ICS 25.040
N 10

中华人民共和国国家标准

GB/T 40211—2021/IEC/TS 62443-1-1:2009

工业通信网络　网络和系统安全 术语、概念和模型

Industrial communication networks—Network and system security—Terminology, concepts and models

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

2021-05-21 发布　　2021-12-01 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

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/TS 62443-1-1:2009《工业通信网络　网络和系统安全　第1-1部分:术语、概念和模型》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下:

——GB/T 18336.1—2015　信息技术　安全技术　信息技术安全评估准则　第1部分:简介和一般模型(ISO/IEC 15408-1:2009,IDT)

——GB/T 20720.1—2019　企业控制系统集成　第1部分:模型和术语(IEC 62264-1:2013,IDT)

本标准做了下列编辑性修改:

——修改了标准名称。

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。

引　言

本标准的主题是工业自动化和控制系统的安全。为了适用于不同的应用(如:行业类型),每条术语都进行宽泛的解读。

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

本标准中的术语“安全”是指防止非法或有害的渗透,有意或无意的妨碍正常的和预期的运行、或不适宜的访问 IACS 的保密信息。本标准特别关注的计算机安全,包括计算机、网络、操作系统、应用和系统的其他可编程组件。

本标准的读者包括所有的 IACS 用户(包括设施运行、维护、施工和用户组织公司的一部分)、生产者、供应商、政府组织在内的、被影响的、控制系统计算机安全、控制系统实践者和安全实践者。因为信息技术(IT)和操作人员、工程人员以及制造商组织之间的互相理解和合作对于任何信息倡议取得全面成功都是非常重要的,本标准也是那些负责 IACS 和企业网络集成人员的参考资料。

本标准主要涉及以下几个典型的问题:

a) IACS 安全应用的范围是什么?

b) 如何使用统一术语定义安全系统的需要和要求?

c) 以什么基本概念为基础以便用于活动、系统属性和行动的进一步分析,这些对提供电子安全控制系统来说非常重要?

d) 如何对 IACS 构件进行分组或分类以用于定义和管理安全?

e) 控制系统应用中,不同的安全目标是什么?

f) 这些目标是如何建立和修改的?

每个问题都在本标准中详细介绍。

工业通信网络　网络和系统安全 术语、概念和模型

1　范围

1.1　概述

本标准是技术规范，定义了用于工业自动化和控制系统(IACS)安全的术语、概念和模型，是系列标准中其他标准的基础。

为了全面清晰地表达本标准的系统和组件，可以从几个方面定义和理解覆盖的范围，包括：

——所含功能性的范围；

——特定的系统和接口；

——选择所含活动的准则；

——选择所含资产的准则。

以下几节是对这些内容的介绍。

1.2　所含的功能性

本标准的范围能够描述为组织信息和自动化系统内的功能性范围。该功能性可以典型地以一个或更多的模型来描述。

本标准主要集中于工业自动化和控制，这在参考模型中有所描述(见第6章)。虽然考虑了业务系统和工业系统间进行数据完整性的交换，业务计划和物流系统并不在本标准的范围内。

工业自动化和控制包括了过程工业中典型常见的监视控制构件。也包括SCADA(监督和数据采集)，该系统常被组织用于操作关键基础设施。包括：

——输变电和配电；

——供气和供水管网；

——石油和燃气生产运营；

——燃气和液体传输管道。

除此之外，SCADA系统也可以应用在其他的关键和非关键基础设施中。

1.3　系统和接口

在所含的全部IACS中，该标准覆盖了系统中可能会改变或影响到工业过程的功能安全、安全和可靠运行。这些包括但不限于：

a)　工业控制系统及其相关通信网络，包括分布式控制系统(DCS)、可编程逻辑控制器(PLC)、远程终端单元(RTU)、智能电子设备、SCADA系统、网络化电子传感和控制、计量和管道传输系统以及监视和诊断系统[本标准中，工业控制系统包括基本过程控制系统和安全仪表系统(SIS)，不管它们是否物理上分离或整合]。

b)　与第6章描述的参考模型中第3层或更下层相关的系统。诸如先进或多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、生产执行系统、管道泄漏检测系统、工作管理、停电管理以及电能量管理系统。

c)　用于提供控制、功能安全、生产或远程操作功能以实现连续、批量、离散以及其他过程的相关内

部接口、人机接口、网络接口、软件接口、机器或设备接口。

1.4 基于活动的准则

IEC 62443-2-1 提供了用于定义与生产操作相关活动的准则。已经有了确定该技术规范范围的相似列表。如果一个系统在执行过程中应考虑下列因素，该系统应在 IEC 62443 系列覆盖的范围内进行设计：

a) 可预见的过程操作；
b) 过程或人员安全；
c) 过程可靠性或可用性；
d) 过程效能；
e) 过程可操作性；
f) 产品质量；
g) 环境保护；
h) 合规；
i) 产品销售或储运交接。

1.5 基于资产的准则

本标准所包含的系统满足下列任何准则，或者其安全性对于保护满足这些准则也是必须的：

a) 资产具有制造或运行过程的经济价值；
b) 资产完成制造或运行过程所必须的功能；
c) 资产代表制造或运行过程中的知识产权；
d) 资产在制造或运行过程中对运行和维护安全是必须的；
e) 资产在制造或运行过程中对保护员工、承包商和来访者是必须的；
f) 资产对保护环境是必须的；
g) 资产应保护公众免于受到制造或运行过程中引起的事件影响；
h) 资产符合法律要求，是指用于制造或运行过程的安全目的；
i) 用于灾难恢复所需要的资产；
j) 记录安全事件所需要的资产。

范围中覆盖的系统如果违背该准则可能会导致公众危险、雇员健康或安全、公众信心的损失、与法规的冲突、资产或保密信息的损失或失效、环境污染、和/或经济损失，或影响到实体或本地或国家安全。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 15408-1 信息技术 安全技术 信息技术安全性评估准则 第 1 部分：简介和一般模型(Information technology—Security techniques—Evaluation criteria for IT security —Part 1: Introudction and general model)

IEC 62264-1 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)

3 术语和定义、缩略语

3.1 概述

采用的定义尽可能来自于已经建立的工业资源。一些定义改写自更通用的IT安全定义。

3.2 术语和定义

下列术语和定义适用于本文件。

3.2.1

访问 access

为了使用系统资源而与系统进行通信，或别的互动的能力和手段。

注：访问可能会涉及物理访问(物理上允许在某个区域授权，拥有物理的加密装置，PIN码或访问卡或允许访问的生物特征)或逻辑访问(通过逻辑和物理方法的结合，获得授权登录到系统和应用)。

3.2.2

访问控制 access control

保护系统资源防止未授权的访问；系统资源使用的过程是根据安全策略规定的，并且根据该策略只允许被授权的实体(用户、程序、过程或者其他系统)。

[RFC 2828，有修改]

3.2.3

问责制 accountability

系统属性(包括其系统的所有资源)，以确保一个系统实体的行动可追溯到该唯一的实体，并且该实体可为他的行为负责[10]。

3.2.4

应用程序 application

软件程序，由用户命令或进程事件触发以执行具体功能，而不用访问系统控制、监控或管理权限。

3.2.5

区域 area

现场物理的、地理的或逻辑的资产组的子集。

注：区域可以包括生产线、过程单元和生产设备。区域可以通过本地的网络进行互连，并且包括该区域执行操作的系统。

3.2.6

资产 asset

组织所拥有或保管的物理或逻辑对象，该对象对组织具有潜在或实际的价值。

3.2.7

关联 association

系统实体间的合作关系，通常用于相互传递信息的目的[10]。

3.2.8

保证 assurance

通过系统安全策略的强制实施提供可信性的系统属性。

3.2.9

攻击 attack

对系统具有威胁的破坏，即企图躲避系统安全服务并破坏系统安全策略的故意行为(尤其指方法或

技术)[10]。

注：以下为常见攻击分类：

——主动攻击是指企图改变系统资源或影响其操作。

——被动攻击是指企图使用系统的信息但不会影响系统资源。

——内部攻击是指安全范围内的实体发起的攻击(内部实体)，即被授权访问系统资源的实体未按所授权的方式使用这些资源。

——外部攻击是指范围外部由系统未授权或者不合法的使用者发起的(包括内部人员从安全范围外发起的攻击)，潜在的外部攻击者包括业余攻击者、有组织的罪犯、国际恐怖分子和敌对政府。

3.2.10

攻击树　attack tree

寻找攻击系统安全的途径的正式的、系统的方法。

3.2.11

审计　audit

对记录和活动的独立的审查和检查，来评估系统控制的充分性，以确保与已建立的策略和操作规程一致，并且给出对控制、策略或者程序进行必要改动的建议(见 3.2.100)。

注：审计有三种形式：

——外部审计是由非组织雇员或者承包人实施；

——内部审计是由组织内专门从事内部审计的独立部门实施；

——自我评估控制由组织内部的同行实施。

3.2.12

鉴别操作　authenticate

验证用户、用户设备或者其他实体的身份、数据存储、传输的完整性、暴露信息系统内未经授权的修改；建立传输的有效性。

3.2.13

鉴别　authentication

旨在建立传输、信息或发起方有效性的安全方法，核实接收特定信息类别的个人授权的方法的有效性。

3.2.14

授权　authorization

授予系统实体访问系统资源的权力或权限[10]。

3.2.15

自动车辆　automated vehicle

包括控制系统以能够自主或者远程操作的移动设备。

3.2.16

可用性(性能)　availability (performance)

假定提供了其所需的外部资源，在给定的时刻或者给定的时间内，在给定的条件下执行必要功能时的能力。

注 1：性能来源于可靠性，可维护性和维护支持。

注 2：所需的外部资源，除了维护资源，不影响项目的可用性能力。

3.2.17

边线　border

物理或者逻辑安全区域的边或者边界。

3.2.18

僵尸网络 botnet

能够自主运行的恶意软件的统称。

注：僵尸网络发起方能够远程控制这些恶意软件，可能是出于不正当的目的。

3.2.19

边界 boundary

软件、硬件或者其他物理屏障，限制进入系统或者部分系统。

3.2.20

通道 channel

在通信管道（见 3.2.27）内建立的特定的通信链接。

3.2.21

密文 ciphertext

通过加密后传输的数据，这样其语义信息内容（它的含义）不再是可理解的或者直接能用的。

3.2.22

客户端 client

接收或请求来自服务器端的服务或信息的设备或应用[11]。

3.2.23

通信路径 communication path

源到一个或者多个目的地的逻辑连接，该连接可以是设备、物理过程、数据项、命令或者编程接口。

注：通信路径不仅限于有线或者无线的网络，也包括其他通信方式，例如：内存、程序调用、工厂的状态、可移动的介质和人员的交互。

3.2.24

通信安全 communication security

a) 通信系统中实现和保证安全服务的措施，特指提供数据保密性和数据完整性，以及通信实体认证的措施；

b) 应用安全服务所达到的状态，特指数据保密性、完整性和通信实体认证成功的状态[11]。

注：通常理解为包括密码算法和密钥管理方法，以及实现这些的过程、设备、密钥材料和设备生命周期管理。但是，密码算法、密钥管理方法和过程可能不适用于某些控制系统的应用。

3.2.25

通信系统 communication system

硬件、软件和传播媒体的组合，以便报文从一个应用传输到另一个应用[9]。

3.2.26

危害（泄密） compromise

信息被未授权泄露、修改、替代或者使用（包括密钥和其他关键安全参数）[12]。

3.2.27

管道 conduit

保护安全的通信资产逻辑组。

注：这和保护电缆免受物理损坏的物理管道类似。

3.2.28

保密性 confidentiality

保证信息不被泄露给未授权的个人、过程或者设备[9]。

3.2.29

控制中心　control center

用于运营资产的中心位置。

注 1：基础设施工厂典型地使用一个或者多个控制中心来监管或者协调其操作。如果有多个控制中心(例如：在单独分开的位置上有一个备用的中心)，它们是通过广域网互连的。控制中心包括 SCADA 系统、主机和相关的操作员显示设备以及辅助信息系统，例如历史信息系统。

注 2：在某些行业，更多使用“控制室”。

3.2.30

控制设备　control equipment

包括分布式控制系统、可编程序控制器、SCADA 系统、相关的操作界面控制台和用于管理与控制过程的现场传感控制设备。

注：术语包括用于协调智能电子设备上的控制逻辑和算法执行的现场总线，以及用于监视过程和维护过程的系统。

3.2.31

控制网络　control network

用于连接控制物理过程设备的实时网络(见 3.2.97)。

注：控制网络可以分为若干区域，并且在一个公司或者场所内可以有多个独立的控制网络。

3.2.32

成本　cost

影响公司或者个人的可度量的价值。

3.2.33

对抗(措施)　countermeasure

行动、设备、程序或者技术。这些措施能够降低威胁、脆弱性，可预防、消除攻击和最小化攻击所造成的危害，或者可以发现和报告这些攻击以便采取正确的行动[10]。

注：“控制”在某些上下文中也用于描述这个概念。本文件中采用“对抗措施”这个术语就是为了和文中采用的“过程控制”中的控制这个词不相互混淆。

3.2.34

密码算法　cryptographic algorithm

基于密码科学的算法，包括加密算法、加密哈希算法、数字签名算法和密钥协商算法。

3.2.35

密钥　cryptographic key

通过加密算法执行变换的输入参数。

3.2.36

网络安全　cybersecurity

用于防止关键系统或者信息类资产的非授权使用、拒绝服务、修改、泄露、财政损失和系统损害的行为。

注：目标是降低风险，这些风险包括人身伤害、威胁公共健康、丧失公众或者消费者信任度、泄露敏感资产、不能保护商业资产，或者违背法规。这些概念适用于生产过程的任何系统，包括单机的和网络的设备。系统间的通信可以通过内部报文或者通过任何操作员或机器接口，以便认证、操作、控制，或和任意的控制系统交换数据。计算机安全包括标识、认证、问责制、授权、可用性和隐私。

3.2.37

数据保密性　data confidentiality

信息对未授权的系统实体(未授权的个人、实体或者过程)不可用或者不能被披露的属性。

3.2.38

数据完整性　data integrity

数据在未授权或者意外情况下，不被修改，破坏，或者丢失的属性[10]。

注：该术语描述的是数据值的持续性和保密性，不涉及数据值代表的信息或者值的来源的可靠性。

3.2.39

解密　decryption

使用密码算法和密钥，把密文转换成明文的过程(见 3.2.47)[10]。

3.2.40

纵深防御　defense in depth

提供多重安全保护，特别是在层次上，如果不能阻止攻击就采取延缓策略。

注：纵深防御意指在各层的安全和检测，即便在一个单独的系统，具有以下特征：

——攻击者在不被发现的情况下突破或者绕过每一层；

——某层上的缺陷可以通过其他层的能力来缓解；

——系统安全在全部网络安全范围内由各个安全层组成。

3.2.41

非军事化区　demilitarized zone

逻辑上介于内部和外部的网络段[9]。

注 1：非军事化区的目的是为外部信息交换提供内部网络策略，实现外部非信任源的受限访问，同时屏蔽内部网络免于外部攻击。

注 2：工业自动化和控制系统的上下文中，术语“内部网络”典型地应用于主要重点保护的网络或网段。例如，当其连接到“外部的”商业网络时，控制网络就指“内部的”网络。

3.2.42

拒绝服务　denial of service

对授权访问系统资源的阻止或者中断，或者系统操作和功能的延缓[10]。

注：工业自动化和控制系统的环境中，拒绝服务是指过程功能的损失，而不仅仅是数据通信的损失。

3.2.43

数字签名　digital signature

数据密码变换的结果，正确完成时，提供数据源认证，数据完整性和签名者非抵赖服务[11]。

3.2.44

分布式控制系统　distributed control system

系统单元被分离但是以耦合方式运行的一种控制系统类型。

注 1：分布式控制系统有比那些典型的 SCADA 系统更短的耦合时间常数。

注 2：分布式控制系统通常用于连续过程处理，例如发电、石油和天然气提炼、化工、制药和造纸，也用于离散过程处理，例如汽车、其他食品生产、包装和仓储。

3.2.45

域　domain

由安全策略，安全模型或者安全体系结构定义的环境或者上下文，其中包括系统资源和能够访问这些资源的系统实体集[10]。

3.2.46

窃取　eavesdropping

未授权组织对通信信息的监视或者记录。

3.2.47

加密 encryption

明文转换成密文的密码变换，隐藏了数据的原始意义以阻止该数据被知道或者使用(见 3.2.39)[10]。

注：如果进行反向转换，相反的逆向过程被称为“解密”，解密是将储存的加密数据转换成它的原始状态。

3.2.48

企业 enterprise

生产或运输产品运营和维护基础服务的商业实体。

3.2.49

企业系统 enterprise system

信息技术元素的集合(例如：硬件、软件和服务)，其目的是便于组织商业流程或过程(行政或工程)。

3.2.50

受控设备 equipment under control

用于生产、过程、运输、医疗或其他活动的设备、器械、设施或者工厂[13]。

3.2.51

现场 I/O 网络 field I/O network

连接传感器和执行器到控制设备的通信链路(有线的或无线的)。

3.2.52

防火墙 firewall

两个互连网络间限制数据传输的网际连接设备[10]。

注：防火墙可以是安装在通用计算机上的应用软件或者是专有平台(设备)，用于转发或者拒绝/丢弃网络上的包。典型的防火墙用于定义区域边界。防火墙通过定义规则来限制端口开放。

3.2.53

网关 gateway

连接功能相近但实现不同的两个(或多个)计算机网络的中继装置，且该装置能够使一个网络的主机与另一网络的主机进行通信[10]。

注：也被描述为两个计算机网络转换接口上的中间系统。

3.2.54

地理场所 geographic site

企业物理的、地理的，或者逻辑资产的组合。

注：地理场所可以包括区域、生产线、过程工段、过程工位、控制中心和搬运车，并可通过广域网连接到其他场所。

3.2.55

防护装置 guard

用于不同安全等级(一个网络通常比另一个更安全)的两个网络(或者计算机或者其他信息系统)之间的网关，该网关可信传输两个网络间的信息，或者确保从一个高安全网络到低安全网络中无敏感信息不被泄露，或者在高安全网络中保护数据的完整性[10]。

3.2.56

主机 host

接入到通信子网或网间的计算机，并且该计算机可以使用网络提供的服务与其他附属系统进行数据交换[10]。

3.2.57

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

影响或改变工业过程的功能安全、安全和可靠操作的人员、硬件和软件的集合。

注：系统包括，但不限于：

- 工业控制系统包括分布式控制系统(DCS)、可编程序逻辑控制器(PLC)、远程终端单元(RTU)、智能电子设备、监督控制和数据采集(SCADA)、网络电子传感和控制、监视和诊断系统。(在本文件中，不论物理上是分开的还是集成的，过程控制系统包括基本过程控制系统和安全仪表系统(SIS)功能)。
- 相关的信息系统，例如先进控制或者多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、制造执行系统和工厂信息管理系统。
- 相关的内部、人员、网络或机器接口，为连续的、批处理、离散的和其他过程提供控制、安全和制造操作功能。

3.2.58

初始风险　initial risk

实施控制或对策风险(见 3.2.87)。

3.2.59

内部人员　insider

受信任的人、雇员、承包商或者供应商，通常他们知道公众不知道的信息(见 3.2.74)。

3.2.60

完整性　integrity

系统质量反映了操作系统的逻辑正确性和可靠性，实现保护机械装置的软件和硬件的逻辑完备性、数据结构和存储数据表现的一致性。

注：正常信息安全模式下，完整性常被狭义地理解为保护信息免遭非授权修改或破坏。

3.2.61

侦听　interception；sniffing

捕获和揭露报文内容，或者基于报文目的地或来源地、传输的频率或时长以及其他通信属性，使用通信量分析破坏通信系统的保密性。

3.2.62

接口　interface

为逻辑信息流提供访问模块的逻辑入口点或出口点。

3.2.63

入侵　intrusion

危害系统的非授权行为(见 3.2.9)。

3.2.64

入侵检测　intrusion detection

监视和分析系统事件的安全服务，以便找出在非授权方式下试图访问系统资源的行为，并提供实时或接近实时的警告。

3.2.65

IP 地址　IP address

使用因特网协议及其他协议，为计算机或设备分配的用于标识和通信的地址。

3.2.66

ISO

国际标准化组织。

注：ISO 不是缩写，它起源于希腊字 iso(意为平等)。

3.2.67

密钥管理　key management

在密码系统的生命周期中，处理和控制密钥和相关资料（例如初始化值）的过程，包括请求、生成、分配、储存、加载、约定、归档、审计和销毁这些密钥和相关资料[10]。

3.2.68

生产线　lines

工段　units

工位　cells

实施制造加工、现场设备控制，或者运输功能的较低级别的元素。

注：该级别的实体可通过区域控制网络连接在一起，并且可包括与该实体实施的操作相关的信息系统。

3.2.69

局域网　local area network

在有限的地理区域（通常少于 10 km），用于连接计算机和其他智能设备的通信网络[9]。

3.2.70

恶意代码　malicious code

编写的程序或代码，目的是收集有关系统或用户的信息、破坏系统数据，并为进一步侵入系统提供支点、伪造系统数据和报告或者耗费系统操作和维护人员的时间。

注 1：恶意代码攻击常以病毒、蠕虫、木马或者其他自动传播的形式出现。

注 2：恶意代码也常指“恶意软件”。

3.2.71

制造运行　manufacturing operation

生产、维护和质量保证操作以及它们与生产设施其他活动的关系的组合。

注：制造运行包括：

- 在原材料或部件转换成产品的过程中，协调人员、设备和材料的制造和处理活动；
- 通过物理设备、人员工作和信息系统所执行的功能；
- 制造企业内与生产进度表、使用、能力、定义、历史记录和所有资源状态（人员、设备和材料）相关的管理信息。

3.2.72

防抵赖　nonrepudiation

提供一种安全服务，以防止对通信行为的非法否认[10]。

3.2.73

OPC

在过程控制环境中信息交换的规范集。

注：缩写“OPC”来自“过程控制 OLE（OLE for Process Control）”，“OLE”是“对象链接和嵌入（Object Linking and Embedding）”的缩写。

3.2.74

外部人员　outsider

访问内部时不受信任的人员或团体，他可能是目标组织认识或不认识的（见 3.2.59）。

注：外部人员有可能曾经是（或不是）内部人员。

3.2.75

渗透　penetration

未授权时，成功地访问了受保护的系统资源[10]。

3.2.76

网络钓鱼　phishing

通过伪造邮件引诱接收者浏览貌似合法的网站，使受害者透露信息的一类安全攻击。

3.2.77

明文　plaintext

输入给加密过程的、可被用作加密转换的未加密数据，或通过解密过程输出的数据[10]。

3.2.78

特权　privilege

执行特定功能的授权或一系列授权，尤其是在计算机操作系统环境中[10]。

注：使用特权控制的功能包括：确认报警、改变设定点、修改控制算法。

3.2.79

过程　process

产品或材料的制造、处理或运输时执行的系列操作。

注：本标准中为描述工业自动化和控制系统的控制设备，大量使用了“过程”这一术语。

3.2.80

协议　protocol

两个系统间执行和控制某些关联类型（例如通信）的规则集（例如格式和规程）[10]。

3.2.81

参考模型　reference model

用一致的方式描述模块和系统接口的结构。

3.2.82

可靠性　reliability

在规定的时间周期内，在规定的条件下系统执行所要求功能的能力。

3.2.83

远程访问　remote access

在安全区域的范围内，在不同地理位置赋予与本地相同的系统使用权。

注：“远程”的定义随着情况的变化而变化。例如，访问可以来自距离指定区域很远的位置，但是仍然在公司或者组织的区域内。与从公司区域外部并且很远的位置来的访问相比，访问风险可能比较低。

3.2.84

远程客户端　remote client

控制网络外部的资产。通过通信链接，临时或永久地连接到控制网络内部主机，以便直接或间接访问控制网络的部分控制设备。

3.2.85

抵赖　repudiation

参与通信的某一实体拒绝承认参与了全部通信或部分通信。

3.2.86

残余风险　residual risk

采取安全控制或者对抗措施后仍存在的风险。

3.2.87

风险　risk

以概率的形式表示特定威胁利用特定脆弱性造成特定后果的预期损失[10]。

3.2.88

风险评估　risk assessment

系统地辨识重要系统资源的潜在脆弱性和威胁，基于发生的概率量化损失风险和后果，并（可选地）建议如何对各对抗措施分配资源以使总风险最小的过程。

注1：资源类型包括物理资源、逻辑资源和人力资源。

注2：风险评估常与脆弱性评估相结合，以辨识脆弱性并量化相关风险。周期地执行这些内容是为了反映组织机构的风险裕度、脆弱性、规程、人员和技术上的变化。

3.2.89

风险管理　risk management

基于风险评估来辨识和采用与所保护的资产价值相称的对抗措施的过程。

3.2.90

风险缓解控制　risk mitigation controls

风险对抗措施和业务连续性计划的结合。

3.2.91

风险裕度等级　risk tolerance level

组织机构可接受的残余风险的等级。

3.2.92

基于角色的访问控制　role-based access control

基于身份的访问控制的形式，其中所识别和控制的系统实体在机构或过程中处于功能性位置[10]。

3.2.93

路由器　router

在OSI第三层上的两个网络之间的网关，在网络间中继和直接传递数据包。路由器最常见的形式是传递因特网协议（IP）数据包[10]。

3.2.94

（功能）安全　safety

免于不可接受的风险[3]。

3.2.95

安全仪表系统　safety-instrumented system

用于实现一个或者多个安全仪表功能的系统[3]。

注：安全仪表系统由传感器、逻辑解算器和执行器的任意组合组成。

3.2.96

安全完整性等级　safety integrity level

离散的等级（四个中的一个），用于规定分配给安全仪表系统的安全仪表功能的安全完整性要求[3]。

注：安全完整性等级4是安全完整性的最高等级，安全完整性等级1是安全完整性的最低等级。

3.2.97

安全网络　safety network

连接安全仪表系统并用于安全相关信息通信的网络。

3.2.98

秘密　secret

信息的受保护状态，以防止除预期获得的系统实体之外的任何系统实体获得[10]。

3.2.99

安全 security

a) 保护系统所采取的措施；

b) 由建立和维护保护系统的措施而产生的系统状态；

c) 能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态[10]；

d) 基于计算机系统的能力，能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统功能，却保证授权人员和系统不被阻止[13]；

e) 防止对工业自动化和控制系统的非法或有害的入侵，或者干扰其正确和计划的操作。

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

3.2.100

安全体系结构 security architecture

描述安全服务的设计图和一组规则，要求系统满足用户需求，提供实现服务所要求的系统元件，并且要求系统元件的性能等级能够应对有威胁的环境[10]。

注：本标准中，对故意或者非故意的安全事件，安全体系结构将可以保护控制网络。

3.2.101

安全审计 security audit

独立的审查和检查系统的记录和活动，以确定系统控制的充分性，保证与已建立的安全策略和规程相一致，检测是否违反安全服务，以及建议对抗措施的改进[8]。

3.2.102

安全组件 security components

用于提高工业自动化和控制系统安全性能的资产，诸如防火墙、认证模块或者加密软件（见 3.2.33）。

3.2.103

安全控制 security control

见 3.2.33。

注：本标准使用“对抗措施”这个术语，就是为了和文中采用的过程控制中的术语“控制”进行区分。

3.2.104

安全事件 security event

在系统中出现与系统安全相关的事件[10]。

3.2.105

安全功能 security function

防止未授权电子干预的区域或者管道功能，这些干预能影响或改变在区或管道内的设备和系统的正常功能。

3.2.106

安全事故 security incident

系统或者网络的不利事件或者这种事件发生的威胁[9]。

注：术语“近乎发生”有时用于描述在稍有不同环境下可能成为事故的事件。

3.2.107

安全入侵 security intrusion

安全事件或多个安全事件的组合，其构成安全事故，其中入侵者在未经授权情况下获得或者试图获得对系统（或系统资源）的访问[10]。

3.2.108

安全等级 security level

基于该区域或者管道的风险评估，与区域或管道的设备和系统所需要的对抗措施有效性及固有安全属性相对应的等级[12]。

3.2.109

安全目标 security objective

安全目标通过使用一定的减轻措施实现。例如，保密性、完整性、可用性、用户真实性、访问授权、问责制等。

3.2.110

安全边界 security perimeter

应用了安全策略和安全体系结构的区域分界线（逻辑的或物理的），即系统资源得到安全服务保护的区域分界线[10]。

3.2.111

安全性能 security performance

程序的符合性和措施的完整性，确保了安全措施的持续有效性和适用性。包括特定威胁的保护、泄密后分析、业务需求变更、新威胁、脆弱性信息的审核，以及控制系统的周期审计。

注：要求用测试、审计、工具、措施或者其他方法来评定实际的安全性能。

3.2.112

安全策略 security policy

规范或限定系统或组织如何为保护其资产提供安全服务的规则集合[10]。

3.2.113

安全规程 security procedure

精确描述了安全实践是如何实现和执行的。

注：安全规程是通过人员培训、使用当前可用的技术来实现。

3.2.114

安全程序 security program

从策略的定义和通信到最佳行业实践的实现，以及目前执行的操作和审计等管理安全所有概念的统称。

3.2.115

安全服务 security services

用于提供保密性、数据完整性、认证或信息防抵赖的机制[10]。

3.2.116

安全违规 security violation

来自外部入侵或内部无意违反安全策略的行为或事件。

3.2.117

安全区 security zone

共享通用安全需求的逻辑资产或物理资产的集合。

注 1：本标准中所用的“区”都是指安全区。

注 2：一个区和其他区要有明显的边界。一个安全区的安全策略在其内部和边缘都要强制执行。一个安全区可以包括多个不同等级的子区。

3.2.118

传感器和执行器 sensors and actuators

连接到过程装置和控制系统的测量和执行元件。

3.2.119

服务器 server

给客户端设备和应用提供信息或服务的设备或者应用[10]。

3.2.120

侦听 sniffing

见 3.2.61。

3.2.121

欺骗 spoof

伪装成授权用户执行未授权的行为[10]。

3.2.122

监督控制和数据采集系统 supervisory control and data acquisition system;SCADA system

一种松散的耦合分布监视和控制系统,常用于输配电系统、油气管道、给水和污水处理系统。

注:监督控制系统也用于批量的、连续的、离散的制造工厂,以集中监视和控制生产场所的活动。

3.2.123

系统 system

由相互作用、相互关联、相互依赖的多个要素构成的一个复杂的整体。

3.2.124

系统软件 system software

为特定的计算机系统或者计算机系统家族设计的特定软件,用于辅助操作和维护计算机系统以及相关程序和数据[11]。

3.2.125

威胁 threat

当有违反安全而引起伤害的环境、能力、行动或事件时,出现安全违规的可能性。

3.2.126

威胁行为 threat action

对系统安全的攻击[10]。

3.2.127

威胁代理 threat agent

发生威胁行为的代理。

3.2.128

流量分析 traffic analysis

即使数据被加密或者不可以直接使用,根据数据流的显著特征(包括身份、来源和目的地以及位置、数量、频率、持续发生的时间)而做出的信息推论。

3.2.129

木马 Trojan horse

该计算机程序貌似为有用的功能,但是具有隐蔽和潜在的逃避安全机制的恶意功能,通常通过激发具有合法授权的系统实体来对其进行调用。

3.2.130

受信任的通道　trusted channel

在两个安全区域内能够提供安全通信的通信链路。

3.2.131

不受信任的通道　untrusted channel

在两个安全区域内不能够提供安全通信的通信链路。

3.2.132

用例　use case

用于获取潜在功能需求的技术，采用一个或者多个场景以传达系统如何连接到终端用户或者其他系统以达到特定目标。

注：典型的用例视系统为黑盒子，而且与系统的交互，包括系统响应，能够从系统外面感知。用例比较流行，是因为它们简化了需求的描述，并且避免了假设功能性是如何被实现的问题。

3.2.133

用户　user

不管是否授权，能够访问系统的个人、组织实体或者自动化过程[10]。

3.2.134

病毒　virus

通过将自身副本插入到其他可执行的代码或文件中进行传播的，可自我复制或者自我衍生的程序。

3.2.135

脆弱性　vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点，可被利用来危害系统的完整性或安全策略[10]。

3.2.136

广域网　wide area network

用于连接远距离（例如国内或跨国）的计算机、网络和其他设备的通信网络[11]。

3.2.137

窃听　wiretapping

通信系统中侦听和访问数据流中的数据和其他信息的攻击方式[10]。

注1：虽然术语最初指与电导体进行机械连接以链接两个节点，现在指从任何类型的媒介上读信息，媒介用于链接或者直接从节点上读取，例如网关或者子网交换机。

注2："主动窃听"试图改变数据或者影响数据流；"被动窃听"仅试图侦察数据流并且得到数据流中包含的信息。

3.2.138

蠕虫　worm

能够独立运行的计算机程序，能够将自身完整的工作版本传播给网络上的其他主机，并且可以破坏性地消耗计算机资源[10]。

3.2.139

区　zone

见3.2.117。

注：本标准中如果没有特别说明的术语"区"都是指安全区。

3.3　缩略语

下列缩略语适用于本文件。

ANSI：American National Standards Institute（美国国家标准研究所）

CIA：Confidentiality，Integrity，and Availability（保密性、完整性和可用性）

CN:Control Network(控制网络)
COTS:Commercial off the Shelf(商用现货)
CSMS:Cyber Security Management System(网络安全管理系统)
DCS:Distributed Control System(分布式控制系统)
DDoS:Distributed Denial of Service(分布式拒绝服务)
DoS:Denial of Service(拒绝服务)
DMZ:Demilitarized Zone(非军事化区)
FIPS:U.S. Federal Information Processing Standards(美国联邦信息处理标准)
IACS:Industrial Automation and Control System(工业自动化和控制系统)
IEC:International Electrotechnical Commission(国际电工委员会)
IEEE:Institute of Electrical and Electronics Engineers(电子和电气工程师协会)
I/O:Input/Output(输入/输出)
IP:Internet Protocol(因特网协议)
IT:Information Technology(信息技术)
LAN:Local Area Network(局域网)
NASA:U.S. National Aeronautics and Space Administration(美国国家航空航天局)
NOST:NASA Office of Standards and Technology(NASA 标准和技术办公室)
OSI:Open Systems Interconnect(开放系统互连)
PLC:Programmable Logic Controller(可编程逻辑控制器)
RTU:Remote Terminal Unit(远程终端单元)
SCADA:Supervisory Control and Data Acquisition(监督控制和数据采集)
SIL:Safety Integrity Level(安全完整性等级)
SIS:Safety-Instrumented System(安全仪表系统)
WAN:Wide Area Network(广域网)

4 现状

4.1 概述

工业自动化和控制系统在复杂的环境下运行。组织越来越需要信息在工业自动化和业务之间共享,在一个项目中的合作伙伴可能是另外一个项目中的竞争对手。然而,由于工业自动化和控制系统的设备是直接和工艺过程相连的,安全遭到破坏的后果不仅仅是丧失了商业保密或在信息传送中发生中断,还可能带来潜在的对人员或生产造成损失、破坏环境、违反法律法规和危及运行安全等更严重的后果。这可能会衍生出组织所不期望的结果,甚至可能对所在地区或国家的基础设施造成破坏。

威胁不仅仅来自外部,内部具有一定技术能力的人员恶意或无意的行为也可能导致严重安全风险。另外,工业自动化和控制系统还经常和其他业务系统相连。对运行系统的修改和测试还会对系统的运行产生没有意识到的影响。控制系统区域之外的人对系统所进行的安全测试,更加剧了这些影响的数量和程度。综合上述因素,显而易见,潜在的对工业过程获得未授权或破坏性访问的风险并不是微不足道的。

虽然技术变化和合作伙伴关系可能对业务行为是有益的,但也增加了破坏安全的潜在风险。正因为对于业务的威胁增加了,所以对于安全的需要也随之增加。

4.2 当前系统

工业自动化和控制系统是从单个的、独立的、专用操作系统和网络向互联的系统和使用商用技术(即,操作系统和协议)的应用逐渐演化的。工业自动化和控制系统正在通过各种通信网络与企业管理系统和其他业务应用集成。随着这种集成度的增加,带来了包括以下在内的巨大商业价值:

a) 增加了工业控制系统各项活动的可见性(工作进程、设备状态、生产进度),从业务层面集成工业过程系统,可以提高分析的能力,从而降低成本,提高生产力;

b) 集成制造和生产系统,可以更直接获得商业信息,有利于形成具有快速响应能力的企业;

c) 通用的接口降低了总体维护成本,并允许对生产过程的远程支持;

d) 对过程控制系统的远程监视可以降低成本并有利于更快速地解决问题。

通过定义模型、术语和信息交换的标准,使得工业自动化和控制系统行业以一致的方式分享信息是可能的。然而,这种交换信息的能力增加了有恶意企图的个人进行攻击或误操作的脆弱性,从而给使用工业自动化和控制系统的企业带来潜在的风险。

在物理硬件、编程和通信方面,工业自动化和控制系统的配置非常复杂。这种复杂性使得下列问题难以确定:

——授权谁可以访问电子信息;

——用户何时能访问信息;

——用户访问何种数据或功能;

——访问请求源的位置;

——如何请求访问。

4.3 当前趋势

下面几个趋势使得工业自动化和控制系统的安全变得越来越重要:

a) 近年来对商业和个人计算机系统的恶意代码攻击显著增加。与前些年比,每年企业报告发生未经授权企图(无论是有意的还是无意的)访问电子信息的案例逐渐增多。

b) 工业自动化和控制系统转向 COTS 操作系统和协议,并与商业网络互联。使得这些系统和目前商业系统和桌面设备容易遭到同样的软件攻击。

c) 因特网上用于自动攻击的工具随处可得到。现在使用这些工具的外部威胁包括网络犯罪分子和网络恐怖分子,他们很可能拥有更多的资源和知识去攻击工业自动化和控制系统。

d) 工业领域的共同投资、合作联盟以及外包服务,随着组织或团体数量的增加,使得工业自动化和控制系统的安全变得更加复杂。在开发这些系统的安全措施时应考虑这些情况。

e) 非法访问的焦点,已经从业余黑客或对企业不满的员工扩展到有预谋的犯罪或恐怖活动,这些犯罪或恐怖活动意图对更大的组织机构或设施造成影响。

f) 采用工业文件协议,例如作为工业自动化和控制系统与现场设备之间的通信的因特网协议(IP)。使用 IP 协议,工业自动化和控制系统与现场设备在网络层会受到同商用系统一样的攻击。

这些趋势结合,大大增加了组织设计、运行工业自动化和控制系统的风险。同时,工业控制系统的安全正在受到更加显著和广泛的关注。这种变化需要建立结构化的导则和规程,来规范工业自动化和控制系统的安全,以及工业自动化和控制系统与其他系统的连接。

4.4 潜在影响

了解开放式操作系统和网络特性的人,具有潜在的入侵控制台设备、远程设备、数据库、在某些情况

下是控制平台的可能性。入侵工业自动化和控制系统可能出现的后果包括：

a) 未授权访问、窃取或滥用保密信息；
b) 向未经授权的目的地发布信息；
c) 丧失过程数据和生产信息的完整性或可靠性；
d) 丧失系统的可用性；
e) 扰乱过程，导致过程的功能出错，降低产品质量，丧失生产能力，危及过程安全，或造成向环境的排放；
f) 设备损坏；
g) 人员伤害；
h) 违反法律法规；
i) 带来公共健康和信任的风险；
j) 对国家安全造成威胁。

5 概念

5.1 概述

本章描述几个基本概念，这些概念构成了后面章节以及 IEC 62443 其他标准的基础。特别是解决了下列问题：

a) 哪些是用于描述安全的主要概念；
b) 哪些重要概念构成了完整的安全程序的基础。

5.2 安全目标

传统的安全主要关注三个目标：即保密性、完整性和可用性，通常用 CIA 缩写来表示。典型办公或商业系统的信息技术(IT)安全策略一般最为关注信息的保密性，以及为此要采取的必要的访问控制。完整性的优先级被列为第二，而可用性最低。

在工业自动化和控制系统的环境下，这些目标的优先级往往是不同的。这些系统的安全最关注维持系统所有部件的可用性。存在与由工业自动化和控制系统控制、监视甚至影响的工业机器相关联的内在风险。因此，完整性经常被置于第二重要的位置。而通常保密性的重要性更差一些，因为数据经常是未经过加工的，需要在上下文中经过分析才具有一定价值。

时间响应也很重要。控制系统可以要求 1 ms 范围内的系统响应时间，而传统商业系统在 1 s 或几秒内完成操作就可以了。

某些情况下，两者的优先级完全是相反的，见图 1。

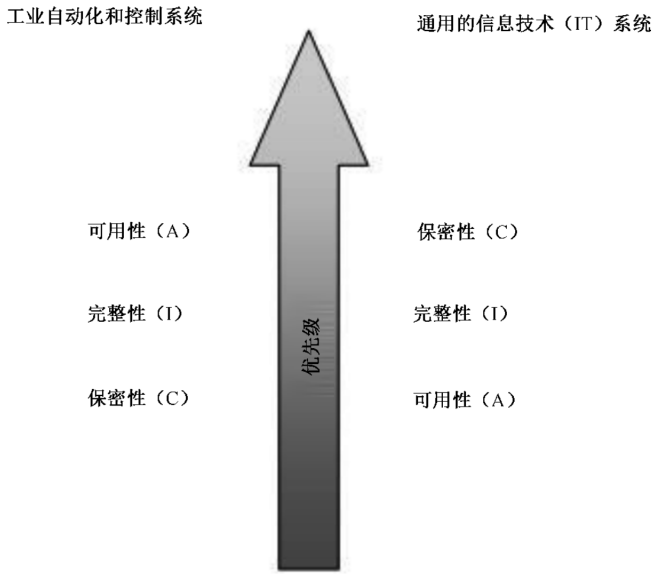

图 1　IACS 和通用 IT 系统目标比较

根据应用场景的不同，系统的完整性也可具有最高优先级。某些运行要求各个部件或系统具有不同的优先级目标（即完整性或可用性可优先于保密性，或反之），从而使得组织采取不同的应对措施达到这些安全目标。

5.3　基本要求

图 1 所示简单的 CIA 模型还不足以使人们完全理解工业自动化和控制系统安全的要求。虽然 IEC 62443 系列的其他部分会给出详尽的清单，但一些工业自动化安全的最基本要求还是在这里列出。这些要求包括：

a）　访问控制（AC）：控制对被选设备、信息或二者的访问，防止未经授权查询设备或信息。

b）　使用控制（UC）：控制对被选设备、信息或二者的使用，防止未经授权操作设备或使用信息。

c）　数据完整性（DI）：保证被选通信通道上数据的完整性，防止未经授权的修改。

d）　数据保密性（DC）：保证被选通信通道上数据的保密性，防止被窃听。

e）　限制数据流（RDF）：限制通信通道上的数据流，防止向未经授权的信息源发布信息。

f）　事件及时响应（TRE）：对于任务关键型或安全关键型的情况，通过通知合适的主管机构、报告所必需的破坏的法律证据、自动采取及时的纠正行动以对破坏安全的事件作出响应。

g）　资源可用性（RA）：保证网络资源的可用性，防止拒绝服务攻击。

上述的所有要求都在本标准范围内，只是有些更详细的内容见 IEC 62443 系列的其他部分。例如，数据完整性和数据保密性的技术要求细节见 IEC 62443 的其他部分。

5.4　纵深防御

一般通过单一措施或技术很难达到安全的目标。比较高级的方法是使用纵深防御的概念，即通过分层或步进的方式采用多重措施。例如，入侵检测系统可以用来通知防火墙已被突破。

5.5　安全上下文

安全上下文构成了解释术语和概念的基础，并给出了安全各要素之间的相互关系。这里所说安全

的意思是防止对工业自动化和控制系统的正常和预期运行过程的非法或有害的入侵和干扰。

安全上下文基于威胁、风险、措施的概念，以及它们相互之间的关系。这些概念的关系可以用一个简单的模型来表示。图 2 复制的是 ISO/IEC 15408-1(通常规则)里的一个模型。图 3 是对这种相互关系的另一种不同的观点。

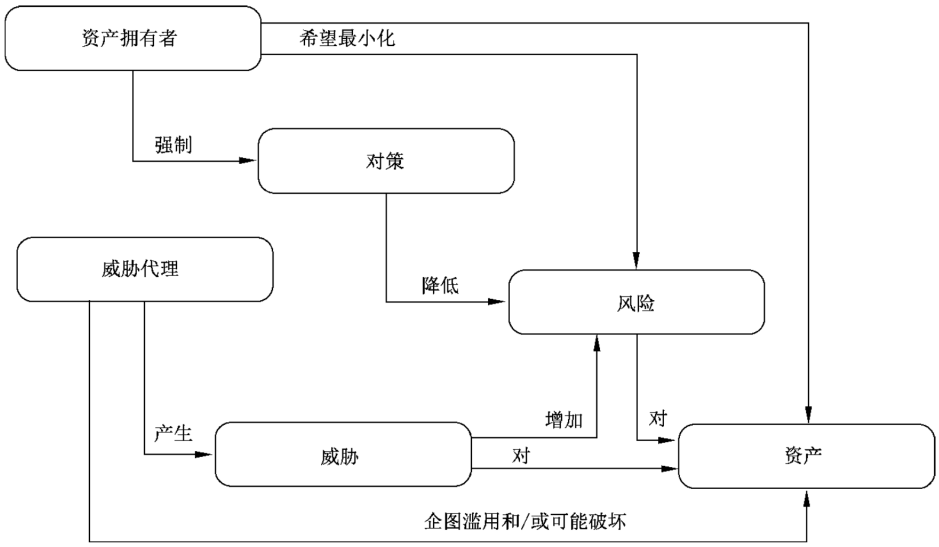

图 2　上下文要素相互关系

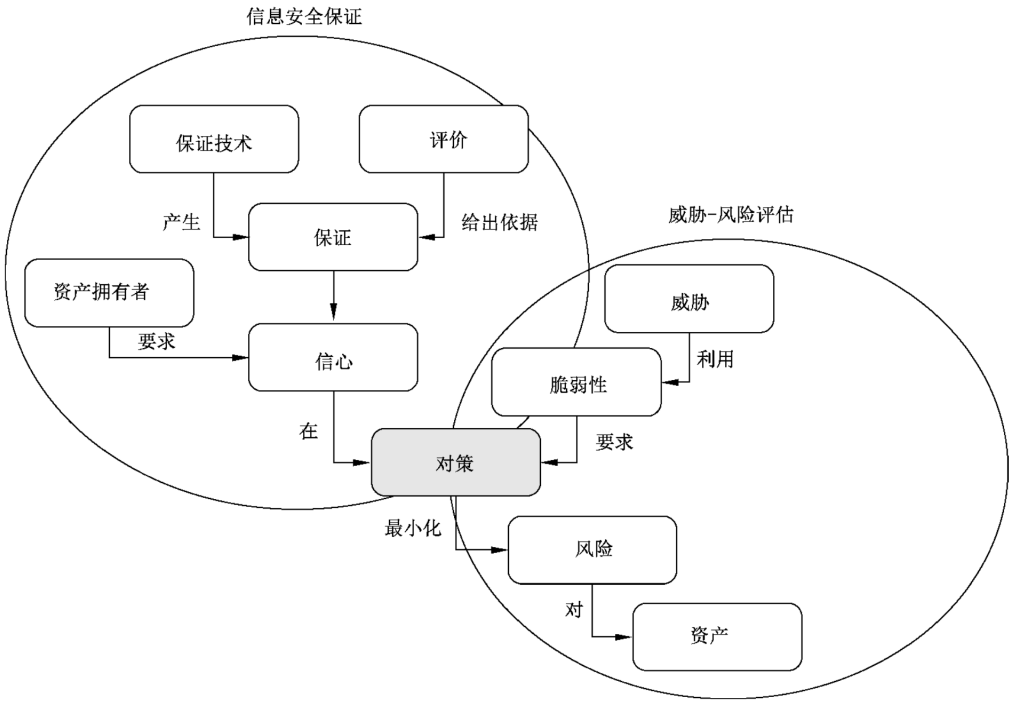

图 3　上下文模型

图 3 的上下文模型给出了与安全保证和威胁—风险评估两个相互关联的过程有关的一套扩展概念集。

5.6 威胁—风险评估

5.6.1 概述

在威胁-风险评估过程中，资产受风险的影响，可以通过采取对抗措施降低风险，对抗措施应针对会被不同威胁利用的脆弱性。下面这些条款将对这些要素进行详细描述。

5.6.2 资产

5.6.2.1 概述

资产是安全程序关注的焦点。它们是被保护的对象。为了充分理解对于IACS环境的风险，首先要生成一个被保护的资产清单。资产可以分为物理资产、逻辑资产和人员资产。

a) 物理资产：物理资产包括一个组织的任何物理部件或一组部件。在工业环境下，物理资产可能包括控制系统、物理网络部件和传输媒介、传送系统、墙、房间、厂房、材料，以及通过各种形式参与到控制、监视、生产过程分析，或支持一般业务活动的任何其他物理对象。受控于自动化系统并构成设备的资产是最重要的物理资产。

b) 逻辑资产：逻辑资产具有信息属性。这可以包括知识产权、算法、专有的实践技术、特殊工艺或其他构成组织运转或革新能力的信息要素。更进一步，这类资产可以包括公众的信誉度、买方的信任，或其他衡量尺度，它们一旦受到破坏，会直接影响业务。逻辑资产的形式可以是个人的记忆、文件、物理介质中包含的信息或其他信息资产的电子存储记录。逻辑资产还可以包括测试结果、合规数据或其他任何敏感、专用的，以及会提供或产生竞争优势的信息。丧失逻辑资产经常会对组织产生非常持久的和破坏性的后果。

过程自动化资产是一种特殊形式的逻辑资产。它们包括执行工业过程的自动逻辑。这些过程高度依赖于对精确定义事件的重复或连续的执行。过程资产的损害可能通过物理方法（例如，破坏媒体）或非物理方法（例如，未经授权的修改），导致对过程某种程度上丧失其完整性或可用性。

c) 人员资产：人员资产包括人员以及它们所拥有的与生产活动相关的知识和技能。人员资产还可以是自动生产过程所不包含的资质、特定的设备知识或其他活动，或紧急情况下所需的重要技能。很少有工艺设施是完全自动的，由于人为因素造成的运行故障可能会对生产造成重大影响，虽然系统从物理上或逻辑上还相对完整。例如，一个错误的报警可能会导致人为触发停机并对生产造成影响，虽然并没有对工业自动化和控制系统产生任何物理或逻辑上的破坏。任何伤及人员的事故或攻击都被认为是影响了人员资产。

5.6.2.2 资产估值

界定一个对象是否能称为物理资产或逻辑资产，其首先应被一个组织所拥有或保管，并且对组织有价值。价值的评估可以是定性的或定量的。一些组织认为定性评估是合适的，因为它们在风险分析过程中也是用定性的方法表述资产损失。

a) 资产定量估值：给出定量的评估值，与之相关的是精确的资金损失。可能依据更换成本、失销成本，以及其他资金方面的度量。定量分析需要严格的成本分析以获得精确的数值，但不能为组织提供关于损失的潜在影响的清晰描绘。

b) 资产定性估值：定性损失通常用更为抽象的方式来表述损失，例如百分比或类似于低影响、高影响、无影响这样的相对值。很多资产仅能用定性损失来分析。风险评估过程可以从定性评估开始，来证实高风险，并论证为降低风险而在补救措施上的资金投入行为的有效性，然后再

用定量分析作为支持，给出详细的风险情况描绘。

价值可以按照产生损失的类型来进行分类：

c) 直接损失：直接损失代表的是更新资产的成本。对物理资产而言，包括设备本身更新的成本。逻辑资产与其实用价值比较，直接损失相对较低，因为存储资产的媒体一般成本比较低。

d) 间接损失：间接损失代表了由于丧失资产组织将会面对的任何损失。这可以包括生产过程的停工期、返工或其他由于资产丧失导致的生产成本。物理资产的间接损失一般包括由于部件损坏对下游产生的影响。逻辑资产的间接损失一般更大，包括丧失公共信任，由于违规丧失生产许可，由于泄露了知识产权丧失竞争优势（如保密过程的技术）。

5.6.2.3 损失分类

综合资产类型和价值评估的信息，可以列出各种资产的损失类型，见表1。

表1 资产的损失类型

资产类型	直接损失	间接损失	定性或定量
物理	可能产生高的直接损失，主要是由于资产更新产生的成本。直接损失来自生产过程丧失完整性或可用性，以及干扰了生产过程的准确顺序或协调性而导致的物理资产的破坏	损失造成的下游影响包括丧失控制、其他资产的丧失或破坏，以及停工损失等	可以从对高风险的定性分析开始，然后再定量分析获得更精确的结果
逻辑	直接损失较小，因为存储媒体通常价格低廉且容易更换	高的间接损失，经常是由于丧失知识产权、专有程序的损害或违规造成的。由于设备损坏或物质释放产生的间接损失可以导致停工、返工、重新设计，或其他为恢复工业过程控制的工作	大部分是定性的，但有些下游影响可以定量评估
人员	按照人员伤害的程度可以从低到中等确定直接损失。可以短时间内恢复的小的伤害可能对公司的直接损失比较小，虽然伤害对个人的影响还会持续一段时间	按照人员伤害程度，以及该人对生产过程的重要性，间接损失可以是从低到高。按照个人所需恢复时间的不同，产生的加班成本或临时替换成本也会有很大不同。如果评估中考虑到社会责任以及潜在的诉讼和裁决的因素，永久性致残或死亡可能会产生高的间接损失	对生产立即产生定性影响，紧接着会产生人员恢复或替换的定量影响

5.6.3 脆弱性

简单来讲，脆弱性是系统、部件或组织固有的弱点。

脆弱性可能是来自有意的设计选择，也可能源于错误理解运行环境的偶然情况。脆弱性还有可能在设备老化直至最终被淘汰的过程中显现。与正常运行或受控的设备相比，这种情况通常发生在较短的时间内。脆弱性不仅仅限于电子或网络系统。了解物理（包括人员）和电子脆弱性之间的相互作用，

对于建立有效的工业自动化和控制系统安全是至关重要的。

一个最初只包含有限脆弱性的工业自动化和控制系统，随着环境变化、技术变化、系统部件的故障，替换部件的不可用、人员流动以及更高级的威胁的出现，可能会变得更加易受攻击。

5.6.4 风险

5.6.4.1 概述

风险通常定义为用概率表示的预计损失，这里的概率是指特定的威胁利用特定的脆弱性造成特定的后果的几率。风险是威胁、脆弱性和后果的函数，由于特定威胁或脆弱性对组织的资产造成特定损害，因而后果对组织造成负面影响。威胁和脆弱性可以用可能性来表示，可能性是特定行为发生的概率。

资产拥有者在估计风险时应归类并包括缓解或修补的成本。它们还应当采取适当的对抗措施来缓解最严重的安全问题，以达到最低的经济损失。

任何合理的风险评估方法都应采用层次化的方法对所有涉及的系统进行分析，从最靠近威胁的系统开始，逐渐深入。基本的风险评估过程包括三步：

a) 风险初始评估；

b) 实施风险缓解对抗措施；

c) 评估残余风险。

第2步和第3步可以根据需要重复进行，以将该残余风险降低到可接受的水平。特别的，第2步还包括评估现有控制和实施计划，增加补救措施或其他对抗措施。更具体的确定风险过程的描述将在IEC 62443以后部分给出。

需要考虑的典型风险通常包括：

a) 人员安全的风险，例如死亡或受伤；

b) 过程安全风险，例如设备损坏或业务中断；

c) 安全风险，例如成本、违法或损害品牌形象；

d) 环境风险，例如违规，违法或有重大影响；

e) 业务连续性的风险，例如业务中断。

5.6.4.2 风险容忍等级

定性风险分析的结果包括一份资产或情况清单，包含总体可能性和后果分级。按照分级对各项风险做出适当的响应属于管理责任。一些组织可以接受相对比较高的风险等级（例如有强劲增长势头的公司），另外一些公司则相反，面对风险则更趋向保守。因此，一定程度的残余风险对一个组织是可以接受的，但对另一个组织可能就不能接受。即使在同一公司内部，不同工厂也表现出不同的风险承受意愿和能力。管理宜明确定义和理解组织对风险承受的意愿和能力，才能够更好地分析已被识别的残余风险的响应级别。

一般来说，处理工业自动化和控制系统的安全问题不会引入新的风险，但对已经存在风险可能会有不同的看法。例如，工业自动化领域通常对功能安全的风险给予更多关注。

工业自动化和控制系统安全不必重新使用定义风险容忍等级的过程，只需从组织其他风险管理实践中获得即可。

5.6.4.3 风险响应

对风险可以有几种潜在响应。组织可以根据不同的环境，采取一些组合行动。

a) 设计排除风险：一种缓解形式是修改设计以排除风险。一些风险存在仅仅是由于可以“访问”，而“访问”是并不需要的。禁用不必要的功能或限制对功能的访问可以降低风险。组织可以采取适当的业务决策，就不会产生风险。这些响应包括拒绝某些事情，无论是对新的供应商的产品、系统或关系。

b) 降低风险：通过实施对抗措施可以降低被攻击的可能性或后果，将风险降低到一个可接受的水平。这里关键是达到一定的安全水平，而不是排除风险。

c) 接受风险：还有一种选择是接受风险，将它看作是开展业务的代价。组织需要承担一定的风险，而且不是总能有效地缓解或转移风险。

d) 转移或分担风险：也可以通过建立保险或协议来转移部分或全部风险到第三方。一个典型的例子是外包实现某些功能或服务。这种方法不是总有效，因为可能不能覆盖所有资产。安全策略可以恢复某些破坏，但不可能恢复像丧失客户信任这样的逻辑资产的损失。

e) 排除或重新设计多余的或无效的控制：好的评估过程将识别这些需要处理的控制，以便更加关注有效的控制。

5.6.5 威胁

5.6.5.1 概述

威胁描述了对一个系统可能的行为。它们可能表现为不同形式，但最为常见的两种形式是：

a) 偶然的事故：某人对正确的程序和策略不熟悉，或由于无意疏忽导致偶然风险。也可能是由于组织不了解所有风险，在运行复杂的工业自动化和控制系统时，偶然的事故使这些风险呈现出来。

b) 未经确认的修改：对操作系统、应用程序、配置、连接和设备进行升级、修改或其他改变，可以给工业自动化和控制系统或对应的生产过程带来没有预料到的安全威胁。

用“威胁代理”来描述代表威胁的实体，也就是通常所说的对手或攻击者。威胁代理可以以不同的形式出现，例如包括：

c) 内部人员：内部人员是指可以信任的人、雇员、合同承包商或那些掌握了公众所不了解的信息的供应商。即使不是有意进行破坏，内部人员也可以产生威胁。例如，内部人员旁路掉安全控制手段进行工作的结果可能就会产生威胁。

d) 外部人员：外部人员是指不为内部访问所信任的个人或团体，它们可能为目标组织所知，也可能不为其所知。外部人员在某个时间也许曾经是内部人员，也许不是。

e) 自然灾害：自然事件包括风暴、地震、洪水以及龙卷风，这些通常被认为是物理威胁。

威胁付诸行动就变成攻击(有时叫入侵)。无论设计部件和系统，或在某地或某组织内部实施安全计划，都可以模拟攻击，以便采取适当的对抗措施来识别并检测攻击。例如，可以采用案例建模和攻击树的方法。

威胁可能是被动的或主动的。下面条款将分别进行描述。

5.6.5.2 被动威胁

被动信息的收集能为潜在入侵者提供有价值的信息。威胁代理经常通过与雇员、合同承包商随意的语言交流来收集被动信息。当然，设施内部或外部的人员也可以通过视觉观察来收集被动信息。被动信息收集可以包括倒班数据、设备运行数据、后勤供给、巡逻计划以及其他脆弱性。被动信息收集可能难以被探测到，特别是当信息从不同的信息源被零星收集的情况下。保持对好奇人员、摄影师以及一些经常在它们责任区域外活动的人的持续观察可以帮助组织判断出正在遭受被动信息收集，特别是在

与精确背景调查信息结合时。

侦听是一种被动威胁的例子。它是监视通信流中数据的行为。搭线窃听、截取信息流中的数据是最为常见的侦听方法。侦听可能很复杂。侦听各种通信网络的数据的工具随处可见。虽然这些设备通常被用于配置管理、网络故障诊断以及分析数据通信量,但它们也可以用于收集任何发生在跨网络数据交换的特定数据。例如,包侦听和密码侦听过程中,攻击者通过远程交换机或计算机潜伏在网络上。侦听工具被动监视通过网络发送的信息,并将泄密的信息送到磁盘上,这些信息随后可以被下载并用来分析,从而获得用户的身份和密码。

5.6.5.3 主动威胁

5.6.5.3.1 概述

主动威胁可以以各种形式出现,分别在下面段落中描述。

5.6.5.3.2 通信

通信攻击意图是中断工业自动化和控制系统的通信。通信攻击可以通过各种方式进行。通信攻击可以发生在系统内各个层次上,从计算机处理器往上各层,以及从企业外部,以“拒绝服务”方式对通信系统进行攻击。

5.6.5.3.3 数据库注入

注入是攻击基于数据库的网站的一种形式,在该网站上攻击者通过在与因特网相连的系统上,利用不安全代码、旁路防火墙执行未经授权的命令。注入攻击用于从数据库窃取通常无法获得的信息,和/或通过载有数据库的计算机获得对组织机构的主机访问。

5.6.5.3.4 重放

信号可以从控制系统通信路径上被截获,且稍后进行重放,以提供对安全系统的访问或伪造工业自动化和控制系统的数据。潜在入侵者可以重放访问控制信号、生物信号以及其他系统信号,从而获得对安全区域或系统的非法访问,隐藏非法活动或提供虚假干扰信息。一个系统可以联合多条路径进行数据采集、信号传输和控制,防止从一个地方收集对各个子系统、部件、应用或数据库的重放信息。

5.6.5.3.5 欺骗与假冒

在网络连接中,这些词汇用来形容硬件和软件可能被愚弄的各种方法。黑客可以伪造一个电子邮件的标题,使其看起来像来自某地、某人的信息,而实际这不是它的真正来源。例如,IP 欺骗,使得一个信息看似来自授权的 IP 地址。

5.6.5.3.6 社会工程

威胁代理还企图通过哄骗个人出示安全信息来获取其他数据。社会工程之所以成功是因为它的受害者本能地希望相信其他人或自然地希望可以帮助别人。这些社会工程的受害者被哄骗释放信息,而他们自己没有意识到这些信息可以用来攻击计算机网络。

5.6.5.3.7 网络钓鱼

网络钓鱼是安全攻击的一种,通过发一个伪造邮件引诱网站上的接收者,邮件看上去有合法来源,从而引诱受害者出示信息。网络钓鱼依赖于社会工程,即人们趋向于相信一个品牌的安全性,总是将他

与品牌的信任度相关联。

5.6.5.3.8 恶意代码

恶意代码的目的是可以收集系统或用户信息，破坏系统数据，为进一步入侵系统提供立足点，伪造系统数据和报告，或给系统运行和维修人员带来长期困扰。恶意代码攻击可以采取病毒、蠕虫、自动利用代码(automated exploit code)或木马的形式。

病毒是一个程序或插入另一个程序的一小段代码，它们在用户不知晓的情况下被下装到计算机中，并违背用户的意愿而运行。病毒还能自我复制。所有计算机病毒都是人为制造的。一个简单的病毒可以一遍一遍地自我复制，产生相对容易。即使一个简单的病毒也是危险的，因为病毒会很快占用所有可用的存储空间，并将导致整个系统停止工作。更为危险的病毒可以旁路掉安全系统，自己在网络上传播。

自动利用代码被植入系统来收集信息，或当特定事件或业务发生时通知某人或其他系统。一个相对简单的自开发代码可以收集信息以便用于将来入侵、财务开发(financial exploitation)或统计目的(营销)。自动利用代码能利用其他资源或系统中已有的应用来强化收集信息和破坏数据的能力。一个全自动利用代码一般称为蠕虫病毒。蠕虫病毒是一个独立的程序或算法，它可以在计算机网络上自我复制并进行恶意攻击，例如耗尽计算机资源，也可能导致系统瘫痪。

木马是伪装成良性应用的破坏性程序。与病毒不同，木马不自我复制，但它们具有破坏性。一种最险恶的木马病毒是一个声称可以摆脱病毒的程序，而实际上反过来它是将病毒带入计算机。

恶意代码能够以僵尸网络形式传播，收集所泄密的在通用命令和控制设施的机器运行程序。僵尸网络制造者可以远程控制一组设备，通常带有恶意的目的。

5.6.5.3.9 拒绝服务

拒绝(或降级)服务攻击影响网络、操作系统或应用资源的可用性。基于网络的拒绝服务最常见的形式是分布式拒绝服务(DDoS)的攻击，这种攻击通过杠杆作用可以危及多个设备，从而对网络、设备或应用造成重大损失。

5.6.5.3.10 权限提升

为提升对系统的有效攻击，威胁代理首先获得访问权限是必需的。伴随着权限的提升，攻击者可以采取一些本来能够被防御的攻击行动。

5.6.5.3.11 物理破坏

物理破坏攻击的目的是破坏或使物理部件(即硬件、软件存储设备、连接设备、传感器和控制器)失效，这些是工业自动化和控制系统的组成部分。这些攻击表现形式可以是对部件的物理攻击，或通过计算机使得系统执行某个行动，从而导致部件的物理损坏、破坏或功能丧失。

5.6.6 对抗措施

对抗措施是要采取的行动或预案，目的是将风险降低到可接受的水平或满足安全策略。它们一般不能消除风险。要采取的对抗措施的特性取决于要应对的威胁的特性。

有几种可能的措施应对外部威胁，例如：

a) 用户和/或计算机鉴别；

b) 访问控制；

c) 入侵检测；

d) 加密；

e) 数字签名；

f) 资源隔离和分离；

g) 恶意软件的扫描；

h) 系统活动的监视；

i) 物理安全。

一旦发生内部威胁，可能需要采取不同的对抗措施，因为攻击者可能有能力旁路诸如访问控制等常规措施。这种情况下有必要将重心放在写入策略、职责分离、行为监视、系统审计和加密措施等对抗措施上。

被动威胁，例如侦听，很难被检测，因为侦听工具只是读取所连接媒介上传输的信息，并不在信号路径上产生信号。硬连接侦听通过先进通信控制设备可以被检测，例如智能数据网络交换机，但无线侦听，即使用非常精良和昂贵的无线远程通信技术也几乎无法被检测到。可以通过控制和关闭电厂无用的声音和数据端口，以及提供智能通信控制设备，降低侦听访问的发生。

5.7 安全程序成熟度

5.7.1 概述

受到日益增长的计算机安全风险的驱使，很多组织采取了积极的方法来解决针对他们的 IT 系统和网络的安全风险。它们开始意识到网络安全问题的解决是一个连续的过程，而不是一个具有显著的起点和终点的项目。

历史上提供和支持商业信息系统和工业自动化和控制系统的组织一直运行在两个相互排斥的领域。它们都不能理解对方的需求和专业技术。当它们将普通的 IT 安全实践在工业自动化和控制系统上实施的时候产生了大量的问题。

在某些情况下，安全实践对立于将生产连续性和安全性最大化的普通的功能安全实践。因为目前工业自动化和控制系统中采用了大量的开放信息技术，所以需要额外的知识来安全地运用这些技术。IT 和制造、生产性组织宜协同工作并把它们的知识和技能共同应用于解决安全问题。在具有很高潜在健康、安全以及环境事故的行业，将过程安全管理(PSM)和物理安全人员相结合是很重要的。

一个成熟的安全程序的目标是集成计算机安全的所有方面，包括桌面和商业计算系统以及工业自动化和控制系统。图 4 显示了很多业务所面临的集成过程。很多组织对它们的商业计算机系统有很具体的和完整的计算机安全程序，但是并没有完全针对 IACS 开发出网络安全管理实践。

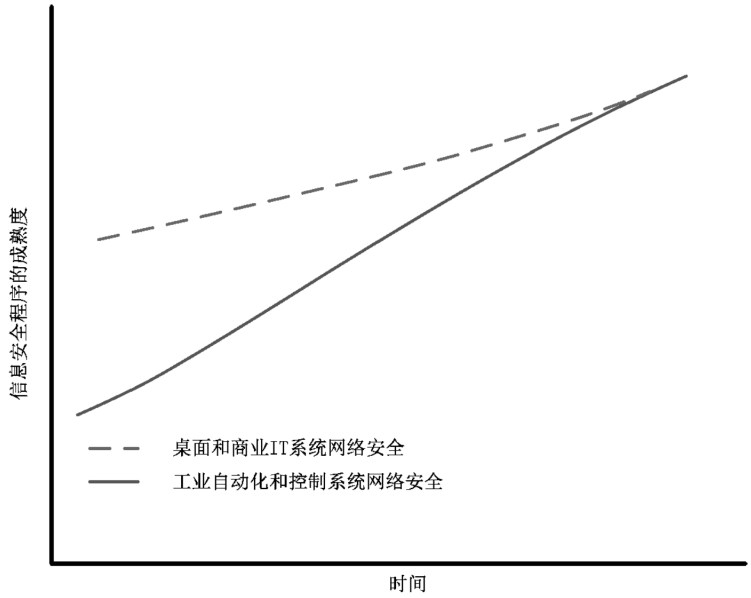

图 4　商业 IT 和 IACS 网络安全集成

一个常见的错误就是把解决计算机安全当作一个有起始和结束日期的项目。在这种情况下，安全性水平经常随着时间推移而下降，如图 5 所示。当新的威胁和脆弱性随着技术的改变而产生的时候，网络安全风险总是在改变。需要一个新的方式来维持安全并且把风险控制在一个可接受的水平。

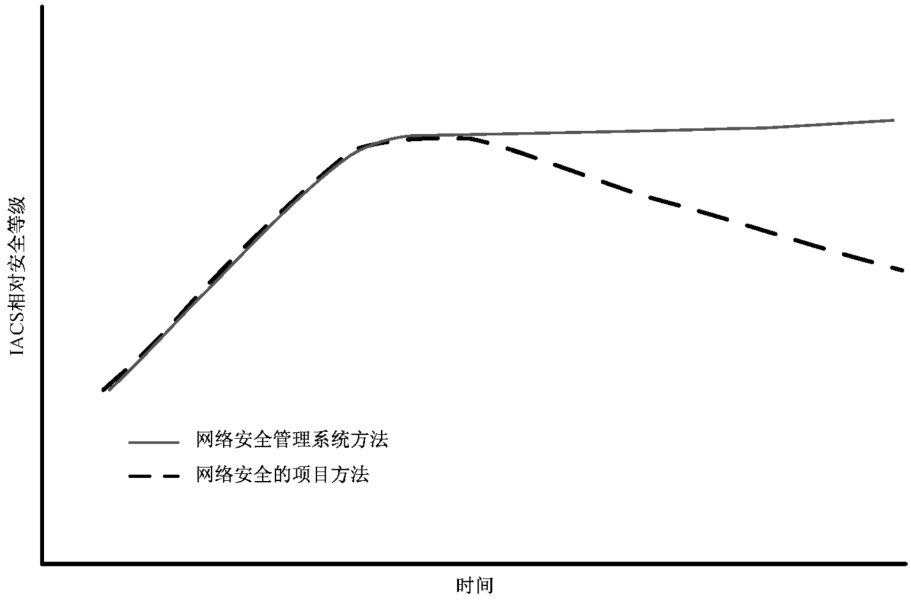

图 5　网络安全等级随时间的变化

建议开发并且实现整个组织范围内的网络安全管理系统，包括采取纠正措施防止随着时间推移安全等级下降的趋势以及评估风险的程序元素。IEC 62443-2-1 中详细描述了网络安全管理系统的关键元素。

每个组织实施网络安全管理系统的过程由于组织目标和对风险的容忍程度而不同。将网络安全集成到组织的文档实践是一种文化的改变，需要花费时间和资源。如图 6 所示，它不能一步实现。它是一

个为达到网络安全性的循序渐进的标准化过程。要实施的安全实践需要跟风险水平相称，在不同的组织中也是不一样的，甚至在基于全局目标和需求的同一个组织内部不同的实践之间也是不一样的。在一个组织中为每个级别的系统制定的策略和规程也可以是不同的，因为风险水平和安全要求也可能是不同的。一个网络安全管理系统要建立包容这些区别的总体程序。

对于成功解决以上提及的 IACS 的网络安全风险，关键是教育和提高认识，有以下几点可供选择：

a) 培训 IACS 的职员以理解当前的信息技术和网络安全问题；

b) 教育 IT 职员以理解 IACS 技术以及过程安全管理规程和方法；

c) 开发(安全)实践以综合所有组织的协同应对网络安全问题的技能。

为成功实施网络安全程序，需要适当结合风险缓解项目和网络安全管理系统(CSMS)程序开发两方面的人员。为达到所需的集成的成熟的网络安全程序状态，来自多组人员的技能和理解的典型范围见图 6。

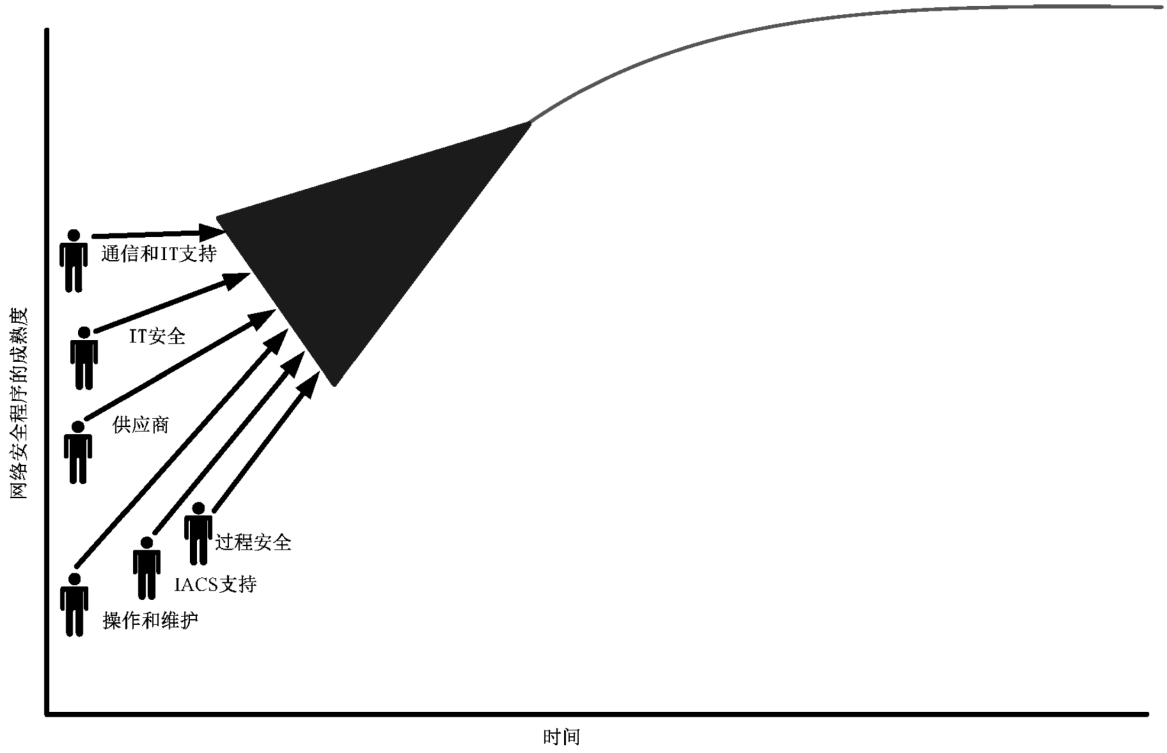

图 6 用于 CSMS 开发的综合资源

5.7.2 成熟度阶段

可以用包含若干个阶段的生命周期来描述一个网络安全程序的相对成熟度。每个阶段包含一个或者多个步骤。

工业自动化和控制系统的分区或控制系统内的控制区域可能处于不同成熟度阶段。这种情况出于以下原因：预算限制、脆弱性以及威胁评估、基于风险分析结果的计划、自动化升级、拆除或者更换计划、出售设施或者业务的一部分或者有其他资源可用于将安全系统升级到更成熟的阶段。

通过按照表 2 中的阶段和步骤对工业自动化和控制系统部分中取得的进展进行评估，组织可以获得对安全成熟度更详细的评估。

表 2　安全成熟度阶段

阶段	步骤
概念	识别 概念
功能分析	定义
实施	功能设计 详细设计 建设
运行	运行
	符合性监视
回收和处置	处置 拆解

表 3～表 7 描述了成熟度生命周期中的阶段和步骤。

表 3　概念阶段

步骤	描述
识别	识别需要保护的财产、资产、服务以及员工。 开始开发安全程序
概念	继续开发安全程序。 对资产服务以及需要某种程度保护的职员进行建档。 把针对企业的潜在的内部、外部威胁进行建档。 建立安全任务、愿景和价值。 为工业自动化和控制系统、设备、信息系统以及职员开发安全策略

表 4　功能分析阶段

步骤	描述
定义	继续开发安全程序。 为工业自动化和控制系统、设备、生产系统、信息系统和职员建立安全功能需求。 针对潜在危险清单对设施和相关服务执行脆弱性评估。 发现和确定工业自动化和控制系统的法律要求。 执行针对潜在脆弱性和威胁的风险分析。 将风险、对企业的潜在影响和潜在的缓解方法进行归类。 将安全工作划分到可控的任务和模块，以便进行功能设计的开发。 为工业自动化和控制系统的安全部分建立网络功能定义

表 5　实施阶段

步骤	描述
功能设计	在本阶段完成安全程序的开发。 定义企业范围、装置范围和控制区域的安全需求。定义潜在的活动和事件并建档，执行功能需求和实施计划以实现安全的企业。 定义功能性安全组织和结构。 定义实施计划中需要的功能。 定义和发布安全区域、边界和访问控制门户。 完成和发布安全策略及规程
详细设计	定义物理和逻辑系统以执行此前定义的功能化的安全需求。 实施培训程序。 完成实施计划的开发。 启动资产管理和变更管理程序。 为被保护区域设计边界和访问控制门户
构建	执行实施计划。 为完成被保护区域以及在企业内的边界，安装物理的安全设备、逻辑应用、配置和员工规程。 激活和维护访问控制门户的属性。 培训程序完成。 资产管理和变更管理程序起作用，并开始运行。 安全安全系统完成交接，并准备由运行和维护人员接收

表 6　运行阶段

步骤	描述
运行	安全设备、服务、应用和配置都已完成，并由运行人员和维护人员接收。 员工已培训，并就安全事项继续培训。 维护人员监视企业、装置或者控制区域部分的安全性，并保持运行正常。 资产管理和变更管理处于运行和维护状态
符合性监视	内部审计。 风险审核。 外部审计

表 7　回收和处置阶段

步骤	描述
处置	淘汰的安全系统被正确地拆解和处置。 为保护区域更新或重建安全边界。 访问控制门户被生成，重新定义，重新配置或者关闭。 向员工通报关于安全系统及事项的变更及其对相关系统的影响
拆解	知识产权被适当地收集、建档并安全地保存或者销毁。 访问控制门户以及相关链接被关闭。 向员工通报安全系统及事项的拆解及其对剩余安全系统的影响

5.8 策略

5.8.1 概述

安全策略使得组织能够为了维持可接受的安全水平而遵循一致的程序。策略被定义在企业中的不同层级，从建立在企业层级的治理或管理策略到定义安全管理细节的操作策略。最特定等级的策略是安全审计能够检验其符合性的组织文档。

所谓安全策略是指定或规定组织如何保护其敏感、关键系统资源的规则。策略无歧义地指明什么是强制性的。因为策略是强制性和无歧义的，因此可以审计。组织的安全策略也将法律法规以及合同义务考虑在内。它们是审计检测该组织实际业务的标尺。

补充策略的是规程。安全规程详细定义了提供某种安全机制的必要步骤。因为它们的详细程度，规程是应用于一个特定事项。它们属于特定技术。策略引用了这些规程并强制它们的使用。

和策略及规程相对的是导则。导则不是强制性的。它们是描述做某些事情的一种方法，这些事情是想做的但不是强制性的。因为导则不是强制的并且可能是含糊的，所以不能审计实践是否遵从导则。导则在一些时候是由没有权威去要求其被遵守的团体所撰写的。导则不适于描述那些应被强制的实践。

因为每个组织不同部分的策略和规程经常是不同的，所以它们之间的充分协调是很重要的。尤其是工业自动化和控制系统的安全策略宜与通用 IT 安全的类似策略相互协调。如果各方之间有很好的工作关系，并且良好协同的策略集合能够支持这种关系，安全程序将能更好地发挥作用。

各种策略和规程结构上的一致性将增加整体的策略和规程集合的协调性。每个策略和规程文档都有一个简短但是对其目的精确的说明。它也有一个定义文档适用范围的说明。以及对它想要降低的风险、文档的关键原则的描述。这些公共的条目通过提供关于策略或规程的意图的信息来引导读者。它们还通过描述文档的意图在文档被修订时提供有益的指南。

系统生命周期的不同阶段不同安全策略问题的行规。安全策略和规程可只针对某个生命周期阶段。某些策略和规程可规定它们只和某个阶段有关。关注所有不同阶段以及特定阶段的所有策略和规程都放在安全策略和规程的集合中。

安全策略和规程包含组织如何测量符合程度以及如何更新策略的使用说明。组织经常在执行或者评估审计的时候意识到需要更新策略。审计可以发现策略和规程中的模糊之处，以及部分策略和规程没有清晰地定义所需的过程和结果。审计能指出对抗措施和规程所需的增补。审计还可以指出需要重新被评估、调整或者可能剔除的需求。

策略和规程宜允许不可预见的环境导致其无法被遵守。策略还宜指出如何将对抗策略和规程的例外进行文档化和批准。对批准的例外进行文档化使得安全状态变得清晰，而不是在策略和规程中保留模糊和不精确。

此外，组织宜在策略中明确哪些是要求，哪些是选择性建议。精确地使用以下助动词将去除模糊性，如“应(shall)”“宜(should)”“可以(may)”以及“是(is)”。策略声明可以在其介绍章节对这些词进行定义以实现更高的精确性。“应”用于要求；“宜”用于推荐；“可以”用于选择性的建议，它可以适用于针对一个要求所提供的选择性。词组“在可能时(when possible)”或者“除非必要(unless necessary)”将引起歧义，除非声明中还描述了如何判断这些情况是否“可能”或者“必要”。

策略和规程标识出人员职责。过程-控制员工是否应对控制网络负责，是否应对控制网络和企业网络之间的一个非军事化区(DMZ)负责？如果企业信息系统部门负责需要过程-控制员工完成特定操作的条件，那么需要描述这些操作。

那些刚刚开始创建其安全程序的组织，策略和规程是一个很好的起点。开始的时候，它们可以涵盖

该组织在近期能够处理的安全实践集合。随着时间的推移和组织能力的提高,可以修订和强化策略和规程。它们可以被落实到位,而不用等待购买和安装系统及设备。

5.8.2 企业级策略

企业级策略对安全程序授权并且设定其方向。它指明了组织总体的安全目标。

最高管理者的策略声明宜足够周到,在组织结构变化、系统和安全技术变化以及威胁种类变化中,都保持恰当和精确。策略因此可以是稳定的,只有当组织在安全上的基本定位发生改变时,才需要重写。然而,策略声明还应是无歧义的,它清晰地指出其要求。

企业级策略指明责任区域,并且为这些区域分配责任。策略可定义 IT 部门和装置运行之间的关系,并指明它们不同的责任。策略可区分控制系统和企业网络不同的安全目标。例如,保持保密性可以是企业网络安全的最高级别的考量,然而保持连续运行可以是控制系统的最高级别的考量。

此外,策略指明适用于组织的特定标准和法规。它可以指明培训是安全程序中的一个重要组成部分。策略还可以指明策略违规的后果。

管理活动宜将策略贯彻到整个组织,使得所有员工都理解。

5.8.3 操作性策略和规程

操作性策略和规程是在组织的较低层级上建立的,用于规定企业级策略是如何在一套特定情况下实施。安全规程将策略付诸实施。它们定义了组织如何实现目标以及如何满足策略的要求。规程建立起解决策略所关注的过程。

规程针对一个安全程序所需的所有组成部分,包括:

a) 系统设计;
b) 采购;
c) 安装;
d) 过程操作;
e) 系统维护;
f) 人员;
g) 审计;
h) 培训。

规程指明特定的活动,谁负责活动的绩效以及什么时候执行这些活动。

书面的规程描述了当情况发生变化时变更它们(指规程)的过程。每个策略或规程有一个明确的所有者,它负责识别何时需要更新并且负责保证更新的完成。

宜测量策略和规程的有效性,以检查它们是否适用于它们期望的目的。宜测量组织产生的费用,以利于组织判断风险的降低和实施策略的费用之间是否平衡。如果此平衡是不可接受的,策略和规程将不得不调整。规程还需更新以反映技术的变化。

规程能够支持审计。安全审计对观察到的组织行动与书面规程进行比较。

5.8.4 策略和规程涵盖的主题

5.8.4.1 概述

策略和规程可以涵盖若干个主题。每个组织都是不一样的,宜确定适用于它的工业自动化和控制系统的适当的策略和规程。可能的主题包括以下条款。

5.8.4.2 风险管理

要开发一个高性价比的安全程序，提供一个统一、适当的安全层，而不需要过于昂贵的超出足够安全范围的设备或者规程，风险管理是十分重要的。不过风险管理是复杂的，而且需要针对组织进行裁剪。基于风险管理的策略定义了如何确定一个可以接受的风险等级以及如何控制风险。该等级根据特定组织环境和目标的不同而不同。确定风险等级的过程宜周期性地重复进行，以适应环境的改变。

5.8.4.3 访问管理

系统安全性的提高可以通过把访问权限限定给那些需要且可信的用户。访问管理策略辨别用户的不同角色，以及每个角色访问不同类别（物理的或逻辑的）资产的权限。它规定了保护资产职员的责任，以及维护访问管理规程管理者的责任。这些访问特权的授权宜由管理层批准并详细文档化，而且周期性地进行审查。出于保护数据保密性的需要，访问管理与系统完整性和可用性相比一样重要，甚至更加重要。

5.8.4.4 可用性和连续性的规划

这一领域中的策略为备份和恢复提供了必要的框架和期望的需求，以及业务连续性和灾难恢复的规划。它们还定义了存档特性（例如数据需要被保留多久）。

5.8.4.5 物理安全

控制系统的安全取决于包含控制系统的空间物理安全。工厂的场地可能在为控制系统编写安全策略之前就有一个物理安全策略。然而，与系统物理访问有关的策略与那些涉及非系统资产的策略可以不同。例如，所有炼油厂的员工几乎可以对装置栅栏内的所有设施具有通用访问权，但是对 IT 机房的访问仅限于 IT 相关的人员——就是为了防止意外的损坏。控制系统安全策略宜包含对物理安全策略的引用，并声明其相关性。控制系统的安全策略宜包含足够的物理安全性的规定，使得场地中的任何特定应用对于控制系统而言是物理安全的。例如，一个策略可以声明“某些设备应被锁在柜子里，并且钥匙应保存在一个受限的地方”。

5.8.4.6 体系结构

策略和规程描述控制系统的安全配置，包括以下事项：

a) 推荐的网络设计；
b) 推荐的防火墙配置；
c) 用户授权和鉴别；
d) 不同过程控制系统之间的相互连接；
e) 无线通信的使用；
f) 域和信任关系；
g) 补丁管理（包括鉴别）；
h) 防病毒管理；
i) 就以下方面完成系统加固：关闭软件端口，禁用或者避免未使用的或者危险的服务，禁用移动存储设备；
j) 对外部网络的访问（如因特网）；
k) email 的恰当使用。

5.8.4.7 便携式设备

便携式设备构成固定设备所有的安全风险，但是由于它们的可移动性使得它们不容易被常用从安装到审计的安全规程所涵盖。它们的移动性使得当它们离开物理安全区域的时候更容易发生(数据)损坏，当它们连接到安全区域的时候更容易发生信息拦截。因此经常需要一个特殊的策略涵盖便携式设备。该策略宜要求和固定设备一样的安全保护，但是提供这样保护的技术和管理机制可以不同。

5.8.4.8 无线设备和传感器

取代有线使用射频传输的控制设备已经在某些控制系统应用中使用很多年。当成本下降以及新标准出现时，一部分缘于安装成本的降低，在自动化和控制系统中的潜在应用进一步扩大。有线和无线设备的关键区别在于后者的信号在物理安全边界内不受局限，使得它们更容易受到拦截和损坏。因此一个专门针对无线设备的策略适用于在业务中正在使用或者将来可能采用无线设备或传感器的组织。该策略可以规定何种应用可以使用无线设备，要求何种保护和管理机制，以及有线和无线网络如何互联。

5.8.4.9 远程访问

远程访问绕过了系统边界的本地物理安全控制。它将对信任区域的访问扩展到一个完全不同的地理位置，包括一台可能没有经过物理上位于信任区域的计算机的安全检查的计算机。宜采取不同的安全机制，以提供和信任区域一样等级的安全性。

5.8.4.10 人员

人员事项一般在企业人事和IT安全策略中定义。控制系统安全策略提供具体细节，而更通用的策略并不包含在控制系统方面。例如控制系统安全策略将协调带有人员筛查和监视实践的控制系统的访问角色。

5.8.4.11 分包商策略

安全事项包括涉及分包商的工作，它们的角色例如供应商、集成商、维护服务提供方或者咨询方。一个涵盖分包商的安全策略针对的是和那些可能带来脆弱性的分包商的相互作用。该策略指明各方的责任，它解决随着项目阶段的进展，随着材料和系统的交付而变化的责任。该策略可要求特定的条款写入与分包商的合同。

对合同程序员如果没有适当的管理，应用的完整性会受到损害，或者程序代码可能无法维护。发现非常合格的合同程序员是很重要的，它们遵守组织的编程和文档标准，执行充分的测试，同时还值得信赖和守时。

5.8.4.12 审计

系统的安全性要定期审计，以测量与安全策略和实践的符合度。安全策略针对审计的需求并规定职责、周期以及纠正措施的要求。综合的审计规程不仅针对安全性，还针对诸如过程的效率和效能以及合规等其他方面。

5.8.4.13 安全策略的更新

要监视安全策略以确定策略自身是否需要修改。监视安全策略是每个安全策略和规程文档的一部分，并且企业的安全策略要规定整体的方法。每个操作性策略和规程文档都包含一个声明，指出何时以及由何人来审查和更新该策略。

培训程序宜适用于新雇员、操作、维护、升级和后续计划。培训程序宜很好地文档化、结构化并且定期更新,以适应操作环境的变化。

5.9 安全区

5.9.1 概述

每种情况都有不同的可接受安全性等级。对于大的或复杂的系统,对所有组成部分都采取同样等级的安全性是不实际的或不必要的。使用安全区或受保护区域的概念来说明不同。安全区是具用相同安全需求的物理、信息、应用资产的逻辑编组。这一概念适用于一部分系统包含在安全区而其他的都处于安全区域之外的电子环境。区之中还可以有区或者子区,这可以提供分层的安全性,提供纵深防御并且解决多层次安全性需求。纵深防御可以通过对安全区分配不同的属性完成。

一个安全区有一个边界,介于被包含的和被排斥的元素之间。区的概念还隐含着从区内和区外对资产访问的需求。这定义了必要的访问和通信,允许信息和人员在安全区内和区间的移动。区可以被认为是被信任的或不被信任的。

安全区能以物理概念(物理区)或者逻辑方式(虚拟区)定义。物理区的定义通过物理位置把资产分组。这种类型的区容易确定哪个资产在区内。虚拟区的定义是通过将资产或部分物理资产编组进安全区来实现,这个组合或者基于功能性,或者基于其他特性而不是资产的实际位置。

5.9.2 确定需求

5.9.2.1 总则

当定义安全区的时候,一个组织宜首先评估安全需求(安全目标),然后确定一个特定资产宜在区内还是在区外。安全需求可以分为以下类型。

5.9.2.2 通信的访问

对于在安全边界内有价值的一组资产,它们需要被链接到安全区外的资产。这个访问可以有多种形式,包括资产(产品)和人员(雇员或厂商)的物理移动,或与安全区外实体的电子通信。

远程通信是与相互不靠近的实体之间的信息的传送。为实现这一技术规范的目的,远程访问被定义为与所针对的安全区边界之外的资产进行通信。

本地访问通常被认为是在单个安全区内的资产之间的通信。

5.9.2.3 物理访问和接近

物理安全区被用于限制对一个特定区域的访问,因为在那个区域内的所有系统都要求它们的操作员、维护人员和开发人员有同样的信任级别。这并不排除一个更高级别的物理安全区嵌入在一个较低级别的物理安全区内,或者一个更高级别的通信访问区嵌入在一个较低级别的物理安全区内。对于物理区,锁门或者其他物理手段能够防止非授权的访问。边界就是墙或者柜子,用于对访问进行约束。物理区宜具有与其期望的安全等级相称的物理边界,并且和其他资产安全性规划相一致。

物理安全区的一个例子是一个典型的制造工厂。被授权的人员由一个授权机构(安全警卫或者ID)允许进入工厂,而未被授权的人员由同样的机构或者栅栏限制进入。

安全边界之内的资产需要被保护以达到一个给定的安全等级或策略。边界内所有的设备宜采用相同的最小的安全性需求等级。换句话说,它们宜被保护,以符合相同的安全策略。保护机制可因被保护的资产而不同。

根据定义,安全区之外的资产在一个不同的或者更低的安全等级。它们不以相同的安全等级被保

护，并且不以相同的安全等级或策略被信任。

5.10 管道

5.10.1 概述

信息需要在安全区内流入与流出。甚至在非网络化系统中，也会存在一些通信（如：为创建和维持系统，可编程设备的间断连接等）。为涵盖通信的安全方面以及提供包括通信特殊要求的结构，本标准定义了专门的安全区：通信管道。

管道是一种特殊类型的安全区，成组信息按逻辑被编成信息组在区内或在区外流动。它可能是单个服务（即单一以太网）或由多个数据载体组成（多根网络电缆和直接的物理存取通路）。与区一样，它由物理的与逻辑的两种结构组成。管道可连接区内的实体，或连接不同区的实体。

与区相同，管道可以是可信的或不可信的。典型的可信管道是不越过区边界，在区内通过通信处理。越过区边界的可信管道需要使用端到端的安全处理。

不可信管道是与区端点不具有相同安全等级的管道。在这种情形下，实际的通信安全由单个通道负责，如图 7 所示。

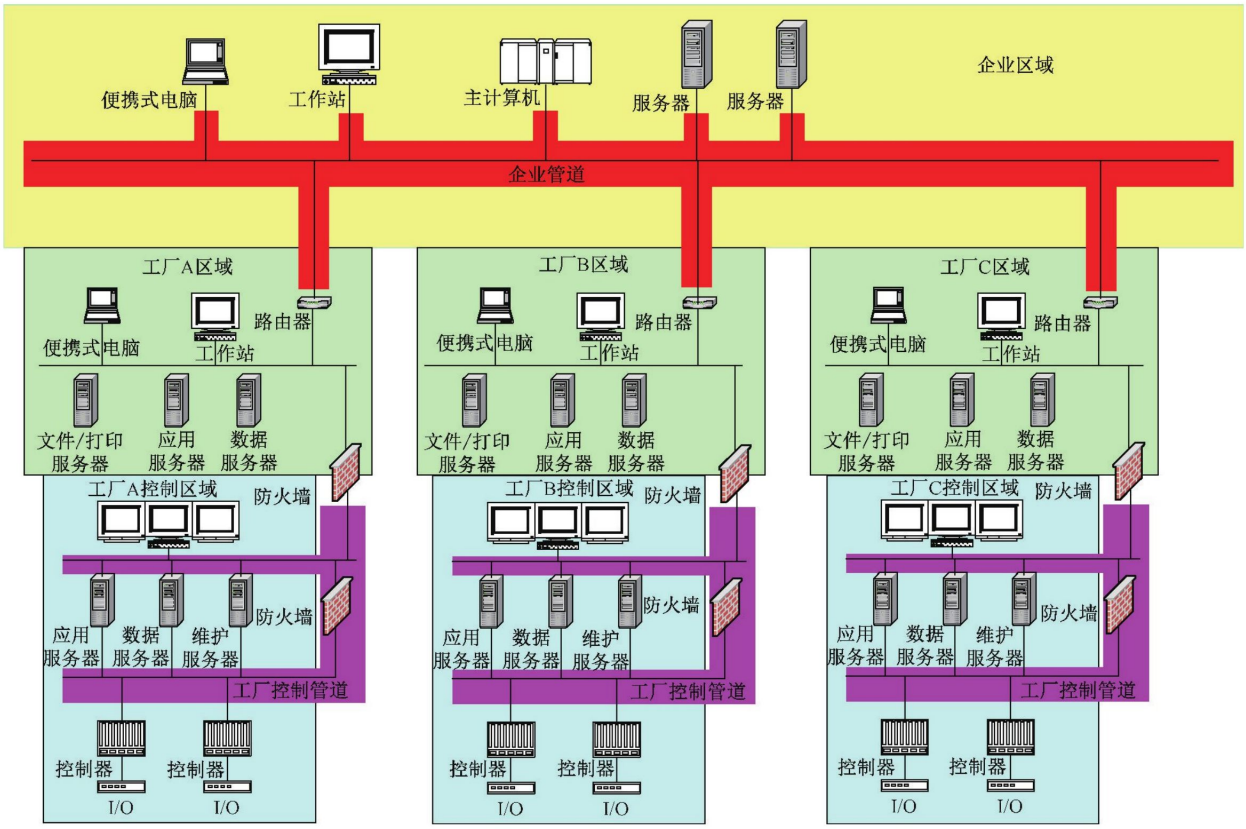

图 7 管道示例

含有三个厂区的企业见图 7，每个厂区有自己的总部。三个厂区都连接至企业网络中，以便与厂区总部以及其他厂区进行通信。图中定义了四个可能的管道（也有其他的定义方式，为简洁起见在此忽略）。第一种管道企业管道位于图中的顶部。它将不同位置的多个厂区连接到企业数据中心。如果采用租用通信或专用通信来构建广域网（WAN），则认为是可信管道。假如同时采用公用网络和专用网络，则被视为不可信管道。管道包括组成厂区连接的所有通信设备和防火墙。

图 7 中在每个厂区表示了第二种管道的例子，每个厂区有各自的可信管道进行控制通信。

5.10.2 通道

通道是建立在通信管道内的特定通信连接，它们继承了用作通信媒体的管道的安全属性(即安全管道内的通道将保持安全管道的安全等级)。通道有可信的或不可信的。

可信通道是允许与其他安全区进行安全通信的通信连接。可信通道能用于将虚拟安全区扩展到包含物理安全区之外的实体。

不可信通道是与被研究的安全区不在同一个安全等级的通信路径。在接收信息前，到参考区(该区定义为不安全通信)的通信和从参考区来的通信都需要验证。

5.11 安全等级

5.11.1 概述

安全等级概念是以区为基础，而不是基于单个设备或系统来思考安全问题。通常 IACS 由多个厂家的设备与系统组成，所有功能协调一起为工业操作提供集成自动化功能。正如单个设备的功能能力有助于 IACS 的能力一样，单个设备的安全能力和实施对抗策略需要相互作用来达到该区所期望的安全等级。安全等级为使用具有不同固有安全能力的对抗措施及设备做决策时，提供了一个参考框架。

安全等级为区安全提供了定性的方法。作为一种定性方法，安全等级定义适用于比较和管理组织内的区安全。因更多的数据变成可提供，和对危险、威胁和安全事件的精确应答能力的发展，该概念为选择和验证安全等级提供了定性的方法。它既适用于最终用户也适用于 IACS 和安全产品的供应商。在区内，它被用来选择 IACS 设备和使用的对抗措施，在整个工业环节中，它被用于识别和比较不同组织的区的安全。

采用安全等级方法的组织宜定义每个等级表示的内容，以及在区中如何测量安全等级。整个组织宜始终使用该定义或特性。安全等级用于识别区内综合性分层纵深防御策略，该策略包括硬件、基于软件的技术对抗措施以及管理类对抗措施。

基于对管道或区的风险评估，安全等级宜与区或管道的系统、设备的固有安全属性和对抗措施所要求的效果一致。安全等级方法提供了对区或管道进行风险分类的能力，也有助于定义在区或管道内用于阻止未授权的电子入侵，防止未授权读出，或影响设备和系统正常功能的对抗措施宜实现的效果。安全等级是区和管道的属性，而不是设备、系统或系统中任何部分的属性。

推荐最少使用三个安全等级。三个等级的定性描述见表 8。组织为描述其特定的安全需求，可在此基础上扩展和定义额外的安全等级。

表 8 安全等级

安全等级	定性描述
1	低
2	中
3	高

5.11.2 安全等级类型

5.11.2.1 概述

安全等级可以被定义为以下三种不同的类型：

a) SL(目标):区或管道的目标安全等级;
b) SL(达到的):区或管道已实现的安全等级;
c) SL(能力):与区或管道相关的对抗措施的安全等级能力,或区或管道内的设备或系统固有的安全等级能力。

5.11.2.2 SL(目标)——目标安全等级

SL(目标)宜分配给一个区,也可以分配给一个管道。区和管道的 SL(目标)在风险评估时确定。只要使用该管道的区在风险评估中考虑了该管道相关的安全属性,则没必要再给该管道分配目标安全等级。风险评价宜考虑相关区或管道的安全被损害的可能性和结果。风险评估可以是定性的、半定量的或定量的。SL(目标)确定用于防止区或管道内安全被损害的对抗措施、设备和系统宜实现的效果。

对抗措施可以是:

a) 技术性对抗措施(防火墙、防病毒软件等);
b) 管理性对抗措施(策略和规程);
c) 物理性对抗措施(锁门等)。

影响区和管道 SL(目标)确定的因素有:

d) 已定义区边界和管道的网络结构;
e) 将与被考虑区域进行通信的区域的 SL(目标);
f) 用于区通信的管道的 SL(目标),如果已分配;
g) 对区内设备和系统的物理访问。

区域内,计算 SL(目标)宜基于安全层及它们对整体的影响。

5.11.2.3 SL(达到的)——达到的安全等级

区或管道的 SL(达到的)取决于区或管道内设备和系统的固有安全属性和/或用于防止区或管道的安全被损害的对抗措施的属性。SL(达到的)是时间的函数,由于对抗措施的降级、新的脆弱性、已调整的危险或攻击方法、安全层的破坏、设备和系统的固有安全属性,SL(达到的)会随时间降低,直到以上内容被审查、更新或升级。

目的是确保在任何时候区或管道的 SL(达到的)大于或等于该区或管道的 SL(目标)。

5.11.2.4 SL(能力)——对抗措施、设备或系统的安全等级能力

SL(能力)用于定义区或管道内与区或管道的安全相关的对抗措施及设备和系统的固有安全属性。它是对抗措施、设备或系统涉及的安全属性效果的度量。

对抗措施、设备或系统涉及的安全属性的示例如下:

a) 证明对等实体的真实性;
b) 保护消息的真实性和完整性;
c) 保护消息/信息/通信的保密性;
d) 确保问责制(不可否认性);
e) 强制访问控制策略;
f) 防止拒绝服务攻击;
g) 维护平台信任度;
h) 检测篡改;
i) 监视安全状态。

区或管道内对抗措施、设备或系统的SL(能力)有助于达到基于该区或管道内对抗措施、设备或系统所涉及的相关安全属性的SL(达到的)。

5.11.3 区或管道中影响到SL(达到的)的因素

5.11.3.1 概述

区或管道的SL(达到的)取决于几个因素。区或管道的SL(达到的)可以用这些因素的函数表示：

$$SL(达到的) = f(x_1, \cdots, x_n, t) \quad \cdots\cdots(1)$$

式中：

x_i(1≤i≤n)包括但不限于：

x_1：与区或管道相关的对抗措施，以及区或管道内设备和系统的固有安全属性的SL(能力)；

x_2：与之建立通信的区域的SL(达到的)；

x_3：管道类型及用于与其他区域通信的管道相关的安全属性(仅适用于区域)；

x_4：对抗措施的效果；

x_5：区或管道内对抗措施、设备和系统的固有安全属性的审计和测试间隔；

x_6：攻击者可用的专业知识和资源；

x_7：设备和系统的对抗措施和固有安全属性的降级；

x_8：入侵检测；

t：时间。

这些参数在下面的条款中有更详细的描述。

5.11.3.2 对抗措施和固有安全属性的SL(能力)

区或管道内对抗措施、设备和系统涉及的相关安全属性及其效果有助于实现区或管道的SL(达到的)。

对抗措施可以针对多个安全属性，但是如果所有属性都与区或管道的安全无关，那么这些对抗措施则无益于区或管道SL(达到的)的实现。与此类似，如果区或管道内的设备和系统的固有安全属性与区或管道的安全无关，那么它们也无益于区或管道SL(达到的)的实现。

5.11.3.3 建立通信区域的SL(达到的)

区或管道的安全不能孤立考虑。它受与之进行通信的其他区域的SL(达到的)影响。

例如，考虑利用串行链路与DCS通信的化工厂内的SIS。假设DCS和SIS位于两个独立的区域，那么SIS区域的SL(达到的)将受DCS区域的SL(达到的)影响。

5.11.3.4 管道类型及与管道相关的安全属性

管道可以是具有固有安全属性的点对点链路、LAN或WAN。管道可包括增强管道安全属性的对抗措施。有助于管道安全的管道的安全属性也将有助于实现管道的SL(达到的)。一个区用来与其他区通信的管道的安全属性将有助于实现区域的SL(达到的)。

5.11.3.5 对抗措施的效果

使用技术和管理对抗措施能帮助达到区或管道所要求的SL(目标)。

涉及不同安全属性的各种技术对抗措施都可用于工业自动化和控制系统(IACS)的实现。技术对抗措施宜涉及与区域相关的安全属性，但是如果那些安全属性对于该区域没有效果，那么它们对该区域

SL(达到的)的达到帮助很小或者完全没有帮助。技术对抗措施的示例包括入侵检测系统(IDS)、防火墙和防病毒软件。

技术对抗措施效果评价宜考虑以下因素:

a) 开发过程:书面规程和质量管理计划等的可用性。这将有助于减少系统差错,例如可能影响安全的软件缺陷或内存泄露。

b) 测试:对抗措施、设备或系统涉及的每个安全属性的测试等级。测试数据可以从以前被评估的系统中推断得出。

c) 数据采集:由于相似对抗措施、设备或系统中的一个缺陷导致区或管道被损害的次数;对抗措施、设备或系统发现脆弱性的频率和严重性。

当技术对抗措施不可行时宜使用管理对抗措施。管理措施的示例如限制对 IACS 部件的物理访问。

5.11.3.6 对抗措施的审计和测试间隔

基于审计和/或测试至少与区域相关的安全属性的程序规定,宜定期审计和/或测试对抗措施以及设备和系统的固有安全属性的效果。在某些情况下,新脆弱性的发现也可以触发一次审计或测试。

5.11.3.7 攻击者可用的专业知识和资源

攻击者可用的专业知识和资源(包括工具和时间)会影响区或管道的 SL(达到的)。宜假定工业可接受攻击者的能力和工具。攻击者损害区域安全的可用时间取决于区或管道已实现的应用和对抗措施。

5.11.3.8 对抗措施降级

设备和系统的对抗措施和固有安全属性事实上将随时间而降级,从而降低区或管道的 SL(达到的)。设备和系统的对抗措施和固有安全属性的降级由以下因素导致:

a) 新脆弱性的发现;

b) 攻击者技能的提高;

c) 攻击者对现有对抗措施的熟悉;

d) 攻击者可使用更好的资源。

5.11.3.9 入侵检测

设备和系统的对抗措施和固有安全属性可能包括入侵检测。检测到入侵后的可用响应时间会影响区域和管道的 SL(达到的)。

5.11.4 对抗措施和内在安全属性对设备和系统的影响

用于实现 SL(目标)的设备和系统的对抗措施和固有安全属性的使用可能导致通信性能的降级。由于设备和系统的对抗措施和固有安全属性导致的通信性能的降级需要被评价,以确保区域仍能满足最小功能要求。

例如,响应速度对于 IACS 是一个重要要求。对抗措施可能增加通信延迟,这在某些应用中是不能接受的。

5.12 安全等级生命周期

5.12.1 概述

一旦确定了区域边界和管道，安全等级就成了 IACS 区域的安全生命周期的一个重要部分。认识到安全等级生命周期是区域和管道的随着时间推移变化的安全级别是重要的。意识到安全等级生命周期始终关注于区域和管道的安全等级是重要的。它不宜与区域内组成 IACS 的实际物理资产的生命周期阶段混淆。虽然资产生命周期和区域安全等级生命周期间有许多重叠和互补活动，但是它们每个有不同的触发点导致从一个阶段进入另一个阶段。而且，物理资产的改变可能引起一系列安全等级活动或者安全脆弱性的改变，或者一个资产可能触发另一个物理资产的变更。

图 8 描述了安全等级生命周期。在安全生命周期的评估阶段给区域分配 SL(目标)。在实施阶段执行对抗措施以满足区域要求的 SL(目标)。一个区域的 SL(达到的)依赖于多种因素。为了确保区域的 SL(达到的)始终优于或等于 SL(目标)，必要时，在安全生命周期的维护阶段宜审计和/或测试并升级对抗措施。

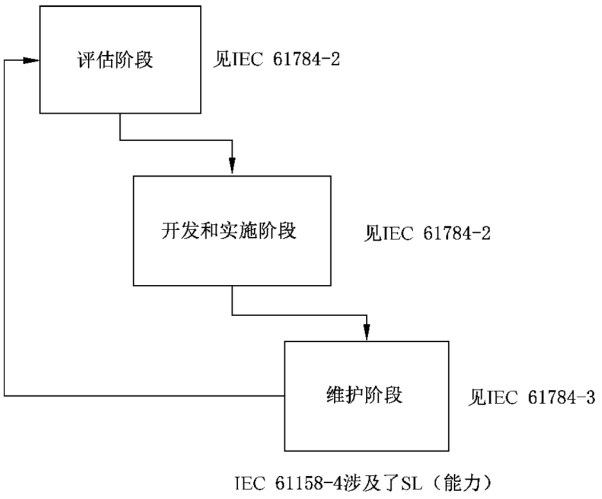

图 8 安全等级生命周期

5.12.2 评估阶段

安全等级生命周期的评估阶段所示的活动见图 9。在给区域分配 SL(目标)前，需建立以下内容：

a) 区域边界；

b) 组织的风险容忍准则。

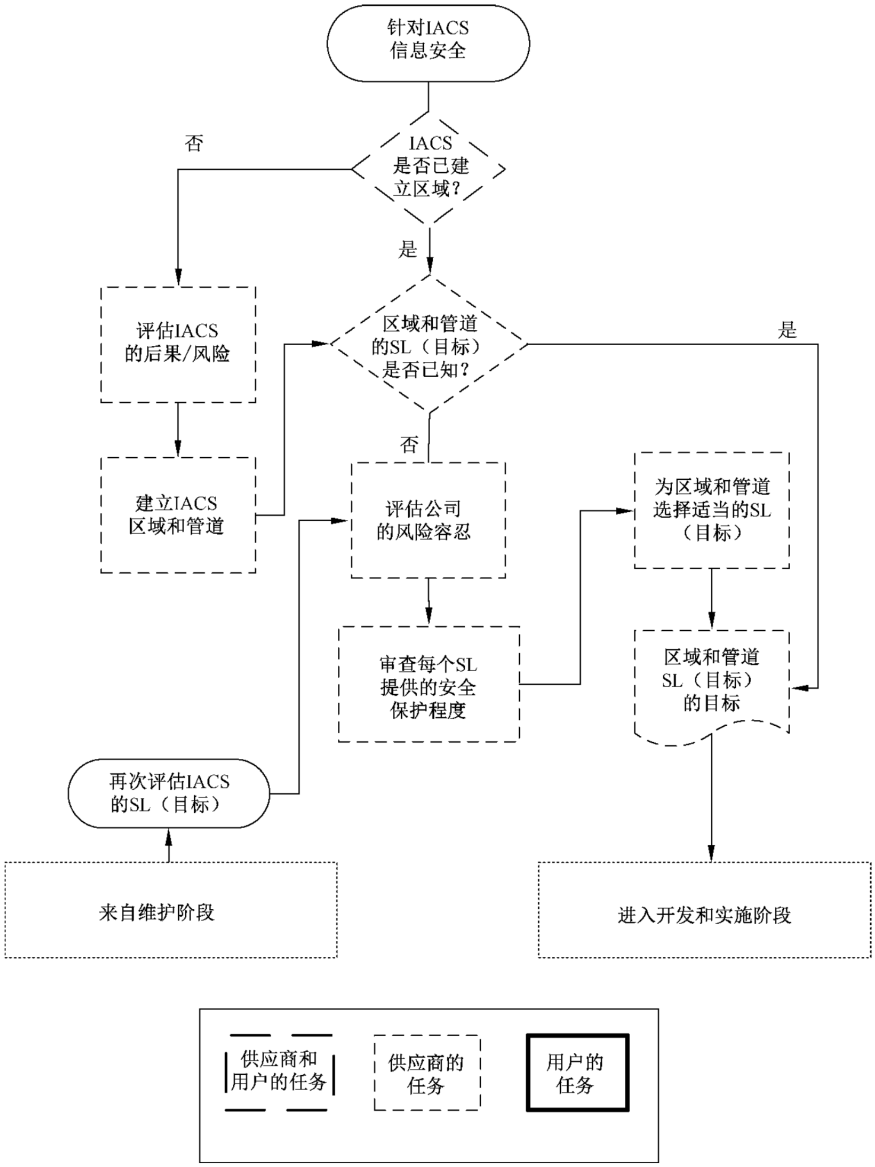

图 9　安全等级生命周期——评估阶段

宜对区域执行风险评估，并给区域分配 SL(目标)。与评估阶段相关的风险评估和其他的相关活动的细节见 IEC 62443 以后的部分。

5.12.3　开发和实施阶段

一旦在评估阶段给区域分配了 SL(目标)，就宜执行对抗措施以实现区域的 SL(达到的)大于或等于 SL(目标)。在安全等级生命周期的实施阶段，有关新建或现有 IACS 区域的所有活动见图 10。在根据区域的安全要求确认系统后，SL(达到的)就已确定。

与实施阶段相关活动的细节见 IEC 62443 以后的部分。

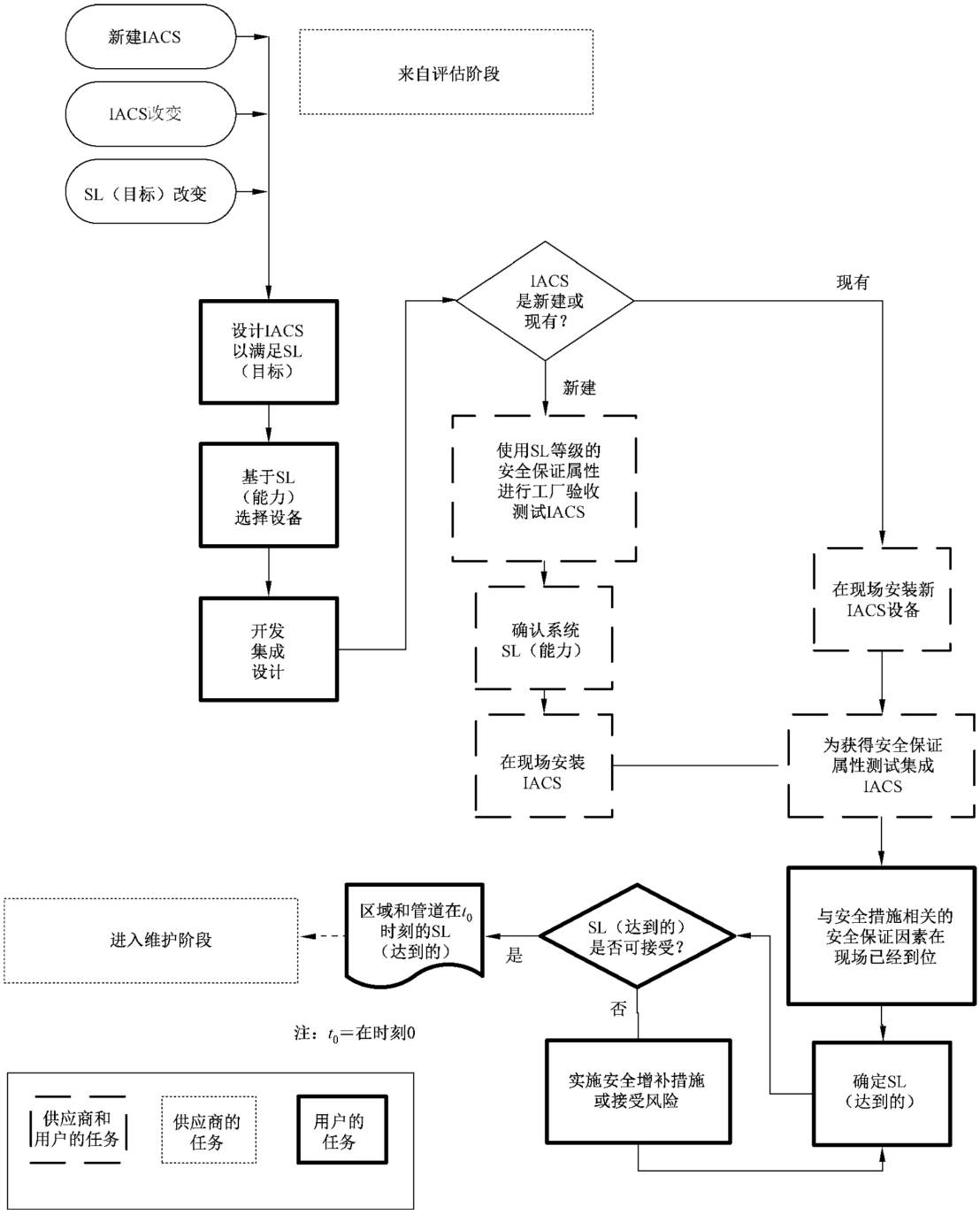

图 10　安全等级生命周期——实施阶段

5.12.4　维护阶段

设备和系统的对抗措施和固有安全属性会随时间而降级。区域(包括与区域相关的管道)的安全属性宜定期或者当发现新脆弱性时进行审计和/或测试,以确保区域的 SL(达到的)始终大于或等于 SL(目标)。与维护区域的 SL(达到的)相关的活动见图 11。

与维护阶段相关活动的细节见 IEC 62443 以后的其他部分。

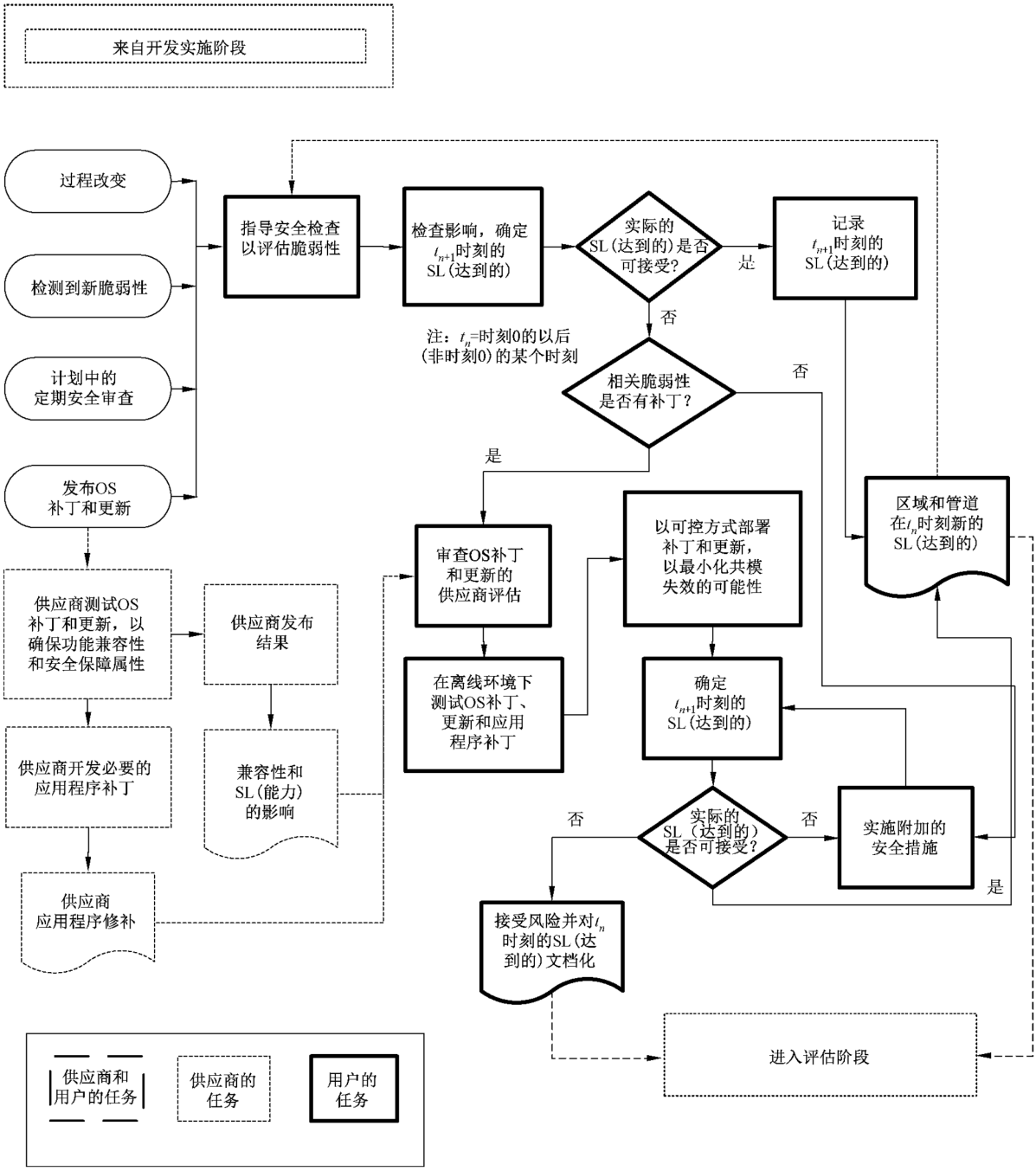

图 11　安全生命周期——维护阶段

6　模型

6.1　概述

本章描述了可用于设计恰当安全程序的一系列模型。其目的是使用通用的框架和词汇，按照处理安全问题所必须的详尽程度来识别环境的安全需求和重要特征。这些模型表示为不同的形式，包括：

a)　参考模型，为所遵从的更详细模型提供总体概念基础。

b) 资产模型，描述 IACS 内资产间的关系。

c) 参考体系结构，描述资产的配置。参考架构对每个企业或企业内的部门都是唯一的。依赖于被审查 IACS 范围，参考架构对每个状况也是唯一的。

d) 区模型，依据已定义特征将参考架构元素进行分组。它为策略、规程和指南的定义提供了环境，并转而应用于资产。

所有这些信息被用于开发管理 IACS 安全的详细程序。

以下将更详细描述每个模型的主要类型。

6.2 参考模型

6.2.1 总则

参考模型为下面更详细信息建立了参考框架。随着开放系统互联(OSI)的 ISO 七层模型的成功，术语“参考模型”被广泛接受。美国国家航空航天局(NASA)NASA 标准和技术办公室(NOST)将其定义为：

“参考模型是理解某些环境实体间重要关系的框架，也是制定支持这些环境的一致性标准或规范的框架。参考模型基于少量的统一概念，可被用于教育和向非专业人士解释标准的基础。”[8]

参考模型描述了一个集成制造或生产系统的通用视图，表示为一系列逻辑层级。本系列标准使用的参考模型，见图 12。该模型来源于 IEC 62264-1 中使用的通用模型。

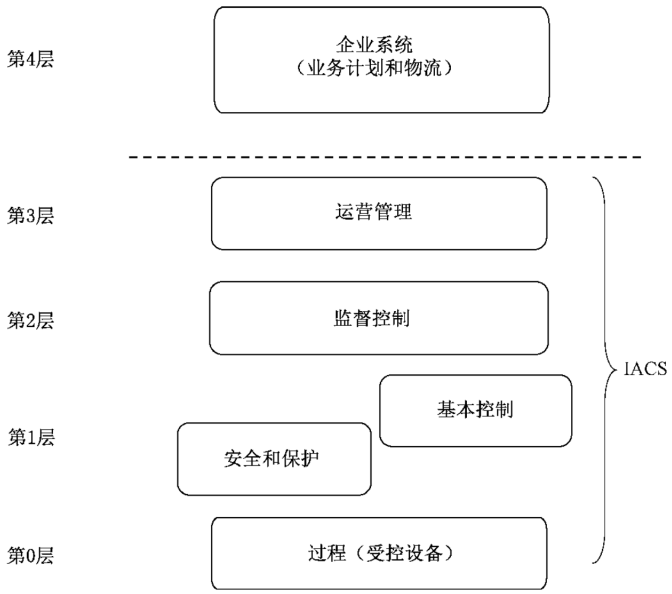

图 12 IEC 62443 使用的参考模型

与参考模型有微小差异的视图可被用于 SCADA 应用。该视图见图 13。

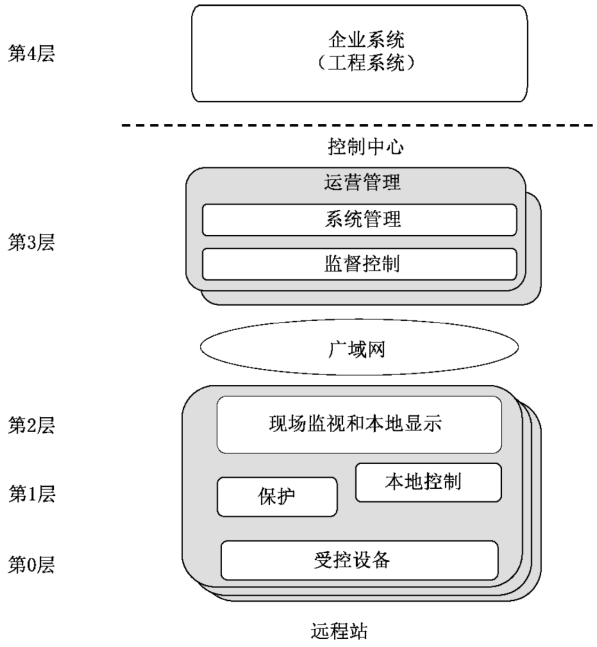

图 13　SCADA 参考模型

6.2.2　参考模型层级

6.2.2.1　概述

这些模型包括相同的基本层级，每种模型表示一种特定的功能类。层级定义基于 IEC 62264-1 中的功能等级模型，并描述了从过程（第 0 层）到企业（第 4 层）的功能和活动。

在下面的条款中，更详细地描述该模型的每个层级。

6.2.2.2　第 4 层——企业系统

本层在 IEC 62264-1 中被描述为业务计划和物流，它定义了包括管理制造组织所需的商业相关活动的功能。功能包括企业或区域财务系统和其他企业架构组件，如用于企业中单个工厂或现场的生产计划、运营管理和维护管理。鉴于本技术规范的目的，本层也考虑工程系统。

第 4 层包括下列活动：

a）　收集和维护原材料、备件的使用和可用库存，为原材料和备件的购买提供数据。

b）　收集和维护全部能源使用和可用库存，为能源采购提供数据。

c）　收集和维护全部在制品和生产库存文件。

d）　收集和维护与客户需求相关的质量控制文件。

e）　收集和维护机械和设备使用、用于预防和预测性维护计划的生命周期历史文件。

f）　收集和维护导入人事部门和会计部门的人力资源使用数据。

g）　建立基本工厂生产计划。

h）　基于可用资源变更，可用能源、电力需求等级和维护要求，变更已接收订单的基本工厂生产计划。

i）　根据基本工厂排产，制定最优预防性维护和设备更新计划。

j) 确定每个库存点的原材料、能源、备件和在制品的最优库存等级。该功能也包括物料需求计划(MRP)和备件采购。

k) 无论何时当大批量生产被中断时,则有必要变更基本工厂生产计划。

l) 基于上述所有活动的能力计划。

6.2.2.3 第3层——运营管理

第3层包括管理生产所要求的最终产品的工作流程的功能。包括:生产调度、详细生产计划、可靠性保证和生产全现场控制优化。

第3层包括下列活动:

a) 报告包括可变制造成本的区域生产;

b) 收集和维护与生产、库存、人力资源、原材料、备件和能源使用相关的区域数据;

c) 执行工程功能所要求的数据采集和离线分析。它可能包括统计质量分析和相关控制功能;

d) 执行所需的人员功能,如:工作周期统计(例如:时间、任务)、休假计划、劳动力计划、发展计划、内部培训和人员资质;

e) 为自身区域建立当前的详细生产计划,包括:维护、运输和其他生产相关需求;

f) 在执行第4层建立的生产计划时,本地优化自身生产区域的成本;

g) 当自身责任区域发生工厂生产中断时,变更生产计划以进行补偿。

6.2.2.4 第2层——监视控制

第2层包括监视和控制物理过程的功能。典型地,工厂中存在多个生产区域,如:精炼厂的蒸馏、转换、配比,或者发电厂汽轮机平台和煤处理设施。

第2层包括下列功能:

a) 操作员人机界面;

b) 操作员报警和警报;

c) 监视控制功能;

d) 过程历史采集。

6.2.2.5 第1层——本地或基本控制

第1层包括感知和操作物理过程的功能。

过程监视设备从传感器读取数据,必要时执行算法,并维护过程历史记录。过程监视系统的例子包括油罐测量系统、连续排放监视、旋转设备监视系统和温度指示系统。过程控制设备与此类似。它从传感器读取数据,执行控制算法,将输出发送到最终元件(例如:控制阀或挡板驱动装置)。第1层控制器直接连接到过程中的传感器和执行器。

第1层包括连续控制、顺序控制、批控制和离散控制。许多现代控制器在单个设备内包含了全部控制类型。

第1层也包括安全和保护系统[1)],它监视过程,并在超出安全限值时将过程自动返回安全状态。它也包括了监视过程,并把即将可能发生的非安全状态向操作员告警的系统。

传统上,安全和保护系统由物理上独立的控制器执行,但是近年来在一个共同架构内使用逻辑独立的方法执行已成为可能。为确保安全功能的完整性,参考模型中的描述强调了这种独立(逻辑的或物理的)的必要性。第1层的设备包括,但不限于下列设备:

1) 这些系统指如IEC 61511系列标准中定义的安全仪表系统。

a) DCS 控制器；

b) PLC；

c) RTU。

安全和保护系统经常包括可能与网络安全要求不一致或不相关的附加功能安全需求。这些系统包括 IEC 61511 中给出的用在化工和石化工厂的安全系统、IEC 61513 中给出的核电厂安全或安全相关系统、IEEE 电力工程协会标准中给出的保护功能。

6.2.2.6 第 0 层——过程

第 0 层是实际物理过程。该过程包括各领域大量不同类型的生产装置，这些领域包括但不限于：离散制造、烃加工、产品配送、制药、纸浆和造纸、电力。

第 0 层包括直接连接到过程和过程设备的传感器和执行机构。

6.3 资产模型

6.3.1 总则

现代控制系统是由复杂的计算机网络和许多执行一系列任务的组件构成的，用以确保化工厂、汽车零部件生产厂、管道、发电设施、输电和配电网以及许多其他类型的工业设施、运输系统、公用设施的安全、高效的运行。

这些系统曾经一度与企业的其他计算机隔离，并且使用专用的硬件、软件和网络协议。这种情况不会再出现了，因为控制系统供应商采用了商业上现成、价格低廉的信息技术，并且由于业务需要，推动了控制系统与业务信息系统的集成。

从安全的角度来看，关注点在于控制设备本身、设备使用者、控制系统组件间的连接，以及业务系统和其他网络间的互连。

本标准针对在多个工业领域广泛应用的工业自动化和控制系统。因此，资产模型要自上而下、通用性好，以能满足不同场景下部署的控制系统。如图 14 所示。

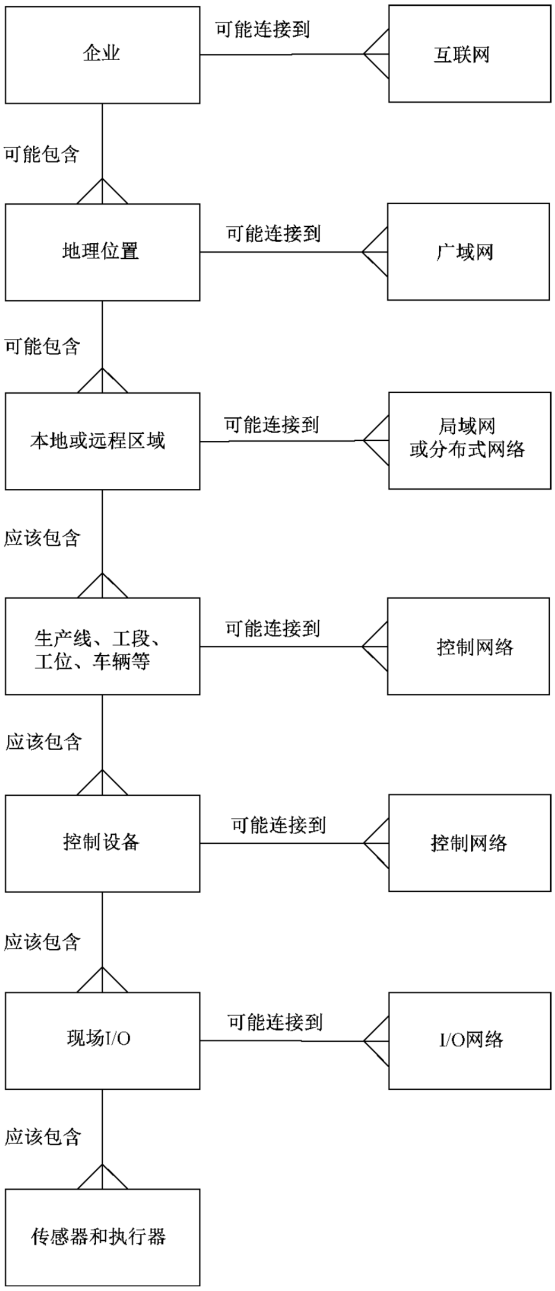

图 14　过程制造资产模型示例(地理场所)

由于网络在安全中起到了重要的作用,资产模型明确地包含了层次结构上位于每个层次的网络元素。在每一层,设备(或设施)由适当类型的网络连接起来。尽管各个网络之间可以互相连接,但该模型没有描述这种连接。

与参考模型一样,SCADA 应用的图示稍有不同。一个典型的 SCADA 资产模型如图 15 所示。

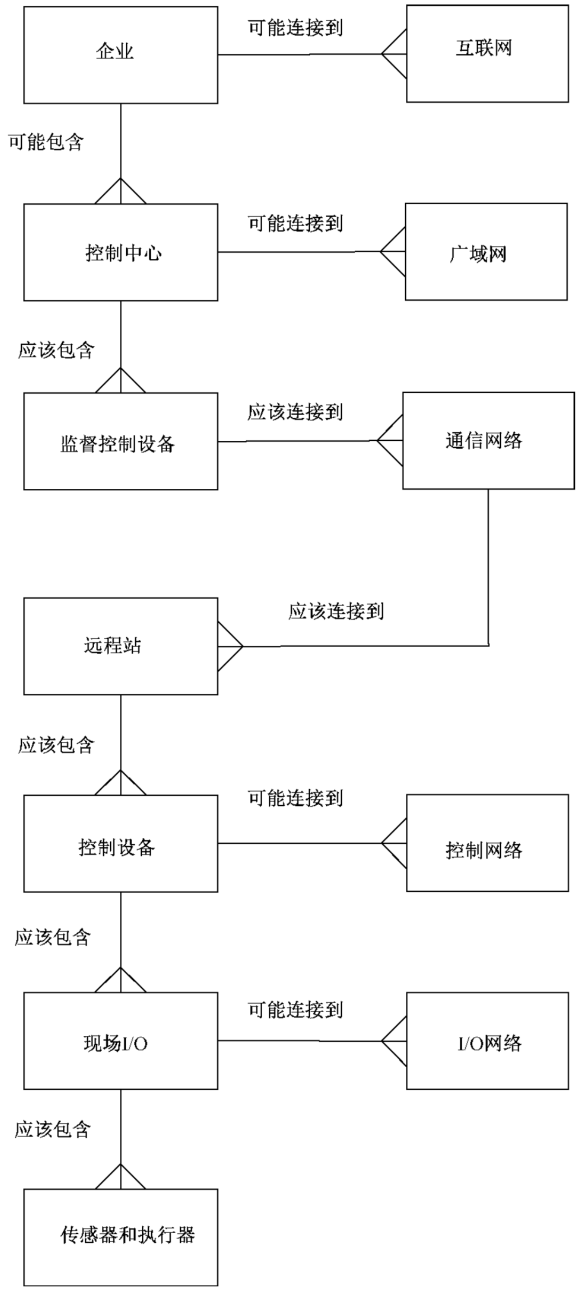

图 15　SCADA 系统资产模型示例

这个资产模型描述了可能出现在各个层次的辅助信息系统。这些系统虽然不直接控制过程，但是它们通过收集数据、发送配方和过程指令来与控制设备交互。工段、区域和站信息系统也可以作为资料库在整个企业范围内为用户提供生产信息，并且可以与运行在企业数据中心的企业资源计划应用交互。

可以根据需要，对这个模型进行裁剪或扩展以反映被审视中的实体，假定它与其他模型和视图是一致的。比如，一个工厂只有一个区域，那么就可以忽略参考体系结构提供的区域分类，后续的区域反映裁剪后的资产模型。

6.3.2　企业

企业是一个商业实体，它能生产和运输产品，或经营和维持基础设施服务。企业通常与因特网相连，以便与其他企业通信或为员工提供信息和服务（如电子邮件）。企业通常运行一个或多个数据中心，

以支持信息处理要求。IT 资产支持的业务过程的安全性超出了本标准的范围。

6.3.3 地理场所

6.3.3.1 概述

场所是企业资产物理、地理或逻辑分组的子集。它可能包含区域、制造生产线、过程工位、过程工段、控制中心和车辆等。场所之间可以通过广域网连接起来。场所可能包括信息系统，比如协调生产活动的制造执行系统。

6.3.3.2 控制中心

控制中心是一种特殊的场所。基础设施工厂通常使用一个或多个控制中心来监督或协调其操作。如果企业有多个控制中心(如一个独立的场所中的备份中心)，它们通常通过广域网连接起来。一个控制中心包含 SCADA 的主机、相关的操作显示设备，以及辅助信息系统(如历史数据库)。

6.3.3.3 远程站

远程站包含的设备有 PLC、远程终端单元(RTU)和智能电子设备(IED)。这些设备负责本地到站的监视和控制操作。远程站通过通信网络(有时指遥测网络)连接到控制中心。远程站也可以相互连接(为了实现某种功能，例如在输电网中变电站间的继电保护)。

6.3.4 区域

区域是场所资产的物理、地理、或逻辑分组的子集。它可能包含制造生产线、过程工位、过程工段。区域之间可以通过场所中的 LAN 连接起来，并可能包含区域内执行操作相关的信息系统。

6.3.5 流水线、工段、工位、车辆

区域由底层设备构成，它们执行制造、基础设施控制、车辆管理等功能。这一层的实体可通过区域控制网络连接起来，并可能包含与实体操作相关的信息系统。

6.3.6 监督控制设备

监督控制设备包括计算机服务器、HMI、局域网和通信设备，它们允许操作者远程管理和控制分散在大范围内的设施。

6.3.7 控制设备

控制设备包括 DCS、PLC、运动控制器、智能驱动器和用来管理和控制过程的操作者接口控制台。它也包括现场总线网络，其控制逻辑和算法运行在协调其行为的智能现场设备上。

6.3.8 现场 I/O 网络

现场 I/O 网络是连接现场设备与控制设备的通信链路(有线或无线)。

6.3.9 传感器和执行器

传感器和执行器是连接过程设备的终端元件。

6.3.10 受控设备

控制系统底层资产是构成受控设备的资产。这个层也被称作物理或运行过程。

6.4 参考体系结构

参考体系结构由资产模型中定义的实体组成。用于审查和分析的每种具体情景都有特定的参考体系结构。根据所执行的业务功能和被审视的功能，每个组织可以创建一个或多个参考体系结构。一个组织拥有覆盖所有操作设施的单一企业参考体系结构是很常见的。每种设施或每类设施可以拥有更具体的参考网络体系结构图，可以在企业模型上扩展。制造功能的简单参考体系结构的例子如图 16 所示。

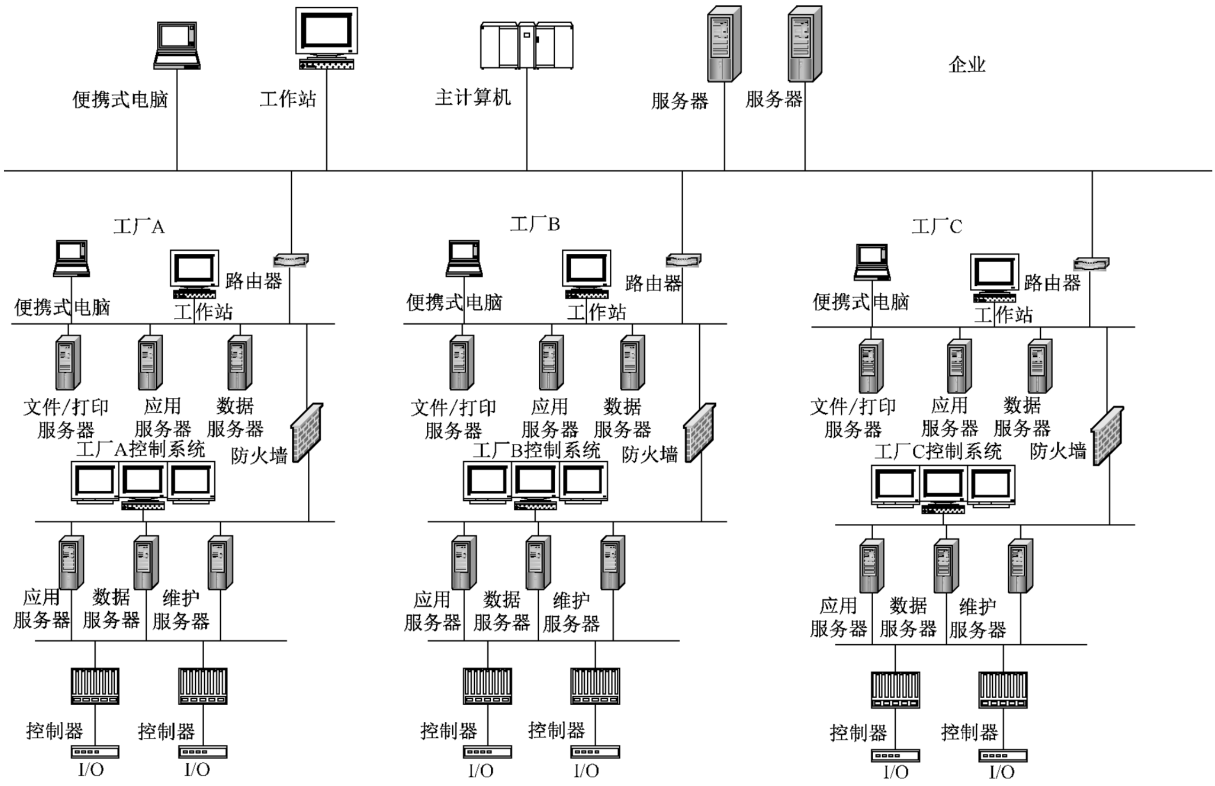

图 16 参考体系结构示例

6.5 区和管道模型

6.5.1 概述

区和管道模型是从参考体系结构发展而来。它用来描述企业内部或企业子集内部资产的逻辑编组。资产可以分组为实体(如业务、设施、场所或 IACS)，该实体可以用于分析安全策略和需求。这个模型可以帮助评估常见的威胁、脆弱性和用来保护分组资产所要达到所需安全等级的相应对抗措施。通过这种形式的资产编组，可以为区域成员的所有资产定义一种安全策略。然而，这种分析可以用于决定基于区域内执行的活动所需的恰当保护。

注：本标准中无限制的术语“区”都假设为安全区。

6.5.2 定义安全区

构建安全程序时，区是促使程序成功的最重要工具之一，且区的恰当定义是过程的最重要方面。定义区时，组织应该利用参考体系结构和资产模型来制定合适的安全区和安全等级来满足工业自动化和

控制系统安全策略所要求的安全目标。

当在一个物理设备内部执行不同级别的活动时，一个组织既可以把物理设备映射到更严格安全要求上，也可以创建一个具有独立区域安全策略的独立区，这个策略是这两个区之间的协调策略。这种情况的一个典型示例出现在过程历史数据服务器中。为了提高效率，服务器需要访问关键控制设备，这些设备是收集数据的数据源。但是，为了满足向监督者和过程优化提供数据的业务需求，需要一种比典型控制系统安全要求所允许的对设备更自由的访问。

如果包含不同安全等级活动的多个应用运行在单一的物理设备上，那么可以创建一个逻辑区域边界。这种情况下，对特定应用的访问被限制为拥有访问相应应用特权的人。一个例子是运行在 OPC 服务器上的单个机器和 OPC 基于客户分析的工具。对 OPC 服务器的访问被限制为拥有更高优先权的人，而使用 OPC 客户端插件对电子表格进行访问则对每个员工都是可以的。

6.5.3 区识别

区可以是独立资产的编组、子区的编组、或独立资产与主区内编组成子区的资产的组合。区具有继承特性，即一个子区（或分区）需要满足父亲区所有的要求。简化的多工厂区模型如图 17 所示。这里，企业区是父区，每个工厂是一个拥有包含在工厂子区内的控制子区的子区或分区。

注：显著优势是将安全区域与设施中的物理区或区匹配，例如控制中心与控制安全区匹配。

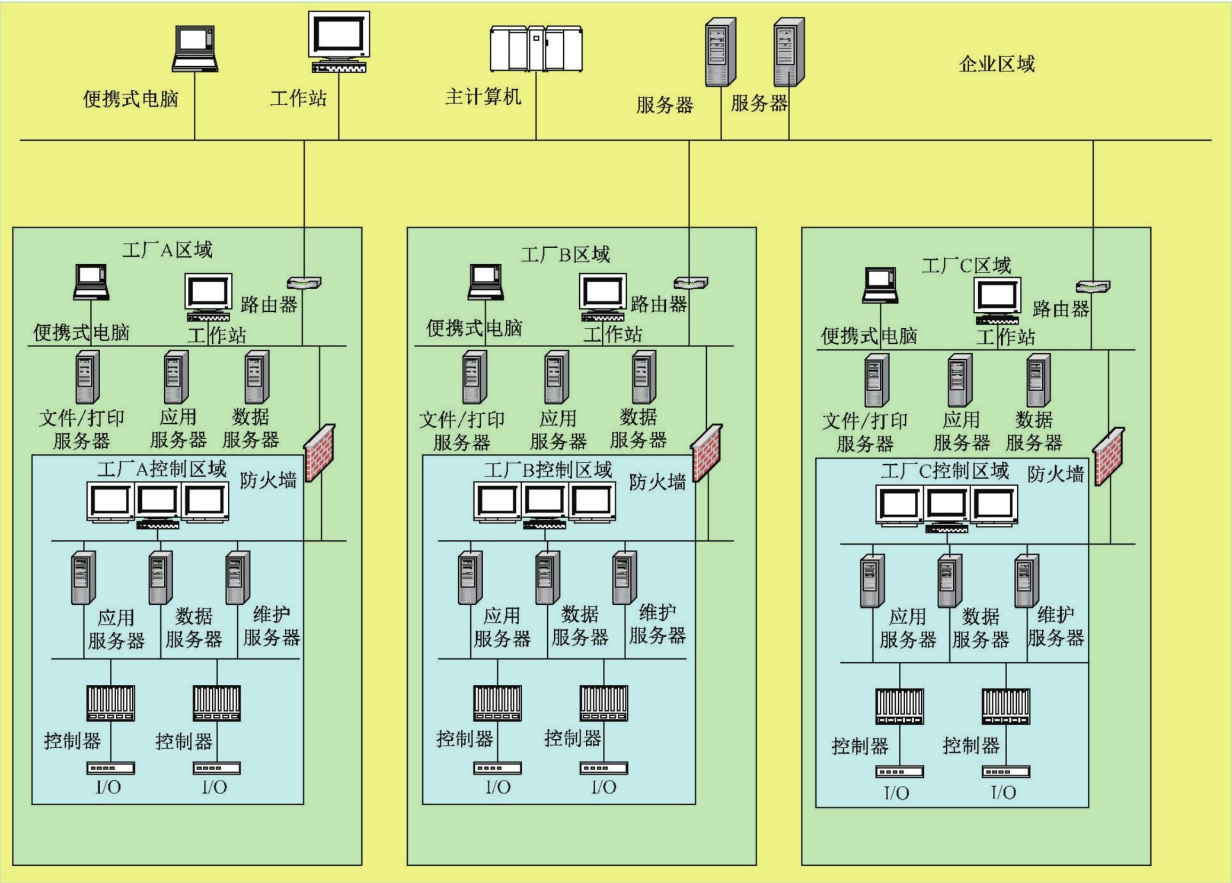

图 17 多工厂区示例

相同的企业体系结构可以被分组成独立的区，如图 18 所示。这种模型中，区策略是相互独立的，每一个区可以有完全不同的安全策略。

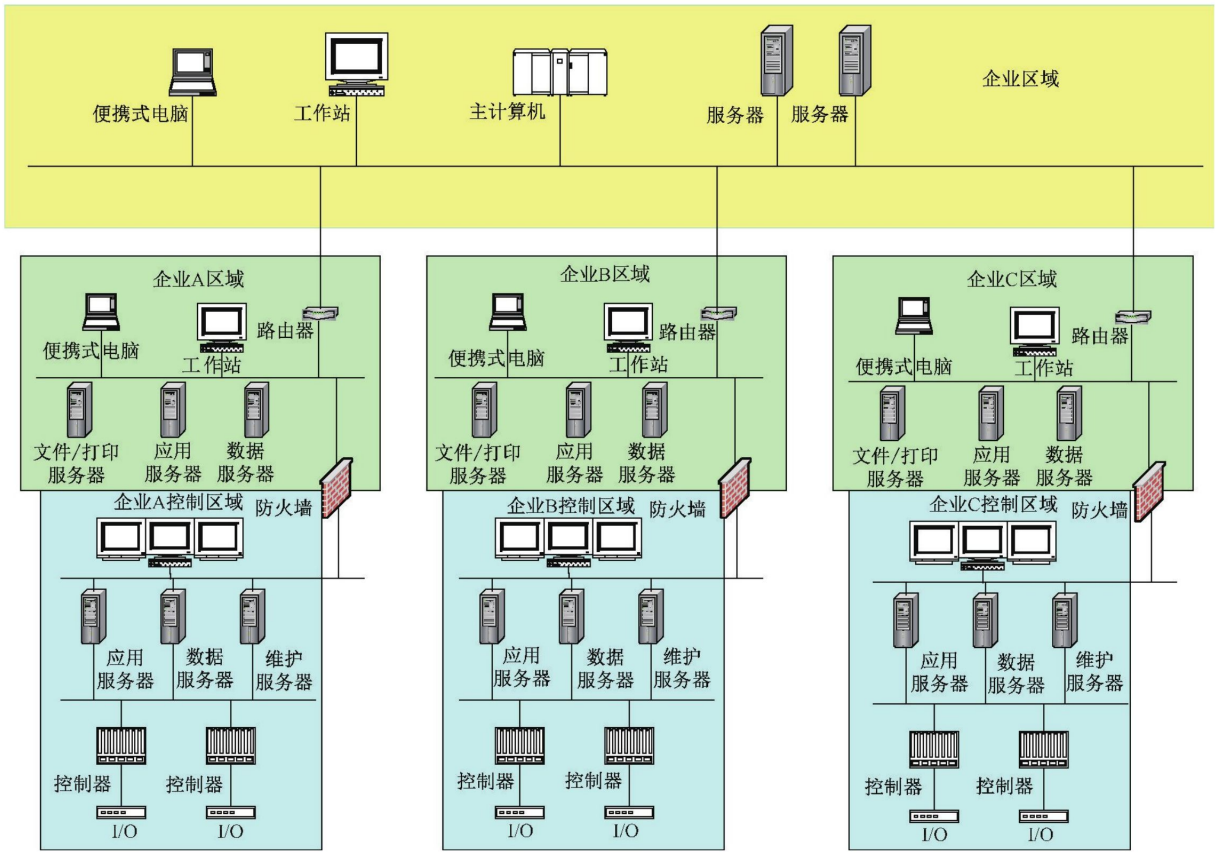

图 18　分离区例子

SCADA 应用可以构建类似的模型，如图 19 和图 20 所示。

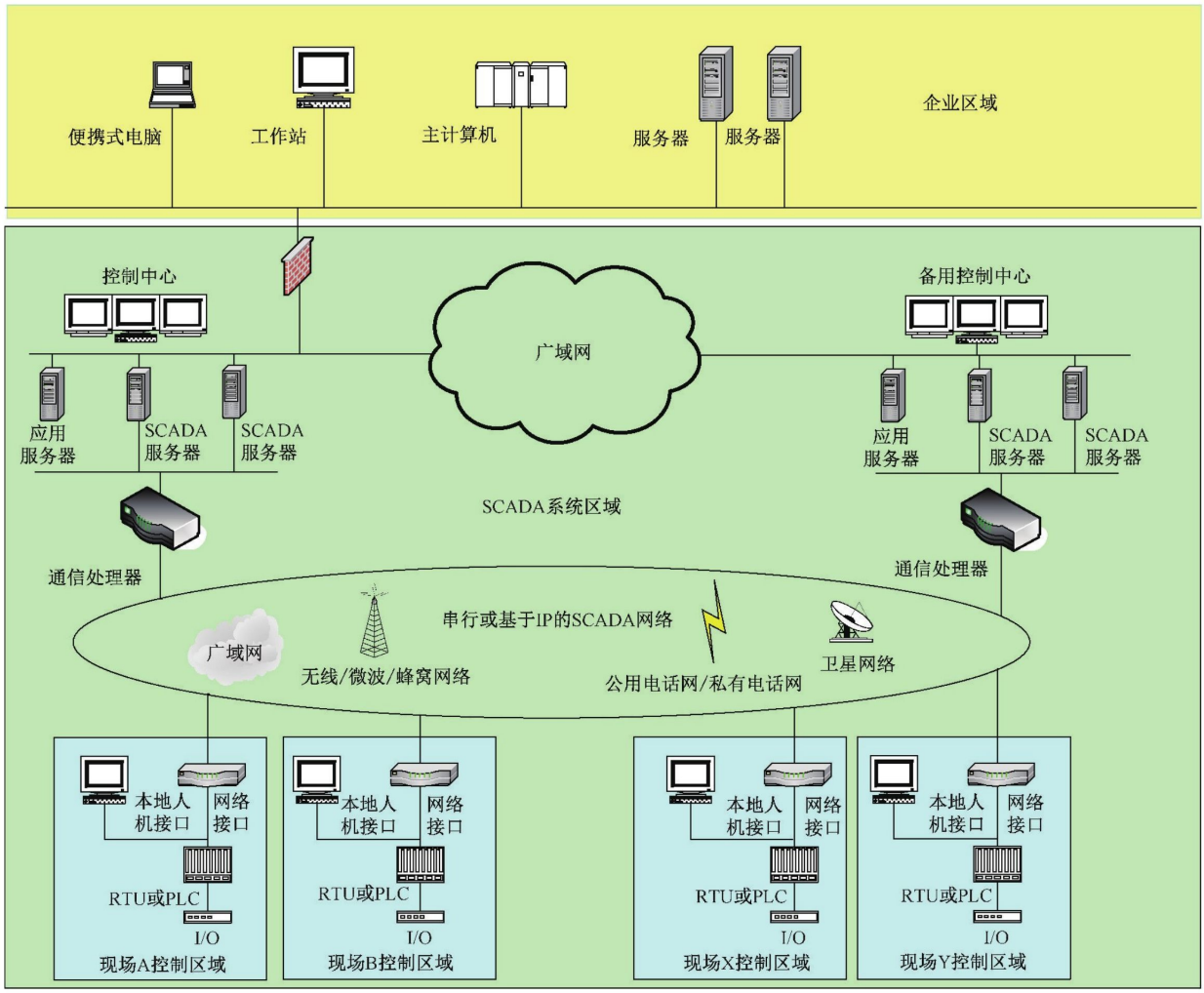

图 19　SCADA 区例子

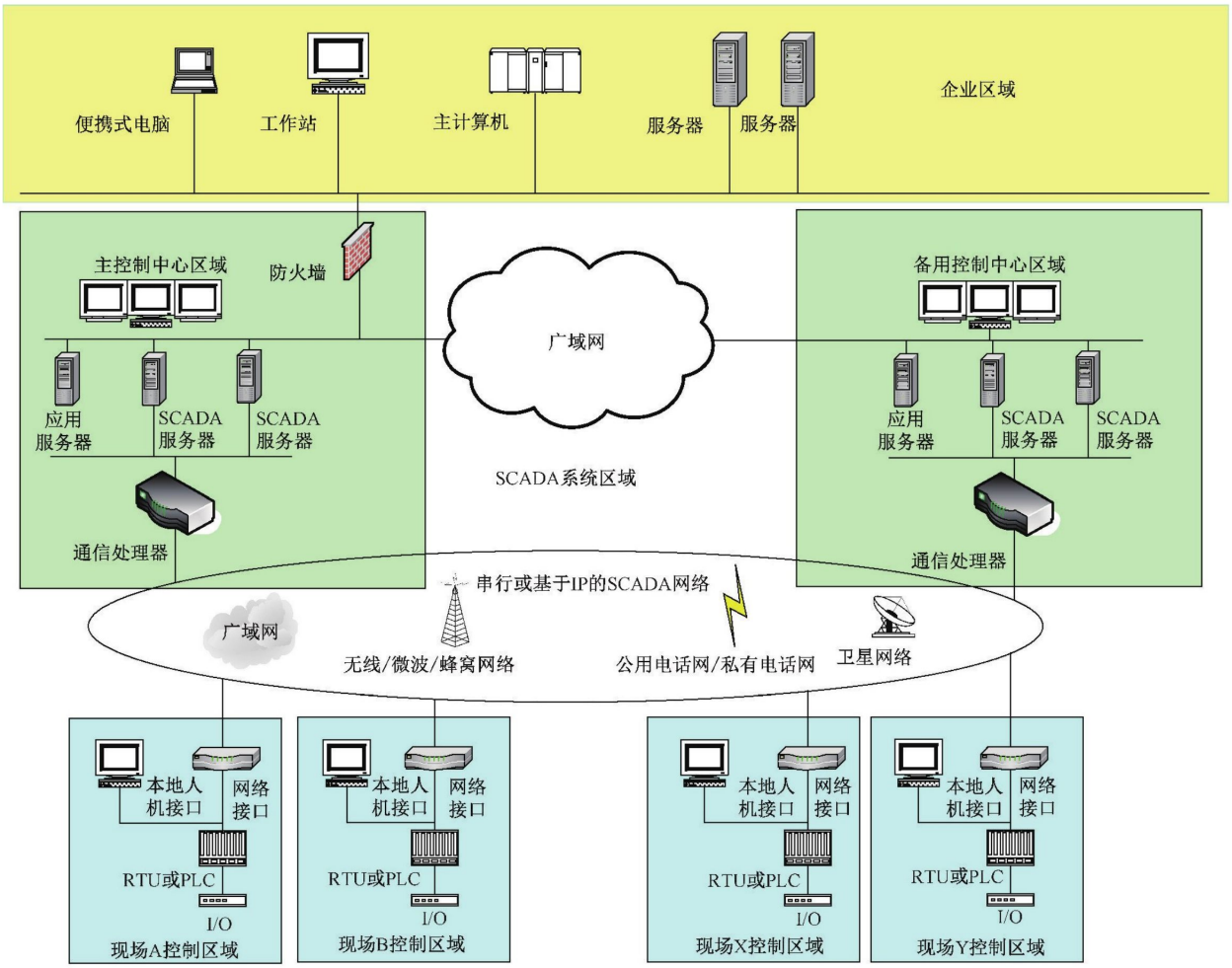

图 20　SCADA 分离区例子

6.5.4　区特征

6.5.4.1　总则

每一个区域有一个特征集和其属性的安全要求。可以表现为以下几种形式的属性：

a）　安全策略；

b）　资产清单；

c）　访问要求和控制；

d）　威胁和脆弱性；

e）　安全违规的后果；

f）　经授权的技术；

g）　变更管理的过程。

下面条款详细描述了这些属性。

6.5.4.2　安全策略

每一个区有一个控制文件，用以描述整体的安全目标及如何确保到达安全等级目标。这包括以下

几部分：

a) 区范围；
b) 区安全等级；
c) 组织结构和职责，用以执行安全策略；
d) 区相关的风险；
e) 满足要求目标的安全策略
f) 实施的安全措施；
g) 区域内所允许的活动类型；
h) 允许访问区的通信类型；
i) 区属性的文件。

上述几点都被文档化，并且融入区的安全策略，用于指导和测量区内所包含资产的构建和维护。

6.5.4.3 资产清单

为了维护区内的安全，一个组织需要维护一张所有资产（物理的和逻辑的）的列表。该列表用于评估风险和脆弱性，并决定和维护满足安全策略目标的恰当的安全措施。清单的准确性是满足安全策略所设定的安全目标的关键因素。当区域内的资产有变化、电子连接改变、为保证满足安全目标将新资产加入区域时，应更新清单。

物理资产和组件是区域内包含的物理设备。一些例子包括以下设备：

a) 计算机硬件（如：工作站、服务器、仪表、控制器、电源、磁盘驱动器和备份磁带）；
b) 网络设备（如：路由器、交换机、集线器、防火墙或物理电缆）；
c) 通信链路（如：总线、链路、调制解调器和其他网络接口、天线）；
d) 访问鉴别和授权设备（如：域控制器、认证服务器、读卡器和扫描仪）；
e) 开发系统硬件；
f) 仿真和培训系统的硬件；
g) 外部系统硬件；
h) 备件库存；
i) 监视和控制设备（如：传感器、开关和控制器）；
j) 参考手册和资料。

逻辑资产包括区域内使用的所有软件和数据。例子如下：

k) 计算机系统软件（如：应用程序、操作系统、通信接口、配置表、开发工具、分析工具和实用程序）；
l) 操作系统和应用程序工具集的补丁和升级；
m) 数据库；
n) 数据档案；
o) 设备配置文件；
p) 为备份和恢复而维护的软件和数据副本；
q) 设计基础文件（如：功能要求，包括信息和资产、安全分类和保护等级、物理和软件设计、脆弱性评估、安全边界、基线测试、装配和安装文件）；
r) 供应商资源（如：产品更新、补丁、服务包、实用程序和验证测试）。

6.5.4.4 访问要求和控制

根据其自身的性质，区域意味着访问被限制在所有可访问实体的一小部分中。区域的安全策略需

要阐明区域所需的访问,以满足业务目标和如何控制访问。

6.5.4.5 威胁和脆弱性评估

一个给定的区域存在威胁和相应的脆弱性。组织需要识别和评估这些威胁和脆弱性,确定引起区域内资产不能满足其业务目标的风险。对威胁和脆弱性文档化的过程发生在威胁和脆弱性评估中,威胁和脆弱性评估是区域安全策略的一部分。

存在许多可能的对抗措施用以减少利用区域内给定的脆弱性造成威胁的风险。安全策略需要列出合适对抗措施的类型用以满足区域内安全等级的要求,并在成本与风险间进行权衡。

6.5.4.6 经授权的技术

随着工业自动化和控制系统不断演化以满足不断改变的业务需求,进行改变所利用的技术需要得到控制。这些系统中使用的每一种技术都带来了一系列的脆弱性和相应的风险。为了最小化给定区域内的风险,区域安全策略需要一张区域中允许的和不允许的动态技术列表。

6.5.4.7 改变管理过程

需要一个正式和准确的过程来维护给定区域内资产清单的准确性以及区域安全策略变化的方式。一个正式的过程可以确保区域内的改变和添加不会损害安全目标。另外,需要一种方法来适应安全威胁和目标的改变。威胁和脆弱性以及与它们相关的风险,将随时间变化的。

6.5.5 定义管道

管道是用于特定通信过程的安全区。作为安全区,管道是一个资产逻辑编组(这种情况下是通信资产)。一个安全管道用于保护通道的安全,这与物理管道保护电缆免受物理损害的方式一样。管道可以视为被用来连接各个区或在一个区内通信的物理管道。内部(区内)外部(区外)管道包住或保护提供资产连接的通信通道(概念上的电缆)。通常,在IACS环境中,管道与网络一样。也就是说,管道由导线、路由器、交换机,以及补充未来通信的网络管理设备。管道可以是不同网络技术的编组,也可以是单个计算机中出现的通信通道。管道可以用于分析区内或区间通信存在的威胁和脆弱性。

管道可以认为是包含数据和/或为区域间的通信提供物理连接的物理通道。管道可以包含多个子管道,以便提供一对一或一对多的区域通信。可以通过实现恰当的区域安全策略为管道提供保密通信。

6.5.6 管道特性

6.5.6.1 总则

从物理上讲,管道可以是连接区间通信的电缆。

管道是一类不含有子区的区域。也就是说,管道不是由子管道组成的。管道是通过共享给定通信信道的所有区列表定义的。使用管道中通道的物理设备和应用程序定义了管道的端点。图21中突出显示了企业管道。

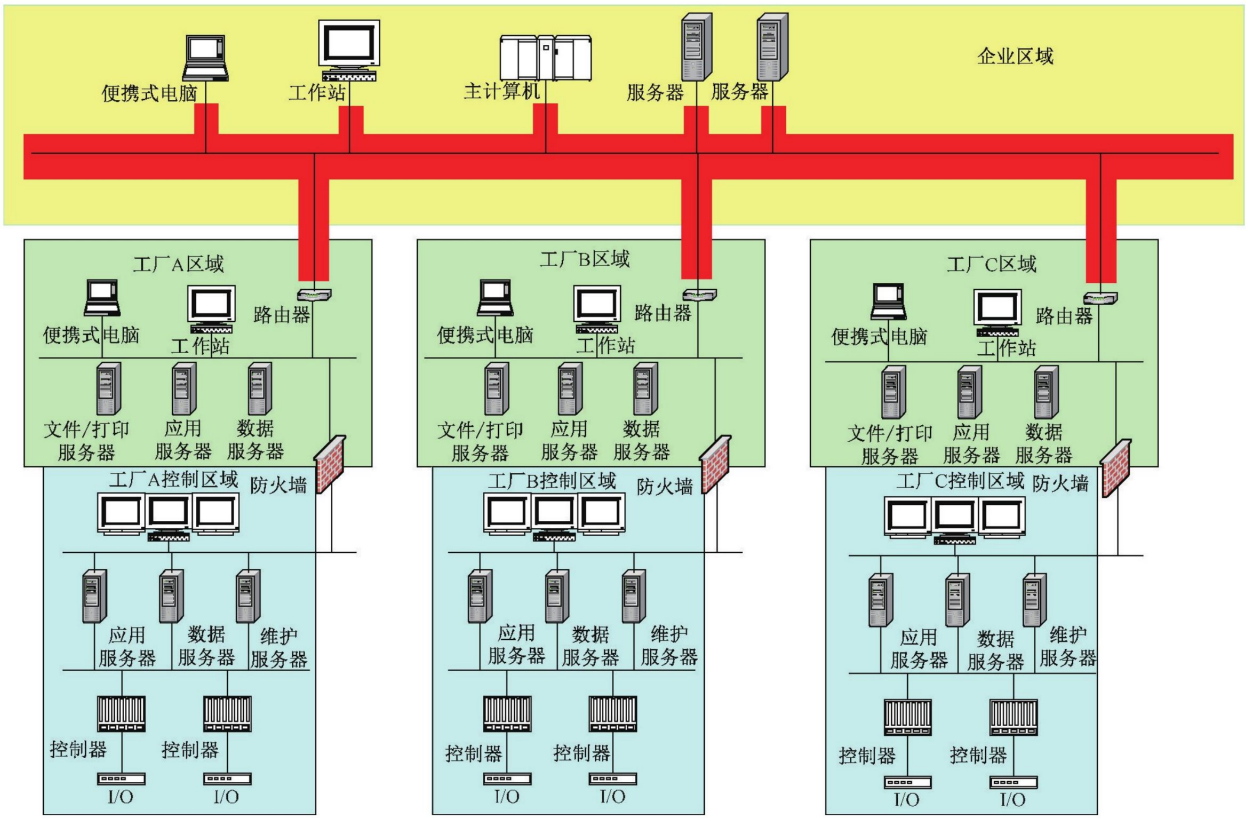

图 21　企业管道

与区一样，SCADA 应用中可以构建类似的视图。图 22 给出了一个例子。

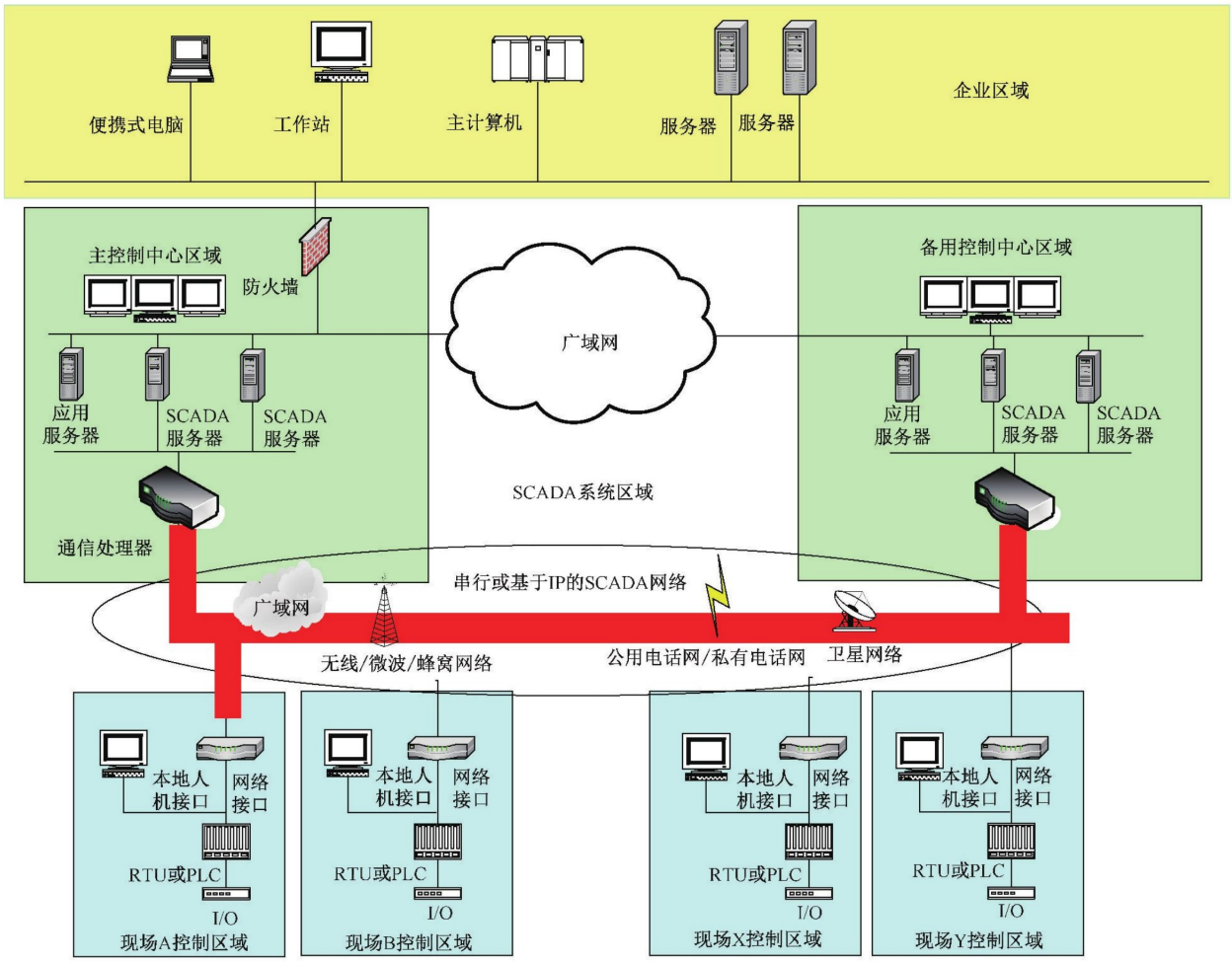

图 22　SCADA 管道例子

与区域相似，每个管道有一个特征集和其属性的安全要求。可以表现为以下几种形式的属性：

a）　安全策略；

b）　资产清单；

c）　访问要求和控制；

d）　威胁和脆弱性；

e）　安全违规的后果；

f）　授权的技术；

g）　变更管理的过程；

h）　连通的区。

6.5.6.2　安全策略

每一个管道有一个控制文件，用以描述整体的安全目标及如何确保到达安全等级目标。这包括以下几部分：

a）　管道范围；

b）　管道安全等级；

c) 组织结构和职责,用以执行管道安全策略;

d) 管道相关的风险;

e) 满足要求目标的安全策略;

f) 实施的安全措施;

g) 管道内所允许的通道类别;

h) 管道属性的文件。

上述几点都被文档化,并且融入管道的安全策略,用于指导和测量管道内所包含资产的构建和维护。

6.5.6.3 资产清单

与区清单一样,需要一份通信资产精确列表。

6.5.6.4 访问要求和控制

根据其自身的性质,管道意味着访问被限制在所有可访问实体的一小部分中。管道的安全策略需要阐明对管道所需的访问,以满足业务目标和如何控制访问。

6.5.6.5 威胁与脆弱性评估

一个给定的管道存在威胁和相应的脆弱性。组织需要识别和评估这些威胁和脆弱性,引起管道内资产不能满足它们业务目标的风险。对威胁和脆弱性文档化的过程发生在威胁和脆弱性评估中,威胁和脆弱性评估是区域安全策略的一部分。

存在许多可能的对抗措施用以减少利用管道内给定的脆弱性造成威胁的风险。在成本与风险间进行权衡的基础上,安全策略宜列出合适对抗措施类型。

6.5.6.6 授权的技术

随着工业自动化和控制系统不断演化以满足不断改变的业务需求,进行改变所利用的技术需要得到控制。这些系统中使用的每一种技术都带来了一系列的脆弱性和相应的风险。为了最小化给定管道内的风险,管道安全策略需要一张管道中允许的技术动态列表。

6.5.6.7 变更管理的过程

需要一个正式和准确的过程来维护给定管道策略的准确性以及变化方式。一个正式的过程可以确保管道内的改变和添加不会损害安全目标。另外,需要一种方法来适应安全威胁和目标的变更。威胁和脆弱性以及与它们相关的风险,将随时间变化的。

6.5.6.8 连通的区

也可以根据连通的区描述一个管道。

6.6 模型间的关系

前面所描述的模型相互关联,并且与组成安全程序的策略、规程和导则相关。它们之间的关系如图23所示。

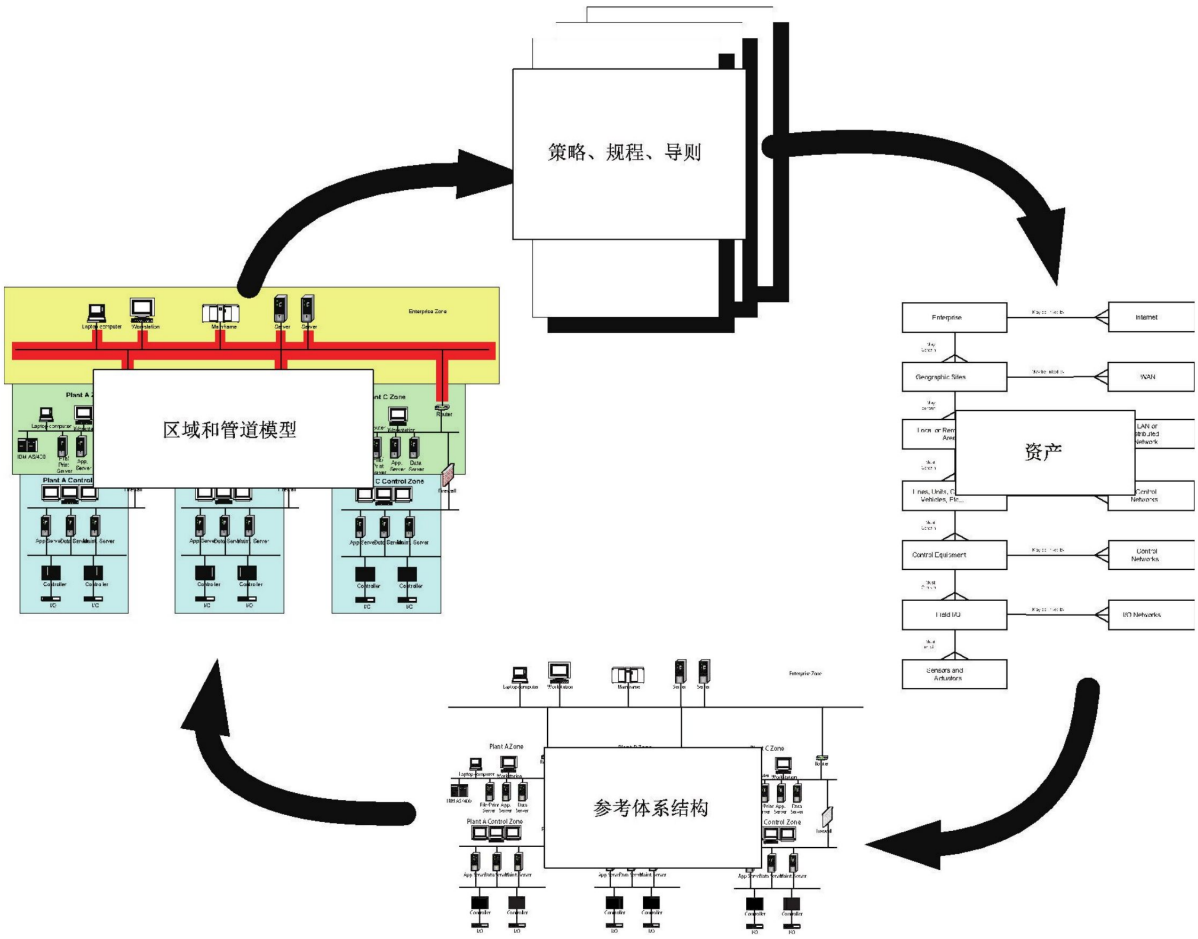

图 23　模型之间的关系

开发这样一个程序的过程的更详细信息参考 IEC 62443-2-1。

参 考 文 献

[1] IEC 60050 International Electrotechnical Vocabulary,available at〈http://www.electropedia.org〉

[2] IEC 61508-4 Functional safety of electrical/electronic/programmable electronic safetyrelated systems—Part 4: Definitions and abbreviations

[3] IEC 61511-1 Functional safety—Safety instrumented systems for the process industry sector—Part 1: Framework, definitions, system, hardware and software requirements

[4] IEC 61511-3 Functional safety—Safety instrumented systems for the process industry sector—Part 3: Guidance for the determination of the required safety integrity levels

[5] IEC 61512-1 Batch control—Part 1: Models and terminology

[6] IEC 61513, Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems

[7] IEC 62264-3 Enterprise-control system integration—Part 3: Activity models of manufacturing operations management

[8] IEC 62443-2-1 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program6

[9] IEC Glossary available at 〈http://std.iec.ch/glossary〉

[10] ISO 7498-2 Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture

[11] RFC 2828 Internet Security Glossary,available at 〈http://www.faqs. org/rfcs/rfc2828. htm l〉

[12] FIPS PUB 140-2 Security requirements for cryptographic modules, available at〈http://csrc. nist.gov/publications/fips/fips 140-2/fips1402. pdf〉

[13] CNSS Instruction No. 4009 National Information Assurance Glossary (AI), available at 〈http: //www. cnss. gov/Assets/pdf/cnssi_4009. pdf〉

[14] NASA/Science Office of Standards and Technology (NOST), ISO Archiving Standards—Fourth US Workshop—Reference Model Definitions, available at 〈http://ssdoo. gsfc. nasa. gov/nost/isoas/us04/defn. html〉

[15] SANS, Glossary of Terms used in Security and Intrusion Detection, available at 〈http://www.sans.org/resources/glossary. php〉

中 华 人 民 共 和 国
国 家 标 准
工业通信网络　网络和系统安全
术语、概念和模型
GB/T 40211—2021/IEC/TS 62443-1-1:2009
*
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 5 月第一版
*
书号:155066·1-67460

GB/T 40211—2021/IEC/TS 62443-1-1:2009

GB/T 40211-2021