信消息的能力。

9.5.2 原由和附加指南

普通的个人间通信系统包括但不限于:电子邮件系统、社交媒体(例如 Twitter、Facebook、图片库等)或允许任意类型的可执行文件传输的通信系统。这些系统通常用作与控制系统操作无关的私人目的,因此其所增加的风险通常会超过收益。

此类普通目的的通信系统通常被用作攻击媒介向控制系统引入恶意软件,向控制系统外部位置传递可读授权的信息和引入过量网络负载,这些可能产生安全问题或被利用发起针对控制系统的攻击。很多其他系统要求所涉及的应用,例如,大范围的其他系统要求应用,包括本标准中描述的针对个人间通信系统的使用限制和受限的数据流,可以提供充分的补偿对抗措施来满足这个要求。

控制系统可以提供使用此类双向通信系统的能力,但仅限于控制系统内服务器和/或工作站间的通信。需要注意的是,此 SR 需要支持 8.3 SR 4.1——信息保密性相关的要求。

控制系统可以限制电子邮件或其他消息传送方案,这些方式利用出站消息提供内部电脑到外部电脑的通信。这些内部到外部的通信可以被限制为仅允许发送系统警示或者其他由计算机生成的信息消息给控制系统外的使用者或系统。为了防止具有明确读授权的信息被传递,预置的消息(可以将内容限定在一定范围内)宜被用于传递警示或状态信息。在系统生成消息时,可以不让使用者添加附件或其他信息作为出站消息。

9.5.3 增强要求

9.5.3.1 SR 5.3 RE 1——禁止所有普通目的的个人间通信

控制系统应提供禁止传输、接收个人间消息的能力。

9.5.3.2 空白

9.5.4 信息安全等级

与 SR 5.3——普通目的的个人间通信限制有关的四个 SL 等级要求是:

- SL-C(RDF,控制系统)1:SR 5.3
- SL-C(RDF,控制系统)2:SR 5.3
- SL-C(RDF,控制系统)3:SR 5.3(1)
- SL-C(RDF,控制系统)4:SR 5.3(1)

9.6 SR 5.4——应用划分

9.6.1 要求

控制系统应提供根据重要程度对数据、应用和服务进行划分的能力,以方便实施分区模型。

9.6.2 原由和附加指南

应用划分可通过使用不同的计算机、不同的中央处理单元、不同的操作系统实例、不同的网络地址以及这些方法的组合或其他恰当方法，运用物理或逻辑手段来实现。应用或服务划分的例子，包括但不仅限于，应急和/或安全系统、闭环控制应用、操作员站以及工程师站。

9.6.3 增强要求

无。

9.6.4 信息安全等级

与 SR 5.4——应用划分有关的四个 SL 等级要求如下：

- SL-C(RDF，控制系统)1：SR 5.4
- SL-C(RDF，控制系统)2：SR 5.4
- SL-C(RDF，控制系统)3：SR 5.4
- SL-C(RDF，控制系统)4：SR 5.4

10 FR 6——对事件的及时响应

10.1 目的和 SL-C(TRE)描述

在事故被发现时，对安全违规的响应包括通知权利部门，汇报所需的安全违规证据，并及时采取纠正措施。

- SL 1——监视 IACS 操作，当事故被发现时，通过收集与提供用于质询的司法证据进行事故响应。
- SL 2——监视 IACS 操作，当事故被发现时，通过主动收集并周期性汇报司法证据进行事故响应。
- SL 3——监视 IACS 操作，当事故被发现时，通过主动收集并尽力向相关权利机构提供司法证据进行事故响应。
- SL 4——监视 IACS 操作，当事故被发现时，通过主动收集并向相关权利机构准实时提供司法证据进行事故响应。

10.2 原由

资产所有者宜通过他们的风险评估方法学，建立安全策略、规程以及所需的、适当的通信和控制线路，来响应安全违规。衍生的规范性建议和指南宜包括收集、报告、保存和自动关联司法证据的机制，以确保及时采取纠正措施。监视工具和技术的使用不宜对控制系统的运行性能产生不利影响。

10.3 SR 6.1——审计日志可访问性

10.3.1 要求

控制系统应提供授权人员和/或工具以只读方式访问审计日志的能力。

10.3.2 原由和附加指南

控制系统生成有关该系统中所发生事件的审计记录(见 6.10，SR 2.8——可审计事件)。为了支持审计日志的筛选，冗余信息的鉴定和移除，安全事故事后调查期间的审查和报告活动，访问这些审计日

志是有必要的。该访问不宜更改原始审计记录。一般来说,审计提炼和报告的生成宜由独立的信息系统执行。手动访问审计记录(例如,屏幕浏览或打印输出)足以符合基本要求,但其对于更高级别的 SL 则是不充分的。编程访问一般用于为分析机制提供审计日志信息,如 SIEM 等。关于审计日志的创建、保护和访问的 SR,详见第 5 章、第 6 章和第 9 章。

10.3.3 增强要求

10.3.3.1 SR 6.1 RE 1——审计日志的编程访问

控制系统应提供使用应用编程接口(API)编程访问审计记录的能力。

10.3.3.2 空白

10.3.4 信息安全等级

与 SR 6.1——审计日志可访问性相关的四个 SL 要求为:

- SL-C(TRE,控制系统)1:SR 6.1
- SL-C(TRE,控制系统)2:SR 6.1
- SL-C(TRE,控制系统)3:SR 6.1(1)
- SL-C(TRE,控制系统)4:SR 6.1(1)

10.4 SR 6.2——连续监视

10.4.1 要求

控制系统应通过普遍接受的的安全行业实践和建议,提供针对所有安全机制的连续监视能力,以便及时检测、描述和报告安全漏洞。

注:响应时间是本地事务,超出本标准范畴。

10.4.2 原由和附加指南

控制系统的监视能力可通过多种工具和技术完成(例如,IDS、IPS、恶意代码防护机制和网络监视机制)。随着攻击变得更复杂,这些监视工具和技术将需要同时变得更加复杂,例如包括基于行为分析的 IDS/IPS。

宜在控制系统内(例如,选定的周边位置以及支持关键应用的服务器群附近)战略性部署监视设备来收集基本信息。监视机制也可能部署在控制系统内的特定位置,用来追踪特定的事务。

监视宜包括适当的报告机制,以允许及时的事件响应。为了使报告聚焦,并使得所报告的信息量达到接收者所能处理的程度,类似于 SIEM 的机制被广泛用于关联各个事件的汇总报告,用于记录大量发生的原始事件内容。

此外,这些机制可被用于追踪控制系统安全变化的影响(见 6.10,SR 2.8——可审计事件)。预先安装的取证工具有助于事件分析。

10.4.3 增强要求

无。

10.4.4 信息安全等级

与 SR 6.2——连续监视相关的四个 SL 要求如下:

- SL-C(TRE,控制系统)1:不选择

- SL-C(TRE,控制系统)2:SR 6.2
- SL-C(TRE,控制系统)3:SR 6.2
- SL-C(TRE,控制系统)4:SR 6.2

11 FR 7——资源可用性

11.1 目的和 SL-C(RA)描述

确保控制系统的可用性,以应对基本服务降级或被拒绝。

- SL 1——确保控制系统在正常生产条件下可靠运行,并防止由一个实体的不经意的或巧合的行为导致的 DoS 状况。
- SL 2——确保控制系统在正常和异常生产条件下可靠运行,并防止由实体使用少量资源、通用技能和低动机的简单手段导致的 DoS 状况。
- SL 3——确保控制系统在正常、异常和极端生产条件下可靠运行,并防止由实体使用一般资源、IACS 特殊技能和一般动机的复杂手段导致的 DoS 状况。
- SL 4——确保控制系统在正常、异常和极端生产条件下可靠运行,并防止由实体使用扩展资源、IACS 特殊技能和高动机的复杂手段导致的 DoS 状况。

11.2 原由

本系列 SR 的目的是在应对各种 DoS 事件时,确保控制系统是能复原的。这包括部分或全部系统功能在不同级别上的不可用性。特别是,控制系统中的安全事故不宜对 SIS 或其他功能安全相关功能造成影响。

11.3 SR 7.1——拒绝服务保护

11.3.1 要求

控制系统应提供在 DoS 事件时在降级模式下运行的能力。

11.3.2 原由和附加指南

存在各种技术可限制,或者在某些情况下消除 DoS 状况的影响。例如,边界保护设备可筛选特定类型的数据包,以保护设备在内部可信赖的网络上运行并避免受到 DoS 事件的直接影响,或者限制信息流的单向外传。特定而言,如第 4 章所示,针对控制系统的 DoS 事件不宜对任何安全相关系统造成不利影响。

11.3.3 增强要求

11.3.3.1 SR 7.1 RE 1——管理通信负荷

控制系统应提供管理通信负荷(例如,通过速率限制),以便减轻 DoS 事件中信息泛滥影响的能力。

11.3.3.2 SR 7.1 RE 2——限制 DoS 影响其他系统或网络

控制系统应提供限制所有使用者(人员、软件进程和设备等)导致的 DoS 事件影响其他控制系统或网络的能力。

11.3.4 信息安全等级

与 SR 7.1——拒绝服务保护相关的四个 SL 等级要求为:

- SL-C(RA,控制系统)1:SR 7.1
- SL-C(RA,控制系统)2:SR 7.1(1)
- SL-C(RA,控制系统)3:SR 7.1(1)(2)
- SL-C(RA,控制系统)4:SR 7.1(1)(2)

11.4 SR 7.2——资源管理

11.4.1 要求

控制系统应提供通过安全功能限制资源使用的能力,以防止资源耗尽。

11.4.2 原由和附加指南

资源管理(例如,网络分段或优先方案)防止一个有较低优先权的软件进程对控制系统内任何有较高优先权的软件进程造成延迟或干扰。例如,启动网络扫描,对一个操作系统进行修补和/或反病毒检查,可对正常操作造成严重干扰。数据流速率限制方案宜被作为一种缓解技术。

11.4.3 增强要求

无。

11.4.4 信息安全等级

与 SR 7.2——资源管理相关的四个 SL 等级要求如下:

- SL-C(RA,控制系统)1:SR 7.2
- SL-C(RA,控制系统)2:SR 7.2
- SL-C(RA,控制系统)3:SR 7.2
- SL-C(RA,控制系统)4:SR 7.2

11.5 SR 7.3——控制系统备份

11.5.1 要求

控制系统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,以及使用者级和系统级的信息备份(包括系统状态信息)的能力。

11.5.2 原由和附加指南

最新备份的可用性对于控制系统故障和/或错误配置的恢复是很重要的。这一功能的自动运行可确保所有需要的文件被备份,并减少操作者的额外开销。尽管控制系统恢复不常使用,用于事后取证活动的信息(例如,审计日志)宜明确包含在备份中(详见 10.4,SR 6.2——连续监视)。如果最终备份包含保密性信息,则宜考虑加密(见 8.5,SR 4.3——加密使用)。

11.5.3 增强要求

11.5.3.1 SR 7.3 RE 1——备份验证

控制系统应提供验证备份机制可靠性的能力。

11.5.3.2 SR 7.3 RE 2——备份自动化

控制系统应提供根据可配置的频率自动进行备份的能力。

11.5.4 信息安全等级

与 SR 7.3——控制系统备份相关的四个 SL 等级要求为：

- SL-C(RA,控制系统)1:SR 7.3
- SL-C(RA,控制系统)2:SR 7.3(1)
- SL-C(RA,控制系统)3:SR 7.3(1)(2)
- SL-C(RA,控制系统)4:SR 7.3(1)(2)

11.6 SR 7.4——控制系统恢复和重构

11.6.1 要求

控制系统在受到破坏或发生失效后，应提供恢复和重构控制系统到一个已知的安全状态的能力。

11.6.2 原由和附加指南

恢复和重构控制系统到一个已知的安全状态，意味着所有系统参数(无论是缺省参数还是可配置参数)均被设为安全值，同时重新安装关键的安全补丁，并重新设置安全相关的配置参数，系统文件和操作进程应是可用的，应在安全设置下重新安装和配置应用和系统软件，信息是最新的，装载的是已知的安全备份信息并且应对系统进行充分测试和功能验证。

11.6.3 增强要求

无。

11.6.4 信息安全等级

与 SR 7.4——控制系统恢复和重构相关的四个 SL 等级要求如下：

- SL-C(RA,控制系统)1:SR 7.4
- SL-C(RA,控制系统)2:SR 7.4
- SL-C(RA,控制系统)3:SR 7.4
- SL-C(RA,控制系统)4:SR 7.4

11.7 SR 7.5——应急电源

11.7.1 要求

控制系统应提供应急电源切换能力，这种切换应不影响当前的安全状态或文档定义的降级模式。

11.7.2 原由和附加指南

存在这样的实例，例如作为补偿对抗措施的物理门禁可能受电源供应失效影响，此时应急电源宜能够用于供应相关系统。如果不能，则应在发生此类紧急情况的时候，采取其他补偿对抗措施。

11.7.3 增强要求

无。

11.7.4 信息安全等级

与 SR 7.5——应急电源相关的四个 SL 等级要求如下：

- SL-C(RA,控制系统)1:SR 7.5

- SL-C(RA,控制系统)2:SR 7.5
- SL-C(RA,控制系统)3:SR 7.5
- SL-C(RA,控制系统)4:SR 7.5

11.8 SR 7.6——网络和安全配置设置

11.8.1 要求

控制系统应提供这样的能力,根据控制系统供应商提供的指南中推荐的网络和安全配置进行系统设置。该控制系统应为当前部署的网络和安全配置设置提供一个接口。

11.8.2 原由和附加指南

这些配置设置属于控制系统组件的可调节参数。为了能够检测并纠正与经过检验的和/或所推荐的配置设置的任何偏离,控制系统需要根据安全策略和规程支持监视和控制配置变更。为了增强安全性,可通过代理软件自动收集当前设置并与已批准的设置相比较,实施自动化检查。

11.8.3 增强要求

11.8.3.1 SR 7.6 RE 1——当前安全设置的机器可读报告

控制系统应提供以机器可读格式生成当前安全设置列表报告的能力。

11.8.3.2 空白

11.8.4 信息安全等级

与 SR 7.6——网络和安全配置设置相关的四个 SL 等级要求如下:

- SL-C(RA,控制系统)1:SR 7.6
- SL-C(RA,控制系统)2:SR 7.6
- SL-C(RA,控制系统)3:SR 7.6(1)
- SL-C(RA,控制系统)4:SR 7.6(1)

11.9 SR 7.7——最小功能

11.9.1 要求

控制系统应提供明确阻止和/或限制使用不必要功能、端口、协议和/或服务的能力。

11.9.2 原由和附加指南

控制系统能够提供多种功能和服务。其中一些功能和服务对于支持基本功能可能是不必要的。因此,宜默认禁用超过基线配置以上的功能。此外,有时候控制系统单个组件提供多种服务是很方便的,但是相对于限制组件所提供的服务,这种做法会增加风险。由商用现货设备普遍提供的许多功能和服务可进行裁剪,如电子邮件、互联网语音传输协议(VoIP)、即时通讯(IM)、文件传输协议(FTP)、超文本传输协议(HTTP)和文件共享等。

11.9.3 增强要求

无。

11.9.4 信息安全等级

与 SR 7.7 最小功能性相关的四个 SL 等级要求为：

- SL-C(RA,控制系统)1:SR 7.7
- SL-C(RA,控制系统)2:SR 7.7
- SL-C(RA,控制系统)3:SR 7.7
- SL-C(RA,控制系统)4:SR 7.7

11.10 SR 7.8——控制系统组件详细目录

11.10.1 要求

控制系统应提供报告当前已安装组件及其相关特性列表的能力。

11.10.2 原由和附加指南

一个控制系统组件详细目录可能包括但不仅限于组件 ID、能力和修订版本。组件详细目录宜与 SuC 相一致。宜部署正式的配置管理过程，以保持对组件详细目录基线变化的控制(详见 IEC 62443-2-1)。

11.10.3 增强要求

无。

11.10.4 信息安全等级

与 SR 7.8——控制系统组件详细目录相关的四个 SL 等级要求如下：

- SL-C(RA,控制系统)1:不选择
- SL-C(RA,控制系统)2:SR 7.8
- SL-C(RA,控制系统)3:SR 7.8
- SL-C(RA,控制系统)4:SR 7.8

附 录 A
（资料性附录）
SL 矢量讨论

注 1：本附录是基于论文《安全保证等级：描述信息安全要求的矢量方法》[28]。针对 IEC 62443 系列标准的变化及评审的意见，本附录中的内容相对于论文原文进行了修改。

注 2：本附录中的大多数内容将成为 IEC 62443-1-1 和 IEC 62443-3-2 内容。当本标准发布时，上述文件正在进行编写和/或修改，因此并未包含信息安全等级矢量的内容。本附录是为了帮助读者了解信息安全等级矢量的概念。本附录中的内容是参考性的，在其他标准文本中，将有正式内容取代本附录内容。

A.1 概述

功能安全系统已使用安全完整性等级（SIL）的概念接近二十年。这使得一个组件的功能安全完整性能力，或一个已部署的系统功能安全完整性等级可以用一个数字来表示。该数字基于组件或系统的失效概率，定义了一个保护因子，用以确保人和环境的安全与健康。计算一个安全系统所需求的保护因子过程，虽然复杂，却是可以管理的，因为组件或系统由于随机硬件失效而发生事故的概率，是可以定量计算的。根据这些失效对 HSE（健康、安全、环境）的潜在影响，可以计算出总体风险。

信息安全系统具有更多的应用，更多的结果集，以及更多的情景导致一个可能的事件。信息安全系统既保护 HSE，同时它又应该保护工业过程本身、公司专有信息、公众信任以及国家安全，此种情况下，随机的硬件失败不是失效的根本原因。在某些情况下，它可能是犯下善意错误（无意犯错误）的雇员，而在另一些情况下，它可能是一个处心积虑要制造事件并隐藏证据的蓄意攻击者。信息安全系统复杂性的上升，使得将保护因子压缩为一个数字变得更加困难。

A.2 信息安全等级

A.2.1 定义

以下是 IEC/TS 62443-1-1:2009 的 5.11.1 的一段摘录。它很好地解释了信息安全等级是什么，如何使用。

信息安全等级提供了一个定性的方法来处理一个区域的信息安全问题。作为定性的方法，信息安全等级定义用于在组织内比较和管理区域信息安全。随着越来越多的数据可用以及风险、威胁和安全事故的数学可表达程度的开发，这个概念将转变为信息安全等级（SL）的选择和验证这样的定量方法。这将对最终用户公司、IACS 供应商和信息安全产品的供应商都适用。它将被用于选择区域内使用的 IACS 设备和对抗措施，并确定和比较整个行业领域不同组织的区域安全性。

在发展的第一阶段，IEC 62443 系列标准倾向于使用定性 SL，使用术语如“低”“中”和“高”。资产所有者将针对其特定应用，提出自己的定义。IEC 62443 系列的长期目标是，将尽可能多的安全等级和要求实现定量的描述，要求和度量尽可能在多个企业和行业建立可重复应用的标准。实现这一目标需要时间，因为在工业安全系统中应用这些标准和数据需要更多的经验，来验证这个定量方法。

当把要求映射到不同的安全等级 SLs 时，标准开发者需要描述不同 SLs 及他们之间的区别的参考框架。本附录的目的是提出这样的参考框架。

A.2.2 安全等级 SLs 类型

SLs 被划分为三个不同的类型:目标、实现和能力。这些类型彼此相关,并与信息安全的全生命周期不同方面有关联。

- 目标 SL(SL-T)是一个特定系统所需要的信息安全等级。这通常都是由系统风险评估所决定的,并且这也决定了确保系统正常操作所需要的安全水平。
- 已实现的 SL(SL-A)是指一个特定系统的实际信息安全等级。在提供系统设计或系统已就位时,这些是可以度量的。这可以用于确立一个信息安全系统是否满足最初设定的 SL 目标。
- 能力 SL(SL-C)是组件或系统在合适配置的条件下能够提供的信息安全等级。这些等级陈述了一个特定组件或系统在合适的配置和集成条件下,能够满足 SL 目标,而不需要额外的补偿对抗措施。

根据 IEC 62443 系列标准,每个 SL 的目的是在所述的安全生命周期的不同阶段中使用。从特定系统的目标开始,组织将需要进行设计,其中包括达到预期效果所需要的功能要求。换句话说,设计团队将首先开发用于一个特定系统所必需的目标 SL。然后,他们将设计系统来满足这些目标,这需要一个迭代的过程,其中每次迭代后对所实现的 SL 进行测量,并与目标 SL 进行比较。作为该设计过程的一部分,设计者会选择具有必要能力 SL 的组件和系统来满足目标 SL 要求——或在这样的系统和组件不可用时,带补偿对抗措施的系统或组件可作为补充。当系统开始运行时,实际的 SL 将被测量为实现的 SL,并与目标 SL 相比。

A.2.3 使用 SLs

当设计一个新的系统(绿色区域),或修改现有的系统(棕色区域)的信息安全,第一步是将系统分成不同的区域,并定义连接这些区域的管道。如何实现这一点的详细资料在 IEC 62443-3-2 中给出。一旦该系统的区域模型建立,在结果分析的基础上,每个区域和管道被分配一个目标 SL,它描述各区域或管道所需的安全性。在此区域和管道的初始分析中,没有必要完成一个详细的系统设计。这足以描述在区域中的资产和区域之间的连接宜提供的功能,以满足安全目标。

图 A.1 和图 A.2 显示系统被分解成由管道连接的区域的高等级示例。图 A.1 是载氯卡车装载站控制系统的图形表示。配有这一图片的完整用例将在 IEC/TR 62443-1-4 进行讨论。它有五个区域:基本过程控制系统(BPCS)、SIS、控制中心、工厂 DMZ 和企业。BPCS 和 SIS 区域都使用 PLC 进行装载站不同方面的操作,SIS 采用了在安全系统使用的特殊功能安全 PLC(FS-PLC)。通过使用边界保护装置,两个 PLC 以不可路由的串行或以太网方式连接。每个 PLC 均连接到本地交换机上,通过工程师站编程,通过 HMI 操作。在 BPCS 和 SIS 区还含有一个仪表资产管理系统(IAMS)来测量和测试仪器。包含多台工作站和 BPCS 的控制中心都连接到工厂 DMZ。一个工厂 DMZ 可以容纳各种部件和系统,例如,图中所示的历史数据库和维护工作站。工厂 DMZ 连接到企业网,这个企业网包含企业无线局域网和 web 服务器。图中显示了多个域控制器和边界防护设备,一些补偿对抗措施可以用来提高安全性。

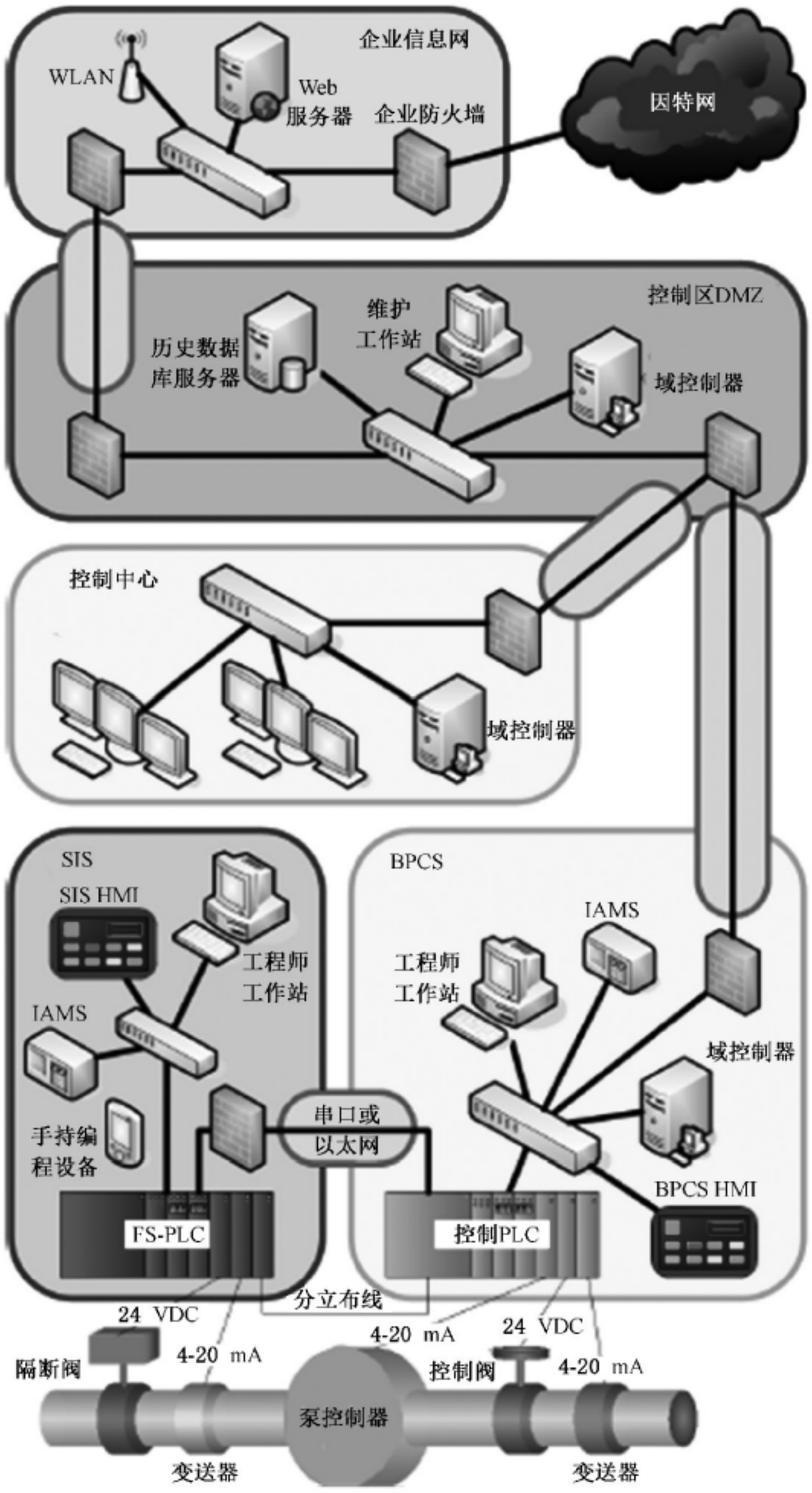

图 A.1 展示区域和管道的高等级过程工业示例

图 A.2 是一家制造工厂的示意图，定义了四个区域：企业网、工业/企业 DMZ 以及两个工业网络。企业基础设施具有无线局域网和因特网连接。许多公司通过在其系统的重要部分使用 DMZ 来隔离网络通信。在此特定示例中，每个工业网络运行相对独立，有其各自的 PLC、现场设备及人机界面。

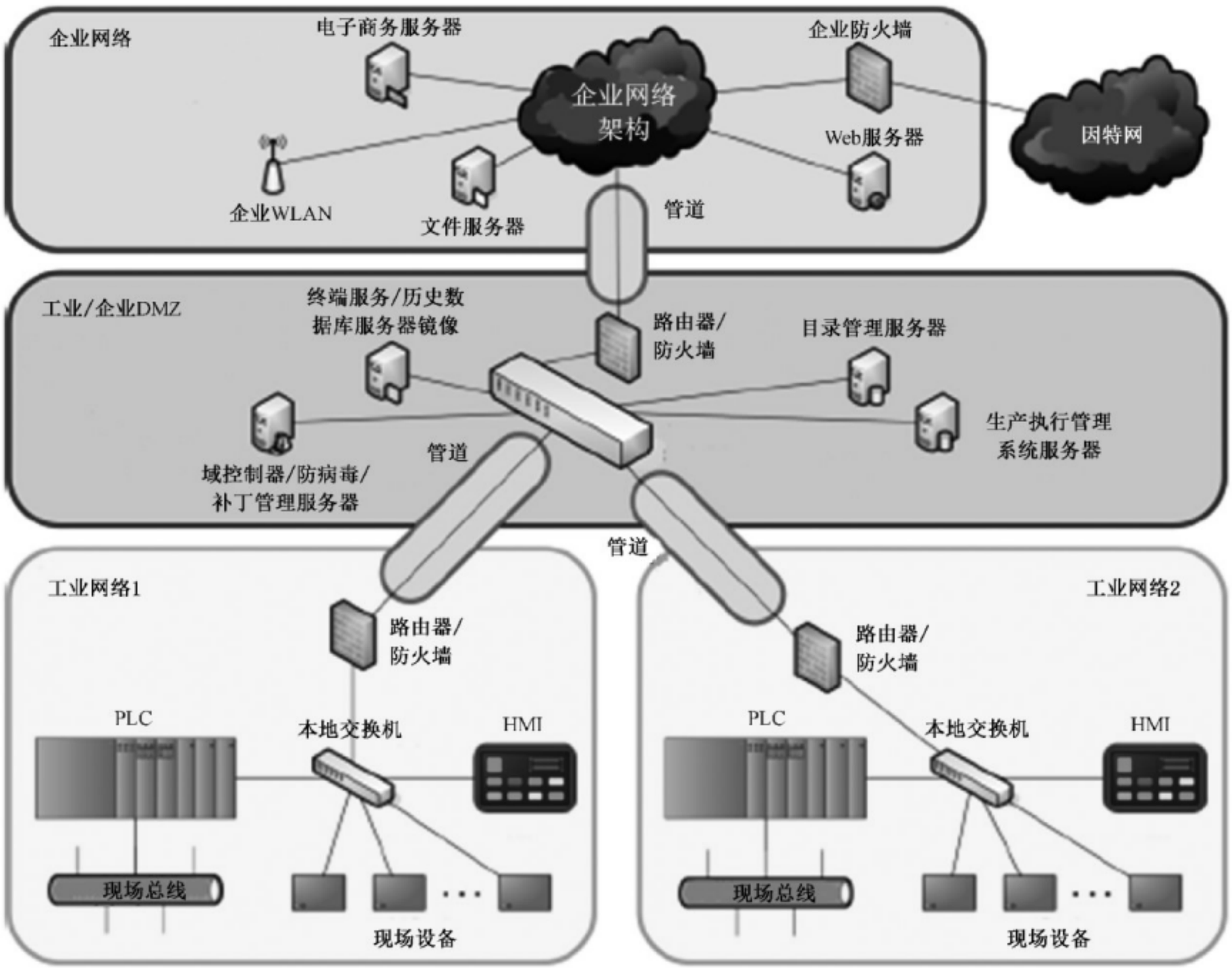

图 A.2　展示区域和管道的高等级制造工业示例

在确定目标 SL 后，系统可进行设计(绿色区域)或重新设计(棕色区域)来满足这些目标 SL。设计过程通常是在整个过程中系统设计多次与目标进行比较的迭代过程。IEC 62443 系列的多个部分包含了设计过程不同方面的编程和技术要求指南。IEC 62443-2-1 在设计过程的编程方面提供了指导，而 IEC 62443-3-3(本标准)和 IEC 62443-4-2[10] 定义了系统级和组件级的技术安全要求，以及与其相关的不同能力 SL。

在系统设计过程中有必要评估不同的组件和子系统的信息安全能力。对于不同的信息安全能力，通过比较在 IEC 62443 系列中定义的特性及能力要求，产品供应商应该对这些组件或系统提供这些信息安全能力。这些能力 SL 可用于确定一个给定的组件或系统是否能够满足目标 SL。产品供应商或系统集成商还应该提供有关如何配置组件或系统的指导，来满足声明的 SL。

在一个特定的设计中，可能会有一些组件或系统不能完全满足目标 SL。如果组件或者系统的能力 SL 低于目标 SL，那么需要考虑补偿对抗措施以满足目标 SL 的需要。补偿对抗措施可能包括更改组件或系统的设计以增加其能力，选择另一个组件或系统以满足目标 SL 或添加额外的组件或系统以满足目标 SL。在设计过程中的每次迭代后，系统设计实现的 SL 宜被重新评估，与系统的目标 SL 进行比较。

一旦系统设计得到批准和实施，该系统需要进行评估以防止或缓解系统安全等级的恶化。宜在系统修改期间或之后定期对系统进行评估。IEC 62443-2-1 对操作安全程序的必要步骤以及如何评估其有效性提供了指导。在确定实现的 SL 之后，有必要评估该系统是否仍然符合原有的目标 SL(例如，使用 IEC 62443-3-3 的系统要求)。如果系统不满足这些需求，可能有多个原因，包括缺乏维护程序或需

要重新设计系统部件。

本质上,控制系统安全能力的确定与一个给定的使用背景无关,但在给定的背景下使用是为了达到系统架构、区域和/或管道的目标 SL(见图 A.3)。

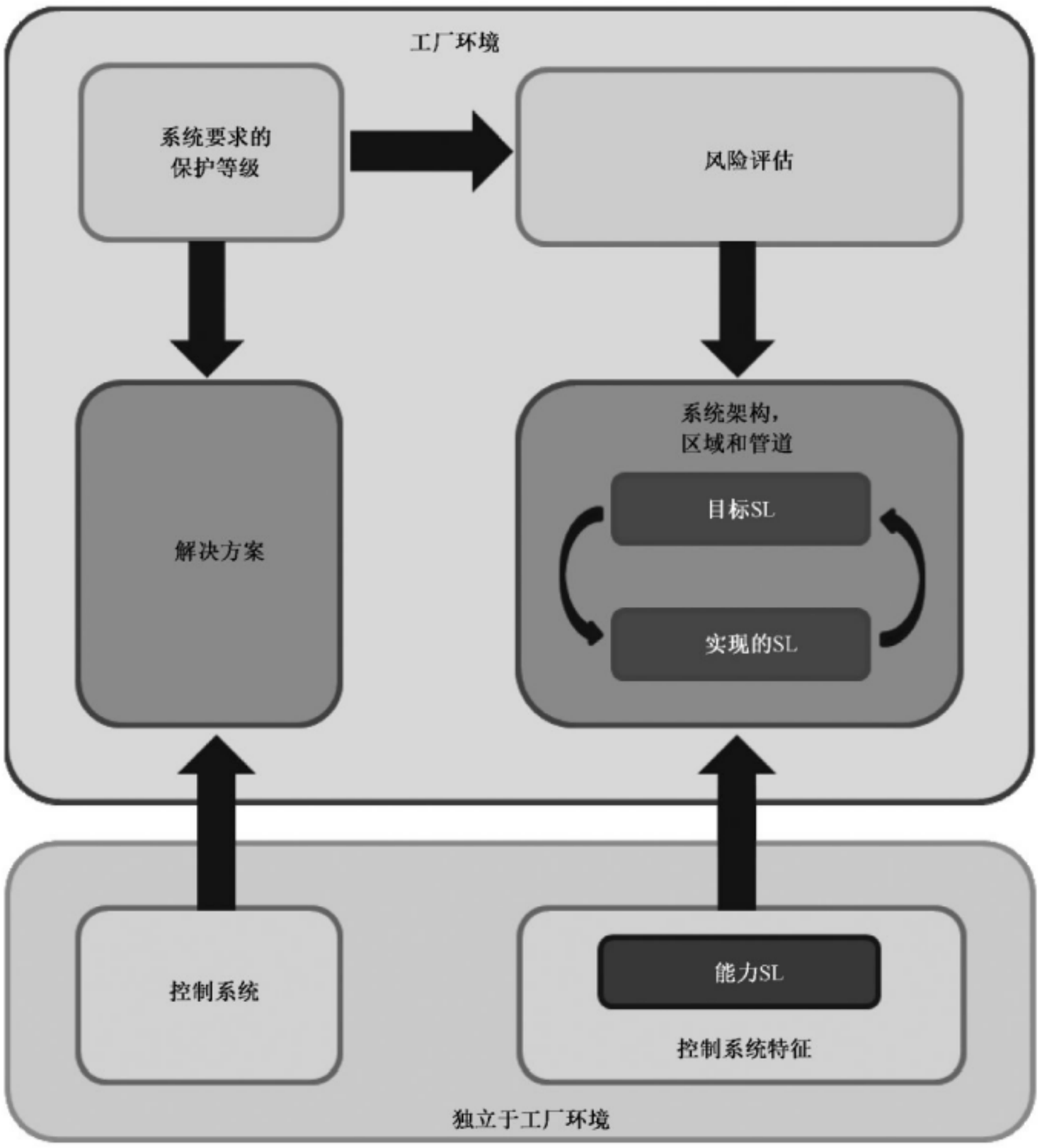

图 A.3 不同 SL 类型的使用关联性示意图

A.3 SL 矢量

A.3.1 基本要求

SL 是基于在 IEC 62443-1-1 中所定义的 7 项基本安全需求:

1) 标识和鉴别控制 Identification and authentication control(IAC);
2) 使用控制 Use control(UC);
3) 系统完整性 System integrity(SI);
4) 数据保密性 Data confidentiality(DC);
5) 受限的数据流 Restricted data flow(RDF);
6) 对事件的及时响应 Timely response to events(TRE);
7) 资源可用性 Resource availability(RA)。

可能使用 SL 矢量,而不是将 SL 归结为单个数字,该矢量使用 7 个 FR 代替单一的保护因子。对

于不同的 FR,这个 SL 矢量可利用语言定义不同 SL 之间的区分。这种语言是基于 FR 涉及的信息安全系统或针对安全目标的攻击相关联的附加后果。在 SL 的定义中使用的语言,可以包含这样的实用解释,一个系统是如何比另一个更安全,而无需关联每一件事到 HSE 后果。

A.3.2 等级定义

A.3.2.1 概述

IEC 62443 系列定义了五种不同级别(0,1,2,3 和 4)的 SL,每个安全级别的安全等级逐步递增。当前 SL 的定义模型依赖于越来越复杂的威胁防护,对于应用什么类型的 SL 则差别很小。对于 SL-C,这意味着资产所有者或系统集成商在配置一个特定的组件或系统时,根据所面对的越来越复杂的威胁而应具备的防护能力。对于 SL-T,这意味着资产所有者或系统集成商通过风险评估,确定一个特定区域、组件或系统应具备的威胁防护水平。对于 SL-A,这意味着资产所有者、系统集成商、产品供应商和/或它们的任何组合已配置了区域、系统或部件,以满足该 SL 所定义的特定的安全要求。

用于每个 SL 的语言使用了如非正式、巧合的、简洁的、复杂的和扩展的这样的术语。语言有意模糊,以便基本语言适用于 IEC 62443 系列的所有文件中。这个系列中的各个文件将确定适用于其特定目的的 SL 要求。

而 IEC 62443 全部系列对每一个 SL 的要求会有所不同,因此每个 SL 宜防护的内容需要有一个普适的理解。以下各节将为如何区分 SL 提供指导。

A.3.2.2 SL 0:没有特定或必需的信息安全保护要求

SL0 依据其应用的情境而具有多重含义。这意味着在定义 SL-C 时,组件或系统不能满足 SL 1 的一些 FR 要求。这个组件或系统可能将处于一个较大的区域,在那里其他元件或系统将提供补偿对抗措施。在定义一个特定区域的 SL-T 时,该资产所有者已确定其风险分析结果,针对相关组件或系统的特定 FR,不是全部的 SL 1 的具体要求都是必需的。这更可能发生在系统或区域中的某些组件上,它们无法以任何方式对 FR 的具体要求有所帮助。在确定 SL-A 时,这意味着特定区域针对特定 FR 也可能无法满足 SL 1 的某些要求。

A.3.2.3 SL 1:防止随机或巧合的违规

随机或巧合的安全违规通常是由于安全策略的宽松应用导致。就像外部威胁一样容易,这些安全违规是通过无恶意的员工引起。许多此类违规行为与安全程序有关,通过加强策略和规程将可能处理这样的问题。

图 A.1 所示,一个简单的例子是操作员能够改变 BPCS 区域内工程师站上一个设置点,使其值超过工程师设定的特定值范围。系统没有执行恰当的认证,以及使用控制限制以禁止由操作员引起的改变。在图 A.1 中,另一个例子是从 BPCS 区域和 DMZ 区域之间跨管道以明文形式发送的口令,这样网络工程师在排除系统故障时,可查看口令。系统没有加强相应的数据保密性来保护口令。在图 A.2 中,第三个例子是一个工程师欲访问工业网络＃1 中的 PLC,但实际上却访问了工业网络＃2 中的 PLC。该系统并没对数据流进行限制以阻止工程师访问错误的系统。

A.3.2.4 SL 2:安全防护防止使用少量资源、通用技能、低动机的简单手段进行蓄意破坏

简单的手段,并不需要进攻者掌握很多知识。攻击者并不需要信息安全、域或被攻击的特定系统的详细知识。这些攻击的矢量是公知的,并且有协助攻击者的自动工具。这些工具被设计来攻击大范围的系统,而不是针对特定的系统,因此,攻击者并不需要显著动机或手头有现成的资源。

采用图 A.1,一个例子是,感染了工厂 DMZ 区域维护工作站的一种病毒,会蔓延到 BPCS 工程师工

作站,因为它们都使用相同的通用操作系统。使用图 A.2,另一个例子是,利用从因特网下载的 Web 服务器通用操作系统的公知漏洞,攻击者挟持了一个企业网络的 Web 服务器。攻击者使用 Web 服务器作为据点,对企业网络或工业网络的其他系统发起攻击。还使用图 A.2,第三个例子是当位于工业网络 #1 的操作员通过 HMI 浏览网站时,下载了木马病毒的工业网络 #1 在路由器和防火墙内开辟了一个到因特网的危险途径。

A.3.2.5 SL 3:安全防护防止使用一般资源、IACS 专业技能、一般动机的复杂手段进行故意入侵

复杂的手段要求先进的信息安全知识、先进的域知识、目标系统的先进知识或者以上几项综合知识。攻击者在追踪到一个 SL 3 系统之后,将很可能会使用针对特定系统定制的攻击矢量对定向目标发起攻击。攻击者可以利用尚未出名的操作系统、工业协议的弱点、特定目标的具体信息来破坏系统安全或者其他入侵比 SL 1 或 SL 2 复杂的系统所需的更强的动机、更高级的技巧和知识。

复杂的手段,例如基于哈希表进行口令或密钥的破解工具。这些工具可供下载,但如果应用这些手段需要系统知识(例如基于哈希算法的口令或破解方法)。使用图 A.1,另一个例子是一个攻击者通过以太网控制器的漏洞进入控制 PLC 后,将继续通过系列串行管道获得进入 FS-PLC 的权限。利用图 A.2,第三个例子是一个攻击者从企业的无线网络利用暴力破解通过工业 DMZ 防火墙,从而入侵历史数据库。

A.3.2.6 SL 4:安全防护防止使用扩展资源、IACS 特殊技能、高动机的复杂手段进行故意入侵

SL 3 和 SL 4 很相似,它们都涉及利用复杂手段入侵有安全要求的系统。不同之处在于,为达到自己的目的,攻击者动机更高,能利用的资源更多。这将会运用到高性能的计算资源,大量的计算机或者很长的时间周期。

利用扩展资源的先进手段的一个例子是使用超级计算机或计算机集群进行基于哈希算法的暴力破解。另一个例子是一个僵尸网络利用大量的攻击矢量在同一时间对系统发起攻击。第三个例子是有组织性的犯罪组织,有动机和资源,并花费数周时间试图分析系统,发现和利用“零日”漏洞。

A.3.3 SL 矢量格式

相比单个数值,矢量能更好地描述一个安全区域、管道、组件或系统的信息安全要求。针对每个基本要求,该矢量可能含有一个明确的 SL 要求或一个零值(见 A.3.1)。

格式→ SL-?(\[FR,\]域)={ IAC UC SIDC RDF TRERA }

这里

SL-? =(要求)SL 类型(见 A.2.2).可能的格式有:

SL-T=目标 SL

SL-A=实现的 SL

SL-C=能力 SL

\[FR,\]=(可选)显示 SL 值适用的 FR。为了增加可读性,FR 采用缩写形式写出,替代数字形式。

域=(要求)SL 应用的适用域。域可指区域、控制系统、子系统或组件。图 A.1 中显示了不同域的例子,SIS 区域、BPCS 区域、BPCS HMI、工厂 DMZ 域控制器、工厂 DMZ 到控制中心管道和 SIS 到 BPCS 串行管道。在本标准中,所有的要求都是针对一个控制系统,所以术语“域”的使用与它在其他 IEC 62443 系列文件中的意义不同。

示例 1:SL-T(BPCS 区域)={ 2 2 0 1 3 1 3}

示例 2:SL-C(SIS 工程师工作站)={ 3 3 2 3 0 0 1}

示例 3:SL-C(RA,FS-PLC)=4

注:最后一个例子仅指 7 维 SL-C 矢量的 RA 分量。

附 录 B
（资料性附录）
SR 和 RE 到 FR SL 等级 1-4 级的映射

B.1 概述

本附录旨在给读者提供一个全面的指导关于在 FR-by-FR 的基础下，根据 SR 定义和与之关联的 RE，SL 级别 0 到 4 级是如何区别的。

B.2 SL 映射表

表 B.1 显示在一个限定的系统能力 SL——SL-C(xx、控制系统)中，哪种系统级别需求适用于哪种 FR。对于一个给定的 FR，满足给定 SL-C 要求的系统等级要求被复选标记指明。因此，例如，针对 FR5 的 SL=1 系统安全能力[或 SL-C(RDF，控制系统)=1]包括四个已定义的 SR 基本要求。无法满足这四个 SR 的系统，会有 SL-C(RDF、控制系统)=0。为满足 SL-C(RDF、控制系统)=2，系统需要支持四个 SR 基本要求，外加 RE(1)的 SR 5.1 和 SR 5.2。另一例子，只有 SR 6.1 基本要求满足 SL-C(TRE、控制系统)=1，但是所有的 SR 定义应该满足 SL-C(TRE、控制系统)=2。请参考 A.3.3 来了解整个 SL 矢量是怎样被定义的。

表 B.1 SR 和 RE 对 FR SL 等级 1-4 的映射表

SR 和 RE		SL 1	SL 2	SL 3	SL 4
FR 1——标识和鉴别控制(IAC)					
SR 1.1——人员标识和鉴别控制	5.3	√	√	√	√
SR 1.1 RE 1——唯一标识和鉴别	5.3.3.1		√	√	√
SR 1.1 RE 2——对于非受信网络的多因素身份鉴别	5.3.3.2			√	√
SR 1.1 RE 3——对于所有网络的多因素鉴别	5.3.3.3				√
SR 1.2——软件进程和设备标识和鉴别	5.4		√	√	√
SR 1.2 RE 1——唯一性标识和认证	5.4.3.1			√	√
SR 1.3——账户管理	5.5	√	√	√	√
SR 1.3 RE 1——统一账户管理	5.5.3.1			√	√
SR 1.4——标识符管理	5.6	√	√	√	√
SR 1.5——鉴别器管理	5.7	√	√	√	√
SR 1.5 RE 1——软件进程身份证书的硬件安全	5.7.3.1			√	√
SR 1.6——无线访问管理	5.8	√	√	√	√
SR 1.6 RE 1——唯一性标识和鉴别	5.8.3.1		√	√	√
SR 1.7——基于口令的鉴别强度	5.9	√	√	√	√
SR 1.7 RE 1——人员口令的生成及使用有效期限制	5.9.3.1			√	√

表 B.1（续）

SR 和 RE		SL 1	SL 2	SL 3	SL 4
SR 1.7 RE 2——所有使用者口令的有效期限制	5.9.3.2				√
SR 1.8——公钥基础设施证书	5.10		√	√	√
SR 1.9——公钥鉴别强度	5.11		√	√	√
SR 1.9 RE 1——公钥鉴别的硬件安全	5.11.3.1			√	√
SR 1.10——鉴别器反馈	5.12	√	√	√	√
SR 1.11——失败的登录尝试	5.13	√	√	√	√
SR 1.12——系统使用提示	5.14	√	√	√	√
SR 1.13——通过不可信网络的访问	5.15	√	√	√	√
SR 1.13 RE 1——显式访问请求批准	5.15.3.1		√	√	√
FR 2——使用控制(UC)					
SR 2.1——授权执行	6.3	√	√	√	√
SR 2.1 RE 1——所有使用者的授权执行	6.3.3.1		√	√	√
SR 2.1 RE 2——许可到角色映射	6.3.3.2		√	√	√
SR 2.1 RE 3——主管超驰	6.3.3.3			√	√
SR 2.1 RE 4——双重确认	6.3.3.4				√
SR 2.2——无线使用控制	6.4	√	√	√	√
SR 2.2 RE 1——识别并报告非授权的无线设备	6.4.3.1			√	√
SR 2.3——便携式和移动设备使用控制	6.5	√	√	√	√
SR 2.3 RE 1——便携式和移动设备安全状态的加强	6.5.3.1			√	√
SR 2.4——移动代码	6.6	√	√	√	√
SR 2.4 RE 1——移动代码完整性检查	6.6.3.1			√	√
SR 2.5——会话锁定	6.7	√	√	√	√
SR 2.6——远程会话终止	6.8		√	√	√
SR 2.7——并发会话控制	6.9			√	√
SR 2.8——审计事件	6.10	√	√	√	√
SR 2.8 RE 1——集中管理,系统范围的审计踪迹	6.10.3.1			√	√
SR 2.9——审计存储容量	6.11	√	√	√	√
SR 2.9 RE 1——当审计记录存储容量达到临界值时,要求告警	6.11.3.1			√	√
SR 2.10——审计处理失败响应	6.12	√	√	√	√
SR 2.11——时间戳	6.13		√	√	√
SR 2.11 RE 1——内部时间同步	6.13.3.1			√	√
SR 2.11 RE 2——时间源完整性保护	6.13.3.2				√
SR 2.12——抗抵赖	6.14			√	√
SR 2.12 RE 1——针对所有使用者的抗抵赖	6.14.3.1				√

表 B.1（续）

SR 和 RE		SL 1	SL 2	SL 3	SL 4
FR 3——系统完整性					
SR 3.1——通信完整性	7.3	√	√	√	√
SR 3.1 RE 1——加密完整性防护	7.3.3.1			√	√
SR 3.2——恶意代码防护	7.4	√	√	√	√
SR 3.2 RE 1——入口和出口恶意代码防护	7.4.3.1		√	√	√
SR 3.2 RE 2——集中管理和恶意代码保护报告	7.4.3.2			√	√
SR 3.3——信息安全功能验证	7.5	√	√	√	√
SR 3.3 RE 1——安全功能验证的自动化机制	7.5.3.1			√	√
SR 3.3 RE 2——正常操作过程中的安全功能验证	7.5.3.2				√
SR 3.4——软件和信息完整性	7.6		√	√	√
SR 3.4 RE 1——完整性破坏的自动通知	7.6.3.1			√	√
SR 3.5——输入检验	7.7	√	√	√	√
SR 3.6——确定性输出	7.8	√	√	√	√
SR 3.7——出错处理	7.9		√	√	√
SR 3.8——会话完整性	7.10		√	√	√
SR 3.8 RE 1——会话结束后使会话 IDs 无效	7.10.3.1			√	√
SR 3.8 RE 2——唯一性会话 ID 生成	7.10.3.2			√	√
SR 3.8 RE 3——会话 ID 的随机性	7.10.3.3				√
SR 3.9——审计信息保护	7.11		√	√	√
SR 3.9 RE 1——一次性写入介质的审计记录	7.11.3.1				√
FR 4——数据保密性					
SR 4.1——信息保密性	8.3	√	√	√	√
SR 4.1 RE 1——通过不可信网络存储或传输的保密性保护	8.3.3.1		√	√	√
SR 4.1 RE 2——跨区域边界的保密性保护	8.3.3.2				√
SR 4.2——信息留存	8.4		√	√	√
SR 4.2 RE 1——共享内存资源的清除	8.4.3.1			√	√
SR 4.3——加密的使用	8.5	√	√	√	√
FR 5——受限的数据流(RDF)					
SR 5.1——网络分区	9.3	√	√	√	√
SR 5.1 RE 1——物理网络分区	9.3.3.1		√	√	√
SR 5.1 RE 2——与非控制系统网络的独立	9.3.3.2			√	√
SR 5.1 RE 3——关键网络的逻辑和物理隔离	9.3.3.3				√
SR 5.2——区域边界防护	9.4	√	√	√	√
SR 5.2 RE 1——默认拒绝,例外允许	9.4.3.1		√	√	√

表 B.1（续）

SR 和 RE		SL 1	SL 2	SL 3	SL 4
SR 5.2 RE 2——孤岛模式	9.4.3.2			√	√
SR 5.2 RE 3——失效关闭	9.4.3.3			√	√
SR 5.3——普通意图个人间通信限制	9.5	√	√	√	√
SR 5.3 RE 1——禁止所有普通意图个人间通信	9.5.3.1			√	√
SR 5.4——应用划分	9.6	√	√	√	√
FR 6——对事件的及时响应(T RE)					
SR 6.1——审计日志可访问性	10.3	√	√	√	√
SR 6.1 RE 1——审计日志的编程访问	10.3.3.1			√	√
SR 6.2——连续监视	10.4		√	√	√
FR 7——资源可用性(RA)					
SR 7.1——拒绝服务保护	11.3	√	√	√	√
SR 7.1 RE 1——管理通信负荷	11.3.3.1		√	√	√
SR 7.1 RE 2——限制 DoS 影响其他系统或网络	11.3.3.2			√	√
SR 7.2——资源管理	11.4	√	√	√	√
SR 7.3——控制系统备份	11.5	√	√	√	√
SR 7.3 RE 1——备份验证	11.5.3.1		√	√	√
SR 7.3 RE 2——备份自动化	11.5.3.2			√	√
SR 7.4——控制系统恢复和重构	11.6	√	√	√	√
SR 7.5——应急电源	11.7	√	√	√	√
SR 7.6——网络和安全配置设置	11.8	√	√	√	√
SR 7.6 RE 1——当前安全设置的机器可读报告	11.8.3.1			√	√
SR 7.7——最小功能性	11.9	√	√	√	√
SR 7.8——控制系统组件详细目录	11.10		√	√	√

参 考 文 献

注 1：本文献不但引用了标准使用的源头参考信息，而且还引用了可以帮助读者更好地了解整个网络安全及开发一个网络安全管理系统的参考源信息。本目录中，不是所有的参考文献都引用在本标准全部文本中。根据来源不同，将所有引用进行分类。

已发布的和正在研究的，关于 IEC 62443 系列其他部分的引用：

注 2：所有的引用不一定是已经出版的材料，有一些是正在进行中的。被列出来的内容是目前已经完成的并且认证的 IEC 62443 系列的一部分。

[1] IEC/TR 62443-1-2 Industrial communication networks—Network and system security—Part 1-2:Master glossary of terms and abbreviations[1]

[2] IEC/TS 62443-1-3 Industrial communication networks—Network and system security—Part 1-3:System security compliance metrics[2]

[3] IEC/TR 62443-1-4 Industrial communication networks—Network and system security—Part 1-4:IACS security lifecycle and use-case[3]

[4] IEC/TR 62443-2-2 Industrial communication networks—Network and system security—Part 2-2:Implementation guidance for an IACS security management system[4]

[5] IEC/TR 62443-2-3 Industrial communication networks—Network and system security—Part 2-3:Patch management in the IACS environment[5]

[6] IEC 62443-2-4 Industrial communication networks—Network and system security—Part 2-4:Installation and maintenance requirements for IACS suppliers[6]

[7] IEC/TR 62443-3-1 Industrial communication networks—Network and system security—Part 3-1:Security technologies for industrial automation and control systems

[8] IEC 62443-3-2 Industrial communication networks—Network and system security—Part 3-2:Security levels for zones and conduits[7]

[9] IEC 62443-4-1 Industrial communication networks—Network and system security—Part 4-1:Product development requirements[8]

[10] IEC 62443-4-2 Industrial communication networks—Network and system security—Part 4-2:Technical security requirements for IACS components[9]

其他参考标准：

[11] ISO/IEC Directives, Part 2:2011 Rules for the structure and drafting of International Standards

[12] ISO/IEC 19790 Information technology—Security techniques—Security requirements for cryptographic modules

1 正在考虑中。

2 即将出版。

3 正在考虑中。

4 正在考虑中。

5 正在考虑中。

6 即将出版。

7 正在考虑中。

8 正在考虑中。

9 正在考虑中。

[13] ISO/IEC 27002 Information technology—Security techniques—Code of practice for information security management

[14] NERC CIP-002 Cyber Security—Critical Cyber Asset Identification

[15] NERC CIP-003 Cyber Security—Security Management Controls

[16] NERC CIP-004 Cyber Security—Personnel & Training

[17] NERC CIP-005 Cyber Security—Electronic Security Perimeter(s)

[18] NERC CIP-006 Cyber Security—Physical Security of Critical Cyber Assets

[19] NERC CIP-007 Cyber Security—Systems Security Management

[20] NERC CIP-008 Cyber Security—Incident Reporting and Response Planning

[21] NERC CIP-009 Cyber Security—Recovery Plans for Critical Cyber Assets

[22] NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

[23] NIST SP800-52 Guidelines for the Selection and Use of Transport Layer Security(TLS) Implementations

[24] NIST SP800-53 Rev. 3 Recommended Security Controls for Federal Information Systems and Organizations

[25] NIST SP800-57 Recommendation for Key Management

[26] NIST SP800-82 Guide to Industrial Control Systems (ICS) Security

[27] NIST SP800-92 Guide to Computer Security Log Management

其他文件和已出版资源：

[28] Gilsinn, J.D., Schierholz, R., Security Assurance Levels: A Vector Approach to Describing Security Requirements, NIST Publication 906330, October 20, 2010.

[29] IETF RFC 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

[30] Digital Bond Bandolier project, available at http://www.digitalbond.com/tools/bandolier/

[31] Open Web Application Security Project (OWASP), available at http://www.owasp.org/

中华人民共和国
国家标准
工业通信网络 网络和系统安全
系统安全要求和安全等级
GB/T 35673—2017/IEC 62443-3-3:2013
*
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
2017年12月第一版
*
书号:155066·1-58728

GB/T 35673-2017