ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T XXXXX—XXXX/IEC 62443-3-2:2020

工业自动化和控制系统安全 系统设计的安全风险评估

Security for industrial automation and control system Security risk assessment for system design

(IDT)

（征求意见稿）

（完成时间：2023.03）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布 XXXX－XX－XX 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：机械工业仪器仪表综合技术经济研究所。。。

本文件主要起草人：。。。

：

引　言

如何确保工业自动化和控制系统（IACS）的安全并不简单，这是有充分理由的。因为安全是一个风险管理问题，每一个IACS都会给组织带来不同的风险，这取决于它所面临的威胁、产生这些威胁的可能性、系统中固有的脆弱性以及系统被破坏时的后果。此外，拥有和运营IACS的每个组织对风险的容忍度都不同。

本文件旨在定义一套工程措施，指导组织评估特定IACS的风险，确定并应用安全对策，将风险降低到可承受的水平。

本文件中的一个关键概念是IACS安全区域和管道的应用。IEC TS 62443-1-1中介绍了区域和管道。

本文件是与ISA99联合编写的。ISA99是国际自动化学会下属的工业自动化和控制系统安全委员会(ISA)。

本文件的使用者包括资产所有者、系统集成商、产品供应商、服务提供商和合规性管理机构。

本文件通过将确定的目标安全等级（SL-T）与IEC 62443-3-3中规定的所需可实现安全等级（SL-C）达成一致，来为确定安全对抗措施提供依据。

工业自动化和控制系统安全　系统设计的安全风险评估

1　范围

本文件适用于：

a)　为工业自动化和控制系统（IACS）制定被评估系统（SUC）；

b)　将 SUC 划分为区域和管道；

c)　评估每个区域和管道的风险；

为每个区域及管道建立目标安全等级 (SL-T)并记录安全性要求。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 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）

3　术语和定义

下列术语和定义适用于本文件。

3.1 术语和定义

下列术语和定义适用于本文件。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库:

a) ISO 在线浏览平台: https://www.iso.org/obp

b) IEC　电子百科: http://www.electropedia.org/

3.1.1

通道 channel

资产之间的特定逻辑或物理的通信链路。

注：通道有助于建立连接。

3.1.2

合规性管理机构 compliance authority

有权确定管理文件中规定的安全评估的充分性或实施的有效性的实体机构。

注：示例包括政府机构、监管机构、外部和内部审计机构。

3.1.3

管道 conduit

连接两个及以上区域、满足共同安全要求的通信信道的逻辑分组。

3.1.4

保密性 confidentiality

保留对信息获取和披露的授权限制，包括保护个人隐私和专有信息的手段。

3.1.5

后果 consequence

事件的后果，通常描述为特定事件造成的健康和安全影响、环境影响、财产损失、信息损失（例如知识产权）和/或业务中断成本。

3.1.6

对抗措施 countermeasure

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

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

3.1.7

网络安全 cyber security

为保护计算机或计算机系统免受未经授权的访问或攻击而采取的措施。

注：是指IACS中的计算机系统

3.1.8

数据流 dataflow

软件之间、硬件之间或硬件与软件之间数据的流动。

3.1.9

外部网络 external network

仅连接到SUC但不属于SUC的网络。

3.1.10

影响 impact

与后果有关的最终损失或损害的度量。

示例:某一事件的后果是工业泄漏。该泄漏造成的影响是约70万RMB的罚款和约17万RMB的清理费用。

注 ： 影响可表示为受伤和/或死亡人数、环境损害程度和/或损失程度，如财产损害、材料损失、知识产权损失、产量损失、市场份额损失和恢复成本。

3.1.11

可能性 likelihood

某个事件发生的机率。

注 1: 在风险管理术语中，“可能性”一词用于指发生某事的可能性，无论是客观地或主观地、定性地或定量地定义、测量或确定的，还是用一般术语或数学方法描述的（如给定时间段内的概率或频率）。

注 2 : 在估计信息系统风险管理的可能性时，考虑了许多因素，如威胁源的动机和能力、类似威胁的历史、已知脆弱性、目标的迷惑性等。

[来源: ISO 指南 73:2009 [13] 1, 3.6.1.1 和 ISO/IEC 27005:2018 [12], 3.7]

3.1.12

流程危害分析 process hazard analysis

对与工业过程相关的潜在危险进行有组织和系统的评估

3.1.13

残余风险 residual risk

实施现有对抗措施后仍然存在的风险（例如，净风险或实施对抗措施后的风险）。

3.1.14

风险 risk

损失预期，表示为特定威胁利用特定脆弱性造成特定后果的可能性。

3.1.15

安全等级 security level

SL

SUC、安全区域或管道不受脆弱性影响并按预期方式工作的置信度。

3.1.16

安全边界 security perimeter

围绕受安全区域控制和保护的所有资产的逻辑或物理界线。

3.1.17

被评估系统 system under consideration

SUC

提供完整自动化解决方案所需的确定的IACS资产集，包括任何相关的网络基础设施资产。

注：一个SUC由一个或多个区域和相关管道组成。SUC中的所有资产属于某个区域或管道

3.1.18

威胁 threat

可能对组织运作（包括使命、职能、形象或声誉）和/或包括IACS的组织资产产生不利影响的情况或事件。

注1：情况包括违反安全策略，有意或无意阻止访问数据或导致如控制逻辑/参数、保护逻辑/参数或诊断等数据损毁、披漏或修改的个人。

3.1.19

威胁环境 threat environment

有关威胁信息的综合，如威胁源、威胁向量和趋势，这些威胁可能对已定义的目标（例如，公司、设施或SUC）产生不利影响。

3.1.20

威胁源 threat source

恶意利用脆弱性的意图和方法，或可能意外地利用到脆弱性的情况和方法。

3.1.21

威胁向量 threat vector

使威胁源能获取访问资产的路径或手段。

3.1.22

可承受风险 tolerable risk

组织认为可接受的风险水平

注：组织在确定可容忍风险时应考虑法律要求。 ISO 31000 [14]和 800-39 [16]中提供了建立可容忍风险的相关指导

3.1.23

未缓解的网络安全风险 unmitigated cybersecurity risk

在考虑任何网络安全对抗措施之前，系统中存在的网络安全风险等级。

注：这一等级有助于确定制定的应对措施需要降低多少网络安全风险

3.1.24

脆弱性 vulnerability

系统设计、实施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。

3.1.25

区域 zone

基于风险或其他条件区分的逻辑或物理资产分组，如资产的关键性、操作功能、物理或逻辑位置、所需访问权限（例如:最低权限原则）或负责组织。

注: 逻辑或物理资产的集合，是一种根据其共同安全要求、关键性（例如：财务、健康、安全（safety）或环境影响）、功能、逻辑和物理（包括位置）关系对被评估系统的划分方式。

3.2 缩略语

下表定义了本文件使用的缩略语和首字母缩略语

ANSI American National Standards Institute 美国国家标准协会
BPCS Basic process control system 基本过程控制系统
CERT Computer emergency response team 计算机安全应急响应组
CRS Cyber security requirements specification 网络安全要求规范
DCS Distributed control system 分布式控制系统
HMI Human machine interface 人机界面
HSE Health, safety and environment 健康、安全与环境
HVAC Heating, ventilation and air-conditioning 暖通空调系统
IACS Industrial automation and control system(s) 工业自动化和控制系统
ICS-CERT Industrial control system CERT 工业控制系统 CERT
IEC International Electrotechnical Commission 国际电工委员会
IIoT Industrial Internet of Things 工业物联网
IPL Independent protection layer 独立保护层
ISA International Society of Automation 国际自动化学会
ISAC Information Sharing and Analysis Centers 信息共享和分析中心
ISO International Organization for Standardization 国际标准化组织
MES Manufacturing execution system 制造执行系统
NIST[US] National Institute of Standards and Technology [美国]国家标准与技术研究所
PHA Process hazard analysis 流程危害分析
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 监视控制与数据采集
SIS Safety instrumented system 安全仪表系统
SUC System under consideration 被评估系统
SL Security level 安全等级
SL-A Achieved SL 实现的安全等级
SL-C Capability SL 能力安全等级
SL-T Target SL 目标安全等级
SP [US NIST] Special Publication [美国国家标准与技术研究所]特殊出版物
USB Universal serial bus 通用串行总线
ZCR Zone and conduit requirement 区域和管道要求

3.3 约定

本文件使用流程图来说明需求之间的工作流程。这些流程图是资料性的，可以使用其它工作流程。

4 区域、管道和风险评估要求

4.1 概述

本章描述了将SUC划分为区域和管道的要求，以及评估网络安全风险和确定每个定义区域和管道的SL-T的要求。本章中介绍的要求称为区域和管道要求（ZCR）。本章还提供了每项要求的基本原理和附加指南。图1是一个工作流程图，描述了建立区域和管道以及评估风险所需的主要步骤。我们将步骤编号以表示它们与ZCR的关系。

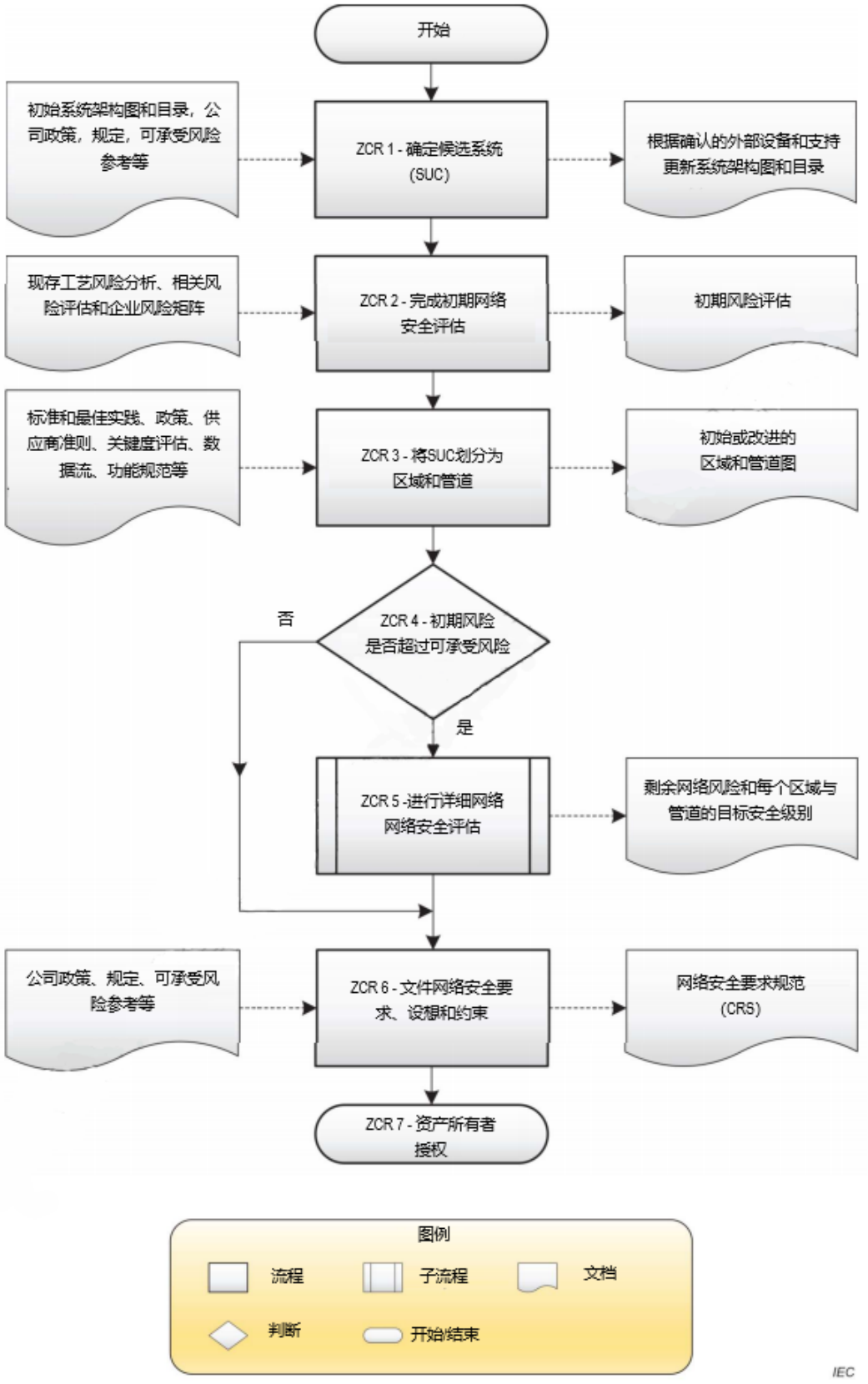
开始
初始系统架构图和目录，公司政策，规定，可承受风险参考等
ZCR 1 - 确定候选系统(SUC)
根据确认的外部设备和支持更新系统架构图和目录
现存工艺风险分析、相关风险评估和企业风险矩阵
ZCR 2 - 完成初期网络安全评估
初期风险评估
标准和最佳实践、政策、供应商准则、关键度评估、数据流、功能规范等
ZCR 3 - 将SUC划分为区域和管道
初始或改进的区域和管道图
否
ZCR 4 - 初期风险是否超过可承受风险
是
ZCR 5 -进行详细网络网络安全评估
剩余网络风险和每个区域与管道的目标安全级别
公司政策、规定、可承受风险参考等
ZCR 6 - 文件网络安全要求、设想和约束
网络安全要求规范(CRS)
ZCR 7 - 资产所有者授权
图例
流程
子流程
文档
判断
开始/结束
IEC

图1 工作流程图

4.2 ZCR 1:确认 SUC

4.2.1 ZCR 1.1: 确认 SUC 边界和接口

4.2.1.1 要求

组织应明确地确认SUC，包括安全边界的清晰划分和SUC所有接口的识别。

4.2.1.2 原由和附加指南

组织通常拥有并运行多个控制系统，尤其是具有多个工业设施的大型组织。这些控制系统中的任何一个都可以定义为SUC。例如，在一个工业设施中通常至少有一个控制系统，但通常有多个系统来控制设施中的各种功能。

该要求规定，确认SUC是为了进行网络安全分析。SUC的定义应包括提供完整自动化解决方案所需的所有IACS资产。

系统清单、架构图、网络图和数据流可用于确定和说明SUC描述中包含的IACS资产。

注：SUC可以包括多个子系统，如基本过程控制系统（BPCS）、分布式控制系统（DCS）、安全仪表系统（SIS）、监视控制和数据采集（SCADA）和IACS产品供应商包。还可能包括新兴技术，如工业物联网（IIoT）或基于云服务的解决方案。

4.3 ZCR 2: 初始网络安全风险评估

4.3.1 ZCR 2.1: 进行初始网络安全风险评估

4.3.1.1 要求

组织应对SUC进行网络安全风险评估，或确认之前的初始网络安全风险评估仍然适用，以确定最坏情况下可能因干扰、违反、中断或禁用任务关键型IACS运行而导致的未缓解的网络安全风险。

4.3.1.2 原由和附加指南

初始网络安全风险评估的目的是初步了解SUC在受到损害时可能带给组织的最坏情况影响。通常根据对健康、安全、环境、业务中断、生产损失、产品质量、财务、法律、监管、声誉的影响进行评估，此评估有助于确定详细风险评估的优先级，并有助于将资产划分到SUC内相应的的区域和管道中。

对于潜在危险过程，宜参考IEC 61511-2[8]中定义的流程危害分析（PHA）和功能安全评估结果，作为初始网络安全风险评估的一部分，以确定最坏情况的影响。各组织还宜考虑来自各国政府、特定行业的信息共享和分析中心（ISAC）和其他相关来源的威胁情报。

初期风险的评估通常通过建立可能性、影响和风险之间关系的风险矩阵来完成（例如，企业风险矩阵）。风险矩阵示例见附录B。

4.4 ZCR 3: 将 SUC 划分为区域和管道

4.4.1 概述

4.4.2~4.8.1描述了将SUC划分为区域和管道的ZCR，并为每项要求提供了原由和附加指南。4.4.2规定了在SUC内建立区域和管道的基本要求。4.4.3~4.4.7旨在根据行业最佳实践，为区域资产分配提供指导方案。此清单仅供参考，并不完全详尽。

4.4.2 ZCR 3.1: 建立区域和管道

4.4.2.1 要求

组织应将IACS和相关资产划分到已确定风险的区域或管道中。分组应基于初始网络安全风险评估的结果或其他标准，如资产的关键性、操作功能、物理或逻辑位置、所需访问权限（例如，最低权限原则）或负责组织。

4.4.2.2 原由和附加指南

将资产分为区域和管道的目的是确定那些具有相同安全要求的资产，并确定降低风险所需的相同安全措施。可根据详细风险评估的结果调整IACS资产分配。但这只是一般要求，应特别注意安全相关系统，包括安全仪表系统、无线系统、直接连接到互联网端点的系统、与IACS连接但由其他实体（包括外部系统）和移动设备管理的系统。

例如，一个设施可首先划分为多个运行区域，如材料储存、加工、精加工等。运行区域通常可进一步划分为功能层，如制造执行系统（MES）、监控系统（如人机界面[HMI]），主控制系统（例如，BPCS、DCS、远程终端单元[RTU]和可编程逻辑控制器[PLC]）和安全系统。IEC 62264-1[9] 中定义的普渡参考模型等模型通常用作该划分的基础。IACS产品供应商参考体系结构也会有所帮助。

4.4.3 ZCR 3.2: 区分业务和 IACS 资产

4.4.3.1 要求

IACS 资产所属区域应与业务或企业系统资产所属区域从逻辑或物理区分开来。

4.4.3.2 原由和附加指南

业务和IACS是两种不同类型的系统，需要划分为不同的区域，因为它们的功能、负责的组织、初始风险评估的结果和位置往往有根本上的不同。了解业务和IACS之间的基本区别以及IACS影响健康、安全和环境（HSE）的能力非常重要。

4.4.4 ZCR 3.3: 区分安全相关资产

4.4.4.1 要求

安全相关的IACS资产所属区域应与非安全相关的IACS资产所属区域从逻辑或物理上区分开。若应特殊情况不能将它们区分，则应将整个区域定义为一个安全相关区域。

4.4.4.2 原由和附加指南

与安全相关的IACS资产通常具有不同于基本控制系统、基本控制系统组件和基本控制系统组件相连组件的安全要求。安全相关区域通常需要更高级别的安全保护，因为如果该区域受到危害，则可能会产生更严重的健康、安全和环境后果。

4.4.5 ZCR 3.4: 区分临时连接设备

4.4.5.1 建议

允许与SUC进行临时连接的设备应与拟永久连接至IACS的资产划分为一个或多个单独的区域。

4.4.5.2 原由和附加指南

临时连接到SUC的设备（例如，维护便携式计算机、便携式处理设备、便携式安全设备和通用串行总线[USB]设备）比永久属于该区域的设备更可能受到不同的和更广泛的威胁。因此，这些设备应在一个或多个单独的区域中建模。我们关心的主要问题是，由于这些设备连接的临时性，它们可能还能够连接到区域外的其他网络。不过，也有例外。例如，仅在单个区域内使用并且从不离开该区域的物理边界的手持设备可以划分在该区域中。

4.4.6 ZCR 3.5: 区分无线设备

4.4.6.1 建议

无线设备应位于与有线设备分开的一个或多个区域中。

4.4.6.2 原由和附加指南

无线信号不受围栏或机柜的控制，因此比普通有线网络更容易访问。由于接入可能性的增加，它们比有线设备更容易受到不同的和更广泛的威胁。

通常，无线访问点被建模为无线区域和有线区域之间的管道。根据无线访问点的能力，可能需要额外的安全控制（例如防火墙）来提供适当的隔离级别。

4.4.7 ZCR 3.6: 区分通过外部网络连接的设备

4.4.7.1 建议

允许通过SUC外部网络连接到SUC的设备应被划分到一个或多个单独的区域

4.4.7.2 原由和附加指南

组织为了维护、优化和报告的目的而向员工、供应商和其他业务伙伴等人员授予远程访问权限的情况并不少见。由于远程访问位于SUC的物理边界之外，因此应将其建模为一个或多个具有自身安全需求的单独区域。

4.5 ZCR 4: 风险比较

4.5.1 概述

4.5.2 包括一个用于比较初始风险和可承受风险的ZCR。

4.5.2 ZCR 4.1: 比较初始风险和可承受风险

4.5.2.1 要求

应将4.3中确定的初始风险与组织的可承受风险进行比较。如果初始风险超过可承受风险，组织应按4.6中定义进行详细网络安全风险评估。

4.5.2.2 原由和附加指南

此步骤的目的是为了确定初始风险是否可承受或需要进一步缓解。

4.6 ZCR 5: 执行详细网络安全风险评估

4.6.1 概述

本ZCR讨论了IACS的详细风险评估要求，并提供了每项要求的原由和附加指南。本ZCR中的要求适用于每个区域和管道。如果区域或管道具有类似的威胁、后果和/或类似的资产，则允许同时分析多个区域或管道组，前提是此类分组能够实现优化分析。如果区域是标准化的（例如，来自某参考设计的多个实例的复制），则允许使用已有分析成果。图2所示的流程图说明了网络安全风险评估工作流程。

任何详细风险评估方法（如ISO 31000[14]、NIST SP 800-39[16]和ISO/IEC 27005[12]）均可作为参照，前提是所选方法满足风险评估要求。初始和详细风险评估方法应来自同一框架、标准或来源，并且必须使用一致的风险等级制，以便保证结果的一致性和连续性。

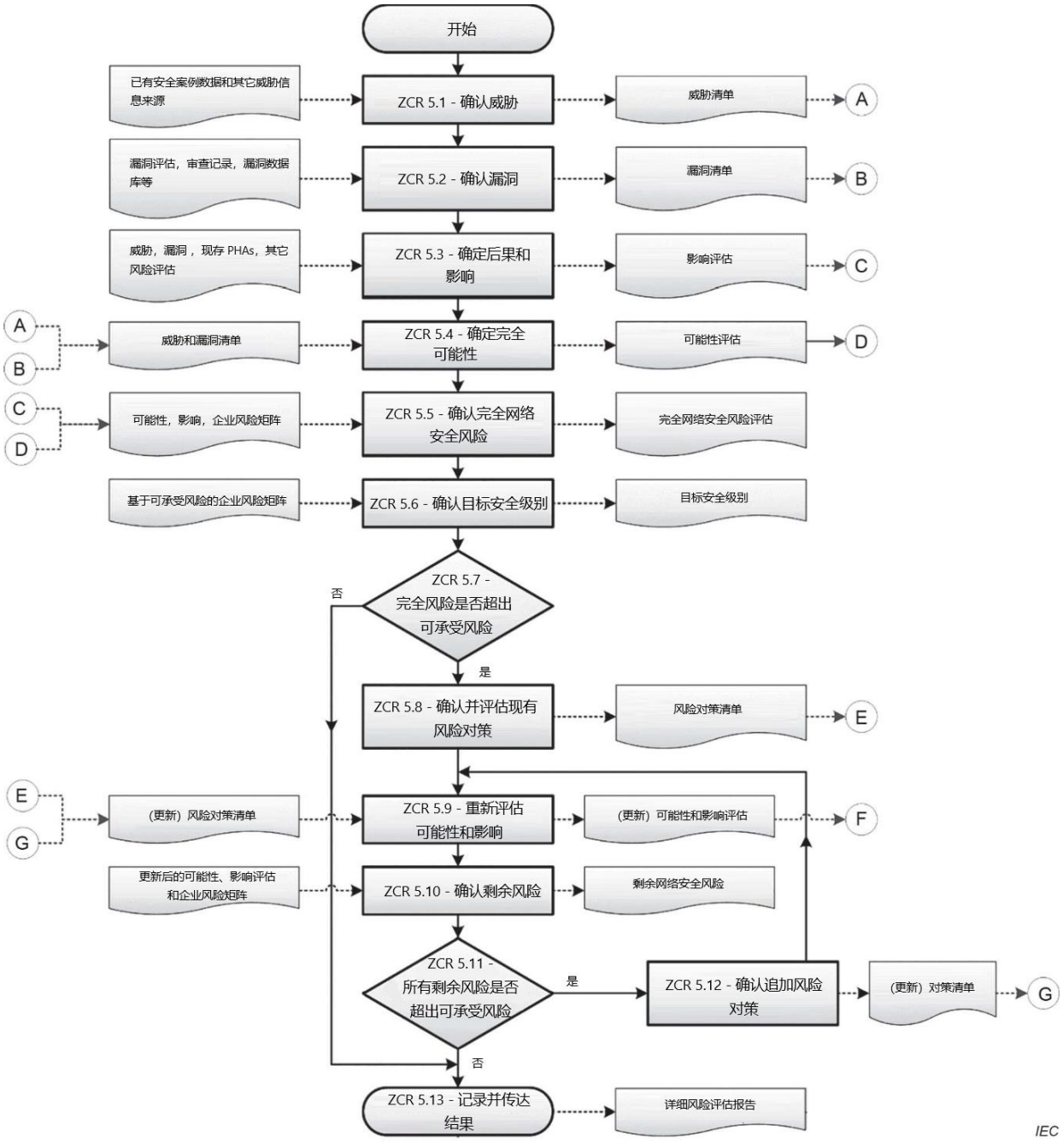

图2　区域或管道的详细网络安全风险评估工作流程图

4.6.2 ZCR 5.1:确认威胁

4.6.2.1 要求

应制定一份可能影响到区域或管道内所含资产的威胁清单。

4.6.2.2 原由和附加指南

为了进行安全风险评估，准备一份全面而现实的威胁清单非常重要。威胁描述应包括但不限于以下内容：

a) 威胁来源描述；
b) 对威胁源的能力或技能水平的描述；
c) 对可能的威胁向量的描述；
d) 标识潜在受影响的资产。

威胁描述的一些示例如下：

- 员工非恶意地物理访问过程控制区，并将USB存储设备插入其中一台计算机；
- 授权支持人员使用受感染的笔记本电脑以逻辑方式访问过程控制区；
- 员工非恶意地打开会泄漏其凭证的钓鱼电子邮件。

考虑到可能存在大量威胁，可以通过将来源、受影响资产、访问点等分组来进行总结。

4.6.3 ZCR 5.2: 确认脆弱性

4.6.3.1 要求

对区域或管道进行分析，以识别和记录与区域或管道内包含的资产（包括访问点）相关的已知脆弱性。

4.6.3.2 原由和附加指南

威胁若要成功入侵，必须利用资产中的一个或多个脆弱性。因此，有必要确认与资产相关的已知脆弱性，以便更好地了解威胁向量。

识别IACS脆弱性的一种普遍接受的方法是执行脆弱性评估。有关IACS网络安全脆弱性评估的更多信息，见ISA-TR84.00.09[15]。

此外，有关IACS中已知和常见脆弱性的信息来源有很多，如工业控制系统计算机应急响应小组（ICS-CERT）、IACS产品供应商等。

4.6.4 ZCR 5.3: 确定后果和影响

4.6.4.1 要求

对每种威胁情况进行评估，以确定后果和威胁成功入侵时的影响。应根据对风险领域（如人员安全、财务损失、业务中断和环境）的最坏影响记录后果。

4.6.4.2 原由和附加指南

评估网络威胁的最坏情况影响是执行安全控制成本/收益分析的重要参照。如果最坏情况的影响很小，风险评估小组可以选择继续处理下一个威胁。

应审查现有PHA和其他相关风险评估（如信息技术、功能安全、业务和人身安全），以协助确定后果和影响。

影响的度量可以是定性的，也可以是定量的。一种方法是使用组织定义的后果量表作为其风险管理体系的一部分（示例见附录B）。

4.6.5 ZCR 5.4: 确定威胁未缓解的可能性

4.6.5.1 要求

对每个威胁进行评估，以确定未缓解的可能性，即威胁出现的可能性。

4.6.5.2 原由和附加指南

在风险管理术语中，“可能性”一词是指某事发生的机率，无论是客观地或主观地、定性地或定量地定义、测量或确定，还是用一般术语或数学方法描述（例如，给定时间段内的概率或频率）。评估可能性的一种常用方法是使用由组织定义的，作为其风险管理体系一部分的半定量可能性量表（示例见附录B）。本文件允许采用定性或定量方法。

在估计未缓解的可能性时，考虑了许多因素，如威胁源的动机和能力、类似威胁的历史、已知脆弱性、目标的吸引力等。

在确定未缓解的可能性时，不应考虑评估区域或管道的现有网络安全对抗措施；他们应该假设被淘汰。然而，确定可能性可以确认IACS组件和任何非网络独立保护层（IPL）固有的对抗措施，如物理安全、机械防护（如压力安全阀）或为降低可能性而制定的应急程序。

在详细风险评估过程中，对可能性进行了两次评估：为了确定完全风险，首先在不考虑任何现有对抗措施的情况下进行初步确定。而后在4.6.10中重新评估，考虑现有对抗措施及其有效性，以确定残余风险。

仅评估后果的风险评估方法可满足本文件的要求。这种方法通常不会在确定未缓解的安全风险时考虑其可能性，并隐式地假设可能性是恒定不变的（例如，假设可能性始终存在或定量地为“1”）。

4.6.6 ZCR 5.5: 确定未缓解的安全风险

4.6.6.1 要求

每个威胁未缓解的网络安全风险应结合4.6.4中确定的影响程度和4.6.5中确定的未缓解的可能性度量来确定。

4.6.6.2 原由和附加指南

未缓解的网络安全风险的确定通常使用风险矩阵来完成，该矩阵建立了可能性、影响和风险之间的关系，如企业风险矩阵（示例见附录B）。

4.6.7 ZCR 5.6: 确定目标安全等级

4.6.7.1 要求

应为每个安全区域或管道设立目标安全等级。

4.6.7.2 原由和附加指南

SL-T是特定IACS、区域或管道所需的安全等级。其目的是将这些信息明确传达给负责设计、实施、运行和维护网络安全的人员。

SL-T可以表示为单个值或矢量。参考GB/T 35673-2017附件A，了解SL矢量法的讨论。

建立SL-T没有现有的规定方法。一些组织选择基于未缓解的网络安全风险和可承受风险之间的差异建立SL-T。而其他组织选择根据本文件附录A和GB/T 35673-2017中提供的SL定义建立SL-T。另一种方法是使用风险矩阵（示例见附录B）定性确定SL。从SL的合理估计（也可以没有估计）开始，用考虑了SL默示对抗措施的风险矩阵来评估网络安全风险。如果风险不可承受，则提高SL（这意味着要增加额外的对抗措施），直到网络安全风险可承受为止。由此分析得出的SL作为SL-T。

4.6.8 ZCR 5.7: 比较未缓解的风险和可承受风险

4.6.8.1 要求

应将4.6.6中确定的每个威胁的未缓解的风险与组织的可承受风险进行比较。如果未缓解的风险超过可承受风险，组织应决定是否接受、转移或缓解风险。为降低风险，请通过完成4.6.9至4.6.13继续评估威胁。否则，组织可将结果记录在4.6.14中，然后继续处理下一个威胁。

4.6.8.2 原由和附加指南

此步骤的目的是确定未缓解的风险是否可承受或需要进一步评估。

4.6.9 ZCR 5.8: 确认和评估现有对抗措施

4.6.9.1 要求

应识别和评估SUC中的现有对抗措施，以确定用以降低可能性或影响的对抗措施的有效性。

4.6.9.2 原由和附加指南

为了确定残余风险，应在考虑现有对抗措施的存在和有效性的同时，评估其可能性和影响。这一步骤的重点是确认和评估现有的对抗措施。

IEC 62443-3-3通过为每个系统要求分配一个能力SL（SL-C），来提供关于对抗措施类型及其有效性的指导。

4.6.10 ZCR 5.9:重新评估可能性和影响

4.6.10.1 要求

在考虑了对抗措施及其有效性后，重新评估可能性和影响

4.6.10.2 原由和附加指南

4.6.5中确定未缓解的可能性不考虑现有对抗措施。在本步骤中，考虑并使用技术、行政或程序控制等对抗措施来确定缓解后的可能性。同样，4.6.4中确定的后果和影响也应根据确定的对抗措施进行重新评估。

4.6.11 ZCR 5.10: 确定残余风险

4.6.11.1 要求

4.6.2中确定的每个威胁的残余风险应通过结合4.6.10中确定的缓解后可能性度量和缓解后影响值来确定。

4.6.11.2 原由和附加指南

残余风险的确定提供了对当前风险水平的度量以及对现有对抗措施有效性的度量。这是确定当前风险水平是否超过可承受风险参照标准的关键步骤。

4.6.12 ZCR 5.11: 比较残余风险和可承受风险

4.6.12.1 要求

应将4.6.2，ZCR 5.1中确定的每个威胁的残余风险与组织的可承受风险进行比较。如果残余风险超过可承受风险，组织应根据组织的策略确定是否接受、转移或缓解残余风险。

4.6.12.2 原由和附加指南

此步骤的目的是确定残余风险是否可承受或需要进一步缓解。许多组织在其风险管理策略中定义了可承受风险。

4.6.13 ZCR 5.12: 确认附加的网络安全对抗措施

4.6.13.1 要求

如果残余风险超过组织可承受风险,则应确定附加的网络安全对抗措施,如技术、行政或程序控制,以缓解风险，除非组织选择接受或转移风险。.

4.6.13.2 原由和附加指南

当残余风险超过组织的风险承受能力时，需要采取措施将风险降低到可承受的水平。

采取对抗措施降低风险。网络安全对抗措施可以是技术性和非技术性（如策略和程序）的结合。降低风险的另一种方法是将IACS资产从较低安全性区域或管道重新分配到较高安全性区域或管道，以便利用较高安全性区域或管道的安全对抗措施。

IEC 62443-3-3可作为选择适当技术对抗措施的参考。IEC 62443-3-3中确定的对抗措施分配了SL-C等级，这有助于评估对抗措施的有效性。

作为设计过程的一部分，用户可能还需要评估对抗措施的成本和复杂度。

4.6.14 ZCR 5.13: 记录并传达结果

4.6.14.1 要求

详细网络风险评估结果应记录、报告并提供给组织中的适当利益相关者。应指定适当的信息安全等级，以保护文件的机密性。文件应包括每次会议的举行日期以及与会者的姓名和职务。有助于执行网络风险评估的文件（如系统架构图、PHA、脆弱性评估、差距评估和威胁信息来源）应与网络风险评估一起文档化。

4.6.14.2 原由和附加指南

网络安全风险评估应文档化，并提供给组织中的适当人员。网络安全风险评估是可用于多种目的的动态文档，包括测试、审查和未来风险评估。但是，适当保护这些信息也很重要，因为这些信息通常包含有关系统、已知脆弱性和现有安全措施的敏感细节。

4.7 ZCR 6: 记录网络安全要求、假定和约束

4.7.1 概述

4.7.2至4.7.10描述了为实现的SL-T，需要在SUC内记录网络安全要求、假定和约束的要求，并为每项要求提供了原由和附加指南。

4.7.2 ZCR 6.1: 网络安全要求规范

4.7.2.1 要求

应制定网络安全要求规范（CRS），以根据详细风险评估结果以及基于企业或实际特定策略、标准和相关法规的一般安全要求，记录SUC的强制性安全对抗措施。

CRS应至少包含以下内容：

- ZCR 6.2: SUC说明（见4.7.3）；
- ZCR 6.3: 区域和管道图（见4.7.4）；
- ZCR 6.4: 区域和管道属性（见4.7.5）；
- ZCR 6.5: 运行环境假定（见4.7.6）；
- ZCR 6.6: 威胁环境（见4.7.7）；
- ZCR 6.7: 组织安全策略（见4.7.8）；
- ZCR 6.8: 可承受风险（见4.7.9）；
- ZCR 6.9: 监管要求（见4.7.10）。

4.7.2.2 原由和附加指南

应文档化网络安全要求，以确保要求明确传达给所有利益相关者，并得到正确实施。CRS无需编辑成单个文档。许多组织在其他IACS文件中便包括了网络安全要求部分。

注：ISA-TR84.00.09提供了CRS中推荐包含元素的附加指南。

4.7.3 ZCR 6.2: SUC 说明

4.7.3.1 要求

CRS中应包括SUC的高层次描述和描写。CRS至少应包括SUC的名称、功能和预期用途的高层次描述，以及受控设备或过程的描述。

4.7.3.2 原由和附加指南

在CRS中清晰地确定和定义SUC的范围是很重要的。这一要求确保提供的信息量最小化。应包括SUC以及相关数据流和过程流的说明

4.7.4 ZCR 6.3: 区域和管道图

4.7.4.1 要求

组织应：

a) 绘制一张或一组图纸，说明整个SUC的区域和管道分区。

b) 将SUC中的每个资源分配给区域或管道。

4.7.4.2 原由和附加指南

一个SUC的总览图是十分重要的，说明区域和管道边界以及这些边界内包含的资产，以便有效地传达SUC的分区方式。

4.7.5 ZCR 6.4: 区域和管道属性

4.7.5.1 要求

应为每个规定区域和管道确认和文档化以下项目：

a) 名称和/或唯一标识符；

b) 负责组织；

c) 逻辑边界的定义；

d) 物理边界的定义，如适用；

e) 安全标志；

f) 所有逻辑访问点的列表；

g) 所有物理访问点的列表；

h) 与每个访问点相关联的数据流列表；

i) 连接的区域或管道；

j) 资产清单及其分类、关键性和商业价值；

k) SL-T；

l) 适用的安全要求；

m) 适用的安全策略；

n) 假定和外部依赖。

4.7.5.2 原由和附加指南

描述和文档化区域或管道的属性非常重要。上述要求中列出的每个项目都有一个特定的用途，如下所述：

a) 名称和/或唯一标识符：对于设计和文件编制而言，能够唯一地标识每个区域或管道非常重要。

b) 负责组织：负责组织是对区域或管道的安全负责的个人、团体或多个团体。

注意：负责组织和责任组织可以不同。如果不同的话，两个组织都要被认定。

c) 逻辑边界：逻辑边界很重要，因为它描绘了区域或管道与系统其余部分之间的边界。它还有助于确定所有通信进入或离开区域或管道的分界点。

d) 物理边界：如果区域或管道需要物理安全以实现其SL-T，则文档化物理边界非常重要。如果物理安全可以增强（但不是必需的）SL-T，最好将其文档化。

e) 安全标志：必须确定区域或管道是否与安全相关或是否包含与安全相关的资产。

f) 逻辑访问点列表：逻辑访问点是电子信息可以跨越区域或管道逻辑边界的任何地方。需要时确认和文档化逻辑访问点，因为它们可能具有可被威胁利用的脆弱性。

g) 物理访问点列表：物理访问点（例如，围栏、门和围墙）是人员可以物理访问区域或管道资产的任何地方。需要确定和记录物理访问点，以确定监测和防止未经授权访问的适当方法。

h) 数据流列表：为了检测异常，确认和记录整个系统的预期数据流（例如，源、目的地和协议）非常重要，尤其是区域或管道内外的数据流。

i) 连接的区域或管道：确认区域和管道之间的连接非常重要，有助于确认系统中的所有逻辑访问点。通常，这在区域和管道图中会进行说明。

j) 资产清单及其分类、关键性和商业价值：确定每个区域或管道中包含的IACS资产及其分类、关键性和商业价值非常重要，有助于了解该区域或管道受损的后果。在确认后果时，考虑其他区域/管道所受到的后果影响和考虑当前问题区域/管道的后果同样重要。

k) SL-T：SL-T 传达根据风险评估结果确定的区域或管道所需的防护等级。见4.6.7。

l) 适用安全要求：对于每个区域和管道，有必要确定实现SL-T所需的适用安全要求。一些要求可能是SUC中所有区域或管道的共同要求，而其他要求可能是特有的。

注：安全要求规范在完成详细风险评估（见4.6）后才能最终确定。

m) 适用安全策略：对于每个区域和管道，有必要确定实现SL-T所需的适用组织安全策略。一些策略可能是SUC中所有区域或管道的共同策略，而其他策略可能是特有的。

n) 假定和外部依赖：通常情况下，区域或管道的安全性取决于区域或管道外部的因素，如清洁电源和额外的物理和网络安全层。应文档化这些假定和相互依赖关系。

4.7.6 ZCR 6.5:运行环境假定

4.7.6.1 要求

CRS应确认并文档化SUC所在或预计所在的物理和逻辑环境。

4.7.6.2 原由和附加指南

应文档化SUC的物理环境，以确保IACS资产得到适当保护。用于描述物理环境的文档类型包括站点地图、楼层平面图、布线示意图、连接器配置和站点安全计划等。还应参考现有的安全脆弱性评估。

SUC的逻辑环境也应文档化，以便清楚地了解可能连接SUC接口的网络、信息技术、协议和IACS系统。相关文件类型包括网络架构图、系统架构图、电气单线图、暖通空调系统（HVAC）连接、火灾和气体探测与阻燃以及其他相关设计文件。

4.7.7 ZCR 6.6: 威胁环境

4.7.7.1 要求

CRS应包括对影响SUC的威胁环境的描述。描述应包括威胁情报的来源，已有的和新出现的威胁。

4.7.7.2 原由和附加指南

有许多因素可以影响SUC的威胁环境，包括地缘政治倾向、物理环境和系统的敏感性。可参考如下权威来源的示例：

- 计算机安全应急响应组 (CERT)；
- ICS-CERT；
- 公私合作伙伴， 例如信息共享和分析中心
- IACS产品供应商；
- 工业咨询团体；
- 信息安全政府机构；
- 威胁情报部门。

4.7.8 ZCR 6.7: 组织安全策略

4.7.8.1 要求

用于实施组织安全策略的安全对抗措施和特性应包含在CRS中。

4.7.8.2 原由和附加指南

所有系统都需包含由组织建立的基线安全策略。

4.7.9 ZCR 6.8: 可承受风险

4.7.9.1 要求

组织的可承受风险应包含在CRS中。

4.7.9.2 原由和附加指南

利益相关者需了解组织已建立的可承受风险水平，以确保SUC风险水平的一致性。

4.7.10 ZCR 6.9: 法规要求

4.7.10.1 要求

适用于SUC的任何相关网络安全监管要求应包含在CRS中。

4.7.10.2 原由和附加指南

必须确保法规遵从性。

4.8 ZCR 7: 资产所有者批准

4.8.1 概述

4.8.2包含一个ZCR，用以获取资产所有者的批准

4.8.2 ZCR 7.1: 获取资产所有者批准

4.8.2.1 要求

对SUC控制过程的安全性、完整性和可靠性负责的资产所有者管理层应审查和认可风险评估的结果。

4.8.2.2 原由和附加指南

风险评估通常由第三方协助进行，各学科专家参与，他们对工业过程的操作以及IACS和相关IT系统的功能非常熟悉。虽然这些人员具备进行风险评估的知识和技能，但他们通常无权做出是否接受风险的决定。因此，评估结果必须提交给有权作出此类决定的适当管理层。

附 录 A
（资料性）
安全等级

IEC 62443-4-2 [7]将 SL 定义为四个不同的级别（1、2、3和4），每个级别的安全要求都在不断提高。SL 0隐式定义为不需要安全要求或安全保护。

- SL 1: 防止偶然或巧合的违规
- SL 2: 防止使用低动机、少资源消耗、低技能要求的简单手段恶意违规
- SL 3: 防止使用适度动机、适度资源消耗、IACS特定技能要求的复杂手段恶意违规
- SL 4: 防止使用高动机、高资源消耗、IACS特定技能要求的复杂手段恶意违规。

对于SL-T而言，这意味着资产所有者或系统集成商已通过风险评估确定他们需要保护该特定区域、系统或组件免受此级别的威胁。

IEC 62443-3-3将SL分为三种不同类型：目标级别、已实现级别和可实现级别。这些类型虽然相互关联，但主要考虑的安全生命周期的方面不同。

•SL-T是特定IACS、区域或管道所需的安全等级。这通常是通过对系统进行风险评估来确定的，它表明了系统确保其正确运行所需的特定安全等级。

•已实现 SL (SL-A) 是特定系统的实际安全等级。这是在系统设计可用或系统就绪后测定的。它们用于确定安全系统是否满足SL-T中最初设定的目标。

•SL-C 是组件或系统在正确配置时可以提供的SL。该级别表明，当正确配置和集成时，特定组件或系统能够在不需要额外补偿对抗措施的情况下满足SL-T。

根据IEC 62443（所有部分），这些SL中的每一个都将用于安全生命周期的不同阶段。从一个特定系统的目标开始，一个组织将需要构建一个设计，其中包括系统实现预期结果的能力。换句话说，设计团队将首先确定特定系统所需的SL-T，然后，他们再根据SL-T来设计系统以满足目标安全等级。这部分开发通常是一个迭代过程，在每次迭代后，设计师们会对设计方案的SL-A进行测量并与SL-T进行比较。作为设计过程的一部分，设计师将选择具有必要SL-C的组件和系统以满足SL-T要求；或者，如果这些系统和组件不可用，则使用其它可用的系统和组件并用补偿对策来弥补。系统投入运行后，实际的SL将被测定为SL-A，并与SL-T进行比较。

附 录 B
（资料性）
风险矩阵

风险矩阵是风险管理中使用的一种工具，通过评估事故发生的可能性和事故发生后后果的严重性，定性地确定风险水平。

风险矩阵的两个轴分别表示可能性和严重性。可能性和严重性之间的交叉点代表风险等级。最低可能性和最低严重性之间的交集产生最低风险等级。而最高可能性和最高严重性之间的交集产生最高风险等级。交叉点通常采用颜色编码，以表示风险等级的升高，绿色通常代表最低，红色通常代表最高。

尽管风险矩阵总是二维的，但根据可能性和严重程度量表中的类别数量，其维度会有所不同（例如，3 x 3、4 x 4、3 x 5、5 x 5）。

表 B.1 是一个3 x 5的风险矩阵示例。

表B.1 3X5 风险矩阵示例

			严重性	
		A	B	C
可能性	5	高	高	中高
	4	高	中高	中
	3	中高	中	中低
	2	中	中低	低
	1	中低	低	低

可能性级别将整个可能性值范围划分为离散的类别或区间。表B.2是五级别可能性级别的示例。这个例子演示了一些可能性级别如何提供将数据值划分为类别的多种方法。在本例中，提供了引导词、可能性描述和频次。

表B.2 可能性级别示例

可能性级别	引导词	可能性描述	频次（每年）
1	确定的	几乎可以肯定	$>10^{-1}$
2	很可能	大概率会发生	10^{-1} ~ 10^{-3}
3	可能	可能发生或并不罕见	10^{-3} ~ 10^{-4}
4	不太可能	可以想象，但不太可能发生	10^{-4} ~ 10^{-5}

5	罕见的	可能性极低以致于可以假设它不会发生	$<10^{-5}$

类似地，后果或严重性等级将整个严重性值范围划分为离散的类别或区间。表B.3是三级别后果量表的示例。这个例子演示了一些可能性级别是如何提供多种将数据划分为类别的方法的。在本例中，提供了引导词、可能性描述和频次。

表B.3 后果或严重程度级别示例

	操作			财务			HSE		
级别	导致一个站点的停机	导致多个站点的停机	国家基础设施和服务	成本(百万美元)	法律	声誉	现场人员	场外人员	环境
A (高)	>7 天	>1 天	影响多个部门或扰乱社会主要服务	>500	重罪	品牌形象丧失	人员死亡	死亡或重大社会事故	被区域机构文档化案例或造成长期严重大面积损害
B(中)	<2 天	>1 小时	造成不止于企业而是对整个行业的潜在影响	>5	轻罪	客户信任度降低	损失工作日或重伤	投诉或当地社区影响	被当地机构文档化案例
C (低)	<1 天	<1 小时	对行业影响很小甚至没有。对社会几乎没有影响	<5	未造成犯罪	无	急救或可记录伤害	没有投诉	小规模，可控的，不值得报道的事故

尽管存在标准风险矩阵，但在不同环境下，独立项目和组织通常会选择创建自己的风险矩阵或定制现有的风险矩阵。附录B提供了几个额外的风险矩阵示例（见表B.4至表B.6所示），以向使用者强调风险矩阵可能在维度、规模类别、颜色编码、风险等级等方面有所不同，促进风险评估的实体必须获得资产所有者认可的被评估设施的正确风险矩阵。

表B.4 简单 3X3 风险矩阵示例

可能性	高概率	中	高	高
	中概率	低	中	高
	低概率	低	低	中
		无关紧要	一般影响	严重

表B.5 5X5 风险矩阵示例

	后果

		小规模问题（可以被日常流程轻易处理）	可能造成中断（损失介于50万美元到100万美元）	损耗大量时间和资源（损失介于100万美元到1000万美元）	业务严重受损（损失介于1000万美元到2500万美元）	企业生存面临危险（损失大于2500万美元）
可能性	几乎必然（>90 %）	高	高	极高	极高	极高
	比较可能（50% 至90%）	中	高	高	极高	极高
	中等概率（10% 至50%）	低	中	高	极高	极高
	不太可能（3% 至10%）	低	低	中	高	极高
	罕见(<3 %)	低	低	中	高	高

表B.6 3X4 风险矩阵

		严重性			
		可接受（很小或没有影响）	可承受（影响可查觉，但对结果不重要）	不良（影响严重或对结果至关重要）	无法承受（可能导致灾难）
可能性	罕见（风险不太可能发生）	低 - 1 -	中 - 4 -	中 - 6 -	高 - 10 -
	可能（可能发生风险）	低 - 2 -	中 - 5 -	高 - 8 -	极高 - 11 -
	应该（风险将会发生）	中 - 3 -	高 - 7 -	高 - 9 -	极高 - 12 -

参 考 文 献

IEC 62443系列的其他部分参考：

[1] IEC TS 62443-1-1, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models

[2] IEC 62443-2-1, Security for industrial automation and control systems – Part 2-1: Requirements for an IACS security management system

[3] IEC TR 62443-2-3:2015, Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment

[4] IEC 62443-2-4:2015, Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

IEC 62443-2-4:2015/AMD1:2017

[5] IEC TR 62443-3-1:2009, Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems

[6] IEC 62443-4-1:2018, Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

[7] IEC 62443-4-2:2019, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

Other standards references:

[8] IEC 61511-2:2016, Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1: 2016

[9] IEC 62264-1:2013, Enterprise-control system integration – Part 1: Models and terminology

[10] ISO/IEC 18028-4:2005, Information technology – Security techniques – IT network security – Part 4: Securing remote access

[11] ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management

[12] ISO Guide 73:2009, Risk management – Vocabulary

[13] ISO 31000:2018, Risk management – Guidelines

[14] ISA-TR84.00.09, Cybersecurity Related to the Functional Safety Lifecycle

[15] NIST Special Publication (SP) 800-39, Guide for Applying the Risk Management Framework