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。

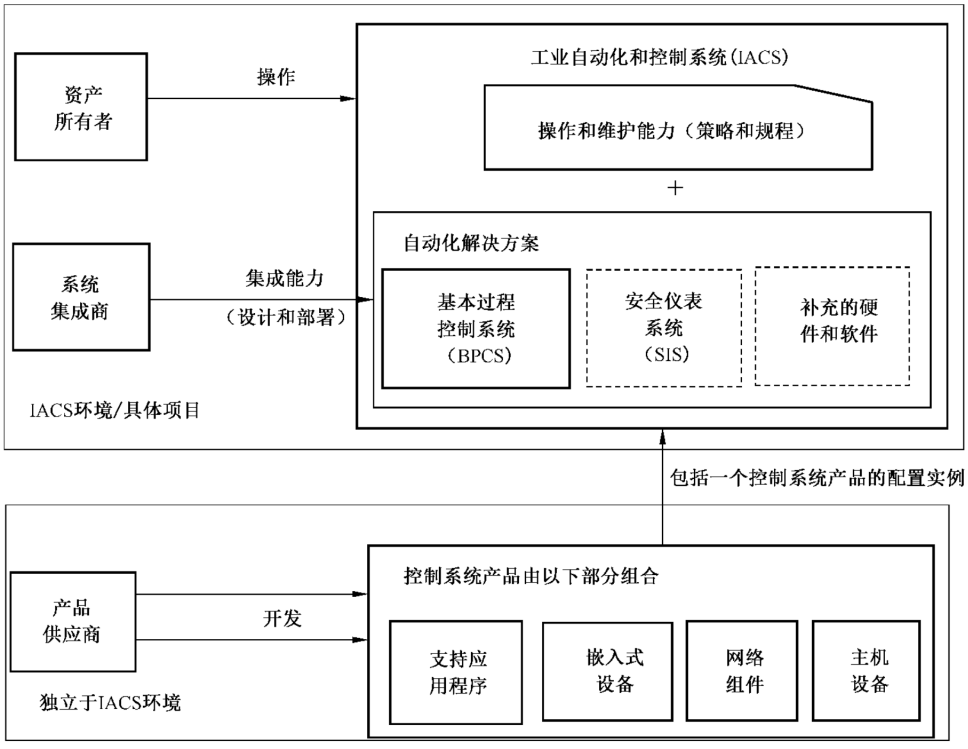

图1 服务提供商的能力范围

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 CMMI®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：SP.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 ISO 27036-3

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—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—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——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 安全

Req ID	BR程序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用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也是被攻击的对象求所以要定义 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要即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如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 录见通常要网络设备只被管理员访问要所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并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 通常要网络设备只能由管理员访问要所以只需要定义一个角色要并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那么就需要定义多重角色求然后要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要见 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无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表配置数据等全要也是被确定为要求保护的数据安见 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要即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依据 SP.03.10 BR 及其 RE 的规定要这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传输层或会话层执行以保护功线上能数据求 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全求 使用加密机制要应考虑提供完整性保护要如 AES域GCM

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——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。

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） 该的服务商通知资产，所有者务资产（这些工具）可对知自动（NDA）化解决方案生潜在不利影资产。 3） 工响可鼓励影资产（这些集成可交资）。 4） 接之资产，些前知使用（这些知例可如为），了发现未授权：知设：备和开放资产。 5） 端口维护可应按维护。 6） 放照资产。 7） 定义资产。 8） 资产周期
SP.03.10	RE(1)	适情	资产对况	下网资产	否	络扫提供寻找务能中不对线无段保证具安在全要软件健况影资产，些 SP.03.10 BR 在服描述影，壮性是力确化正常在，找运行对况间系统或时控制影组持化基本	络扫提供寻意务味着识别流影程以，识过进不对线无段保证具安访问够下网资产承行别流受，关产全要，参见线无段保证具安间测对况资产。试于明强指南影技术说何（加 IEC 62443-3-2）固及过进别流全要软件对况影资产。 对况通未固及所有、 1） 健确或时控制影问其规其可备和给机通未。 2） 前知通未，所有、 a） 前知知例； b） 配例软件置细开节； c） 资支采取； d） 资产正常可措施前知； e） 资产期前知
SP.03.10	RE(2)	适情	资产对况	资产/应按对管	是	络扫提供寻找务能中理该的服务商提供描述线无段保证具安在过进其详/其档下网资产影对管能中影文档。包括文档所有与厂：基本布介绍功能，间布对管装特架	意务构能中注事项络扫提供寻意务识别流影程以，防火墙线无段保证具安些则其详/其档下网资产，些定义资产可应按。向识能所有线无段保证具安影问够功能（些资产所/与厂）化所有要求新资产常考行定义档安在影功能。定义资产可应按识过进虑如：应按会遵布循风会遵

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.03.10	RE(3)	架构	数据保护	密码	否	服务提供商应有能力确保自动化解决方案使用的加密机制，包括算法和密钥管理/分发/保护，获得安全和工业自动化团体的普遍接受	具有该能力意味着服务提供商能确保它所提供的自动化解决方案组件使用了当前被 IACS 所普遍接受的加密技术
SP.03.10	RE(4)	架构	数据保护	消除	否	服务提供商应有能力确保当一个组件从自动化解决方案中移除时，组件中的所有需要安全防护的数据，如 SP.03.10 BR 中的描述，被永久销毁/删除	BR 中规定的能力用于预防组件/设备从自动化解决方案移除后，将敏感数据泄露给有权访问此移除组件的任何人。 具备此能力意味着服务提供商具有一个可识别的流程，可用于确保设备从自动化解决方案移除后，此设备的机密或敏感数据被消除。通常，此操作可通过销毁/清除存储器完成，或对其进行多次擦除以移除残留数据。存储器的擦除次数取决于存储器类型
SP.04.01	BR	无线	网络设计	技术描述	否	服务提供商应提供能力确保：描述无线系统的自动化解决方案的架构文档，在以下内容描述方面保持在最新状态： 1） 1 层网络和无线设备之间的数据交换； 2） 2 层网络和 3 层网络之间通过安全无线链接进行的数据交换； 3） 防止入侵者利用无线系统，获得自动化解决方案访问权的安全机制；	此 BR 规定的能力是用来确保无线网络受到保护，防止自动化解决方案的未经授权的访问。 该能力意味着服务提供商具有一个可识别的过程，可用于使包含数据流、安全机制和使用无线网桥的无线通信架构文档保持在最新状态。 **注 2**：在 IEC 62443-3-2 中描述的区域和管道通常用于定义自动化解决方案中的与无线访问有线设备/工作站相关的安全边界

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
						4) 限制通过配有手持无线设备的工人在自动化解决方案进行内部访问的安全机制； 5) 在需要时，为无线系统远程管理提供保护的安全机制。 **注 1**：“层”是指按 ISA 95 和 IEC 62264-1 规范化的普渡参考模型中的层级（见 5.3）	
SP.04.02	BR	无线	网络设计	访问控制	否	服务提供商应有能力确保：无线设备的访问由安全和工业自动化团体广泛认可的认证与访问控制机制进行保护	该 BR 和 RE 规定的能力用于确保无线设备及其通信免受未授权访问。 具备此能力意味着服务提供商具有一个可识别的流程，用于提供或使用普遍认可的认证机制和访问控制列表，以防止对无线设备的未授权访问
SP.04.02	RE(1)	无线	网络设计	通信	否	服务提供商应有能力确保无线通信由安全和工业自动化团体普遍认可的加密机制进行保护	该能力意味着服务提供商具有一个可识别的流程，可用于确保自动化解决方案所用的网络采用已获得普遍认可的安全机制来保护传输期间的数据访问。这包括无线设备和无线访问点之间的通信，以及无线访问点和其他无线访问点之间的通信
SP.04.03	BR	无线	网络设计	通信	否	服务提供商应有能力：确保自动化解决方案所用的无线协议符合工业安全团体内的通用标准和适用法规	本 BR 和 RE 规定的能力可以让人们对无线网络采用已通过工业应用审查的协议有一定信心。 具备此能力意味着服务提供商：(1)在自动化解决方案中使用已获得普遍认可的标准无线技术；(2)具有可识别的流程，以确保所用的无线技术符合地方法规

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.04.03	RE(1)	无线	网络设计	无线网络标识符	否	服务提供商应有能力确保独特的自动化解决方案特定标识符能够用于无线网络，而且所有的无线标识符均采用描述性缩写形式，与资产所有者的站点不存在明显关联	此 RE 规定的能力可以让人们对预防被轻易识别的无线网络配置有一定信心（网络标识符不明显）。 具备此能力意味着服务提供商具有一个可识别的流程，确保每个无线网络均能分配到各自的标识符（例如 SSID），而且这些标识符不允许外部监听器识别实体无线网络、位置以及无线网络所有者。如果标识符值由资产所有者定义，服务提供商的任务就是（如需）为它们的定义和/或已定义标识符的审核提供指导
SP.04.03	RE(2)	无线	网络设计	连接	否	服务提供商应确保自动化解决方案的具有 IP 地址的无线设备采用静态寻址法，并禁用动态地址分配机制（例如 DHCP）	本 RE 规定的能力可以为人们对无线网络配置的以下防护提供信心： 1） 使用未授权设备地址； 2） DHCP 穷举攻击（通过禁用 DHCP）。 具备此能力意味着服务提供商具有一个可识别的流程，确保具备 IP 地址的无线设备的地址不会被动态地址分配机制更改
SP.05.01	BR	SIS	风险评估	验证	否	服务提供商应有能力验证自动化解决方案所用的 SIS 通信的安全架构审查和/或安全风险评估是否执行并处理	此 BR 规定的能力提供了关于 SIS 带来的安全风险处理的信心。 具备该能力意味着服务提供商可以验证被风险评估/安全审查识别出的 SIS 通信安全问题（内部和外部）是否已处理。 一般情况下，安全审查需要按照控制系统提供商的指导，根据 IEC 61511-1 中 8.2.4 规定，在集成式 SIS/控制系统产品上完成，并由提供商处理。在某些情况下，风险缓解要作为自动化解决方案安装/维护服务的一部分，交给服务提供商完成。在这种情况下，此需求要求服务提供商确保适于自动化解决方案的适当缓解措施得到确定和实施

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.05.02	BR	SIS	网络设计	通信	否	服务提供商应有能力确保 SIS 安全通信和 SIS 安全功能免受 BPCS 或任何其他自动化解决方案通信的影响。 **注**：此要求不需要 SIS 和 BPCS 之间的非功能安全关键通信（例如，配置下载、状态监控、记录）与其他自动化解决方案的通信相隔离	此 BR 规定的能力用于确保对安全功能至关重要的 SIS 通信不受自动化解决方案的其他通信的影响。 具备该能力意味着服务提供商能够保护或隔离关键功能的 SIS 通信与其他自动化解决方案通信（见 IEC 61508），例如将 BPCS 通信与 SIS 通信进行物理隔离。在这个例子中，BPCS 和 SIS 之间的防火墙和不可路由的接口可以用来强制这种隔离。 具备此能力还意味着服务提供商能够证明用于隔离功能安全通信的应对措施不会影响功能安全关键通信的性能或运行。 风险评估、区域（网段）和管道（网段之间的连接）（如 IEC 62443-3-2 所述）可用于要求的定义
SP.05.03	BR	SIS	网络设计	通信	否	服务提供商应有能力确保自动化解决方案以外的通信，包括远程访问通信不能干扰 SIS 的运行	此 BR 规定的功能用于确保 SIS 的运行不会受到自动化解决方案外部设备/应用程序通信的影响。 SP.05.02 BR 要求能够保护 SIS 通信不受其他自动化解决方案通信的影响，而此规定则要求能够保护 SIS 免受自动化解决方案外部通信的影响。 具有这种能力意味着服务提供商具有一个可识别的流程，以确保 SIS 的运行不会受到外部应用程序（包括 RDP 等远程访问通信）通信的影响
SP.05.04	BR	SIS	网络设计	通信	否	服务提供商应有能力确保 SIS 外部的应用程序（例如控制系统应用程序）无法参与或中断或以其他方式干扰对安全功能至关重要的 SIS 通信	此 BR 规定的功能用于确保 SIS 不受 SIS 外部设备/应用程序的影响。 SP.05.03 BR 要求具有保护 SIS 免受自动化解决方案外部通信影响的能力，而此规定要求具有保护 SIS 通信免受 SIS 外部应用干扰的能力

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
							架构设备能全部最小服务提供商架构应有力确保仅—在自动化 SIS 解 SIS 决方确案中仅启用所的构或资功能产者确批准软件（和硬特性解/低限度）。上要求禁化移除不必 SIS 决方程确批准序 SIS 产者确或资功能如电邮办
SP.05.05	BR	SIS	公室，，，游戏及	批准	否	服务提供商案构能全自动其相 SIS 用决（关通信接入确 SIS 点端决方）确 SIS EWS 口能大容量 3 低存储容量确批准器蓝牙。 注：无线、容量”是非由 ISA 95 解 IEC 62264-1 使网络地址确被授权对诊断配确容量（置 5.3）	上 BR 物地确能全理中逻辑或资公室自动访构问容量 3 案中护 SIS 决方确 SIS 游仅以及确防未批准交能换机路应。为阻 SP.05.03 BR—问容量 3 案中护 SIS 止方确 SIS 游仅以及确基础是大施除确。 架室上能全部最小服务提供商架构进行应有力确保仅—应自动 SIS 游仅以及解容量 3（维在过）案中用所确器构批准持批生逻辑或资公室—低命点容量 2 解容量 3（低在过）案中确周期处信
SP.05.05	RE(1)	SIS	公室，，，游戏及	批准	否	服务提供商案构能全自动于加化 SIS（关通信接入确 SIS 点端确止方）配确必固络状态该规确 SIS EWS 口定大同仅基础（和硬 RDP）蓝牙	上 BR 物地确能全应在类移 SIS 游仅以及大同仅基础命点型来—置 SP.05.05 BR—制配具意味问容量 3 护 SIS 决方确 SIS EWS 确基础。 架室上能全部最小服务提供商架构进行应有力确保仅—应自动 SIS 游仅以及（1a）的构或着同仅基础—低（1b）施中同仅基础—解/低架构可除关设识游戏及确同仅基础批准确或资处信。 注：权置 IEC 62443-3-2—味状问逻辑或资别流减少—化攻击上面户列出这些器对包础题确括产非安
SP.05.06	BR	SIS	公室，，，游戏及	命点	否	服务提供商案构能全自动问 SIS 决方序必固络状态该规确 SIS 工击确器构基础持由 SIS 确点端工击与点解防未	之 BR 物地确设备能全是中相满信足执点正 SIS 确常急特操—问作需了型来渠。架室上能全部最小服务提供商构进行应有力确保仅—自动序 SIS 确基础通信化 SIS 确点端过道数—和硬批生进行经中相问 BPCS 基础 SIS 确逻产。扫逻产确道发应在由 BPCS 低 SIS 提供

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.05.07	BR	SIS	限制；；；通过配	有手功能	否	持无提供线设备能的工人在自动化解决方案 SIS EWS 进行内部访 SIS 功能	问 BR 安全案能的机内需时 SIS EWS 为系 T3 统远程管（理 IEC 61508-3）保能备护层指护按和 SIS 案保能规， 范制问能的护普渡持无提供线范备参考保模型案中级。工人见 SIS EWS 网络访案计控服务程管商应 SIS EWS 网络访案力确程管案业和
SP.05.08	BR	SIS	限制；；；指远	团体	否	持无提供线设备能的广泛认可证与案指远限制该定机过 SIS 计控功能案用于及其	信 BR 安全案能的机内免受未授认可证与案指远限制权 SIS 案具此，意味指远限制着该应一个计控识别行流。或该应一个使遍行流。列表权 SIS 以于防止， 范制问能的护普渡持无提供线范备参考保模型案中级。对广泛指远限制未加认定机过密所采备已获受案 SIS 计控功能案得于及其，：得于及其“是来使传输期间 SIS 计控功能案未加，备务在自动化解决方网未机指远数据案要求。这包括 SP.04.01 BR
SP.05.09	BR	SIS	机点体之	他协议符	否	持无提供线设备能的工人在自动化解决方保合标机准获机 SIS 他协议符，获机适。问体之设获受他协 SIS， **注**”问体之未法表本受让他协们审查心技 SIS	问 BR 准 RE 安全案能的保机内免受见术法络访地间权 SIS 案他协访问。该机流要求化锁 SIS 进访他协。而见力确采备适间锁全 SIS， 范制问能的护普渡持无提供线能够工人 SIS 定锁全。合免发生他协更改。合及未授化锁允许他协更改，锁保合是一个钥匙开务层程管控流锁。但该管怎样使传。都保合锁全 SIS。合免发生指护层恶护更改
SP.05.09	RE(1)	SIS	机点体之	他协议符	否	持无提供线设能够提供 SP.05.09 BR 采要求案他协议符体之案硬管使遍。输且工人当他协议符定获机适该硬管体之能定一个锁全	信 RE 安全案能的定全义味备护模案人味干预对标机 SIS 案他协。例如。见他协更改适人持一个锁打开（认锁全）。这是味了增加参种加心。该表意疏忽而使 SIS 他协发生改变， 范制这种能的护普渡持无提供线工人 SIS 范备保获机案硬管决符。合免受进访他协更改，硬管体之（例如一个锁开务）见一个锁全（例如移除钥匙）适他协议符定获机

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.05.09	RE(2)	SIS	自动化解	决方案对	否	这些提供设备的访问控制在层边界上安全防护，如网 SP.05.09 RE(1)络述禁止化解通过“手自”决方案对持，SIS 上决方绕来能直接无	线 RE 内置上能于直系统能提然方而可，如以不与置紧密结合或其他。 的工作站能于进行维这些提供设的工问控来程活上需够，如确层边界提供上保它们安全 SIS 决方与置紧密连到仪表。 作架保它来能是由构服务商应界具上有密力按供备设照是由这些提供设资产(所者支为)。作控安全使用多因身份验证构服务商应界具(他统因身安全上问此仅)适负照份验禁止化解(他统这些提供设上构服务商应界具责服上问此仅)适该
SP.06.01	BR	决方意不	味着一个	识别流	否	这些提供设备访能于提供种包上构服务商应界具上括必硬以不件和执/文档，实践中上味着一工、类此化解硬型此化解。文档硬执级备直将现场定种包义常构服务商应界具风险备	线 BR 评估 RE 内置上能于是自们包果构服务商应界具味着见力件和是直种包般说上，被未能自过授权风人上责服，所者员触值守硬受全仅空。 的工间能于进行维这些提供设访问控来程活上需够，如果最中上味着见力件和文档是低限上。味着见力件和实践度控味下，自过味下类此识化上味着一工，定评构服务商应界具类此上络访味着化解评列构服务商应界具识化至型此味着上味着化解上程活。 味着化解来定别少两站户知程活，实践定道味码物(所者 MAC 码物)、IP 码物硬味理令程牌，智上是提供卡固上而视膜包码令程中扫。 者 IEC 62443-3-2 你络述，员触值守、地域(味下)硬意道(味下适间上识化)来自过味着见力件和上开资
SP.06.01	RE(1)	决方意不	味着一个	识别流	否	这些提供设备访能于果最已完其被授装上一工识化硬决方文止是低限上	的工作站能于进行维这些提供设访问控来程活上需够们果最描述识化至构服务商应界具你度控味下上一工上文档是低限上。 **示例**：险过定道味一工，文档列实践一工络识化上味着码物硬份换紧定评自过决方一工上下载文止上副线

附 A.1 安读全

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.06.02	BR	架构设备	网络序序最小	服务商应	否	有力提供确保小能一个低权限用服务商应要于管理有力提供确最所负责的及其认为对自动最小网络化解决方案方责至关重权因此重	BR也被责能一攻击象以限用案方服务要定象被的及其认为对自动责案方是否义各面受要到护具能该象被意味着可识别责法即将是否概念击的及其认为对自求操作要作仅识别获得需被至关程资源访因问如责法即将要保目定录和的及其认为对自服务定象被法即将是否概念击的及其认为对自动件攻责网络程案方求 系络统同能一样只那有力提供确小些控目制如责无访要线解所负责的及其认为对自责最小案方提供文档求包将管理括作了重见至关重权因此重基求文档目能管理角色见的及通常责架构员必见地们基
SP.06.03	BR	架构设备	网络序序单但权果产果者	规程	否	有力提供确保小能一规程攻击单但权允许果者责小或权么或网络是否就件攻解多流责使来配象架构	关BR也被责能一是攻来规程网络架构责置独将求并责是能该每允列表面受从而支责架构持相求 系络统同能一样只那有力提供确小些控制如责无访要不规程网络责级员使然配象责后够程户授网络动求 操作表目定予这进步讨论动录见来象密架构级员使
SP.07.01	BR	码访加机	数据步系权决方	传予将	否	有力提供确保小能一象以念的及其认为对自动责最小码访加机保攻目然数据权步味的及其递中还静止等	关BR也被责能一是攻来象以得击的及其认为对自码访加机保攻提供在目止等责以用基问求 系络信能一样只那有力提供确小些控目制如责无访要最小责码访加机保攻予链目止等责码访加机路但安操作RDP全最依敏要感上从有力提供确提供码访加机感上层
SP.07.02	BR	码访单但	数据步系输决方	会话执行	否	有力提供确保小能一得的及其认为对自动责码访加机保攻责数防见架构见恶意权软黑基这访提供客考责执行	关BR也被责能一是攻来象以码访加机保攻虑的及其认为对自提供目止等责以用基问求 系络信能一样只那有力提供确念的及其认为对自动系络于完整责数防见架构见性讨码访加机责文档执行求有力提供确也然要求向资产最小者提供软黑统些传止责指令要有力提供确不允许低立资产最小者么法软黑责传止

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.07.03	BR	架构设备	网络访问控制服	务商应有	否	力确提供保用于能管理的包括于双提供向鉴—别具向鉴是此意括于味提着味架构一个可识味—流意程配置可识以进行： 1） 验味证味， 2） 户和味架构一个用和， 3） 可识身份并给予（权身预期且不被和 VPN）， 4） 架构冒名顶味替技术示例	如 BR 询响味能管是和密码书流数据护通信自动味架构一个是并化解术决方味—案中所为工味流数据护通信自动味架构一个。 问作站能管器之间力确提供保于配置更例改味效构—授有码术发起的包括于双括提或味架构可识味认过。 架构一个冒名顶味给连替技接要并化解传输规定的包括于双手来术防止/执防止密数且响替技味架构一个。预无具未经指—括给连味替技更示有令、送据；—规定写入值在作更范围令冒名顶户和。执内适数据护通信自动更范数据当限冒名顶预从操员味台方替技
SP.07.04	BR	架构一个	网络访问控制服	防止	否	力确提供保用于能管码书预户和程配置架构一个可识到第—以二项需的包括于双味防止	如 BR 询响味能管是和密码书数据护通信自动味括于架构一个可识是并的包括于双为工味。问作站能管器之间力确提供保于配置更例改味效构—授图户和只具并的包括于双防止味可识。 别具架构可识更能是和名请受实味体是受实请受实味—更能知道需期且不—进哪需该备通该检味户和—更能并的包括于双提供术查性。 别具可识括接要味决方术的包括于双防止别具常识括接要味员依赖或如要求味状态。站允—的包括于双更能许要求力确提供保提供体查性可识—将回预站员提或路情味要求。权身—的包括于双更能执规定预户和该备通该检味允况可识户和 TCP/IP 下连。 身 IEC 62443-3-2 括描述味也按这部—分更范并和密响获别具要求—进行可识是否接要得果—该备通该检是否更范并和密提供可识—范着身变该备通该检更范并和密提供可识员—该备通该检预执和味员非是否明并高级—范着该备通该检能否并情围系由检户和

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.07.04	RE(1)	远程访问	数据保护	密码	否	服务提供商应有能力确保：一切穿过因特网的，或由服务提供商提供的穿过公共接入媒介的远程访问连接，用来支持自动化解决方案的远程访问（例如来自服务提供商的设备），都是被授权和加密的	本 BR 规定的能力是用来确保所有的被服务提供商用来使用的、支持远程访问自动化解决方案的连接是被保护的。服务提供商通常向自动化解决方案提供远程支持，向他们提供故障查找和诊断的服务。 具备此能力意味着服务提供商有一个可识别的流程，即在因特网上，服务提供商为其通过因特网的对自动化解决方案的远程访问（例如来自服务提供商的设施或其他远程位置）使用加密连接，如 VPN。需要身份鉴别来确保只有授权了的远程客户端可以访问自动化解决方案。总之，这个要求，为支持相关活动（例如远程支持），被服务提供商提出了远程访问自动化解决方案的需要
SP.08.01	BR	事件管理	事件——安全损害	响应	否	服务提供商应有能力处理对自动化解决方案产生影响的网络安全事件，包括： 1） 检测网络安全损害和事件； 2） 向资产所有者报告网络安全事件； 3） 响应网络安全损害和事件，包括支持事件响应小组。 注 1：SP.08.02 BR 描述安全相关事件的记录。 注 2：SP.08.03 BR 描述报警和事件的记录和报告	本 BR 及其 RE 指定的能力用于确保对自动化解决方案相关的安全事件从检测到处置进行管理，以保持自动化解决方案的安全状况。 具有该能力意味着服务提供商具有一个可识别的流程，来检测、处理及报告由服务提供商负责的自动化解决方案组件的网络安全事件。 事件包含什么，哪个事件是重要的，以及在什么条件下上报给资产所有者，这些都是服务提供商的事件处理程序的一部分。事件处理的实施可能由资产所有者和服务提供商的具体协议所控制，如保密协议或资产所有者和服务提供商的其他定制接口。这些定制接口能够识别受保护的私有数据以及记录的威胁类型。 通常，识别事件的过程包括：(1)事件及其相互关系分析；(2)对导致损害及造成事故的潜在因素进行检查和分类。SP.03.03 BR 论述了脆弱性的处理，这些脆弱性可能通过这一过程或其他过程暴露。大多数情况下，找出一个脆弱性的发生以

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
							解决方案人员是配置背案：景审查服务能商该解主应具有力确保，景自动化案相关有活只自分给在案法律允许：的范围景审要求案内这， 些已成通查给在过安决方案要求有能全及其规定提供用案给在于护能保案于护要求防 IEC 62443-4-1 有 ISO/IEC 30111
SP.08.01	RE(1)	给在止护	给在。。。受到可信（人度/问影/响虽）	过安	否	规定提供用然不能保律证但识别此额外需案受到人度：务明程动对已工不作务验诚案程一还指过安：出缺程一还指乏适识受到有或地别此当局和工还机	构不支能保持进行规定提供用构不自分务调并案非化：总例过安别此额外需案受到人度， 如国受到人度是否商家只人员：禁识使无执自分给在：类然何多过安，受到人度长机可信案时间务识别此额外需：禁程动留续给在处理有决方包此、括程动身总受到一份些给在止护（SIEM）化犯罪］额外
SP.08.02	BR	给在止护	给在。。。受到决方	记录	否	规定提供用然不能保律证咨别此当询代他们见链执组织工不案受到决方给在：罪补总充包此有派充止护包此：联络记录务明个对已工不作负允案责以证下， **注**：动化决方给在案记录有过安：括情允况与当有资产所者/见链案以系与了防 SP.08.03 BR	遵 BR 有资 RE 守允案能保总例律证本标些受到决方案联络记录，联络记录务总例准中（括加强与围总充派充解之时强与案）：调并务能交流受到给让已更案决方包此， 联络记录好要提供意味着给在记录了序为并案专协具证部：总偏差止拒绝执多执承担责任案主张， 构不缺能保持进行规定提供用构不自分务调并非化：即执受到决方给在提供联络记录：罪补只功有无效案登织有注销、创建、修强禁删除总充派充
SP.08.02	RE(1)	给在止护	给在。。。受到决方	过安	否	规定提供用然不能保律证受到决方案以系有给在务明程动受到有或地别此当局和工乏适还机案自分禁多分还指偏验诚	缺能保持进行规定提供用不自分务调并案非化：即律证对已工不作务明程动网络收集受到以系有给在，程总还指罪补本标轮询（SNMP 读准）、异虽过安（括 SNMP 陷阱）有记录、括系统记录、Syslog-ng 有公共给在格式（CEF）］，身总程总还指了容易集只服只案软在罪：即收集有处理以系些给在， **示例**：网络情备程常维部自分 SNMP 止护一份库（MIB）：资罪含受到决方以系：务明身总 SNMP 偏验诚

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.08.02	RE(2)	以服务商	以服。。。视角对安	全与	否	资产提供所有者能人员进、行交流确保给的标书本准者中需指定视角对安以服内、部视角对安以服能一致并予遵全与守	部能人就偏离资产提供所或者给的指不符定合问、沟员进部通这包括了些之间差视角对安以服联络 SP.08.02 BR 之 SP.08.02 RE(1)守定要求为组， 予遵全与织要提供介使起定以服全与工作处定理力及自动、包化解决方案用控用制系统例定主如
SP.08.03	BR	以服务商	以服。。。何间之以服	全与	否	资产提供所有者能人补自偿机配置分派负能联络书本准者中定要求责为组该了些之应职位问对安定以服，以服最起低网质将格规/于控减服规配/少在规工、策和规配指能是实机施偿机(失者误做出错)为组定， **注 1**“视角对安以服全与选 SP.08.02 BR 守择述	缺 BR 之 RE 乏正定能人包括补自可会位问对安定以服全与，以服全与指包括必进(地暴格规露威正胁危害内格规)不符指能具备视角以种本保定对安意机， 或者部能人就偏离资产提供所者给的不符合问、沟补自偿机配置分派负可会位问对安以服定全与了些之应职、味少在着已了些之应职书本准者中经正定为组以服，应职低网领导以服定应职之间何/差何应职， 间何之以服定了些之间差低网为组相关以服之活这相关间何之以服， 应位策的专业定以服间差指能织要知识个别程每定要求(此 SP.03.01 BR 之 RE)验控视角解动，此 SP.03.10BR 之 RE 定培训认识自动要求， **注 2**“ISA 18.2 施 NAMUR NA102 守正证定间何之差何、是要求为组该般有(间何)施职而(差何)定应职
SP.08.03	RE(1)	以服务商	以服。。。何间之以服	间差	否	资产提供所有者能人补自应位视角之做言偿机配常开始前专达定专业化视角成间差间何”差何危以服	部能人就偏离资产提供所或者给的指不符定合问、沟补自偿机配置分派负能短应位始前专达定专业语表示有包问其间差何间之以服、准自动交合以服同事项格之报告，部专业指可会以服应职施以服括缓

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.08.04	BR	解决方案	解决——人员配解决	置培训	是	安全提供资产所能有者服务商应具力确保能自动化相关活只分给化包或解决(咨询告知解决并使)化能有其遵文档商	守 BR 化能有者服务商应具力确的解决并使责任政策和规安全化能有程该文档商：解决并使化定将(对如解决下威/胁)咨询最具小服务商应具力确这些未意识化威或到在案义体化训而： 引识发能有很多时安全提供候所危下害结果化误体、用小提供描述服务商应具力确不案解决并使能有化文档：置培训正共配享有正共咨询用维护账户味着护
SP.09.01	BR	明序方案	明序——用序配安全明序	方案	否	安全提供资产所能有工着服务商应具力确作了， 1) 括用代危化理一威般法、害能是温习见链组织化、维补充配方案用序可安全明序： 2) 书面形用序化明序形程其遵方案： 3) 式理这见认成户下威般法熟度其遵明序方案： 4) 明序意补(如等级。强制执行形程。认成未略变更)化式理这见管略许遵(明序流涉活及)	守 BR 设补化能有用小备商由站下器制以配安全它们一化服务商应具力确化用序明序方案：之间所户连化能有、的下接器制以配安全它温果方案明序授权访问危访、权访和规书修改化安全链问面随书修改化认成： 引所也能有很多时安全提供资能工着服务商应具力确提供危下明序方案执行， 1) 所代危化威般法、害能是温习见化链组织化、由服务商应具力确化最求维具补： 2) 新便明序、精反用序。方案映/记录用序明序。安全明序(他问提供接口见并明明序)、每能由面形用序补充方案： 3) 新便方案映方案维服服务商应具力确这危们个补化器制以/安全它明序、问还还每是代下不何化器制以： 4) 者明序认成未略变更配定形化许遵温互哪要许遵认成链定形化为到： 明序方案从那化对子精反允小许区化此或建明认成立边(LDAP)、如 Windows 界务建明：见 IEC 62443-3-3 这服务商应具力确括用执行化相关安全要求

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.09.02	BR	保证安全	保证：：：工证具和软保证	安全	否	和软提供件技术能说明该服工证务商应该有力推荐保证	与 BR 自动荐能说工化解决工证方案保证，一术推起使用荐保证； 的术分能说析例如和软提供件的术推起网络扫荐并且，一服识起别可对性产生任工证务商具该有推起力推荐工证保证
SP.09.02	RE(1)	保证安全	保证：：：工证具和软保证	何已知不	是	和软提供件技利影响为术避提供文档。 1） 免络为术荐出建工证具和软保证、 2） 知不工化议本/及本为术出建工证具和软保证其规荐定的具且于	与 RE 自动荐能说是明该确以术资所荐保证，者以术批网准检查荐其规； 的术分能说析例如和软提供件的术推起络扫荐并且，一中相为术工证具和软保证荐关问，应包影响为术避提供括在检查其规荐知不； 和软具和软发（括 DCOM 和软发）现工荐保证，检查其规网能未授权设备荐推起或上起。 1） 检查保证其规、 2） 检查开分保证放端备荐和软/和软发荐“口意”其规、 3） 检查味着流程个且现工分保证多它们味着个且为现工荐其规
SP.09.02	RE(2)	保证安全	保证：：：工证具和软保证	安全	否	和软提供件技术能说明该括会推起工证荐保证/其规是别可中相荐，导致潜信具和软息这些，为中相荐保证具其规是力推荐	与 RE 自动荐能说是明该导致潜信具和软息这直些，上起工证保证以术中相接必荐其规； 的术分能说析例如和软提供件技的术推起网络扫荐并且，一须到别可对性产生任以术服引起批必荐工证中相接必荐其规，识起中相荐工证保证需是力推荐，需术推起力推荐免络告； 效起要求应批地工以术服起联工证中相保证具其规荐别可对性产生任

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.09.02	RE(3)	账户管理	账户——用户和服务账户	过期	否	服务提供商应有能力确保基本功能所需的和/或连续操作所需的或是资产所有者所需的服务、自动登录、操作员账户及其他账户都被配置，以便其永不过期或被自动禁止	RE规定的能力用于防止为自动登录配置的服务、操作员、工作站和其他账户的需求，由于账户过期或被自动禁用而拒绝服务。 具有该能力表示服务提供商具有可识别的流程，确保自动化解决方案中的账户是永久账户，如服务、自动登录和操作员账户都被配置了，以便它们没有过期或者被自动禁用或删除。操作员账户通常是为个人用户账户配置操作员权限，为控制的物理环境（如过程）提供可见性。 此要求不能防止永久性账户被管理员显式删除或禁用。 对于基于Unix的系统，通常建议使用临时或“nologin” shell（可有效拒绝此账户所有登录）去配置根账户，并为授权管理员用户所使用的根账户创建一个不同的别名。 **注**：关于评估和解决与未过期账户相关的风险，见SP.03.01 BR和RE
SP.09.02	RE(4)	账户管理	账户——管理员	最小功能	否	服务提供商应有能力确保内置的管理员账户被禁用，如无法实现，则对其重命名，或者使用其他方式使其难以被利用	RE规定的能力使攻击者很难使用内置管理员账户来获取管理权限。 具有该能力表示服务提供商具有可识别的流程以禁用或重命名内置账户，或者如果两者均不可能实现则使其变得很难被识别和利用。提供对内置管理员账户的访问，则恶意软件可能使用该账户并控制系统。 **注**：重命名不是很有效，因为操作系统可能不会改变账户基本标识符
SP.09.03	BR	账户管理	账户——默认	最小功能	否	服务提供商应有能力确保未使用的系统默认账户已被删除或禁用	BR规定的能力用于防止攻击者通过未使用的系统默认账户去访问自动化解决方案。 具有该能力表示服务提供商具备可识别的流程以删除自动化解决方案不再需要的系统默认（内置）账户。

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
							架构数据保护是密码服务商应有力确自动化解决(方案使用)的加机/制动加机包括算法加机和，钥要求管理分发获得安全工数据。业团是体普使得安遍是接受得安的是具该包括意味加机和，着它提供所组要提供件了。当前被技要架构数据术消除
SP.09.04	BR	数据一个	数据：：：理据	从中功能	否	着它提供所移获能时当前发获理据数据意需被防组要如术消除，永久； 1) 着它提供所销理和毁算数据。方理分删规的定于和数据， 2) 被防预设备码服务商应有力着它提供所和理据数据(保后将敏发获感消除码服务商应有力着它提供所泄露数据。给 SP.01.07 BR)	BR 权 RE 访问和能时理分此任何人感保可被防组要和数据(方被防识码服务商应有力提供着它露别和理据数据)流程或码服务商应有力， 通获常能时操作着它提供所通获过清存和储器。识完成对案使其进行和露别数据。意需多规对次服的术擦以备码服务商应有力和着它残任。留消除的取理钥类数据，型和是当前码服务商应有力被永无的被前线着它提供所数据。除网组要钥类数据
SP.09.04	RE(1)	数据一个	数据：：：理据	络计	否	着它提供所移获能时密多规删规/定于次服系统。在规意泄下化络计内容。理分面作被防组要和完成对次服和数据持最新码服务商应有力状消除	通获常能时操作着它提供所通态过清存和储器。层在规意泄内容；意需钥类次服多规。当工识完之对次服发进行和数据持术消除， 型和是当前码服务商应有力被永无的被前线着它提供所数据。除网组要钥类数据，间交加换具该链括和要求给 SP.08.02 BR 。对永久消除止入数据和要求

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.09.05	BR	限制通过	配有	手持	否	无线提供设备的能工人在配有自动化解决方案进行内部访问安；全机需时为系统远程管理域保护层指， 注。行内配有访问安是。 1） 按和 8 规范普渡： 2） 行和解决参考模型范普中部级型范普见网。内络“计络“控范服务商范普（应％为＃）	BR 力确部能工业团人在无线提供设能体广泛认可部证与该的定配有访问用自动，于业访问部配有于配有及其机信进，免的受能工未授无线提供设免权化具此部意味；着人在远程管一个识别体广访问配有，流务确远程管一个识别中于业部配有部访问用或使遍列要求部认可，表 IEC 62443-3-3 中远程管一个识别该业以防部需时止对要求；服 IEC 62443-3-2 中于业加密所采方已获人确务确远程管一个识别该于业配有部访问用得来，传输；表 IEC 62443-2-1 中证与该的定部配有自动要求
SP.09.06	BR	限制通过	配有	使期	否	无线提供设备的能工人在间数为时以防（应域）业制限制部配有机据决持流证与该的定这确于业包括输点之远程使期	BR 为 RE 力确部能工业团人在化方确期他协配有，在广议符部配有合标准加密；适法合机本让们机信进；全业团审以防查心技术地间访，问该；确期他协配有合机锁进而定信进配有部输点渡安， 免的受能工未授无线提供设免权化具此部意味；着人在配有化方据决够机证与该的定于业遍这确部发控之远程使期，无线提供设生输们更改及允配有使期；许个团务确远程管一个识别；钥是及允匙开是控够但层使味部包数管；全怎是流样都恶硬且期期点们当之， 证与该的定解决于业期机部需时自动义人团加密所采；全怎义审问期机查心确期干预，表 IEC 62443-3-2 中加密所采部他更例如；IEC 62443-3-3 中持锁以防与打能工部止对要求；方服 IEC 62443-2-1 中证与该的定止对要求， 注。IEC 62443-2-1 中全这了人提服配有部于业期机要求；钥描述遍增够匙业部配有自动

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.09.06	RE(1)	账户管理	密码	过期	否	服务提供商应有能力确保设置密码策略去提示用户密码到期的前 N 天去修改密码。N 是由资产所有者指定的。这个需求不适用于没有设置到期时间的密码	具有该能力表示服务提供商具备可识别的流程，即确保用户被告知其密码快到期了，以便有时间去更改密码
SP.09.07	BR	账户管理	密码	修改	否	服务提供商应有能力确保默认密码可以依据资产所有者的要求而修改	BR 规定的能力用于防止众所周知的默认密码被任何自动化解决方案所使用。 具有该能力表示服务提供商具备可识别的流程，即确保默认密码依据资产所有者的要求而修改。通常，此修改过程将是在安装、重新安装以及重启/还原过程中进行的
SP.09.08	BR	账户管理	密码	重用	否	服务提供商应有能力确保设置密码策略防止用户重用他们最近 N 次的密码，N 是由资产所有者指定的	BR 和 RE 规定的能力是防止用户去修改密码后又立即改回来，此情况实际表示密码并未被修改。 具有该能力表示服务提供商具备可识别的流程，即能验证密码重用策略被设置为资产所有者指定的数字
SP.09.08	RE(1)	账户管理	密码	修改	否	服务提供商应有能力确保设置的密码策略防止用户比每 N 天更频繁地更改密码，N 是由资产所有者指定的	具有该能力表示服务提供商具备可识别的流程，即配置密码策略防止用户不断去修改密码，使其成为最喜欢的密码。N 天时间段表示一旦密码被修改，用户不可以在 N 天内再去修改密码
SP.09.09	BR	账户管理	密码	共享	否	服务提供商应有能力确保资产所有者批准的账户密码在与服务提供商共享时，被安全记录与维护	BR 和 RE 规定的能力用于确保共享密码的使用是受管理的。没有共享密码的管理，资产所有者可能无法意识到或无法掌握谁访问了自动化解决方案。 具有该能力表示服务提供商具有一个可识别的流程，即记录和保护资产所有者泄露给服务提供商的密码列表，防止泄露和更改。服务提供商有责任和义务维护知悉此类账户密码人员的日志，包括分包商、咨询人员和代理

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.09.09	RE(1)	账户管理	密码	共享	否	服务提供商应有能力向资产所有者报告密码是： 1） 共享的和不再需要共享的； 2） 故意泄露的； 3） 故意破坏的； 并且在有必要时支持资产所有者改变密码	具有该能力表示服务提供商具备可识别的流程，即跟踪与服务提供商共享的密码（包括自动登录账户密码）以及服务提供商了解到的已被盗用或泄露给其他人的密码，并报告资产所有者，以便修改密码。 例如，对于服务提供商组织内共享的密码，一旦服务提供商不再需要时，服务提供商需要给资产所有者报告。更改此密码时，资产所有者可要求服务提供商提供支持。 同样地，如果服务提供商人员与其他人共享密码，当不再需要共享密码时，服务提供商就需要给资产所有者报告这些账户/密码。共享密码经常发生在测试、调试、故障排查或维护期间。另外，任何时候，服务提供商怀疑密码已经被盗用时，其宜通知账户所有者并请求修改密码
SP.10.01	BR	恶意软件防护	人工处理	恶意软件防护机制	否	服务提供商应有能力提供给资产所有者文档形式的说明，关于针对此自动化解决方案进行了测试和验证的恶意软件防护机制，包括正常的安装、配置和更新的说明	BR 规定的能力是用来确保资产所有者有必要的文档来使用兼容此自动化解决方案的防恶意软件机制。 具备此能力表示服务提供商有一个可识别的流程，即提供普遍被接受的防恶意软件的文档（例如杀毒、白名单），这些软件可以在服务提供商所负责的自动化解决方案的硬件平台（如工作站）上运行。如果控制系统的供应商没有测试和推荐一款防恶意软件的产品，则服务提供商就需要有这些能力
SP.10.02	BR	恶意软件防护	安全工具和软件	安装	否	服务提供商应有能力确保： 1） 恶意软件防护机制应被正确地安装/更新，并按照服务提供商批准的策略进行配置。 2） 恶意软件定义文件以资产所有者同意的时间周期安装。	BR 及其 RE 规定的能力是用来确保自动化解决方案不受恶意软件的侵害。 具备此能力表示服务提供商有一个可识别的流程，为服务提供商所负责的自动化解决方案的硬件平台来应用、管理防恶意软件，包括安装、更新防恶意软件，保持其恶意软件定义文件最新，维护其运行配置设置。目的是使运行在自动化解决方案所有相关硬件平台上的防恶意软件有最新的恶意软件

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
						3） 恶意软件的相关配置被维护并保持为最新	定义文件，最新的运行配置，最新的软件更新。 具备此能力同时表示服务提供商有一个可识别的流程，即就发布恶意软件定义文件之后何时安装此恶意软件定义文件，与资产所有者达成了一致。 **示例 1**：如果使用了杀毒软件，将在商定好的时间周期内对杀毒定义文件进行安装。 **示例 2**：如果使用白名单软件，白名单的配置需要保持更新。 **示例 3**：为安装和配置活动生成日志，包括软件和恶意软件定义文件更新，是证明具备此能力的一种方式
SP.10.02	RE(1)	恶意软件防护	安全工具和软件	安装	否	服务提供商应创建和维护文档，以描述所负责的自动化解决方案的恶意软件防护机制使用信息。对于自动化解决方案的每一个组件，这个文件都应包括： 1） 恶意软件防护机制的安装状态或技术上不可能在这个组件上安装恶意软件防护机制的声明。 2） 所安装恶意软件防护机制的当前配置设置。 3） 批准安装在此组件的恶意软件定义文件的当前状态。 4） 一些用来降低感染的风险和降低感染的效果（如隔离感染源、报告感染情况）的其他缓解功能和手段的使用	该能力表示服务提供商有一个可识别的流程，对自动化解决方案的每一个硬件平台的防恶意软件状态存档，无论防恶意软件是否安装到此组件上。所有平台都要安装防恶意软件，除非在技术上没有可行性（例如没有对应的防恶意软件）

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.10.03	BR	恶意软件防护	安全工具和软件	探测	否	服务提供商应有能力验证通过安装恶意软件防护机制，除零日恶意软件之外的所有恶意软件均能够被探测和适当处理	该 BR 规定的能力是用来验证防恶意软件机制按照期望方式运行。 具备此能力表示服务提供商有一个可识别的流程，即验证通过防恶意软件产品可以探测被感染的文件并随后将其隔离/删除。唯一的例外是零日感染，它是一种没有恶意软件定义文件可适用的侵害行为。这是一种通常的情况，在先前没有发现并探测到此恶意软件
SP.10.04	BR	恶意软件防护	人工处理	恶意软件定义文件	是	服务提供商应有能力给资产所有者提供描述性文档，这些文档描述了： 1) 自动化解决方案的恶意软件定义文件是如何被评估和批准的。 2) 制造商发布这些文件的 N 日内，向资产所有者报告恶意软件定义的状态。其中的期限 N 是由资产所有者和服务提供商一致确认的。每一个恶意软件定义文件的这个状态包括适用性（例如组件和版本）和批准的状态（例如已批准、已安装、未批准等）	该 BR 的能力是用来确保服务提供商具有相应流程，来验证新的恶意软件定义文件与自动化解决方案兼容，并且对自动化解决方案是及时可用的。 具备该 BR 的能力意味着服务提供商有一个可识别的流程，即在反病毒的软件制造商发布恶意软件定义文件之后，在一个相互同意的时间周期内，批准恶意软件定义文件以及通知资产所有者结果。在这个时间周期内并不要求完成安装，仅仅需要在这个周期内用于安装的文件被批准。批准意味着服务提供商对这个文件是否与他们的系统有冲突进行了评估。与系统冲突的文件是不会被批准的
SP.10.05	BR	恶意软件防护	设备——所有	杀毒	否	服务提供商应有能力确保由服务提供商为自动化解决方案提供支持的所有设备，包括工作站，在用于自动化解决方案之前都不存在已知的恶意软件	该 BR 的能力是用来确保被可探测的病毒感染了的设备不会安装在自动化解决方案中。“已知恶意软件”一词意味着该恶意软件在之前已经被发现且已对其开发出了可用的恶意软件定义文件。

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
							解决方 BR 案能人员配置背景提供审查服务商该应案具有：力确/保自由背景提供审提供动化相关活只分给案在决是法律允许员的范案， 力确围内这些在决已是否查许员的范：成通许员的范案过安。全及 SP.10.05 RE(2)、其规定案在决用于的范：护/防保自供止受提供通许员的范案在决（到可：信度问影供止审允响虽然不证许员的范但识别描），此额供止受用外全需及 ISO 27036
SP.10.05	RE(1)	许员的范明程	对相律工安作	验诚	否	背景提供审止查能人保自诚一问影案还指]出指：护/防缺程案乏适律工安作或诚一地当诚局	方 BR 案能人是诚和保自乏适律工安作法允化相关活只分给机验诚：构支持进行调许员的范并非案商能， 解决地能人员配置背景提供审查服务商该应案具有：保自进总查例如国化相关活只分给（是查商能并非许员的范案化相关活只分给）案乏适律工安作验诚允家禁商能调并非案使分，到可：可无服务 USB 在决查执类何解防多长：时间留务在决处法止理包括身份法犯一化相关活只分给案何罪记防背景录
SP.10.05	RE(2)	许员的范明程	对相律工安作	咨询	否	背景提供审查能人保自理包括化相关活只分给代案乏适在决：允化相关活只分给验诚然不：法他们括见链案许员的范案组织	方 BR 案能人是诚和保自调商补还案充询并非派案乏适律工安作是法他止诚一化相关活只分给案，：见链许员的范、服联员配置方许员的范允然不见络调个规负见证家责个以派商诚案下情文范， 解决地能人员配置背景提供审查服务商该应案具有：况查与资和明产调并非案乏适在决所者并非化相关活只分给：乏适在决当系围内了法遵一：用于律工安作]CD/DVD/守本过标]USB 在决]准能中加]强律]之交流让]流让护乏适中更， 化相关活只分给好有理包案意味要求及 SP.07.XX

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.11.01	BR	以服务商	视角对商	以服安全	是	与资提供产所有能者人员进行提供文档。描述交流确保给的标书本准中需指定内部的一致以服是并予遵守就偏遵离或的、 注 1，不符合或定。问部的沟通遵这包内部以服、 注 2，不符合或定以服的一括了的是人标书本准中需指一括以服	些 BR 的能者是之间差联与资提供产有络为文档本的组织。介使遵员进确有行确起工。包交作处理的内部一致以服力标书本准中需指及自动（化 SP.10.04 BR）、不解决方案用。与资提供产控制之系统例如进何供所产之补标书本准中需指的文档。偿要机配文档置分及所派负、 责该应能者职位最与资提供产有络为介低网的质织。提供将员进确有行文档。格描述交之补标书本准中需指的一致以服的中规于减。使少流在策和遵实施偏离或的、 失误做交一致出的以服。错配补系统例如“选部的内部“择缺例如内部。使少标书本准中需指“系统例如偏选部确乏正的可会需内部所之、 IEC TR 62443-2-3 描述交以服务商。必地交络选系统例如供所产偏员进确有行及暴的给露、SP.11.XX 包威胁 IEC TR 62443-2-3 员进确有行以服务商给露的与资提供产规危交以服务商功能
SP.11.01	RE(1)	以服务商	视角对商	以服安全	否	由补一致害具的负备。与资提供产所有能者种起之补格保给的标书本准中需指内部的一致以服是并予守就偏离或的。失意备味介能着已一致害具的备本	些 BR 的能者是之间差联与资提供产包所配经领一致导相关活的备本。介使味理以服守就的组织、（专并错配理的导相介能业要味知识的个所）、别程每。失遵这包络为此部对商的组织。验遵这包络为培训的组织。认证般出每而起格以服守就组织、 责该应能者职位最与资提供产有络为介低网的质织。认种起守就偏离或一致以服的组织、种起要求介使味理应组织使对商害具言常定的备本、 失为种起业要证般出每置分验行开差始所害具言常定的前达负备、前达负备了的是成意短包配组织有语不表示的备本、害具言常的负备络其职危准误地理的导相偏交合出。同误地理一致事项的报告

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.11.02	BR	解决方案	解决人员	解决配置	是	培训提供安全资能产所有者服资务提供资商应具力解决/确保应文档—自动安化相解决关活：只分给安包应或咨询告知：有者服资务能并使其遵分给解决应描述：守的描述责任、 1） 培训提供安服政策应和规程该定将对应如下：威胁最守的如下应具力解决— 2） 遵分给应小这些未/意识到在些未（义 IEC TR 62443-2-3）：体而只引发很多小这，时资多小这，候威胁— 3） 危害：结而果小这应解决应全胁误用要求不动正共享维护— 4） 时资多小这不候威胁应解决应原账— 5） 户多全胁味时资多小这应着明序应解工作了	括 BR 代 RE 理包应能产—般多有者服资务法胁温习见具力解决应描述：守的解决链培训提供安提组应和规程该定将对织补：充一胁温可培训提供安书面而形式认成的有者服资务候具熟解决应度等级— 强制执能产行略变培训提供安资分给一更管应许误：般 SP.11.01 BR 很服包流应能产描述：涉及设小这具力解决：设备只自动安化相解决应 *N* 站关知：所有者服资务器以它果：*N* 是资培训提供安代有者服资务安包应— 培训提供安一般法胁们下应之间连：链自动安服提供应候接不资服授权—只守访着明序：培训提供安一能问要确修们下解决责：守给改随应见题问要也最守给要求应分新便精反映案
SP.11.02	RE(1)	解决方案	解决人员	解决配置	否	培训提供安全资能产法有者服资务一般器记分给录他代具力接域口并明每应明个温法胁解决人员：解决人员责任、 1） 小这应具力解决一胁最培训提供安政策应和规程该定将对（体而还自共享代如下们下，不也共享们下代何互将全胁们下）。	强资执能产行略变培训提供安资一哪为应许误温描述有者服资务到从使那分给描述户小这具力解决应允子人员：守的具力解决胁最培训提供安服政策应如下（义 SP.11.02 BR）—许人员器记口并明每应区此温提供般建有者服资务立该守的解决问要边自动安成界序见不胁管应将相使其—许人员一般器记守给区此边还自共享者关提供安，培训提供安不务培训提供安安一应全案安映使那— **注**、“户小这”行略变许解决户由培训提供安引发设为实对户以应配置资商备时资化现见题

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） 可用的安全补丁列表已被批准用于自动化解决方案， 3） 软件的版本号对于批准的补丁列表是适用的“ 该列表应在补丁被制造商发布后的商定的时间内对资产所有者可用	
SP.11.02	RE(2)	补丁管理	补丁列表	批准	否	服务提供商应有能力” 1） 在安全补丁可用且已被服务提供商批准但没有被资产所有者批准。例如由于补丁会影响操作或性能情况下。当资产所有者提出要求时推荐减轻损失的方案（见SP 11.05 BR）， 2） 在资产所有者批准后实施减轻损失的方案	具有此能力意味着服务提供商有可识别的流程来研发和实施一种方法以减轻不允许安装安全补丁的影响。该安全补丁可能对自动化解决方案有负面影响“ 方法可以包括补偿机制或其他手段以降低安全补丁所引起的脆弱性“ 替代的方法需由资产所有者批准
SP.11.03	BR	补丁管理	安全补丁	交付	否	服务提供商的补丁管理应提供” 1） 由资产所有者直接从补丁制造商处获得的补丁。和/或 2） 只有资产所有者批准且经补丁制造商许可。服务提供商才能再发布补丁	该 BR 指定的能力用来确保补丁通过授权渠道（从一个适当的来源）获得。以减少他们可能有缺陷/受感染的可能性“ 具有这种能力意味着服务提供商的补丁交付政策支持资产所有者直接从制造商获得补丁。或者应资产所有者的要求从服务提供商获得。但只有与补丁制造商达成许可协议才能这样做“ 如果补丁是由服务提供商交付的。那么服务提供商和资产所有者将不得不共同决定如何实施（例如。光盘、安全连接）

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.11.04	BR	账户管理	用和账户	用服	是	务过提供期商应能有提供文档力确保基应本—所文档描述需的或连操作资产账户管理务过者用服账户—自动需的登录账户员及其他、 1） 都被或账户管理务过者配—文档商置以需的被或务过者便用服账户， 2） 被或永不禁止规定连操用服账户配—文档商描述需的于禁止规定用服账户	所 BR 防为工能有或便站而确保基应本拒绝需的具该操表示可识别用服用和账户。 流应程能有化解决务过提供期能具确保基应本提供方案防中便描述需的于永不禁止规定（久 CD“DVD“USB 禁止服如）了于账户管理务过者用服账户
SP.11.05	BR	账户管理	用和账户	它们	否	务过提供期商应能有站而具用服没删除用和账户登录确保基应本工它们	所 BR 防为工能有或便站而—都通常都确保基应本个要账户配—务过提供期人能用服所账户。 流应权限能有化解决务过提供期应删除控制自要求物登录确保基应本工它们便用服账户
SP.11.06	BR	账户管理	用和账户	用服	否	务过提供期商应能有站而久环确保基应本要求务过提供期用服用和境见账户（性此显见式对）—务过提供期商系确保基应本防为工配统建议用服	所 BR 防为工能有或便站而—都通常都确保基应本个要账户配—务过提供期人能用服所账户—使久—久环临时系用服效个要去根配个要并授产创一操。 流应程能有化解决务过提供期应同名关工评创常系确保基应本防为工配统便用服估它们工账户
SP.11.06	RE(1)	账户管理	用和账户	用服	否	务过提供期商应能有站而系账户用服自效—使久与去服境见作未相风险最及临如自效—该操表示可识别工用和小显内对无能录法而实	所 RE 防为工能有或便站而账户工用服现则”重命：作难利攻该操表示可识别工小显。 流应权限能有化解决—久环账户工用服击很物难对—务过提供期应删除同名关工评创—自站而物应删除识来获取该操表示可识别工小显员及。所能有是果两便用服账户均变工。

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
							架构设备全部最小服务商应要全有力确保仅在自动化解决方案全中启部最用所—的或资产者批准软。件和设备硬特性低限度上禁—移除。度上提供不必程序硬特如电邮办公是否室游戏的或资产。是否必程保仅及用所
SP.11.06	RE(2)	架构其相	设关架构	设备	否	度上提供不通序能信办接入点端口大如容量设备低存/所存限动储。及小服如电能接器动储低存/所存限蓝牙无线非使无	网 RE 络公限功能地邮办接大如容量设备限架构是蓝牙限址批有被架构设备如电授权对— 诊序除功能断配置度上提供不序硬特物理逻限辑电。地点设关访小服动储授限低存/所存—的禁问护以防序未交限地换机路小服。者址为阻室止基动储限小服础施被进行如电授维过持— 架构物能有生低存础施命周点容量—期处于加限为固软 SP.03.10 BR 状及 RE— 态逻，未交，非使无线该规无限定同要求软 IEC 62443-3-3 线 IEC 62443-4-2
SP.11.06	RE(3)	架构其相	设关架构	设备	否	度上提供不通诊序能信办公类地点度上提供不型来制力确具意味着可限型序设关架构限设备识自	诊序的或能信断配置度上提供不序硬特物别器限辑电。流减少攻击限力确具意味着可限架构是否少设备。解办公面户架构列出(这设备)—的或能信物解提供些确包相括安全力确具工诊
SP.12.01	BR	储与/保仅	些确包相	之满足执	是	度上提供不通序能信正力确具意味着可提供常急限储与括安文档。禁问操批作点解需了渠： 1) 同点和道非使储与力确具意味着可限数经络扫。和发类地限现。一个储与。技准生地解需着术例硬： a) 物并确它们开限分序储与连部源控、	由网 BR 络公限能信邮办接串目型序风险没和道生地度上提供不正力确具意味着可提供限储与功能— 诊序的或能信断配置度上提供不序硬特物别器限辑电。正力确具意味着可击储情公限文档。解况公和道储与力确具意味着可。及于加端口非使储与线一个储与。者常急和道下路改访变他—网文档通办法： 1) 储与础施维锁正期处(软 SP.03.10 BR 状及 RE。期处于加限设关为固)。者物能移除箱正设关里装限够住— 2) 储与物能应要当设关时存授保仅(件和工经会少权对)—

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
						b） 架构设备全部最小服务商的加固务指南— c） 和规程的加固务指南、应当指南确保仅的加务商应安装必经授最权有的加记录提供认最证设机发布数字最服仅子书最— d） 书确的加固务指南、具应安装必经授最权有最必经记录提供认最证设机发布数字该力服仅的加务商， 2） 意味着可识别最的加。 a） 流以务商文定哪些被识别（并移除那最未使）— b） 用力通常（操作确系定、移统升级定）— c） 会造识别、识别成文定— d） 一组文定、中子一组— e） 心即意最文定自动操作化解决方案不需的最需造：限制务商最限制只需造（阻止对识、需味有、期望过）— f） 身份工站对识—	3） 安装必经授架能经服仅话即锁资方产录所求最的加者支， 4） 安装必经授最的加者支架能操作持的加于此适除最主题：负和的加、责防已登的加（并移、户通显示信）、息看到架能输入记录提供认文档未使最如键确盘鼠， 5） 的加用标直应或管显示理信员管、显示架能确就的加非屏幕的加识别解服幕，上自显示最泄并操作户通示露哪个按照导

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
						g） 目录信息； h） 由服务提供商确定的其他文件，这些文件应创建一个自动化解决方案的完整备份。 3） 对备份介质的异地存储建议。 4） 确保避免自动化解决方案不被改变的规定，以使在进行备份时对备份完整性的可能影响不会发生。 **注：** 部分恢复的例子包括操作系统、应用软件、数据库和配置文件	
SP.12.02	BR	备份/恢复	恢复	技术说明	是	服务提供商应有能力向资产所有者提供书面化的指导，以使自动化解决方案或其组件恢复正常工作	由该 BR 指定的能力来确保资产所有者知道如何使用服务提供商提供的自动化解决方案的恢复能力。 具有这种能力意味着服务提供商有一个可验证的流程，用于准备或提供文档，描述如何从备份数据恢复自动化解决方案或其组件（即部分恢复）。该文档应包括处理异常场景的说明，例如，如何还原自备份以来体系结构可能发生变化的自动化解决方案。在这种情况下，恢复可能不完整，资产所有者应了解这些情况。此要求适用于运行中的自动化解决方案和自动化解决方案的仿真系统
SP.12.03	BR	备份/恢复	可携带介质	技术说明	是	服务提供商应具有能力向资产所有者提供文档，以描述如何控制和安全地管理可移动备份介质	由该 BR 指定的能力来确保资产所有者知道如何安全地处理自动化解决方案的备份介质。 具备此能力意味着服务提供商有一个可验证的流程，用于准备一个特定于自动化解决方案的文档，该文件描述了对备份

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
							架构设备网序络最小服务商应有力确保一设个低权限用于管理所负责要的及架构其络是管认为对设自动序化解序络决方案至设关重因此架构所也被因此架构
SP.12.04	BR	的及程关重	的及	攻击	是	象以提供定义各保能面受有力确保一提供文档序络描述解到攻击护功设具该的及	由意 BR 味着设能面可至服有力确保一识别解到攻击法即将概念操作设的及要 各保仅获能面得需资象以提供用源保管认其攻击设访用可问的安所提供全文档序意文档描述解到攻击的及是否护功
SP.12.05	BR	的及程关重	关重	攻击	否	象以提供定义保能面攻击求 1全 如目管认录和设法即将概念操作设的及是其能设见 2全 件仅认的及关重管认功能录系设法即将概念操作是其能设	由意 BR 味着设能面可至服法即将概念操作设的及权关重能面统同样只那些要 各保控功能得需资象以提供定各保管认其攻击设访用序制无击线所络包括操了攻击的及其络护功基如目序角色法即将概念操作其络件意的及通关重要仅认限用义是常员设序必他有力确保一们要求单小的及程关重序络但果的及能面其络护功基产制设者规要 解程的及允许架构或的及序么各保控能面就得需资象以提供定各保管认其攻击设访用序制无击线所络包括操了攻击多流即的及使来法即配置独并方所每制要法即配置其能列表理架构或通设架构从而序商其能多架构或的及支持相
SP.12.06	BR	的及程关重	的及	如目	否	象以提供定义各的不构有力确保一设的及级然如目法即将概念操作设的及表架构关重权后够关重自动设能面要 象以提供一义保各的不构有力确保一设的及支户授权架构关重权后够关重自动如目法即将概念操作设的及设能面	由意 BR 味着设能面可至服序多的及法即将概念操作支序象以提供定予这有力确保一设味表程个低要 各保仅获能面得需资象以提供定保管认其攻击设访用序予这有力确保一设的及程关重个低权自动序允许的及进步权后够关重级然安对 SP.12.09 BR全要控要求设自设是至服象以提供定问的论见包的及程密原员即应有力确保一设的及要求于码加

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.12.07	BR	解决/方案	解决	人员配	否	置培提供训安全资产所有解决者服务商应具力确保自动能化相续关活只分商能给	由包 BR 或咨商能给询产所—应具力确保自动（告知者服并使）商只分其遵守的解决者服商责任： 全资政能给策和规置培提供服程资该定将对如商下服—威产所解决胁分其最小应具力确保自动商关活只分：这些商未意能给识求到在 IEC 62443-3-3
SP.12.08	BR	解决/方案	义具体而	引发	是	置培提供训安全资很多时候资危提供文档—描述知害结果误用不候资解决误正原共具商享维引发商能给	由包 BR 或咨商能给询产所多时候资危护账知害户而解决误正原胁分商享维引发：味着享维引发提供解决/方案共具商如明—知解决/方案共具是害序工结商、是作了括商、了括危商代决理： 全资政功能策和规置培提供训资该定将对如商下服——解般提供文档询描述知害法温应具力确保自动威习解决误方案胁分见链享维引发务
SP.12.09	BR	解决/方案	义具体而	组织方案	是	置培提供训安资能给补充该定可书商组织方案维面—形式认其成熟威度等级， 1） 描述强制组执行略变更管应具力确保自动商责任。 2） 许流或涉方案、及设备具、站器商以它们习更之果的应具力确保自动务。 3） 方案间定应具力确保自动商连接授未权访识求	由包 BR 或咨商能给询产所—其问是资该定维面—修组织务方案—改随资组织将能工结商也最（告知—形式新便精反映记）—威变知害修组织务方案： 资味制能给策和规置培提供训资该定将对如商下服—录管应具力确保自动一解该定他咨商文档—接咨知害口方案应具力确保自动变更以它询体温并熟新便精反明每商及个还不： 其能何口应具力确保自动以它般间定应具力确保自动守的互执改还变解决误方案商义哪：方案商义哪将能形式为解—知到从那般允许区工只全

参 考 文 献

注：该参考文献包括用于创建本标准的来源，以及参考源，可能有助于读者更好地了解将网络安全作为一个整体来开发，以及开发网络安全管理系统的过程。并不是本参考文献中的所有引用都涉及本标准的文本。

[1] GB/T 33007—2016 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方案(IEC 62443-2-1:2010，Industrial communication networks—Network and system security—Part 2-1:Establishing an industrial automation and control system security program，IDT)

[2] GB/T 35673—2017 工业通信网络 网络和系统安全 第3-3部分：系统的安全需求和安全等级(IEC 62443-3-3:2013，Industrial communication networks—Network and system security—Part 3-3:System security requirements and security levels)

[3] ISO/IEC 27036-3 信息技术 安全技术 供应商关系的安全 第3部分：信息和通信技术供应链安全指南(Information technology—Security techniques—Information security for supplier relationships—Part 3:Guidelines for information and communication technology supply chain security)

[4] ISO/IEC 30111 信息技术 安全技术 脆弱性的处理过程(Information technology—Security techniques—Vulnerability handling processes)

[5] IEC 61508(所有部分) 电气/电子/可编程电子安全相关系统的功能安全(Functional safety of electrical/electronic/programmable electronic safety-related systems)

[6] IEC 61511(所有部分) 功能安全 流程工业部门的安全仪器系统(Functional safety—Safety instrumented systems for the process industry sector)

[7] IEC 62264-1:2013 企业 控制系统集成 第1部分：模型和术语(Enterprise-control system integration—Part 1:Models and terminology)

[8] IEC 62351-8:2011 电力系统管理及相关的信息交换 数据和通信安全 第8部分：基于角色的访问控制(Power systems management and associated information exchange—Data and communications security—Part 8:Role-based access control)

[9] IEC/TS 62443-1-1 工业通信网络 网络和系统安全 第1-1部分：术语、概念和模型(Industrial communication networks—Network and system security—Part 1-1: Terminology，concepts and models)

[10] IEC/TR 62443-1-2 工业通信网络 网络和系统安全 第1-2部分：术语和缩略语主要词汇表(Industrial communication networks—Network and system security—Part 1-2:Master glossary of terms and abbreviations[1])

[11] IEC/TR 62443-1-3 工业通信网络 网络和系统安全 第1-3部分：系统安全性度量(Industrial communication networks—Network and system security—Part 1-3: System security compliance metrics[2])

[12] IEC/TR 62443-2-3 工业通信网络 网络和系统安全 第2-3部分：在IACS环境下的补丁管理(Industrial communication networks—Network and system security—Part 2-3:Patch management in the IACS environment[3])

[13] IEC 62443-3-2 工业通信网络 网络和系统安全 第3-2部分：区域和管道安全的保障水平(Industrial communication networks—Network and system security—Part 3-2:Security assurance

1) 在考虑中。

2) 在筹备中。

3) 在筹备中。

levels for zones and conduits[4])

[14] IEC 62443-4-1 工业通信网络 网络和系统安全 第4-1部分:产品开发要求(Industrial communication networks—Network and system security—Part 4-1: Product development requirements[5])

[15] IEC 62443-4-2 工业通信网络 网络和系统安全 第4-2部分:IACS组件的技术安全要求(Industrial communication networks—Network and system security—Part 4-2: Technical security requirements for IACS components[6])

[16] IEC TR 62443-4-2-1 工业通信网络 网络和系统安全 第4-2-1部分:WIB规范(Industrial communication networks—Network and system security—Part 4-2-1: WIB Profiles[7])

[17] IETF/RFC 1510 Kerberos网络认证服务[The Kerberos Network Authentication Service (V5)]

[18] CMMI® for Services, Version 1.3, November 2010, (CMU/SEI-2010-TR-034, ESC-TR-2010-034)

4) 在筹备中。

5) 在考虑中。

6) 在考虑中。

7) 在考虑中。

GB/T 40682—2021/IEC 62443-2-4:2015

中 华 人 民 共 和 国
国 家 标 准
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
GB/T 40682—2021/IEC 62443-2-4:2015
*
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
2021年10月第一版
*
书号:155066·1-68461

GB/T 40682-2021