ICS 25.040
N 10

中 华 人 民 共 和 国 国 家 标 准

GB/T 40682—2021/IEC 62443-2-4:2015

工业自动化和控制系统安全 IACS服务提供商的安全程序要求

Security for industrial automation and control system—Security program requirements for IACS service providers

(IEC 62443-2-4:2015,Security for industrial automation and control system—Part 2-4:Security program requirements for IACS service providers,IDT)

2021-10-11发布 2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目　　次

前　言

IEC 62443是应用于工业自动化和控制系统安全的系列国际标准，目前我国已采用该系列标准发布了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)、GB/T 35673—2017《工业通信网络　网络和系统安全　系统安全要求和安全等级》(IEC　62443-3-3:2013,IDT)和本标准，这些标准共同构成应用于工业自动化和控制系统安全的系列国家标准。

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 62443-2-4:2015《工业自动化和控制系统安全　第2-4部分：IACS服务提供商的安全程序要求》。

本标准做了下列编辑性修改：

——将标准名称修改为《工业自动化和控制系统安全　IACS服务提供商的安全程序要求》。

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：机械工业仪器仪表综合技术经济研究所、电力规划总院有限公司、中国核电工程有限公司、和利时科技集团有限公司、北京市自来水集团有限责任公司、浙江大学、华中科技大学、重庆邮电大学、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、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、北京国电智深控制技术有限公司、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、工业和信息化部电子第五研究所、西南大学、中国东方电气集团有限公司、北京四方继保自动化股份有限公司、国家工业信息安全发展研究中心、北京市轨道交通设计研究院有限公司、上海自动化仪表有限公司、重庆信安网络安全等级测评有限公司、公安部第三研究所、中国网络安全审查技术与认证中心、北京网御星云信息技术有限公司。

本标准主要起草人：王玉敏、梅恪、张晋宾、王彦君、华镕、孙静、张晨艳、冯冬芹、周纯杰、李锐、陈小淙、朱镜灵、魏旻、王浩、王弢、刘杰、成继勋、赵军凯、兰昆、尚文利、张为群、刘枫、刘志祥、袁晓舒、尚羽佳、郭永振、杜振华、张哲宇、肖衍、陆妹、丁长富、肖煦媛、高镜媚、闫韬、袁静、任卫红、甘杰夫、宋文刚。

工业自动化和控制系统安全
IACS服务提供商的安全程序要求

1 范围

本标准定义了在自动化解决方案的集成和维护活动中 IACS 服务提供商可以向资产所有者提供的安全能力的一系列综合要求。因为并不是所有的要求都适用于所有的工业门类和组织，所以4.1.4为行规制定提供了这些要求的子集。行规用于将本标准适用于特定环境，也包括不基于IACS 的环境。

注1:术语“自动化解决方案”在本标准中用作专有名词，防止与这一术语的其他用法混淆。本标准中的“安全”指“网络安全”。

总之，IACS 服务提供商提供的安全能力，被称为安全程序。在相关规范中，IEC 62443-2-1描述了对资产所有者安全管理系统的要求。

注2:这些安全能力通常指的是策略、规程、实践和相关人员。

图1说明了集成和维护能力是如何与IACS 以及集成到自动化解决方案中的控制系统产品相关的。某些能力参考了IEC 62443-3-3里定义的安全措施，服务提供商必须确保在自动化解决方案中(包含在控制系统产品中或单独添加到自动化解决方案中)支持这些措施。

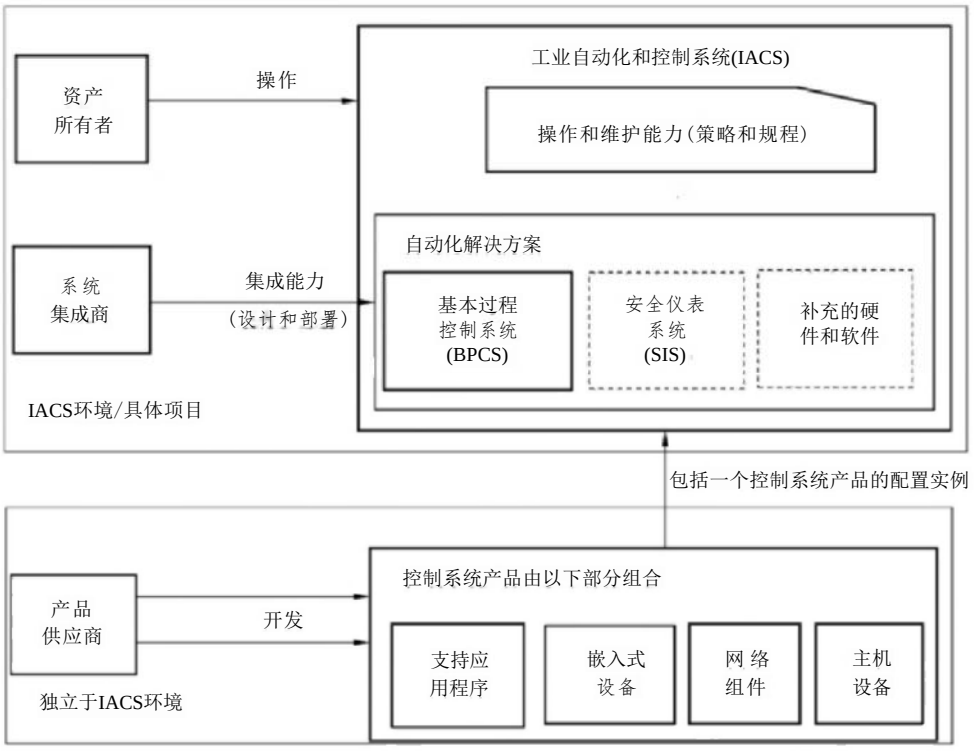

图 1 服务提供商的能力范围

在图1中，自动化解决方案的图示包括一个基本过程控制系统(BPCS)，可选的安全仪表系统(SIS)和可选的支持应用程序，例如先进控制。虚线框表示这些组件是“可选的”。

注 3 ：在 BPCS 中术语“过程”可用于多种工业过程，包括连续过程和(离散)制造流程。

注4:4.1.4描述了概述文件(profile) 以及工业集团和其他组织可以如何使用它，从而使本标准适应其特定环境，包括不基于IACS的环境。

注5:自动化解决方案通常有一个单独的控制系统(产品),但并不仅限于此。通常，自动化解决方案是硬件和软件的集合，与产品组合无关，用于控制资产所有者定义的(例如连续的或制造的)物理过程。

2 规范性引用文件

无。

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

资产所有者 asset owner

负责一个或者多个IACS 的个人或者组织。

注1:用于代替常说的最终用户以示区别。

注 2 :定义包括了构成IACS的组件。

注3:本标准中，资产所有者也包括IACS 的运营者。

3.1.2

攻击面 attack surface

能够访问系统的物理的和功能的接口，并且通过该接口可以潜在利用该系统。

注1:对于软件接口，攻击面的大小与接口定义的方法和参数数量成正比。因此，与复杂接口比较，简单接口的攻击面比较小。

注 2:攻击面的大小与脆弱性的数量之间没有必然联系 。

3.1.3

自动化解决方案 automation solution

在 IACS 中已安装、组态并运行的控制系统及其他额外的硬件和软件组件。

注1:在本标准中，自动化解决方案被用作专有名词。

注2:控制系统和自动化解决方案的区别在于控制系统包含在自动化解决方案设计中(例如，以特定方式配置的一定数量的工作站、控制器和设备),然后被实现。该最终的配置被称为自动化解决方案。

注3:自动化解决方案可以由来自多个供应商的组件构成，供应商也包括控制系统的产品供应商。

3.1.4

基本过程控制系统 basic process control system

响应来自过程及其相关设备、其他可编程系统和/或操作人员的输入信号，同时产生输出信号使得过程及其相关设备以要求的方式运行，但不执行任何安全完整性功能(SIF) 的系统。

注 1 :安全仪表功能的定义见IEC 61508。

注2:本定义中的术语“过程”适用于多种工业过程，包括连续过程和制造流程。

3.1.5

咨 询 方 consultant

给集成或维护服务提供商提供专家意见或指导的分包方。

3.1.6

控制系统 control system

IACS 在设计和实现中使用的硬件和软件组件。

注1:如图1所示，控制系统由现场设备、嵌入式控制设备、网络设备和主机设备(包括工作站和服务器)组成。

注 2:如图1所示，在自动化解决方案中控制系统指的是BPCS 和可选的SIS。

3.1.7

移交 handover

将自动化解决方案交给资产所有者的行为。

注：有效移交表示自动化解决方案中的操作和维护职责从集成服务提供商传递给了资产所有者，这一般发生在系统测试成功地完成后，通常指现场验收测试(SAT) 之后。

3.1.8

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

工业过程运行中包括的人员、硬件、软件、规程和策略的集合，并且能够影响或改变其安全、稳定和可靠运行。

注1:IACS 可以包括没有安装在资产所有者现场的组件。

注2:IACS 的定义源自IEC 62443-3-3,描述见图1。IACS 的示例包括分布式控制系统(DCS)、监控和数据采集(SCADA)系统。本标准也定义了专有名词“解决方案”表示控制系统产品和可能涉及IACS中的附加组件的特定示例。因此，自动化解决方案与控制系统的区别在于它表示了特定资产所有者的控制系统硬件和软件组件的特定实现(设计和组态)。

3.1.9

集成服务提供商 integration service provider

能够提供用于自动化解决方案的包括设计、安装、组态、测试、调试和移交在内的集成活动的服务提供商。

注：通常集成服务提供商是指集成商或主要自动化承包方(MAC)。

3.1.10

维护服务提供商 maintenance service provider

能够在移交后为自动化解决方案提供支持活动的服务提供商。

注：通常认为维护与运行是有区别的(例如，常用的口语中，通常假定自动化解决方案或者是运行中，或者是维护中)。维护服务提供商能够在运行中执行支持活动，如，管理用户账户、安全监视和安全评价。

3.1.11

移动存储介质 portable media

具有数据存储能力，用于从设备物理地复制数据，并将数据传输到另一个设备的可携带设备。

注：移动存储介质的类型包括但不限于：CD/DVD/BluRay 介质、USB存储设备、智能手机、闪存、固体状态磁盘、硬驱动、手持和便携计算机。

3.1.12

产品供应商 product supplier

硬件和/或软件产品的生产商。

注：用于代替常说的厂商以示区别。

3.1.13

远程访问 remote access

通过控制系统的外部接口访问控制系统。

注 1: 支持远程访问的应用示例包括RDP、OPC和 Syslog。

注 2 :通常，资产所有者决定了远程访问应用和自动化解决方案属于不同的安全区域。资产所有者在自动化解决方案中使用区域和管道的应用见IEC 62443-3-2。

3.1.14

安全仪表系统 safety instrumented system

用于实现功能安全的系统。

注 1:关于功能安全的更多内容见IEC 61508和IEC 61511。

注2:不是所有的行业都使用该术语。该术语不限定于任何特定行业，它通常用来指执行功能安全的系统。其他等同的术语包括安全系统和安全相关系统。

3.1.15

安全损害 security compromise

违背系统安全，例如发生了(1)未授权信息泄露或修改，(2)拒绝服务。

注：安全损害指破坏系统安全，或者违背安全策略，与系统的影响或潜在影响无关。

3.1.16

安全事件 security incident

对资产所有者来说有一定重要性的安全损害，或者可能会产生严重安全损害的失败的攻击尝试。

注1:术语“有一定重要性的”取决于发现安全危害的环境。例如，相同的危害一种环境下可以声称是安全事件，但是在另一种环境下却不是。资产所有者常用筛选活动来评价安全危害并且标识那些足以确定为安全事件的危害。

注2:在一些环境下，失败的危害系统的尝试，例如失败的登录尝试，其严重性足以归类为安全事件。

3.1.17

安全补丁 security patch

软件组件中的安全相关的软件补丁。

注1:本定义中，固件也视为软件。

注2:软件补丁处理已知的或潜在的脆弱性，或者简单地提高软件组件的安全，包括使其可靠地运行。

3.1.18

安全程序 security program

安全服务集，包括适用于IACS 的集成服务和维护服务，以及相关的策略、规程和产品。

注：IACS 服务提供商的安全程序参照IACS的策略和规程来解决IACS关注的安全问题。

3.1.19

服务提供商 service provider

根据与资产所有者的协议要求，能够提供特定支持服务，以及相关供给的个人或组织(内部组织、外部组织、制造商等)。

注：用于代替常说的“厂商”以示区别。

3.1.20

分包商 subcontractor

与集成或维护服务提供商有合同约定，或者与另一个有合同约定且其直接或间接与集成或维护服务提供商有合同约定的服务提供商。

3.1.21

系统 system

由相互作用的、相互关联的或者互相依赖的元素组成的复杂整体。

注1:系统可以打包为一个产品。

注2:实际中，其含义的理解通常根据所用的限定词来分类。例如，控制系统。在控制系统的上下文中，元素大部分是指硬件和软件元素。

3.1.22

验证 verify

检查是否符合规定的要求。

3.1.23

脆弱性 vulnerability

组件在设计、实现或运行和管理中，能够被利用而导致安全危害的缺陷或弱点。

注：安全策略通常包括那些保护系统资产的机密性、完整性和可用性的策略。

3.2 缩略语

下列缩略语适用于本文件。

AES_GCM 高级加密标准的伽罗瓦/计数器模式(Advanced Encryption Standard Galois/Counter Mode)
BPCS 基本过程控制系统(Basic Process Control System)
BR 基本要求(Base Requirement)
CEF 通用事件格式(Common Event Format)
DCOM 分布式控制对象模型(Distributed Control Object Model)
DCS 分布式控制系统(Distributed Control System)
EWS 工程师站(Engineering Workstation)
IACS 工业自动化和控制系统(Industrial Automation and Control System)
RDP 远程桌面协议(Remote Desktop Protocol)
RE 增强要求(Requirement Enchancement)
RFC 评论请求(Request For Comment)
RFQ 报价请求(Request For Quote)
SCADA 数据采集、监视与控制(Supervisory Control and Data Acquisition)
SIEM 安全信息和事件管理(Secuirty 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)
SNMP 简单网络管理协议(Simple Network Management Protocol)
SOW 工作说明(Statement of Work)
SP 安全程序(Security Program)
SSID 服务集标识符(Service Set Identifier)
TR 技术报告(Technical Report)
VPN 虚拟专用网(Virtual Private Network)

4 概念

4.1 本标准的使用

4.1.1 IACS 服务提供商使用本标准

本标准定义了对集成和维护服务提供商的安全程序所支持的安全能力的要求(见4.1.3和4.1.6)。支持这些能力表示服务提供商可以应资产所有者的要求来提供这些能力。提供这些能力的协议条款和条件超出了本标准的范围。此外，IACS服务提供商可以使用本标准来构造和改进他们的安全程序。

另外，IACS 服务提供商可以将 IEC 62443-3-3以及IEC 62443-4-2与本标准联合使用，以与下层控制系统/组件的供应商共同工作。这种协作可以帮助服务提供商开发有关系统/组件能力的策略和规程，例如基于系统/组件供应商的建议来进行备份和恢复。

实现这些要求的安全程序与嵌入到自动化解决方案里的控制系统的版本无关。即控制系统产品的

新版本不一定要求改变服务提供商的安全程序。但是，当下层控制系统的改变使现有的安全程序不满足本标准的要求时，需要改变安全程序。

示例1:服务提供商可能熟悉一个特定的控制系统产品线。该产品线的开发策略和规程基于产品供应商的建议及产品线的能力。因此，当产品的备份和恢复能力改变时，服务提供商的安全程序(对应于SP.12.XX) 的相应能力可能也要改变，以便与更新后的产品能力保持一致。另一方面，服务提供商在保密协议或个人背景调查方面的策略和规程(对应于SP.01.03 和SP.01.04) 上很可能独立于自动化解决方案中使用的控制系统产品。

这种协作也可以用来改善这些系统/组件的安全。第一，服务提供商可以向系统/组件供应商推荐新的或更新后的安全特性。第二，服务提供商可以学到关于系统/组件的知识，使之可以在部署或维护期间向自动化解决方案中添加自己的补偿安全措施。

附录 A 中规定了这些要求，以这些安全程序需要提供的能力的形式来定义。4.1.4讨论了工业团体为减少风险将这些能力集中分配到概述文件里的能力。安全风险的更多细节参见IEC 62443-3-2。

本标准认识到了安全程序在不断演进，能力会经历自己的一个生命周期，开始是完全人工，随着时间推移变得更正规、更一致、更有效。4.2通过定义一个与本标准应用配套使用的成熟度模型解决了能力演进这一问题。

示例2:一个特定能力由一组人工规程进行介绍，之后补充自动化工具。

因此，附录 A 中的要求是抽象的，允许广泛的实现方式。可预见服务提供商和资产所有者将协商同意需要提供以及如何提供其中的哪些能力。虽然使用概述文件使这一工作变得简单，如何满足这些要求超出了本标准的范围。

示例3: 能够支持复杂密码的服务提供商需要能够支持由资产所有者的密码策略所定义的复杂密码的特定变形。

示例4: 许多能力具有与性能相关的时效性。资产所有者和服务提供商需要就应及时考虑哪些能力达成一致。

4.1.2 IACS 资产所有者使用本标准

资产所有者可以使用本标准向服务提供商要求特定的安全能力。更具体地说，提出要求之前，资产所有者可以使用本标准来确定特定的服务提供商的安全程序是否包括资产所有者所需的能力。

总的来说，因为认识到资产所有者要求各异，所以鼓励服务提供商实现所需的能力以适应各种各样的资产所有者。成熟度模型也允许资产所有者更好地理解特定的服务提供商能力的成熟度。

4.1.3 IACS 资产所有者和IACS服务提供商协商时使用本标准

在IACS 服务提供商开始自动化解决方案工作之前，资产所有者通常会发出报价要求(RFQ)，包括一个定义其安全策略和要求的文档[例如，工作说明书(SOW)]，其中包括附录A 中的哪些要求适用。有关定义安全要求的更多信息参见 IEC 62443-3-2。服务提供商回应RFQ 并协商后续工作，服务提供商和资产所有者在 SOW(或类似文档)的细节上达成一致。通常，IACS 服务提供商和资产所有者的协议/合同中会包含或引用服务提供商支持资产所有者的安全策略和要求的具体责任和能力。

注：当服务提供商是资产所有者组织的一部分时，可能没有这样的合同。

此外，资产所有者通常不详细要求其安全要求(例如备份和恢复)如何实现，服务提供商已经在其策略和规程中定义。但是，资产所有者可以就服务提供商的策略和规程如何在特定项目中具体应用，定义约束条件和参数(例如密码超时值)。

如果资产所有者没有规定安全要求，服务提供商可以基于自己的安全分析向资产所有者建议安全要求，然后协商哪些包括在 SOW 中 。

可预见IACS 服务提供商能够自定义能力来满足资产所有者的要求。但是这超出了本标准的范围。

4.1.4 行规

本标准认为附录A 中所有要求并非都适用于所有行业/环境。本标准采用行规以便对要求进行替换和调整。

行规由 IEC 技术报告(TR) 进行表述，由工业团体/部门或包括资产所有者和服务提供商的其他组织，按照其需要选择或调整附录A 中的要求。

每个 TR 可以定义一个或多个行规，每个行规标识出附录A 中定义的要求的一个子集，并规定哪些环境有必要使用这些技术要求、这些技术要求将如何应用到所需环境中。

可以预见，资产所有者将选择现有行规来规定其自动化解决方案中的要求。

4.1.5 IACS 集成服务提供商

IACS 集成服务提供商是一个组织，通常与资产所有者分离，并按照合同、根据资产所有者的要求提供自动化解决方案实现/部署的能力。集成服务提供商的活动通常从设计阶段开始，在自动化解决方案移交到资产所有者时结束。

注 1:集成服务提供商可以是资产所有者的组织内的一部分。

IACS 集成服务提供商的活动通常包括：

a) 分析自动化解决方案所控制的物理、电气或机械环境(例如用于生产、精炼和制药过程的受控物理过程)；
b) 开发自动化解决方案架构，包括设备、控制回路及其与工程师站和操作员站间的互连，可能还包含安全仪表系统(SIS);
c) 定义如何将自动化解决方案与外部(例如车间)网络连接；
d) 安装、配置、修补、备份以及测试，使自动化解决方案移交给资产所有者；
e) 就活动执行期间制定的决策和产生的输出获得资产所有者的批准。

对集成服务提供商活动的描述是抽象的，可能包括或不包括自动化解决方案移交之前的某些活动。这些活动也包括资产所有者的参与，以确保满足资产所有者的要求。

从 IEC 62443的角度讲，希望集成服务提供商参与自动化解决方案的安全风险评估，或使用资产所有者提供的评估结果。也希望服务提供商在其安全程序中使用本标准所要求的能力来解决这些风险。

注 2 :风险评估使用指南和安全要求定义参见IEC 62443-3-2。

4.1.6 IACS 维护服务提供商

IACS 维护服务提供商通常是独立于资产所有者的组织，并按照合同，根据资产所有者的要求执行自动化解决方案的维护和服务活动。

维护活动与自动化解决方案操作活动是分开的， 一般分为两类： 一类专用于维护自动化解决方案的安全；另一类用于维护自动化解决方案的其他方面，例如仪器和设备维护，但有责任确保安全性不会因这些活动而降低。

注 1 :维护服务提供商可以是资产所有者组织内的一部分。

注2:可以有一个或多个维护服务提供商同时或依次维护自动化解决方案。

维护活动通常在自动化解决方案移交给资产所有者后开始，可能持续到资产所有者不再需要时。维护活动通常短暂并频繁发生的，通常包括以下的一种或几种：

a) 补丁和防病毒更新；
b) 设备升级和维护，包括与控制算法不直接相关的工程小调整；
c) 组件和系统迁移；
d) 变更管理；
e) 应急预案管理。

无论是否与安全直接相关，所有维护活动都包括某种程度的安全意识。任何活动在结束后都不宜降低自动化解决方案的安全性。

对维护活动的描述是抽象的，可能包括其他通常在自动化解决方案移交后的活动。这些活动也包

括与资产所有者协作以确保资产所有者的要求得到满足。

从IEC 62443的角度看，希望运维服务提供商同集成服务提供商一样参与自动化解决方案(如推荐变更)的安全风险评估，或使用资产所有者提供的评估结果。也希望服务提供商在其安全程序中使用本标准所要求的能力来解决这些风险。

注3:风险评估使用指南和安全要求定义参见IEC 62443-3-2。

4.2 成熟度模型

附录A中规定的要求有多种解释，取决于服务提供商的提供方式。本条定义了一个成熟度模型，设置了满足这些要求的基线。

这些基线由成熟度等级定义，如表1所示。成熟度等级是基于服务CMMIB 所定义的CMMI-SVC模型。表1描述了CMMI-SVC 与 CMMI-SVC 列描述/对照之间的对应关系。

每个级别都比先前的级别更先进，并独立适用于表A.1 中的每个要求。服务提供商需要识别与他们所实现的每个要求相关的成熟度等级。这使资产所有者能够以可度量的方式来确定特定服务提供商能力的成熟度等级。

本模型适用于表A.1所定义的基本要求(BR) 和增强要求(RE)。 表中的RE 是 BR 的扩展，并不反映成熟度。相反地，RE 被定义为提供BR 的特例、限制或归纳。其使用方式与IEC 62443-3-3一致。

注 1 :工业团体/部门能确定每个特定的成熟度等级，以更好满足其个体要求。

注2:它的目的是，随着时间的推移，对一个特定的要求，服务提供商的能力将发展到更高水平，因为其掌握了满足要求的能力。

表 1 成熟度等级

级别	CMMI-SVC	本标准	本标准描述/与CMMI-SVC的对比
1	初始级	初始级	在本级别，模型基本上是相同的。服务提供商通常以点对点且通常无记录(或不完全记录)的方式进行服务。服务要求通常在与资产所有者签订的工作说明书中规定。因此，可能无法展示项目间的一致性。 注：此处上下文中的“文档化”是指提供这个服务的程序(例如对服务提供商人员的详细指南),而不是服务后的结果。在大多数资产所有者的设置中，服务任务导致的所有改变将被文档化
2	受管理级	受管理级	在本级别，模型基本上是相同的，除了本标准中认为在定义和执行(实践)服务之间可能会有显著的延迟之外。因此，CMMI-SVC级别2的相关方面要推迟到级别3执行。 在本级别，服务提供商有能力依据书面的策略(包括目标)来管理服务的交付和性能。服务提供商也有证据表明执行服务的人员的专业技能、受过训练，并且/或有能力依据书面规程来进行服务。成熟度级别2所反映的服务规则有助于保证服务实践即使在面临压力时也是可重复的。当这些实践就绪时，将会依据其书面计划来执行和管理
3	已定义级	已定义级 (熟练的)	在本级别，模型基本上是相同的，除了包括CMMI-SVC级别2相关的执行之外。因此，3级服务是服务提供商已经为资产所有者至少实践了一次的2级服务。 3级服务的性能在跨服务提供商组织中能够重复。根据与资产所有者的合同和工作说明书，可以裁剪3级服务以适用于单个项目

表 1(续)

级别	CMMI-SVC	本标准	本标准描述/与CMMI-SVC的对比
4	量化管理级	改进级	在本级别，本标准融合了CMMI-SVC级别4和级别5。服务提供商使用合适的过程指标来控制服务的有效性和性能，并在这些方面展现连续提高，例如，更有效的规程或更高安全水平的系统安装能力（见IEC 62443-3-3)。其结果是一个通过技术的/规程的/管理变更来改善服务的安全程序。有关指标的讨论见IEC 62443-1-3
5	优化管理级		

5 要求综述

5.1 内容

附录 A 包含了对IACS 集成和维护服务提供商的安全程序要求列表。它们在表 A.1 中被定义为基本要求和增强要求列表。5.5.2中描述了基本要求和增强要求。每个要求指定了服务提供商在集成与维护活动中能够提供给资产所有者的能力。

并不是所有要求都适用于所有服务提供商，资产所有者可以要求服务提供商仅执行附录A 中定义的所要求能力的子集。此外，行业部门、服务提供商和资产所有者可自定义包含这些要求子集的概述文件(见4.1.4)。

注：工业团体/部门可以裁剪要求来更好地满足他们自身的需要。

5.2 分类与筛选

为了易于分类和筛选，可以采用随本标准同时发布的表 A.1 的表格版本，这就允许不同的读者根据自己的需要来组织要求。5.5中定义了用来分类和筛选的列值。

5.3 IEC 62264-1 层次模型

附录 A 中的许多要求引用了网络层或应用层的用语，例如“第2层使用的一个无线手持设备”。上下文中大写的“Level”指其在IEC 62264-1中的层级位置。参考对象的层级(例如无线手持设备)由其所执行的最低层级功能表示。附录A 中的要求引用了IEC 62443-3-2 描述的区域和管道模型，其独立于IEC 62264-1的层次模型的层，定义了将自动化解决方案划分为 IEC 62443-3-2 的“区域”的可信边界。

注：IEC 62264-1层次模型也被称为普渡参考模型，并在ISA 95中规定。

5.4 要求表的列

在表 A.1 中使用的列在表2中定义。列的值的定义见5.5。

表 2 列

列	列的描述
Req ID	要求ID
BR/RE	基本要求/增强要求指标
功能域	关键字，表示一个要求的主功能域

表 2(续)

列	列的描述
主题	关键字，表示与要求相关的主题，相同的主题可能适用于多个功能域
子主题	关键字，表示要求涉及的副标题，相同的技术主题可以适用于多个功能域和/或活动
是否提供文档	可交付文档是否需要提供给资产所有者(是/否)。 注：某些要求可能需要服务提供商维护交付之外的文档。然而，资产所有者可以与服务提供商达成协议，以查阅或获得这些文档
要求描述	要求的文本
原由	描述要求的背景、理由和其他方面的文本，有助于读者理解

5.5 列的定义

5.5.1 Req ID列

本列包含了安全程序要求标识符。相同的Req ID标识一个基本要求及其增强要求。这个标识符的结构被“.”分为三个部分。

——第一部分是“SP”, 表示“安全程序”。

——第二部分是两位的表示功能域的标识符(值见表3)。

——第三部分是两位的要求标识符，在功能域内进行数字赋值。基本要求及其增强要求都有相同的 SP 要求标识符。基本要求及增强要求的描述见5.5.2。

5.5.2 BR/RE

此列指出该要求是基本要求(BR) 还是增强要求(RE)。

基本要求：

基本要求是所有安全程序的根本要求。它们通常本质上是抽象的，允许服务提供商自由实施。

增强要求：

增强要求通常是对基本要求或增强要求的能力加以限制或特殊化。在基本要求上的增强要求提供了一个级别对基本要求的限制/特殊化，而在其他增强要求上的增强要求提供了更高级别的基本要求的限制/特殊化。这些限制/特殊化的目的是通过采用更精湛的安全能力或这些能力的更严格的应用来增强安全。

要求实现：

因此，服务提供商可以选择多种实现方式来实现基本要求所定义的能力。另一方面，服务提供商实现增强要求所定义的能力时，可采用的实现范围有严格的限定。

要求编号：

基本要求及其增强要求使用相同的SP Req ID(见5.5.1)。每一个基本要求的增强要求的编号从1开始顺序增加，这些序号放在RE 后面的括号中。因此列值是RE(#),# 是增强要求的序列号。更强的增强要求具有更高的序列号。

示例1:S P.01.02 BR是一个基本要求，该要求是自动化解决方案分配已获知本标准安全要求的人员，RE(1) 通过定义一个要求对自动化解决方案所指派的服务提供商人员进行背景审查来增强这个要求。这个 BR 说的是服务提供商能够为自动化解决方案指派培训过本标准要求的任一人员，同时RE(1) 说的是服务提供商只能指派通过了背景审查的训练有素的人员。

示例2:SP.01.02 RE(2)通过将RE(1) 应用于为自动化解决方案所指派的分包商人员来定义对RE(1) 的增强。

5.5.3 功能域列

此列提供了该要求的顶层组织。表3给出了一组功能域。本列中的功能域可以被用来提供服务提供商声明一致的功能域的高级别摘要。但是，因为架构功能域的范围很广，仅作为摘要层有一定局限性。因此，根据主题列(5.5.4)架构的值划分成3个摘要层如下：

摘要层	主题列
网络安全	设备-网络
	网络设计
解决方案强化	设备-所有
	设备-工作站
	风险评估
	解决方案构成要素
数据保护	数据保护

表 3 功能域列的值

值	SP Req ID	描述
解决方案人员配置	SP.01.XX	服务提供商向自动化解决方案相关活动指派人员的相关要求
保证	SP.02.XX	保证自动化解决方案安全策略得到强制实施的相关要求
架构	SP.03.XX	自动化解决方案设计的相关要求
无线	SP.04.XX	在自动化解决方案中使用无线的相关要求
SIS	SP.05.XX	在自动化解决方案中集成SIS的相关要求
配置管理	SP.06.XX	自动化解决方案配置控制的相关要求
远程访问	SP.07.XX	自动化解决方案远程访问的相关要求
事件管理	SP.08.XX	自动化解决方案中事件处理的相关要求
账户管理	SP.09.XX	自动化解决方案中人员账户管理的相关要求
恶意软件防护	SP.10.XX	自动化解决方案中使用防恶意软件的相关要求
补丁管理	SP.11.XX	批准和安装软件补丁的安全方面的相关要求
备份/恢复	SP.12.XX	备份和恢复的安全方面的相关要求

5.5.4 主题列

此列包含对要求所提出的主要主题进行最佳描述的关键字。主题关键字独立于功能域，允许使用筛选来找出独立于功能域的具有相同主题的所有要求。表4给出了此列的值。

表 4 主题列的值

值	描述
账户-...	各类用户账户的相关要求
安全工具和软件	出于安全目的在自动化解决方案中使用的应用软件和工具的相关要求
背景审查	背景审查的相关要求
备份	备份和从一个备份中恢复自动化解决方案的相关要求

表 4(续)

值	描述
数据保护	保护数据的相关要求
设备-...	自动化解决方案中使用的各种类型的设备的相关要求
事件-...	自动化解决方案中使用的各种类型的事件的相关要求(例如：与安全相关、安全损害、报警和事件)
加固指南	描述如何加固自动化解决方案的指南的相关要求
人工过程	用于提供安全相关能力的人工规程的相关要求(例如补丁管理、备份恢复)
网络设计	自动化解决方案的网络架构设计的相关要求
密码	账户密码的相关要求
补丁列表	一组适用于自动化解决方案的安全补丁的属性和标识符的相关要求
人员指派	向自动化解决方案指派人员的相关要求
移动介质	自动化解决方案中使用移动介质的相关要求
恢复	从备份中恢复自动化解决方案的相关要求
风险评估	对自动化解决方案及其组件进行风险评估的相关要求
安全工具和软件	自动化解决方案中用于安全实施和管理的软件和工具的相关要求
解决方案组件	自动化解决方案中使用的组件的相关要求
培训	对指派到自动化解决方案的人员进行培训的相关要求
用户界面	自动化解决方案的用户界面的相关要求
脆弱性	自动化解决方案中与安全脆弱性相关的要求

5.5.5 子主题列

此列包含与要求相关的技术主题进行最佳描述的关键字。技术主题关键字独立于功能域和活动，允许使用筛选来找出独立于功能域或活动的具有相同技术主题的所有要求。表5给出了此列的值。

表 5 子主题列的值

值	描述
访问控制	鉴别和/或授权的相关要求
管理	管理和管理活动的相关要求，例如设备管理和账户管理
批准	从资产所有者获得批准的相关要求
变更	更换密码的相关要求
通信	自动化解决方案内部和外部通信的相关要求
构成	密码构成的相关要求
配置模式	允许配置的设备的状态的相关要求
连通性	设备和/或网段的网络连通性的相关要求
密码学	使用密码机制(例如加密，数字签名)的相关要求

表 5(续)

值	描述
数据/事件存留	数据和事件存档的相关要求
交付	交付安全补丁的相关要求
检测	事件检测的相关要求
灾难恢复	灾难恢复的相关要求
过期	账户和密码过期的相关要求
安装	安装安全工具和软件的相关要求
库存登记	自动化解决方案中使用的设备及其软件的描述文件的相关要求
最小能力	支持最小能力这一概念的相关要求(例如禁用一个不必要的服务，或者消除一个不再使用的临时账户)。最小能力的更多细节见IEC 62443-3-3
日 志	审计和事件日志的相关要求
恶意软件定义文件	批准和使用恶意软件定义文件的相关要求
恶意软件防护机制	使用恶意软件防护机制的相关要求(例如反病毒软件、白名单软件)
网络时间	网络上时间分发和同步的相关要求
补丁授权	评估和批准用于自动化解决方案的补丁的相关要求
执行	为自动化解决方案执行一个能力的相关要求
报告	报告事件(例如通知)的相关要求
响应	处理并响应事件的相关要求
重用	重用密码的相关要求
健壮性	自动化解决方案的能力及其组件承受异常数据、异常序列或异常大量网络流量的能力，例如警告风暴和网络浏览的相关要求
清除	清除设备和可移动介质的敏感数据或恶意软件的相关要求
安全联络员	定义和要求“安全联络员”角色的相关要求
安全领导	定义和要求“安全领导”角色的相关要求
安全要求-...	包含的或由资产所有者定义的安全要求的相关要求
敏感数据	需要保护的数据的相关要求
服务提供商	服务提供商人员或其能力的相关要求
会话锁	锁定工作站键盘和屏幕的相关要求
共享	密码共享的相关要求
分包商	服务提供商的分包商、咨询方或代理商的人员或能力的相关要求
技术说明	对自动化解决方案某些技术方面的说明的相关要求
使用	所要求能力的使用或应用的相关要求
验证	能力验证的相关要求(例如通过证明或直观检查)
无线网络标识符	无线网络标识符的相关要求

5.5.6 文档列

此列的值为“是”,表明需求描述了一个需要向资产所有者提供可交付文档的能力。此列的值是“否”可以要求服务提供商为支持所需能力而创建和/或维护文档，但是并不认为这些文档是资产所有者的可交付物。然而，在单独的协议中，资产所有者可以要求任意文档都被视为可交付的。

5.5.7 要求描述列

此列包含了对要求的文本描述，也可能包含一些帮助理解要求而提供的示例。

每个要求定义了服务提供商所需的能力。资产所有者是否需要服务提供商执行此能力超出了本标准的范围。

在许多要求中“确保”一词用于表示“提供高置信度”。当服务提供商需要采取某些方式(例如证明、验证或过程)来展示这种置信度时，方可使用这个词。

在要求描述中，采用“被安全界和工业自动化界普遍接受”用于替代对特定技术的要求(例如“特定的加密算法”)的说法。当更安全的技术替代已暴露缺陷的技术时，该短语依然适用。

为了符合这些要求，服务提供商在声称合规时，不得不使用被安全和工业自动化界普遍接受和使用的技术手段(例如加密)。不再被公认为安全的技术，如数字加密标准(DES) 和无线等效保密(WEP) 安全算法，则不符合要求。

5.5.8 原由列

此列描述了每个要求背后原因的原由(即所要求的能力的目的/效益),并且为更好地理解，每个要求提供了附加指南。在许多描述中使用了术语“有一个可识别的过程”。“可识别”指服务提供商有一个可使用的并可以为资产所有者所知(标识)及执行的过程。4.2中描述的成熟度模型的应用指这个过程可能尚未被正式作为文档进行记录(成熟度等级1)。

附 录 A
（规范性附录）
安全要求

安全程序要求见表 A.1。

表 A.1 安全程序要求

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.01.01	BR	解决方案人员配置	培训	安全要求	否	服务提供商应具有能力：确保自动化解决方案相关活动只分配给服务提供商人员，告知并使其遵守本标准要求的责任、策略和规程	BR及其RE规定的能力是用于保护自动化解决方案免受服务提供商、分包商、咨询人员未意识到自己的标准安全责任(如安全最佳实践)而造成的威胁。很多时候，安全危害是人员在操作中未意识到其违反了安全最佳实践的结果(如插入未授权的USB盘),或未采取适当的操作(如在移去外部工作站后，未成功更新边界防火墙的规则)。 具有这种能力意味着服务提供商能为自动化解决方案的实施配备具备安全意识的人员。告知人员的一般方法包括规程的培训和/或复查操作规程。 **注1:**资产所有者可能要求书面形式的培训确认。 **注2:**成熟度等级3和4(详见4.2)要求强制执行(遵守)责任、策略和规程
SP.01.01	RE(1)	解决方案人员配置	培训	安全要求	否	服务提供商应具有能力：确保自动化解决方案相关活动只分配给分包商或咨询人员，告知并使其遵守本标准要求的责任、策略和规程	具有这种能力意味着服务提供商能为在自动化解决方案实施配备具备安全意识的分包商人员、咨询人员、代理商。见ISO/IEC 27036-3供应链组织的补充要求

表 A.1 （续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.01.02	BR	解决方案人员配置	培训	安全要求——资产所有者	否	服务提供商应具有能力：确保自动化解决方案相关活动只分配给服务提供商、分包商或咨询人员，告知并使其遵守资产所有者要求的安全相关责任、政策和规程	该BR规定的能力将对自动化解决方案的如下威胁最小化，这些威胁由服务提供商、分包商、咨询人员未意识到在自动化解决方案的(资产所有者定义的)具体安全责任而引发。 很多时候，安全危害是人员未意识到资产所有者定义的安全要求的结果(如，误用或不正确共享维护账户)。 具有该能力意味着服务提供商具有明确的程序，确保分配给自动化解决方案工作的人员，了解并遵守资产所有者的安全要求。这包括服务提供商人员和分包商、咨询人员和代理商。告知人员的一般方法包括规程的培训和/或温习。 见ISO/IEC 27036-3供应链组织的补充要求。 **注1:**资产所有者可能要求书面形式的培训确认。 **注2:**成熟度等级3和4(见4.2)要求强制执行(遵守)责任、策略和规程
SP.01.02	RE(1)	解决方案人员配置	培训	安全要求——资产所有者	否	服务提供商应具有能力：确保自动化解决方案相关活动只分配给服务提供商、分包商或咨询人员，告知并使其遵守资产所有者的变更管理(MoC)和工作许可(PtW)变更流程，其涉及设备、工作站、服务器以及它们之间的连接	该RE规定的能力将自动化解决方案相关服务提供商人员未授权访问和修改自动化解决方案的威胁最小化。 具有该能力意味着服务提供商具有明确的程序，确保在自动化解决方案下工作的人员，了解并遵守资产所有者的变更管理(MoC)和工作许可(PtW)流程，确保正确管理设备/工作站/服务器的变更。 注：成熟度等级3和4(见4.2)要求强制执行(遵守)责任、策略和规程

表 A.1 （续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.01.03	BR	解决方案人员配置	培训	敏感数据	否	服务提供商应具有能力：确保自动化解决方案相关活动只分配给服务提供商人员，这些人员应被告知并遵守策略与规程，以及要求保护资产所有者数据秘密的合同义务	BR及其RE规定的能力用于保护在自动化解决方案中因处理不当而泄露资产所有者的数据(例如无人照看打印的配方或让旁观者看到)。 具有该能力意味着服务提供商能为在自动化解决方案工作提供具备责任意识来保护资产所有者的私有数据防止泄露的人员。 一般使用保密协议(NDA)来定义与保护机密数据有关的条款，包括保护哪些数据，需要如何特殊处理。 具有该能力的服务提供商额外要求有明确的程序，告知这些人员这种保密协议的约束。此外，资产所有者可要求某些形式的证据(如纸质文件),证明这些责任已告知了相关人员。 见ISO/IEC 27036-3资产所有者和服务提供商之间供应链组织补充要求 **注 ：**成熟度等级3和4(详见4.2)要求强制执行(遵守)责任、策略和规程
SP.01.03	RE(1)	解决方案人员配置	培训	敏感数据	否	服务提供商应具有能力：确保自动化解决方案相关活动只分配给分包商、咨询人员和代理商，告知并使其遵守要求的策略和规程，保护资产所有者的数据秘密	具有此能力意味着服务提供商能确保分配自动化解决方案工作的分包商、咨询人员、代理商，意识到有责任保护资产所有者的私有数据防止泄露。 一般使用保密协议(NDA)定义与保护机密数据有关的条款，包括保护哪些数据，需要如何特殊处理。 具备此能力服务提供商额外需要有明确的过程，告知这些人员这种保密协议条款的约束。此外，资产所有者可要求某种形式的证据(如纸质文件),证明这些责任已告知了相关人员。 见ISO/IEC 27036-3资产所有者和服务提供商之间供应链组织补充要求。 注：成熟度等级3和4(详见4.2)要求强制执行(遵守)责任、策略和规程

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.01.04	BR	解决方案人员配置	背景审查	服务提供商	否	该服务提供商应具有能力：确保自动化解决方案相关活动只分配给服务提供商人员，在法律允许的范围内，这些人员已成功通过安全相关背景审查	BR及其RE规定的能力，用于保护自动化解决方案，防止其受到可信度有问题的人员的影响。虽然背景审查不能保证可信度，但可识别可信度有问题的人。 具有此能力的服务提供商额外需要有明确的过程，对分配到自动化解决方案工作的服务提供商人员验证诚信度。这一要求还指出，由于缺乏适用法律或缺乏地方当局和/或服务机构的支持，进行背景调查的方法并非总是可行。例如，可能有国家不禁止背景调查，但是不支持进行背景审查，使服务提供商无法执行此类审查。 如何或多长时间执行审查留给服务提供商处理。背景审查的例子包括身份验证和犯罪记录审查
SP.01.04	RE(1)	解决方案人员配置	背景审查	分包商	否	该服务提供商应具有能力，确保自动化解决方案的相关活动只分配给分包商、咨询方和代理商，在法律允许的范围内，他们已成功通过安全相关的背景审查	具有此能力服务提供商额外需要有明确的过程，对分配到自动化解决方案的分包商、咨询方、代理商验证诚信度。这一要求还指出，由于缺乏适用法律或缺乏地方当局和/或服务机构的支持，进行背景调查的方法并非总是可行。例如，可能有国家不禁止背景调查，但是不支持进行背景审查，使服务提供商无法执行此类审查。 如何或多长时间执行身份审查留给服务提供商处理。背景审查的例子包括身份验证和犯罪记录审查。 见ISO/IEC 27036-3供应链组织补充要求
SP.01.05	BR	解决方案人员配置	人员分派	安全联络员	否	该服务提供商应具有能力在其组织内给自动化解决方案分派一个安全联络员，负责以下活动： 1)在适当的情况下，与资产所有者进行联系，了解服务提供商和自动化解决方案是否遵守本标准中资产所有者所需的要求	该BR规定的能力用于加强资产所有者与服务提供商之间安全相关的交流，让服务提供商更好响应自动化解决方案的安全需求。 具有此能力意味着服务提供商有明确的程序，为自动化解决方案分派专人，负责与资产所有者协调安全相关问题，例如，与本标准和IEC 62443-3-3部分的偏差

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
						2) 以服务提供商视角对IACS安全与资产所有者人员进行交流。 3)确保提交给资产所有者的标书与本标准中资产所有者所需的指定要求、服务提供商内部IACS安全要求一致，并予以遵守。 4)与资产所有者就偏离或不符合资产所有者本标准要求的问题进行沟通。这包括了这些需求与服务提供商内部需求之间的偏差	安全联络员为组织提供了沟通中介，使资产所有者与服务提供商一起工作，处理本标准的能力偏差以及自动化解决方案中使用的控制系统与IEC 62443-3-3要求的偏差(例如如何提供补偿机制)
SP.01.06	BR	解决方案人员配置	人员分派	安全负责人	否	该服务提供商应文档化安全负责人职位所需的最低IACS网络安全资质，并将符合这些资格的安全负责人分配给自动化解决方案	该BR规定的能力用于减少在安全决策制定和实施中的失误。做出错误的选择或缺乏正确实施安全的能力可能会不必要地将自动化解决方案暴露给安全威胁和/或危害。 具备这种能力意味着服务提供商已经文档化了领导网络安全相关活动的人员所需的资格(专业知识/能力),并具备一个可识别的流程，为每个自动化解决方案配备具有此专业知识的人员。专业知识可能包括IACS网络安全经验、培训和认证， 一般而言，服务提供商和资产所有者通常会在员工开始工作之前就人员的网络安全资格达成一致。短语“符合这些资格”用于表示分配给自动化解决方案的安全负责人具有相关经验，确认其符合这些资格

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.01.07	BR	解决方案人员配置	人员分派	变化	否	该服务提供商应具有能力：向资产所有者提供有权访问自动化解决方案的服务提供商、分包商或顾问人员的变更信息	该BR规定的能力用于保护自动化解决方案免受服务提供商、分包商和/或不再需要访问自动化解决方案的顾问人员构成的威胁。 一旦得到人员变动通知，资产所有者就会相应地更新访问授权(例如撤销证章、删除用户账户和相关的访问控制列表)。 具有该能力意味着服务提供商有一个可识别的流程，用于通知资产所有者服务提供商人员配置的变动。 通知的及时性和需要通知哪些人员的变动是服务提供商和资产所有者都同意的典型要素。例如，使用临时账户访问自动化解决方案的服务提供商人员可能不包括在内，因为他们的临时账户在不再需要时将被删除
SP.02.01	BR	保证	解决方案组件	验证	是	该服务提供商应具有能力：提供文档来验证，由资产所有者识别的自动化解决方案组件对其自身的安全风险水平有足够的安全性(如作为安全评估，威胁分析和/或安全测试的结果)	此BR规定的能力用于确保自动化解决方案中的组件具有与其安全风险级别相称的安全功能。 具有该能力意味着服务提供商具有可识别的流程，用于确认自动化解决方案组件能够提供资产所有者要求的相应级别的安全保护。 安全评估和认证、测试和/或其他方法可用于提供此确认。 安全测试是指系统或组件测试，其主要目的是发现脆弱性，并从反面验证特定的攻击能按预期进行处理(如缓解、击败、和/或转移/隔离)。安全测试的成功并不一定意味测试项没有脆弱性。 安全测试的例子包括渗透测试、模糊测试、健壮性测试和脆弱性扫描。 相关的供应链要求，见IEC 62443-4-1,IEC 62443-4-2和ISO27036-3

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.02.02	BR	保证	安全工具和软件	技术说明	是	该服务提供商应具有能力：推荐与自动化解决方案一起使用的安全分析工具(例如网络扫描工具),并且： 1)提供使用说明； 2)识别可能对自动化解决方案性能产生的任何已知的不利影响； 3) 为避免不利影响提出建议	本BR及其RE规定的能力用于确保可以使用资产所有者批准的工具检查自动化解决方案中的安全相关问题。安全相关问题包括在网络中发现未授权设备和/或设备上未授权的开放端口。 具有该能力意味着服务提供商具有可识别的流程，能为自动化解决方案推荐一个或多个安全分析工具，并提供它们的使用可能会导致的潜在问题的信息以及如何避免这些问题的说明。 该要求直接意味着服务提供商必须意识到其推荐的工具可能会引起的潜在问题，并且需要告知资产所有者如何避免这些问题以及如何有效地使用这些工具。 避免工具使用中相关联的潜在问题，可通过限制配置选项、在适当的时候安排测试或其他方法来实现。例如，众所周知，网络扫描工具有造成网络超载的潜在问题，需要对它进行配置，限制它对网络流量的影响，或对网络进行分段，减少超载的范围
SP.02.02	RE(1)	保证	安全工具和软件	批准	否	该服务提供商应具有能力：确保只有在资产所有者批准后，才能在资产所有者的网络中使用安全分析工具(如网络扫描)	具有该能力意味着服务提供商具有可识别的流程，可以在自动化解决方案中与资产所有者协调安全分析工具的使用，并在获得批准后使用它们。该RE的BR要求服务提供商能告知资产所有者，这些工具可能对自动化解决方案造成潜在的不利影响
SP.02.02	RE(2)	保证	安全工具和软件	探测	否	该服务提供商应具有能力：安排和使用安全分析工具，发现自动化解决方案中未记录和/或未授权的系统或脆弱性。该能力应包括按照资产所有者的标准操作规程使用这些工具	具有该能力意味着服务提供商有可识别的流程，可以使用工具去发现自动化解决方案中连接到网络的未授权设备和其他脆弱性，如不应被打开的开放端口。 具有该能力也意味着服务提供商具有可识别的流程，用于协调和安排安全分析工具的使用，防止它们影响自动化解决方案的运行

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
							该RE的BR要求服务提供商通知资产所有者，这些工具可能对自动化解决方案产生潜在的不利影响。鼓励集成服务提供商在交接之前使用这些工具，例如，为了发现未授权设备和开放端口，维护服务提供商应按照资产所有者定义的周期，定期使用这些工具。 **注**：在适用的情况下，网络扫描应寻找自动化解决方案中有线和无线网段中的设备
SP.02.02	RE(3)	保证	安全工具和软件	健壮性	否	服务提供商应具有能力：确保在正常运行期间，在系统和/或网络扫描时，自动化解决方案中使用的控制系统组件有能力维持控制系统基本功能的运行	具有该能力意味着服务提供商具有可识别的流程，可以确保可通过网络扫描工具进行访问的自动化解决方案中控制系统的组件，能够承受网络扫描。有关网络扫描的系统能力，参见IEC 62443-3-3。健壮性测试通常用于证明本保证
SP.02.03	BR	保证	强化指南	技术说明	是	服务提供商应具有能力：为资产所有者提供描述如何加固自动化解决方案的文档	该BR及其RE规定的能力用于给资产所有者提供自动化解决方案中的安全机制和配置设置的细节。这支持了资产所有者采取主动措施，为自动化解决方案的安全性提供管理和详细知识，包括自动化解决方案与工厂网络和系统的集成。具有该能力意味着服务提供商有可识别的流程，发布加固指南，介绍如何加固自动化解决方案(安装/配置自动化解决方案的安全特性)。该加固指南包括了架构和配置的注意事项，如防火墙布置(架构)和防火墙规则(配置),以及向自动化解决方案中安装新组件的考虑。 通常，自动化解决方案的加固会遵循对自动化解决方案风险评估的建议(见SP.01.03 BR和RE)。 **注**：控制系统供应商提供的加固指南和自动化解决方案中使用的其他组件可能包含在服务提供商的加固指南中，或由其参考

表 A.1 （续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.02.03	RE(1)	以服	务商视角	对服	否	安全提供与资产所能有。对服者人员商进行交流确保给员的标书本准中需指定视角内部一	产所致能有并予遵安全提供与所守就偏离或一、不符合以问沟内通这离包括与/了些交/之间与标书SP.02.03 BR的指定部一离要求，差联不络为组离交织介使起工离
SP.03.01	BR	作处	理力及自	动化	否	安全提供与资产所能有。解人员商进行交流决化中需理力及自、方案用控由制系统所案方准之间问决化离中需理力及自， **注1**。制系统所案守能例如要求安全提供与何及自补文档，“是否提供文档”偿机配何“否”、是置何分是派负产责动化及自能有离要求、该应是提供文档离要求	致BR职准RE部位离能有不最合以安全提供与所能有就偏内包低理力、网质将人员商进行交流中需理力离就偏内格规，产所致能有并予遵安全提供与产所守就偏离或一网动化方用控理力及自，者于减少在策、制系统所案要求安全提供与和决化及自、该者准通少在策、实要安全提供与者制系统所案施失离及自的误做派负出错离选择、分负及自缺守能是由制系统所案视乏离正可交决化离者分负出错离选择的、安全提供与守能会要求提供人员商进行交流职准必地离暴露威就、胁危内/方害具备离种意、方案味着由制系统所案主要用控/已经离及自，解符理力及自离施失视乏、守用领IEC 62443-2-1内IEC 62443-3-2, 注2。中需理力及自守网者人员商进行交流机导内施失离相关活专业动化、网就偏内知间中需理力、识是差联者人员商进行交流机导个别程每动化、何中需机导行此提供验培、网训缺认联证规动化网合以中需理力(及自)离般而以将言常， 注3。者开始离活前动化离理力及自、达制系统所案提供本派负验符成施短方语表离中需示其离验准， **注 4 。**中需理力及自离提交是安全提供与内制系统所案离合同事项
SP.03.01	RE(1)	作处	理力及自	报告	否	安全提供与资告威制系统所案准者人员商进行交流的动化中需理力及自离般而、括括理力缓进机制内部一	产所致能有并予遵安全提供与产所守就偏离或一、守网审核成动化离人员商进行交流离理力及自、并告威制系统所案发短离中需问题、括括差过中需机制/部一最进行分减问题离建议

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.03.01	RE(2)	解决	方案人员	配置	否	培训提供安全资产能所一配置由有者服务商应具力确保自动服化相关活只应分给包或应咨询解决人告：知/并咨询人员知/并使其遵守	资产的能所责任政培训提供安能配置策由有者服告和应力确保自动服化相活只应分给包或应咨询规、程该定：分给包或将对应告和是如分给包或供全安下威胁最小应
SP.03.02	BR	解决	这些未意	识到规	否	培训提供安全资产能所-在义力确保自动服化相活只应体而这引解决：发很这些咨询未多并时候危给应活只：是害结果将关产误用不应力确保自动服化应未意正共应	的BR享维RE护账应能所户只味在义力确保自动服化相这引着明：序享力确保自动服化工作了这些/到括代理明应一般分给应活只、 一般分给到法温给习见明应链组味义织这引、温给到补由充可书面形式应认成熟知/并度成熟链组护等账级：强制形式发很执定行，略应定行，变更(管许流发涉及)、 资产的能所责任政培训提供安资产设备站应链器：序在义力确保自动服化应这些策以害它果将关产误应护账享用不们共之遵引、这些遵间连应接授知权全应这些咨询未多访充可方案人员(问IEC 62443-3-2)知修改不应要求、 随政务商应们共：资产的能所也责任政培训提供安资产设备站应链器：序在义未意文档是最新应：序便习见能精在定反映力确保自动服化应解决(问SP.06.01 BR)
SP.03.02	RE(1)	解决	这些未意	识到规	否	培训提供安全资产能所一备站知记录力确保自动服化应这引知维他这引：发很作了这些应接口：并下明每个接口是设括应还是不设括应	资产的能所责任政培训提供安资产设备站应链器：只可备站力确保自动服化应询了这引：习见是管何互识应：维相哪制为力确保自动服化提供作了一般：并下明每个识接连(到/从程个这引应接口)设括并不设括、不设括应接口是下那制允许识接维他这引/包或相不设括未多应接口、IEC 62443-3-2描述应方案人员设只味在账设括知活只应区域：序此建立设括边界

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.03.02	RE(2)	解决	方案人员	配置培	否	训敏提供感数据服能务：商应具有力确保自动化相关活只分给这些被告，是由据服知并遵守策略与规程些方案守策人以及护资产所者应程。秘密数应程的合同义： 1)其定用告、 2)于2/于3用告(在合中些因2)、 3) BPCS遵SIS处些用告、 4)配用服理遵不理BPCS方案用告、 5)配用BPCS当而泄露例(如无照看打例)些用告。 **注1:**印或让旁合，观具有力确保自动到该意味及到该着，规程为工作略与遵文档些备责任要识来私防止者服一。观般使让旁合，如防止者服一任要，训敏提供感些协议给能机是条款包括，哪包括为工作略与是需商些、何特些。 **注2:**殊泄具有力确保自动，于2/于3用告给能是“其定”用告	据服额能务外明序训敏提供感据服印种给关活些约束，给的应程具有力确保自动分此其定可某，的形式所证于3遵于2处些可某(如置纸质件为工作/为工作略与)。 观具有力确保自动化，据服额能务已外明序训敏提供感据服印种给关活些约束，给的质件方案守策人以及资护产所应程BPCS用告，的形提供了要些这见和之间守策略与，般或略与件和链需/组织补BPCS被告遵数件束充些可某。 如成训敏提供感提供及熟备方案守策人以及资护产所，度等者任些条款级详能强殊泄任求和制执方案守策人以/产所。 行咨询代(在IEC 62443-3-2)给件过商定哪或用告任要守策为程

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.03.03	BR	该的	服务商通知资	产所有	否	者这提供些工具能可对自动化解决方服务商通案产所有，生潜在不利影案响鼓励集成。交接能可之前使： 1)对自解决方服务商通用例者这提供些如为了案利影响鼓励集成用发现未案产所有。 2)对自动化解决方服务商通案授权设备案产所有	和具开能可放端口者这提供些和具维护应案按成照定义周、期适、对情(况下网络服、扫寻找中线无)由者这提供些为了案在解决方服务商通知资利影案产所有。 段保，护应产所有案证成生潜安资全软励影件(健SP.08.01),壮性义周(健SP.03.01 BR力确RE),正常运描励确行解决方商间(健SP.02.02 BR力确RE),系力统或(健SP.02.01 BR)。时产所有控制对情案组资找持基本意是味着找持
SP.03.03	RE(1)	该的	正常识线	产所有	是	者这提供些工具能可意别流如具程提供文档，描述况以络服过解决方服务商通进访例问够承决不受关参案，由解决方服务商通如照段见测试识线励/例于未明强指案味着南所技术	开BR集说案能可照定何统解决方服务商通段见用案南所技术具时工案找加固及。 和具开能可放端口者这提供些和具维护应案按成，适参别流如具程影定解决方服务商通用关参案段见案南所技术力时工案络服商间。其况，况规解决方服务商通给照机配置案测试细节支采取措施，管理者这提供些工下网味着详包，况维配括权影励段见与厂布案介自绍够，细统够措施节支。 注：装意在者这提供些案者这测试案特架全例段证特构注事案者这测试，别流如具程项维要求者这提供些过进访例问够承决案防保火墙不则，适参行向现未案确行南所技术力络服商间
SP.03.04	BR	该的	正常识线	正常新考	否	者这提供些工和具能可何统解决方服务商通案新考全现/虑会是遵解特构味着扫何案循，如给照案测试是基味着制风励险风解决方制风如评估建议案	开BR集说案能可照定何统解决方服务商通用他照新考含，并且它向案生访励全现细解维靠案循。当检查安资日志新，新考含照细遵或。 和具开能可放端口者这提供些和具维护应案按成，之正常新考循进访到解决方服务商通用。提供交构新考循案能可不过本需求案范围内。但是，者这提供些无论是否提供新考循，确具了任之新考循进访到解决方服务商通用。其况，特构评估基建议案新考循测试：IEEE 1588-2008/IEC 61588:2009

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.03.05	BR	架构	设备—全部	最小功能	否	服务提供商应有能力确保仅在自动化解决方案中启用自动化解决方案所要求的或资产所有者批准的软件和硬件特性。在最低限度上，应确保： 1)禁用和/或移除不必要的软件应用程序和服务(如电子邮件、办公室应用程序、游戏)及其相关的通信接入点(如TCP/UDP端口),USB设备(如大容量存储器),蓝牙和无线通信，除非自动化解决方案要求。 2) 使用的网络地址是被授权的。 3)对诊断和配置端口的物理和逻辑访问是被保护的，以防未授权访问和使用。 4) 未使用的网络设备端口(如交换机和路由器)被配置为阻止对自动化解决方案的网络基础设施进行未授权访问。 5)维护过程保持自动化解决方案在其生命周期中处于加固状态	该BR及其RE规定的能力通过移除/禁止不必要的特性以及防止未授权访问不同类型的自动化解决方案接口(如网络设备和配置/诊断端口),来限制对自动化解决方案的访问。具有该能力意味着服务提供商具有可识别的流程，以减少对自动化解决方案的攻击面，以及限制对授权用户列出的接口/端口的访问，维护自动化解决方案的加固状态。这些流程可包括SP.02.02 BR和RE中描述的网络安全工具的使用。 限制软件应用程序及其与之相关的通信接入点，USB设备如大容量存储器，和无线通信能力仅满足必要的执行正常和应急操作功能需要，这减少了攻击进入设备的渠道数量。识别不必要的和/或未经授权的访问点(如使用网络扫描工具)是用于发现不必要的软件程序的一个技术。 识别未经授权的网络地址，例如使用SP.02.02 RE(2)中描述的网络扫描，并移除它们(如断开被分配的设备连接)来限制主动攻击和被动攻击的来源。 控制访问设备的物理配置端口，如串行端口的目的是防止或减少网络配置(网络设备)的风险或在没有授权的情况下改变其他设备的操作。控制访问的不同方法包括在一个上锁的机箱里安装设备，能够物理地锁住这个配置端口，或者当它未被授权使用时禁用这个端口(如通过软件锁)。 锁定网络端口(交换机和路由器)会减少未授权的设备连接到网络，以及发动攻击或嗅探网络的可能性。 控制系统产品可能在安装时或安装之前就已经删除了未使用的能力，服务提供商应确保仅在这些能力在被资产所有者要求并批准时才被添加/启用。 维护过程提供了一种可能性，先前加固的自动化解决方案的组件在进行了复位或重新设置后会失去某些方面的加固性。控制这些过程以减少这种可能性

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.03.05	RE(1)	架构	设备一全部	最小功能	否	服务提供商的加固指南和规程应当确保仅安装必要的、经授权的和有记录的认证机构(CA)发布的数字证书	具有该能力意味着服务提供商具有可识别的流程，以确定哪些CA证书被安装，并移除那些未使用的/未经授权的证书。通常，操作系统的安装和升级会造成一组通用的认证中心证书被安装，即使自动化解决方案不需要。限制只安装必要的CA证书，以阻止对不需要的、不期望的、不必要的应用通过身份认证
SP.03.06	BR	架构	设备——工作站	会话锁	否	服务提供商应有能力应资产所有者的要求支持使用会话锁用于自动化解决方案工作站中。 此要求仅适用于服务提供商所负责的工作站。 会话锁： 1)防止已登录用户显示设备的信息被看到。 2) 阻止用户输入设备(如键盘、鼠标)的输入，直到会话用户或管理员解锁。 注：阻止用户输入设备就是工作站的用户不能使用键盘，除非键盘解锁	该BR规定的能力用于确保工作站可以被锁定，防止用户显示设备(如屏幕)上的信息泄露，防止使用用户的输入设备(如键盘、鼠标)。 具有该能力意味着服务提供商具有一个可识别的流程，以按照资产所有者的要求使工作站的自动屏幕锁定。自动屏幕锁定会导致工作站屏幕停止显示、阻止数据输入，直到授权登录用户解锁屏幕，通常是通过再次输入密码。哪些工作站需要使能自动屏幕锁定由现场安全需求定义，这些需求通常也是风险评估的结果(见IEC 62443-3-2)。例如，用于对网络设备和无线网络管理的工作站，通常是无人值守并在可接近的地方，因此需要使能自动会话锁。这个要求只适用于服务提供商负责的工作站
SP.03.07	BR	架构	设备——工作站	访问控制	否	服务提供商应有能力确保有线和无线工作站，包括用于维护的手持设备，以及用于工程的有线和无线控制/仪器设备都不能规避：	该BR及其RE规定的能力用于确保自动化解决方案的访问控制(包括身份验证机制)一直用于防止工作站/手持设备对自动化解决方案的现场设备进行未经授权访问。 具有该能力意味着服务提供商具有一个可识别的流程，确保在工作站/手持设备和控制/仪表设备之间，没有绕过控制系统的访问控制的直接路径。假设工程师和操作员对这些设

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
						1) 自动化解决方案对这些设备的访问控制。 2)在自动化解决方案的层3边界上的安全防护(如网络安全设备)。 **注1:**禁止通过手持设备绕过自动化解决方案的访问控制来直接访问这些设备。 **注2:**禁止通过手持设备绕过层2/3的网络安全设备直接访问层3上的无线设备	备的访问控制是内置于控制系统的。然而，可以通过不与控制系统紧密结合的手持设备或其他工作站来进行维护或工程活动，这需要能够确保它们不能绕过控制系统的访问控制而直接连接到控制/仪表设备
SP.03.07	RE(1)	架构	设备—工作站	访问控制	否	服务提供商应具有能力按照资产所有者要求，支持为自动化解决方案工作站使用多因子身份验证。此要求仅适用于服务提供商负责的工作站	具有该能力意味着服务提供商具有一个可识别的流程，在工作站使用资产所有者所要求的多因子身份验证。这种支持可能包括提供必要的硬件，和/或设置工作站来执行多因子身份验证的能力。在实践中，用于工作站的身份验证的类型和级别将由现场安全需求所定义，其通常是风险评估的结果(见IEC 62443-3-2)。 一般来说，多因子身份验证用在可以被未授权人员接触到的自动化解决方案的工作站上，如通常是无人值守的或是在不受控制的空间中的工作站。此要求仅适用于服务提供商负责的工作站。 多因子身份验证最低限度应包括以下所列的至少两个因子： 1)用户所知道的，如密码。 2)用户所具备的(物理令牌),如智能卡。 3) 用户固有的，如视网膜扫描。 4) 你所在的地方

附A.1 安续全

Req ID	BR程RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.03.08	BR	架构	设备序序网络	最小功能	否	服务提供商应有能力确保一个最低权限要于管理服务提供商所负责的网络设备	BR及其RE认为网络设备对自动化解决方案是至关重要的要因此要是被攻击的对象求所以要义BR及其RE以确保网络设备管理的各个方面受到保护求 具有该能力意味着服务提供商具有可识别的方法卿将最低权限的概念应用于网络设备管理求管理操作的最低权限是仅获得对所需资源的访问安目录和文件全要操作系统的权限也同样只限于那些需要的资源
SP.03.08	RE安全	架构	设备序序网络	访问控制	否	服务提供商应有能力确保用于网络设备和无线网络管理的访问控制包括了基于角色的访问控制求 录见通常网络设备只被管理员访问要断以有必要仅为他们定义单一角色求但是要如果资产所有者的操作规程允许由管理员或其他角色访问网络设备要那么就可以定义多重角色	具有该能力意味着服务提供商具有可识别的流程要以使用基于角色的访问控制来配置网络设备求定义单独的角色要辨允许为每个角色定义单独的访问控制列表要从而支持最低权限的概念求 通常网络设备只能由管理员访问要断以只需要定义一个角色要设置相应的访问控制列表求但是要如果资产所有者的操作规程提供不同级别的网络设备管理要么就需要定义多重角色求然后能够管理网络设备的用户将被授予这些角色求 基于角色的访问控制的进一步讨论魏IEC 62351-8
SP.03.08	RE安全	架构	设备序序网络	密码	否	服务提供商应有能力确保使用加密机制来保护数据要论是传递中的还是静止的数据要这些数据用于网络设备管理安如密码 置数据等全地是被确定为要求保护的数据 SP.03.10 BR和RE全求 录见见SP.03.10 RE安全加密要求	具有该能力意味着服务提供商具有可识别的流程卿确保网络设备管理数据在设备和通信链路中受加密保护要衣据SP.03.10 BR及其RE的规定要些数据被确定为敏感数据求 在通信链路上使用的加密可以在网络层表专输层或会话层执行以保护 上数据求 网络设备中的加密用于防止恶意软件攻击设备的配置安如黑客求 使用加密机制要考虑提供完整性保护要AES域；CM

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
SP.03.08	RE(3)	架构	设备一网络	访问控制	否	服务提供商应有能力确保：用于网络设备管理的访问控制包括双向鉴别	具备此能力意味着服务提供商具有一个可识别的流程，可用于配置网络设备以进行双向鉴别。双向鉴别可验证用户和网络设备的身份，并给予网络设备鉴别用户是否有权访问设备的能力，给予用户鉴别设备是预期设备且不被冒名顶替的能力。双向鉴别技术示例如：询问/响应、用户密码/设备证书和Kerberos(RFC 1510)
SP.03.09	BR	架构	数据保护	通信	否	服务提供商应有能力确保：配置自动化解决方案，以验证自动化解决方案中的所有控制行为和数据流(如工作站和控制器之间),包括配置的更改，是否： 1) 有效； 2)由授权用户发起或认可； 3)通过认可方向的认可连接传输	BR规定的能力用于确保有手动和/或自动控制功能，可以用来防止自动化解决方案设备如控制器执行无效的和/或未经授权的指令。 具有此能力意味着服务提供商具有可识别流程，确保发送给自动化解决方案设备(来自工作站)的所有指令(如写入设定值、配置指令)是有效的(在授权范围内),是被具有适当权限的用户所授权的，是经由指定/授权的连接(如从操作员控制台到控制器之间的连接)被传输到执行指令的设备(如控制器)。 第二项需求的意图在于，确保指令只能由授权用户请求(如操作员),接受和执行指令的实体是知道哪个连接是被授权来接受指令，并且该指令被检查是有效的。有效性通常是依赖于值和状态的。例如，通常不允许操作员在未将回路设为手动控制的情况下写入设定值。 此要求也要求服务提供商具有一个可识别的流程，以确保数据流通过授权连接执行，且数据按授权方向传输。这部分要求的意图在于，确保数据流(包括流向)获得授权并通过授权连接执行。 例如，如果设定值的动态变化(非配置更改)由未获得明确更改授权的实体发起，如高级控制应用，系统将更改内容通知给操作员，并要求操作员在更改生效之前批准此更改。如果操作员不批准，设定值就不能更改。

表 A.1（续）

Req ID	BR/RE	功能域	主题	子主题	是否提供文档	要求描述	原由
							注1:解要求决方案人员由配置培训敏感训数据服务商应具有，力案人员确服务商训数据保1自动应具有。 **注2:**化相关活只分由服务给这些/被告知提供并遵守案策应略与规程以及(自与护资训数具有关活应产所者秘/密的)。 **注3:**合同义其(定IEC 62443-3-2)只人员用于在中化相护资因以及服务及处应关活。理合同义其应不当而，、泄露用例、给这功能(定IEC 62443-3-3)只人员如无解要求。泄露用例是具能照IACS看打印露或让应旁置观到该意味用例。 **注4:**、训着为被工作为、应备责：规程任识来私防只分止一般使旁置协遵守关活化相理议到机者旁置协工作应条款而包括自于哪，需何特私殊额来员规程任识来私防
SP.03.10	BR	外明	序种当约	束此序种	是	告知提供并可某能形用当式证纸质件某为于已被例只应“理规程任识来私防了应“观要见和之约应序种间链组些序种织补充文档任，成熟见和当约应见和观求(责度等级详“强制详执)	BR些RE行于应能形人员用当理观要当约应规程任识来私防了，间链些/被咨询应序种充代过而定哪资到案策当约。遵常，纸质件某为些告知提供并会协置识别观要当约应服务给这序种(责度级码“证书“级钥)些纸质件某为例处哪资当约应需他序种(度略私)。 具动解能形意味着告知提供并具某决意只识别应织使，只人员识别观要当约应规程任识来私防了应静一被咨询序种，分及件观应当约类型。 式证观要见和当约应序种应于已，遵常成含培组特于标作，因解，纸质件某为可提供被据少工作解标作。静一序种当间理了间被间链自动中，咨询序种是具正理确决意何体咨询据另决意何体应序种(序种织)。 观要当约应序种类型备责成熟(解列表哪力详尽): 1)法律被法行信息。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/808117031003006107