ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33009.3—2016

工业自动化和控制系统网络安全 集散控制系统(DCS) 第3部分:评估指南

Industrial automation and control system security—Distributed control system(DCS)—Part 3:Assessment guidelines

2016-10-13 发布　　2017-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 33009《工业自动化和控制系统网络安全　集散控制系统(DCS)》和 GB/T 33008《工业自动化和控制系统网络安全　可编程序控制器(PLC)》等共同构成工业自动化和控制系统网络安全系列标准。

GB/T 33009《工业自动化和控制系统网络安全　集散控制系统(DCS)》分为 4 个部分：

——第 1 部分：防护要求；

——第 2 部分：管理要求；

——第 3 部分：评估指南；

——第 4 部分：风险与脆弱性检测要求。

本部分为 GB/T 33009 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由中国机械工业联合会提出。

本部分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)和全国信息安全标准化技术委员会(SAC/TC 260)归口。

本部分起草单位：浙江中控研究院有限公司、浙江大学、机械工业仪器仪表综合技术经济研究所、重庆邮电大学、中国科学院沈阳自动化研究所、西南大学、福建工程学院、杭州科技职业技术学院、北京启明星辰信息安全技术有限公司、中国电子技术标准化研究院、国网智能电网研究院、中国核电工程有限公司、上海自动化仪表股份有限公司、东土科技股份有限公司、清华大学、西门子(中国)有限公司、施耐德电气(中国)有限公司、北京钢铁设计研究总院、华中科技大学、北京奥斯汀科技有限公司、罗克韦尔自动化(中国)有限公司、中国仪器仪表学会、工业和信息化部电子第五研究所、北京海泰方圆科技有限公司、青岛多芬诺信息安全技术有限公司、北京国电智深控制技术有限公司、北京力控华康科技有限公司、北京和利时系统工程有限公司、中国石油天然气管道有限公司、北京匡恩网络科技有限责任公司、西南电力设计院、广东航宇卫星科技有限公司、华北电力设计院工程有限公司、华为技术有限公司、中国电子科技集团公司第三十研究所、深圳万讯自控股份有限公司、横河电机(中国)有限公司北京研发中心。

本部分主要起草人：施一明、冯冬芹、梅恪、王玉敏、王平、王浩、高梦州、徐珊珊、徐皑冬、刘枫、许剑新、陈平、杨悦梅、陈建飞、还约辉、黄家辉、贾驰千、梁耀、刘大龙、陆耿虹、刘文龙、王芳、孟雅辉、范科峰、梁潇、王彦君、张建军、薛百华、许斌、陈小淙、华镕、高昆仑、王雪、周纯杰、张莉、刘杰、朱毅明、王弢、孙静、胡伯良、刘安正、田雨聪、方亮、马欣欣、王勇、杜佳琳、陈日罡、李锐、刘利民、孔勇、黄敏、朱镜灵、张智、张建勋、兰昆、张晋宾、成继勋、尚文利、钟诚、梁猛、陈小枫、卜志军、丁露、李琳、杨应良、杨磊。

工业自动化和控制系统网络安全 集散控制系统(DCS) 第3部分:评估指南

1 范围

GB/T 33009的本部分规定了集散控制系统的安全风险评估等级划分、评估的对象及实施流程,以及安全措施有效性测试。

本部分适用于电力、石油、化工、水利、冶金、建材等各领域针对DCS系统的进行的安全风险评估活动,也适用于指导DCS用户改善和提高生产系统中DCS安全能力的系统维护活动。

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。

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

3 术语、定义、缩略语

3.1 术语和定义

GB/T 20984—2007和GB/T 30976.1—2014界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出了GB/T 20984—2007和GB/T 30976.1—2014中的一些术语和定义。

3.1.1

验收 acceptance

风险评估活动中用于结束项目实施的一种方法,主要由被评估方组织机构,对评估活动进行逐项检验,以是否达到评估目标为接受标准。

[GB/T 30976.1—2014,定义3.1.4]

3.1.2

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)。

[IEC 62443-1-1,定义3.2.2]

3.1.3

可用性 availability

数据或资源能被授权实体按要求访问和使用的特性。

[GB/T 20984—2007,定义3.3]

3.1.4

鉴别　authentication

验证实体所声称的身份的动作。

3.1.5

边界　border

物理或者逻辑安全区域的边或者边界。

[IEC 62443-1-1,定义 3.2.16]

3.1.6

信道　channel

在通信管道内建立的特定的通信链接。

[IEC 62443-1-1,定义 3.2.19]

3.1.7

保密性　confidentiality

数据所具有的特性,即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[GB/T 20984—2007,定义 3.5]

3.1.8

控制系统网络安全　control system security

以保护控制系统的可用性、完整性、保密性为目标,另外也包括实时性、可靠性与稳定性。

3.1.9

服务拒绝　denial of service

阻止或者中断系统资源的授权访问或者挂起系统的操作的功能。

注:在工业自动化和控制系统的情况下,服务拒绝是指过程功能的损失,而不仅仅是数据通信的损失。

[IEC 62443-1-1,定义 3.2.42]

3.1.10

识别　identify

对某一评估要素进行标识与辨别的过程。

[GB/T 30976.1—2014,定义 3.1.2]

3.1.11

网络安全风险　security risk

人为或自然的威胁利用系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

[GB/T 20984—2007,定义 3.6]

3.1.12

完整性　integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

[GB/T 20984—2007,定义 3.10]

3.1.13

制造执行系统　manufacturing execution system

生产规划和跟踪系统,用于分析和报告资源可用性和状态、规划和更新订单、收集详细的执行数据,

例如材料使用、人力使用、操作参数、订单和装置状态及其他关键信息。

注 1：此系统访问材料清单、工艺路线和其他来自于基础企业资源规划系统的数据，典型用于实时车间作业报告和监视将活动数据反馈给基础系统的过程。

注 2：更多的信息参见 IEC 62264-1。

3.1.14

组织　organization

由作用不同的个体为实施共同的业务目标而建立的机构。一个单位是一个组织，某个业务部门也可以是一个组织。

[GB/T 20984—2007，定义 3.11]

3.1.15

残余风险　residual risk

采取了安全措施后，信息系统仍然可能存在的风险。

[GB/T 20984—2007，定义 3.12]

3.1.16

风险接受　risk acceptance

接受风险的决定。

[GB/T 30976.1—2014，定义 3.1.7]

3.1.17

风险分析　risk analysis

系统地使用信息来识别风险来源和估计风险。

[GB/T 30976.1—2014，定义 3.1.8]

3.1.18

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。

3.1.19

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。

3.1.20

安全事件　security incident

系统、服务或网络的一种可识别状态的发生，它可能是对安全策略的违反或防护措施的失效，或未预知的不安全状况。

[GB/T 20984—2007，定义 3.14]

3.1.21

网络安全措施　security measure

为保护资产、抵御威胁、减少脆弱性、降低安全事件的影响而实施的各种实践、规程和机制。

3.1.22

威胁　threat

可能导致对系统或组织危害的不希望事故潜在起因。

[GB/T 20984—2007,定义 3.17]

3.1.23

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保策略。

[GB/T 30976.1—2014,定义 3.1.1]

3.2　缩略语

下列缩略语适用于本文件。

CL:能力等级(Capability Level)

DCS:集散控制系统(Distributed Control System)

DoS:服务拒绝(Denial of Service)

IACS:工业自动化和控制系统[Industrial Automation and Control System(s)]

MES:制造执行系统(Manufacturing Execution System)

ML:管理等级(Management Level)

SL:安全等级(Security Level)

4　DCS 安全风险评估概述

4.1　DCS 系统概述

4.1.1　通用 DCS 系统应用的网络结构

通常 DCS 系统应用是一种纵向分层的网络结构,自上到下依次为过程监控层、现场控制层和现场设备层。各层之间由通信网络连接,层内各装置之间由本级的通信网络进行通信联系,其典型网络结构如图 1 所示。本部分主要对 DCS 系统中的过程监控层、现场控制层网络和现场设备层网络的安全要求进行了要求。各层的说明如下:

——过程监控层:以操作监视为主要任务,兼有部分管理功能。这一级是面向操作员和控制系统工程师的,因而这一级配备有技术手段齐备,功能强的计算机系统及各类外部装置,特别是显示器和键盘,以及需要较大存储容量的硬盘或软盘支持,另外还需要功能强的软件支持,确保工程师和操作员对系统进行组态、监视和操作,对生产过程实行高级控制策略、故障诊断、质量评估。

——现场控制层:现场控制层的主要功能包括:采集过程数据,进行数据转换与处理;对生产过程进行监测和控制,输出控制信号,实现模拟量和开关量的控制;对 I/O 卡件进行诊断;与过程监控层等进行数据通信。

——现场设备层:现场设备层的主要功能包括:采集控制信号、执行控制命令,依照控制信号进行设备动作。

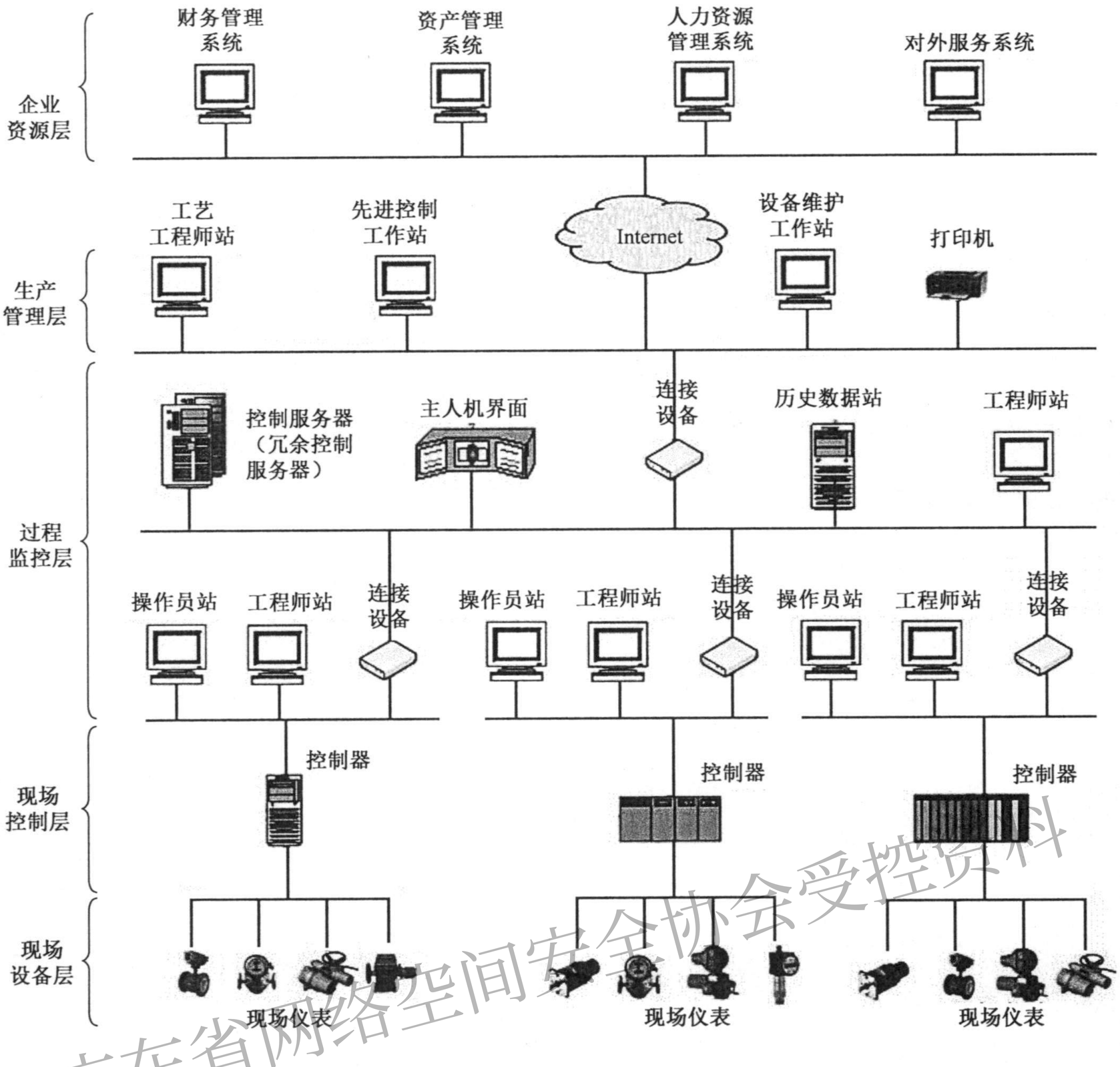


图 1　典型 DCS 系统应用的网络结构示意图

注：将监控层以下的现场控制层网络进行细分，其中现场控制层网络主要包括 DCS 控制器和控制器通信模块、I/O 模块等，现场设备层网络包括现场智能仪表、执行机构、传感器等现场设备和仪表。

4.1.2　DCS 运行安全总体要求

4.1.2.1　实时性要求

DCS 应具备实时响应能力，不允许存在不可接受的延迟和抖动。

4.1.2.2　可用性要求

DCS 具有高可用性需求，一般不允许重启系统，所以部署前需要详尽的测试，在生产过程中的中断操作需要提前计划。

4.1.2.3　安全性要求

DCS 具有安全性要求。DCS 一般部署在重要的生产领域，系统不允许出现安全事故。

4.1.2.4　完整性要求

DCS 具有完整性要求，不允许未授权用户或者恶意程序对信息和数据的修改。

4.1.2.5 稳定性要求

DCS具有稳定性要求。DCS一旦工作不稳定，将存在严重的威胁，导致大批的不合格产品流出，而且加剧设备的损耗等。

4.1.2.6 高可靠性要求

DCS具有可靠性要求。DCS能够在规定的条件下，长期正常执行其设定的控制功能，期间不允许发生停车，且具有很好的耐久性和可维修性。

4.2 DCS安全风险评估流程框架与流程

4.2.1 安全要素及其关系

DCS安全要素的关系如图2所示。

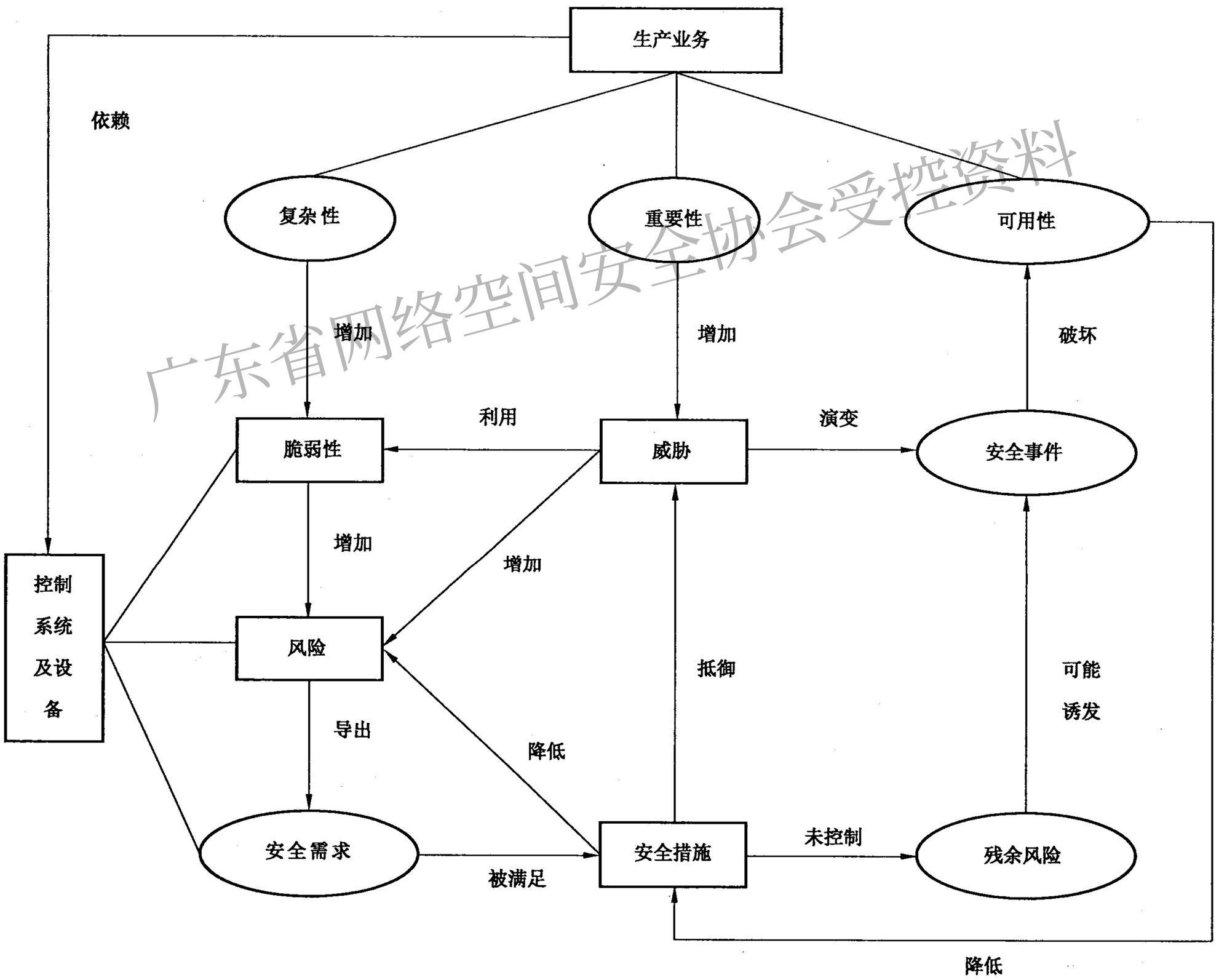


图2 安全风险评估要素关系图

图2中矩形框部分是安全风险评估的基本要素，椭圆部分是基本要素相关的属性。DCS系统安全风险评估主要围绕生产业务、控制系统及设备、脆弱性、威胁、风险、安全措施等基本要素进行，但评估过

程中需要充分考虑业务的复杂性、重要性、可用性、安全事件、残余风险、安全需求等与基本要素相关的属性。

图 2 中基本要素及属性之间主要存在以下关系：

a) 生产业务最终靠工业控制系统及设备实现，依赖程度越高，要求控制系统风险越小；

b) 生产业务的复杂性会影响控制系统的脆弱性，工艺控制环节越复杂，工业控制系统存在的脆弱性越多，脆弱性之间潜在的关联性越强；

c) 生产业务的重要性会影响控制系统的所受到的威胁，负责的工艺流程越重要，其受到的威胁最大；

d) 控制系统自身的脆弱性直接影响控制系统所存在的风险，脆弱性越多，其面临的风险越多；

e) 威胁利用脆弱性，演变为安全事件，损坏控制系统或设备，破坏生产业务的可用性要求；

f) 通过控制系统所面临的风险可以获得系统的安全需求，以满足安全需求为目标，可以确定系统采用的安全措施，采用安全措施可以降低风险，而未能被安全措施控制的残余风险，仍然有可能诱发安全事件，破坏系统正常运行；

g) 控制系统遭受的威胁越多，其可能面临的风险也越大；

h) 生产业务的可用性要求越高，控制系统可采用的安全措施越少。

4.2.2 DCS 安全分析的原理

DCS 风险分析涉及 DCS 资产(软\硬件等)、工艺特征、DCS 的脆弱性与 DCS 的威胁四大要素，如图 3 所示。风险分析的主要内容包括：

a) 对 DCS 资产进行识别，确认与识别 DCS 的系统范围、系统结构、网络结构、采用的通信协议、关键部位的安全防护系统，列举构成 DCS 的设备清单，并对设备进行分组，分析设备间的关联关系、通信协议、设备开放的端口和服务等，以确定 DCS 评估的对象和范围、并整理通信设备的运行和安全特征；

b) 对 DCS 所处生产环境的工艺流程的特征进行识别，分析确定生产工艺流程各产品生产环节中的重要性和复杂度，该工业过程中可能发生的危险事件(爆炸、漏液、释放有毒气体等)，及其可能造成的影响以及影响范围；

c) 对 DCS 的脆弱性进行识别，综合考虑 DCS 在控制方案、防护措施等技术与管理上的脆弱性进行脆弱性梳理，并对其被利用的可能性和严重性、存在的原因进行深入分析；

d) 对 DCS 威胁进行识别，列举系统面临的潜在威胁和威胁的来源，以及发生过的历史安全事件，在此基础上对各种潜在威胁发生的可能性、影响及其后果进行定性或定量评价；

e) 根据威胁及利用脆弱性的难易程度判断安全事件发生的可能性；

f) 根据脆弱性的严重程度及安全事件所作用的 DCS 部位来计算安全事件造成的影响和损失；

g) 根据安全事件发生的可能性以及安全事件出现后的损失，评估安全事件对企业的风险等级；

h) 参照风险等级定义、国家的法律法规及相关标准和公司安全需求，确定 DCS 应具备的管理等级和系统安全能力等级，然后依据 DCS 安全实施流程对系统进行评估，并确定评估结果。

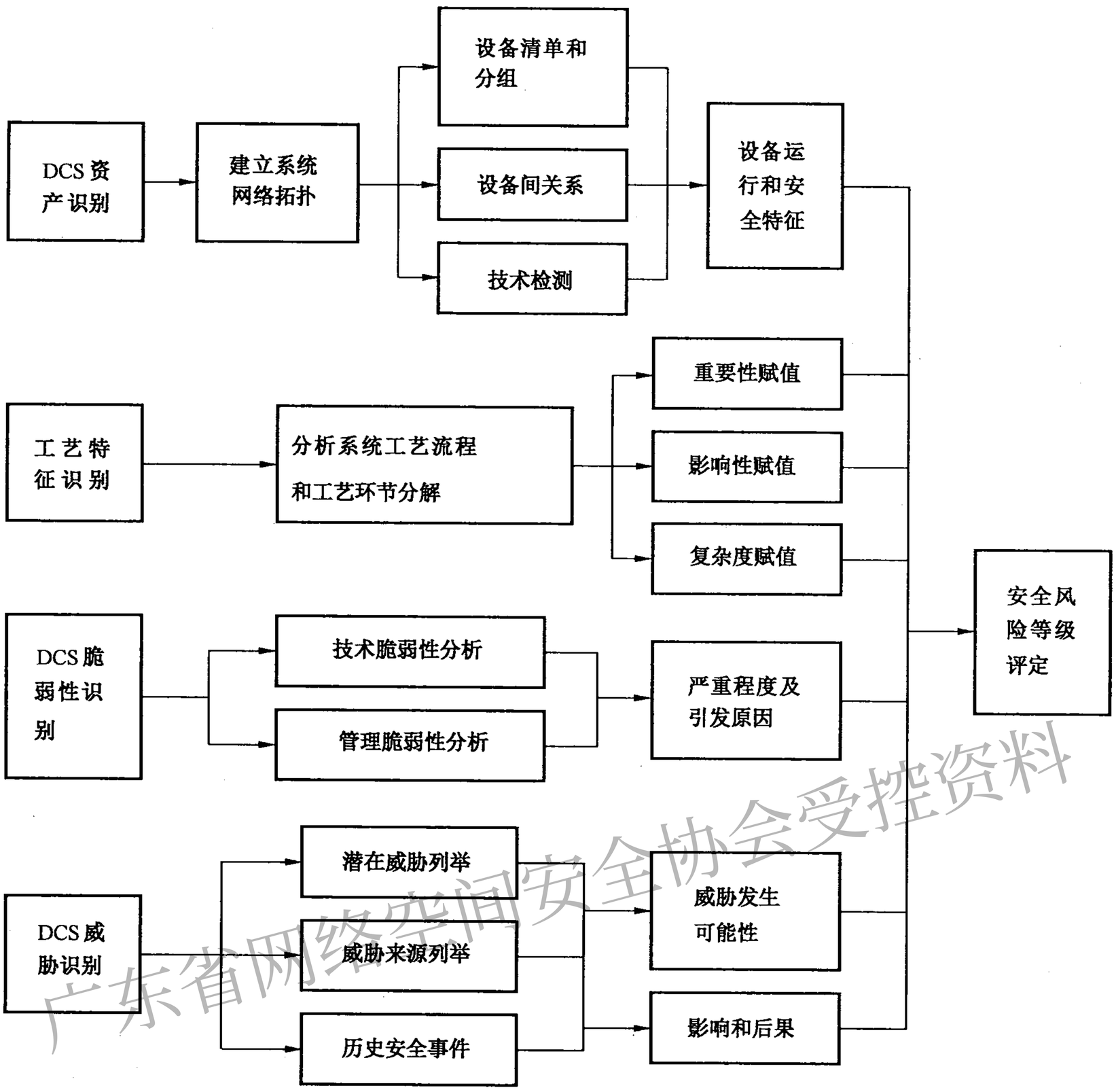


图 3　风险分析原理示意图

4.2.3　DCS 安全风险评估实施流程

DCS 安全风险评估实施的具体流程如图 4 所示。首先对 DCS 系统的设备、工艺特征、脆弱性和面临的威胁进行识别并形成评估过程文档，然后识别系统当前安全措施，并结合上述已识别的系统特征对当前安全措施进行有效性验证，形成评估过程文档，然后对系统的风险进行计算和验证，如果评估得到的风险无法被评估系统接受，需增加安全措施，然后重新评估安全措施的有效性，直至系统风险可以被系统接受为止。

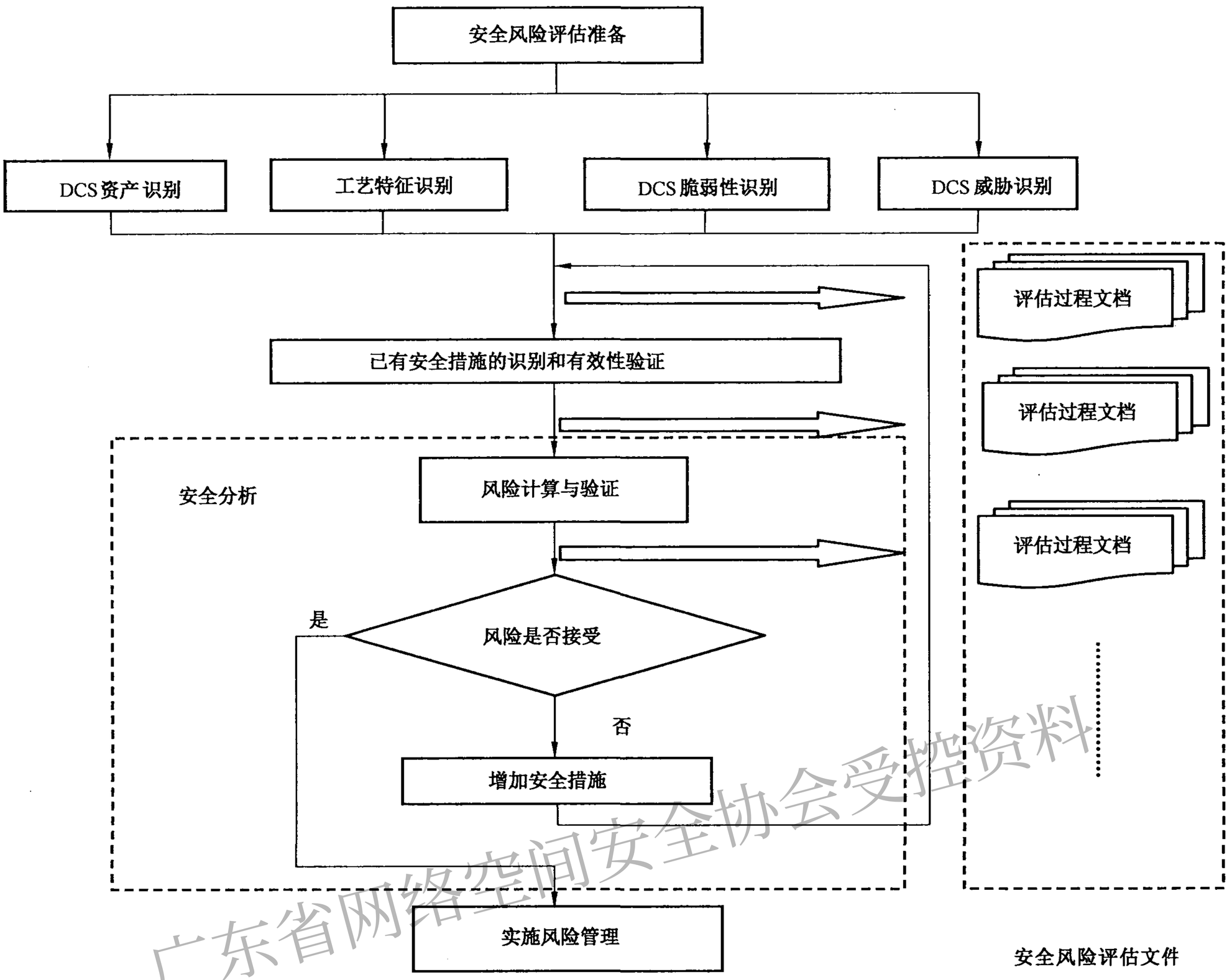


图 4　DCS 安全风险评估实施流程

4.3　评估结果

4.3.1　风险可接受程度

根据工业控制系统的组织机构管理以及系统(技术)能力评估系统的风险,针对风险产生的结果采用网络安全等级(security level, SL)来表示风险管理过程中的不同风险,这样的结果比较直观,根据SL来确定组织机构的整体安全策略和相应的技术防御措施。同时,组织机构应当综合考虑风险控制成本与风险造成的影响,提出一个可接受的风险范围。对某些资产的风险,如果风险计算值在可接受的范围内,则该风险是可接受的,即残余风险在系统允许风险之内说明系统是健壮的,应保持已经有的安全措施;如果风险评估值在可接受的范围外,但是低于不可接受范围的下限值,则该风险需要采取安全措施降低、并控制风险到可接受的程度;如果评估的风险从经济,健康,安全和环境方面进行评估后发现风险是不可以接受的,那么就要对现有的系统重新设计网络安全程序。见图 5。其中的风险评估的工具和方法参见附录 B。

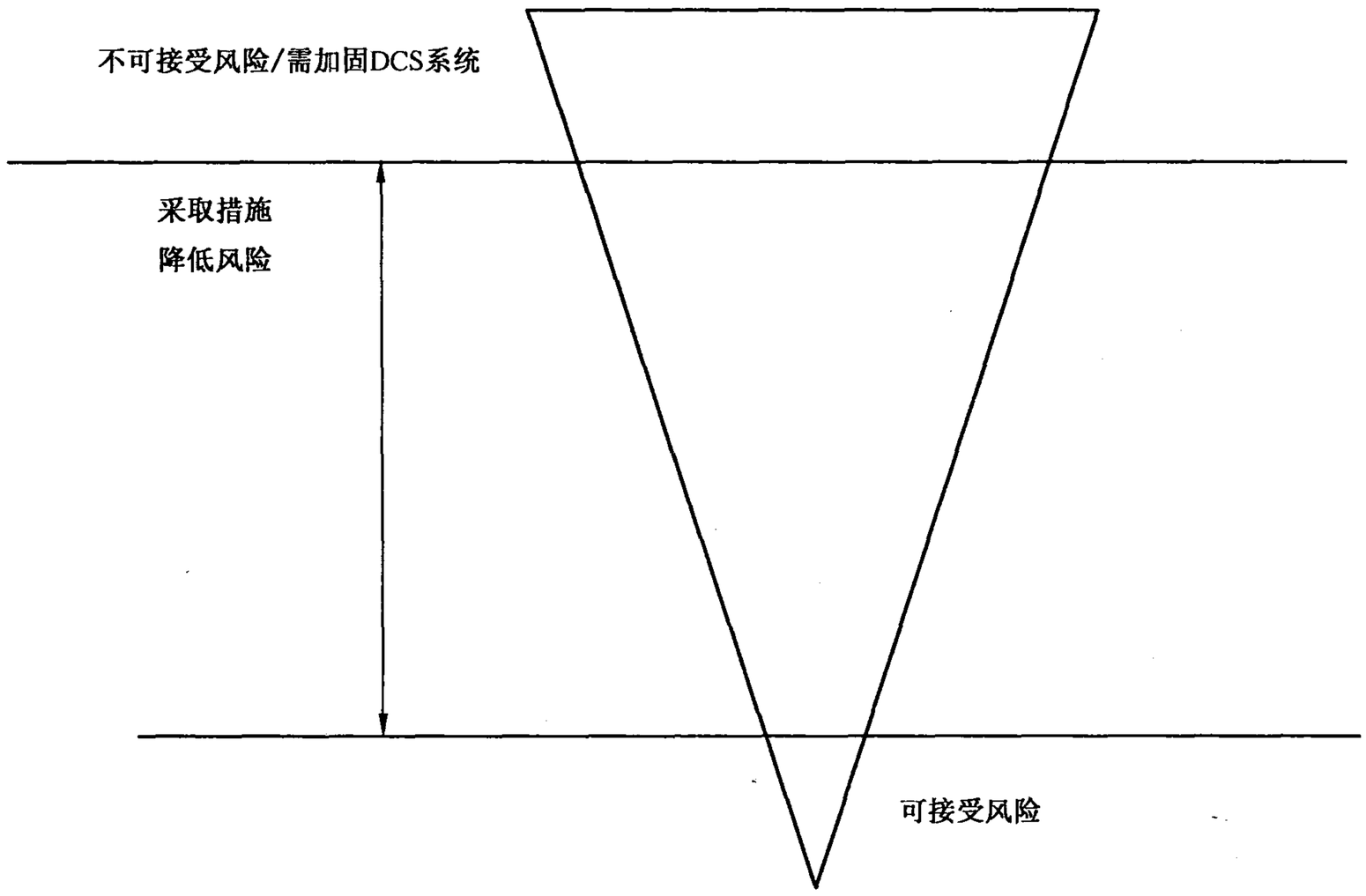


图 5　风险可接受的程度

风险等级处理的目的是为风险管理过程中对不同风险的直观比较，以确定组织安全策略。组织应当综合考虑风险控制成本与风险造成的影响，提出一个可接受的风险范围。对某些资产的风险，如果风险计算值在可接受的范围内，则该风险是可接受的风险，应保持已有的安全措施；如果风险评估值在可接受的范围外，即风险计算值高于可接受范围的上限值，是不可接受的风险，需要采取安全措施以降低、控制风险。另一种确定不可接受的风险的办法是根据等级化处理的结果，设定可接受风险值的基准，达到相应等级的风险都进行处理。

注 1：DCS 利用可供选用的各种配置的功能和元件执行要求的任务，系统的该特征难以仅通过评定每一个单独功能和元件的特征来综合评估一个系统的网络安全能力；

注 2：DCS 网络安全风险评估的深度在很大程度上取决于系统的复杂程度、生产工艺过程复杂度以及边界影响条件以及评估的目的；

注 3：评估的范围可以采用汇总统计表的形式，在一个轴线上列出系统的特性，另一轴线上列出需考虑的安全影响条件。统计表的方格可用于记录对于每一种系统特性哪一种安全影响条件需要加以考虑。

4.3.2　风险评估结果

评估者应根据所采用的风险计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。表 1 提供了一种风险等级划分方法。

表 1　DCS 风险等级的划分

等级	标识	描　述
5	很高	一旦发生将产生非常严重的经济或社会影响，如组织信息破坏、严重影响组织正常经营，经济损失重大、社会影响恶劣
4	高	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定的手段很快能解决
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补

5 评估工作准备

5.1 概述

DCS 系统安全风险评估是对 DCS 所处的系统网络层级结构、数据采集与传输协议、DCS 硬件设备及模块、DCS 监控软件、OPC 软件、网络层级间的防护措施、安全防护设备、安全管理措施及执行情况、生产工艺及流程、人员及场地特征、安全应急响应组织结构等进行全面的安全分析。同时，结合不同行业的具体工业安全需求对 DCS 中的高危性业务(可能存在爆炸、有毒、高腐蚀性气体或严重污染环境液泄漏的业务)关键流程或关键业务的关联性业务、关键业务或控制站进行独立评估。风险评估的准备是整个风险评估过程有效性的基础。组织实施风险评估是一种全面的系统工作，其结果将受到生产行业、业务流程、安全需求、系统规模、系统配置、管理制度等方面的影响。因此，在风险评估实施前，应：

a) 确定 DCS 风险评估的目标；
b) 确定 DCS 风险评估的范围；
c) 组建评估管理与实施团队；
d) 进行系统调研；
e) 确定评估依据和方法；
f) 获得最高管理者对风险评估工作的支持。

5.2 确定 DCS 评估目标

识别与记录组织所应用的 DCS 在技术与管理上的潜在不足，以及可能造成的安全风险(包括人员、环境、社会以及国家安全方面的影响)，维护与保证组织在业务持续性发展上的特定安全需要。

评估的目标，由被评估方给出基本要求，评估方进行调研后，提出具体评估子目标，双方协商后确定具体评估目标。

5.3 确定评估范围

DCS 评估涉及 DCS 的硬件、软件、网络架构、网络协议、现场设备、防护措施、应急响应方案等，重点关注可能会造成严重的人员、环境或社会危害的 DCS 关键生产部位及其关联部位、DCS 核心重要业务流程部位、DCS 关键网络通信部位的系统、人员、管理机构、责任部门等。

5.4 组建评估团队

DCS 评估团队应由管理层、生产工艺工程师、IT 技术人员、现场人员(包括技术人员、操作人员、维护人员等)以及被评估企业的评估负责人等人员组成。可组建由评估方、被评估方领导和相关部门负责人参加的安全风险评估领导小组，聘请第三方相关专业的技术专家和技术骨干组成专家小组。

评估实施团队应做好评估前的表格、文档、检测工具等各项准备工作，进行安全风险评估技术培训和保密教育，制定 DCS 评估过程管理相关规定。可根据被评估方要求，双方签署保密合同，必要时签署个人保密协议。

5.5 系统调研

拟采用问卷调查、现场面谈相结合的方式进行调研，调研内容应至少包括：

a) 企业主要生产业务类型、原料、加工或生产工艺过程、产品及其质量要求；
b) 企业网络架构和网络连接情况(包括外网、内网)；
c) 企业的 DCS 应用情况(主要的控制器、智能设备、传感器、执行器、应用软件、网络设备的型号、安装时间)；

d) DCS 以往安全事故；
e) DCS 网络安全管理制度、责任或管理部门；
f) 关键生产业务部门或部位的运行过程及其相关人员、管理制度、接口情况；
g) 企业组织已经实施的工业控制网络安全措施与规程；
h) 其他企业组织已实施的工业控制网络安全措施与规程的经验；
i) 以往 DCS 的安全风险评估记录与结果；
j) 其他。

5.6 确定评估依据与方法

DCS 安全风险评估依据包括(但不限于)：

a) 现行标准；
b) 行业主管机关的业务系统要求和制度；
c) 系统互联单位的安全要求；
d) 控制系统本身的高实时性、高可靠性与高可用性等要求；
e) 企业自定义的安全需求和要求。

在 DCS 评估方法的选取上，应考虑 DCS 的特殊安全特性，包括网络安全事件发生的不规律、安全事件历史数据的缺乏、脆弱性一旦公开所带来的激增式威胁等；在技术手段的选择中，要充分考虑 DCS 不可停车、实时性和稳定性的运行要求，保证不因评估检测影响当前系统的正常运行。同时根据组织长期的业务经验，确定可用的安全风险评估计算方法(定量或定性、基于场景或基于资产等)，必要时可开展评估依据和评估方法的评审。

5.7 制定评估方案

制定评估方案的目的是为后续评估活动的实施提供一个总体计划，用于指导实施方开展后续工作。评估方案的内容一般包括(但不仅限于)：

a) 组织架构：包括评估团队成员、组织结构、角色、责任等内容；
b) 工作计划：评估各阶段的工作计划，包括工作内容、工作形式、以及希望获得的支持、预期工作成果等内容；
c) 时间进度安排：项目实施的时间进度安排。

5.8 获得支持

上述所有内容确定后，应形成较为完整的安全风险评估实施方案，得到组织最高管理部门的支持、批准；对管理层和技术人员进行传达，在组织架构范围内就风险评估相关内容进行培训，以明确有关人员在评估中的任务。

6 DCS 安全要素识别

6.1 DCS 资产识别

6.1.1 建立资产清单与分组

DCS 资产识别的目的是识别关键的 DCS 设备以及 DCS 中给系统带来潜在风险的设备部件，及其风险特性。如果对 DCS 的设备与网络的部署缺乏一个清晰的了解，将很难定位哪些位置存在风险。评估小组会同 DCS 工作人员应该对不同类别的设备，包括现场的以及远程的进行识别。应重点关注但不局限于控制系统、测量系统、使用 HMI 的中央监控系统，还应包括生产控制操作区域，以及供电区与废

物处理设施等。表 2 是根据功能的不同对 DCS 设备进行的一种分类。

表 2　DCS 资产分类

分　类	示　例
DCS 硬件	过程监控层硬件：工程师站、操作员站、OPC 服务器、HMI 控制台、数据库服务器、远程访问服务器、Web 服务器等设备，以及与现场设备链接的专用设备
	现场控制层硬件：DCS 控制器、IO 模块、RTU、智能现场仪表等
	安全设备：安全仪表系统 SIS 及其相关装置
DCS 应用软件	监控软件：安装在控制台上的图形用户软件、人机交互软件、SCADA 软件等
	编程软件：组态软件
	生产优化软件：MES 软件、资产管理软件、先进控制软件
	系统软件：操作系统、数据库管理系统等
安全保障系统	防火墙、防病毒软件、防恶意(malware)软件、入侵检测系统、入侵防御系统、身份认证系统、DCS 安全审计系统、网络安全统一管理系统等
DCS 数据通信与接入	路由器、交换机、VPN、远程接入方式、无线接入
DCS 网络架构	DCS 网络的拓扑(网络边界、设备连接)、冗余网络配置、边界访问控制、网络带宽等
服务	网络服务：各种网络设备、设施提供的网络连接服务 信息服务：对外依赖该系统开展的各类数据采集与共享服务
人员	掌握重要信息和核心业务的人员，如总工程师、车间主任、制造科长等

在对资产进行识别时需要对其工作原理、基本配置和技术参数进行了解、记录和测试。测试可以为线下、近似或在模拟控制系统的环境下进行，一旦影响正常的 DCS 运行的实时性、可靠性和安全性，则不允许继续测试。

6.1.2　分析检查网络拓扑

在对被评估系统进行详细评估前，应对待评估系统的范围或边界、设备的互联互通关系、设备间通信的方式、通信协议、通信端口进行清晰的了解。

6.1.3　DCS 设备安全属性赋值

可用性、完整性、保密性是评价 DCS 设备的三个安全属性。风险评估中 DCS 设备的价值不是以 DCS 设备的经济价值来衡量，而是由 DCS 设备在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。安全属性达成程度的不同将使 DCS 设备具有不同的价值，而 DCS 设备面临的威胁、存在的脆弱性、以及已采用的安全措施都将对资产安全属性的达成程度产生影响。

具体可用性、完整性、保密性赋值细节见 GB 20984—2007 中的 5.2.2。

6.2　DCS 脆弱性

6.2.1　DCS 脆弱性内容

DCS 脆弱性是指 DCS 系统或部件固有的弱点或后期安装、实施和配置不当造成的弱点，可能来自于有意的设计，也可能来源于错误理解运行环境的偶然情况。环境变化、技术变化、系统部件的故障，部件替换、人员流动或更高威胁事件的发生，可能触发系统中的弱点，使得包含脆弱性的工业自动化控制

系统更加容易受攻击。脆弱性不仅仅局限于电子或网络系统，还包括管理制度、组织结构等，所以不仅要了解物理（包括人员）和电子脆弱性之间的相互作用，熟悉企业对 DCS 系统的相关管理制度和流程也至关重要。

DCS 脆弱性的数据应来自于资产的所有者、DCS 操作者，以及相关业务领域和 DCS 软硬件方面的专业人员等。脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、人工测试等。

脆弱性识别主要从技术和管理两个方面进行，具体的脆弱性识别对象和实施过程参见集散控制系统（DCS）风险与脆弱性检测要求。

6.2.2 DCS 脆弱性赋值

可以根据对工艺的影响程度、技术实现的难易程度、脆弱性的流行程度，采用等级方式对已识别的脆弱性的严重程度进行赋值。对某个资产，其技术脆弱性的严重程度还受到组织管理脆弱性的影响。因此，资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。

脆弱性严重程度可以进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。表 3 提供了脆弱性严重程度的一种赋值方法。

表 3 脆弱性严重程度赋值示例

赋值	标识	定 义
1	较小	如果被利用，将对 DCS 设备造成较小影响
2	一般	如果被利用，将对 DCS 设备造成一般影响
3	严重	如果被利用，将对 DCS 设备造成严重影响
4	特大	如果被利用，将对 DCS 设备造成重大影响

6.3 威胁识别

6.3.1 威胁分类

威胁可能来源于组织内部或组织外部，表现为不同形式，但最为常见的三种形式是：

a) 疏忽或误操作：某人对正确的系统控制流程、工艺过程和安全策略不熟悉，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：对控制系统、工业应用软件、工艺过程、控制参数、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；

c) 蓄意的破坏和攻击：个人或组织通过网络或内部人员对控制系统进行破坏或窃取信息或数据，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。

6.3.2 威胁赋值

判断威胁出现的频率是威胁赋值的重要内容，评估者应根据经验和（或）有关的统计数据来进行判断。在评估中，需要综合考虑以下三个方面，以形成在某种评估环境中各种威胁出现的频率：

a) 以往安全事件报告中出现过的威胁及其频率的统计；

b) 实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；近年来相关组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警；

c) 可以对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。等级数

值越大，威胁出现的频率越高。

表 4 提供了威胁出现频率的一种赋值方法。在实际的评估中，威胁频率的判断依据应在评估准备阶段根据历史统计或行业判断予以确定。

表 4　威胁赋值表

赋值	标识	定　义
1	低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生
2	中	出现的频率中等（或＞1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过
3	高	出现的频率较高（或≥1 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过
4	很高	出现的频率很高（或≥1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过

6.4　工艺特征识别

6.4.1　重要性赋值

工艺重要性应依据该工艺环节遭受破坏后，对整个工业生产或企业经营的影响程度进行综合评定得出。综合评定的方法可以根据组织自身的特点，以对生产和经营过程影响的严重等级作为工艺重要性的最终赋值结果。本部分中，工艺重要性分为四级，级别越高表示工艺对生产过程和企业经营影响越严重，如表 5 所示。组织也可以根据自身实际情况确定工艺重要性的赋值依据和取值。生产业务工艺重要性越高，受到的威胁频率会越高。

表 5　系统工艺重要性定义示例

赋值	标识	定　义
1	很低	不重要，其遭受破坏对生产活动的影响很小，对组织造成很小的损失，甚至可以忽略不计
2	低	不太重要，其遭受破坏可能直接影响生产活动的长期稳定性，会给组织长期正常经营带来安全风险，对组织造成较低的损失
3	中	重要，其遭受破坏可能直接影响核心生产活动，可能导致组织正常经营中的核心业务中断，对组织造成比较严重的损失
4	高	非常重要，其遭受破坏可能导致整个生产活动停止，且没有可替代方案。可能导致组织正常经营中断，给组织造成非常严重的损失

6.4.2　影响性赋值

工艺影响性应依据该工艺环节遭受破坏后，对人员、环境、地区公共财产和国家安全等可能造成的影响进行评定得出。评定的方法可以根据生产工艺过程中各环节的高温、高压、有毒原料生产等特点，以其实际遭受攻击后对外部造成后果的严重程度作为最终赋值结果。本部分中，工艺影响性分为四级，级别越高表示工艺环节遭受破坏后，对外界的影响越严重，如表 6 所示。组织也可以根据自身实际情况确定工艺影响性的赋值依据和取值。生产业务工艺影响性越高，设备价值就越高。

表 6　DCS 系统工艺影响性定义示例

赋值	标识	定　义
1	较小	工艺环节失控，可能对人员安全、环境、地区公共财产安全造成较小范围的破坏
2	小	工艺环节失控，可能对人员安全、环境、地区公共财产安全造成小范围的破坏
3	中	工艺环节失控，可能对人员安全、环境、地区公共财产安全造成局部性的破坏
4	大	工艺环节失控，可能对人员安全、环境、地区公共财产安全造成大面积的破坏，甚至对国家安全造成影响

6.4.3　复杂度赋值

工艺复杂度由工业生产过程的复杂程度和控制系统的复杂程度来综合评定得出。评定的方法可以根据生产工艺过程中工艺环节复杂度、工序数、系统及子系统复合状态、系统的阶段和层次等属性建模进行综合描述。本部分对工艺复杂度给出一个示例，以工艺环节、工序数量、系统层次和系统节点数为衡量依据，将工艺复杂度分为四级，级别越高表示工艺过程及其实现系统越复杂，存在潜在脆弱性可能性越高，如表 7 所示。组织也可以根据自身所处工业行业的工艺特点，建模确定工艺复杂度的评估依据和取值。生产业务工艺的复杂性会影响控制系统的脆弱性，工艺控制环节越复杂，工业控制系统存在的脆弱性越多，脆弱性之间潜在的关联性越强。

表 7　DCS 系统工艺复杂度定义示例

赋值	标识	定　义
1	简单	工艺过程中，工艺环节不大于 3 个，总工序不超过 20 个，系统层次最多为 2 级，I/O 点数不大于 200 点
2	一般	工艺过程中，工艺环节不大于 3 个，总工序不超过 20 个，系统层次最多为 3 级，I/O 点数不大于 1 000 点
3	复杂	工艺过程中，工艺环节不大于 5 个，总工序不超过 50 个，系统层次最多为 3 级，I/O 点数不大于 5 000 点
4	非常复杂	工艺过程中，工艺环节不少于 6 个，总工序超过 50 个，系统层次超过 3 级，I/O 点数大于 5 000 点

7　DCS 风险分析

7.1　风险计算原理

DCS 安全风险由威胁利用控制系统的脆弱性导致安全事件发生的可能性与后果影响程度来共同决定。综合安全事件发生的可能性与安全事件的后果影响程度，判断安全事件对组织的影响。风险计算原理以下面的形式加以说明：

风险值＝R(A,P,T,V)或风险值＝W[L(Ps×T,Pc×V)×Pi×F(Ia,Va)]

其中，R 和 W 表示安全风险计算函数；A 表示 DCS 设备；P 表示 DCS 工艺特征(Pc 表示工艺特征的复杂性，Ps 表示工艺特征的重要性，Pi 表示工艺特征的影响性)；T 表示威胁；V 表示脆弱性；Ia 表示

安全事件所作用的DCS设备价值；Va表示脆弱性严重程度；L表示威胁利用DCS脆弱性导致安全事件发生的可能性；F表示安全事件发生所产生的损失。有以下三个关键计算环节：

a） 计算安全事件发生的可能性

根据威胁出现频率及脆弱性情况，计算威胁利用脆弱性导致安全事件发生的可能性，即：

安全事件发生的可能性＝ L(威胁出现频率，脆弱性)＝ L(Ps×T，Pc×V)

b） 计算安全发生后的损失

根据发生安全事件的DCS设备价值、脆弱性严重程度以及工艺特征影响性系数，计算安全事件发生后的损失，即：

安全事件的损失 ＝ Pi×F(DCS设备价值，脆弱性严重程度)＝ Pi×F(Ia，Va)

c） 计算风险值

根据计算出的安全事件发生的可能性以及安全事件的影响后果，计算风险值，即：

风险值＝W(安全事件发生的可能性，安全事件造成的损失)＝ W[L(Ps×T，Pc×V)×Pi×F(Ia，Va)]

评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。矩阵法通过构造一个二维矩阵，形成安全事件发生的可能性与安全事件的损失之间的二维关系；相乘法通过构造经验函数，将安全事件发生的可能性与安全事件的损失进行运算得到风险值。

附录B中列举了矩阵法和相乘法的风险计算示例。

7.2 风险处理计划

对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划。风险处理计划中明确应采取的弥补弱点的安全措施、预期效果、实施条件、进度安排、责任部门等。安全措施的选择应从管理与技术两个方面考虑。安全措施的选择与实施应参照网络安全的相关标准进行。

对于不可接受的风险在选择适当安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。残余风险的评估可以依据本部分提出的风险评估流程实施，也可做适当裁减。一般来说，安全措施的实施是以减少脆弱性或降低安全事件发生可能性为目标的，因此，残余风险的评估可以从脆弱性评估开始，在对照安全措施实施前后的脆弱性状况后，再次计算风险值的大小。某些风险可能在选择了适当的安全措施后，残余风险的结果仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步增加相应的安全措施。

8 安全风险评估文档记录

8.1 评估文档记录要求

记录安全风险评估过程的相关文档，可参照GB 20984—2007中的文档要求，应符合以下要求(但不仅限于此)：

a） 确保文档发布前是得到批准的；

b） 确保文档的更改和现行修订状态是可识别的；

c） 确保文档的分发得到适当的控制，并确保在使用时可获得有关版本的适用文档；

d） 防止作废文档的非预期使用，若因任何目的需保留作废文档时，应对这些文档进行适当的标识。

对于安全风险评估过程中形成的相关文档，还应规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

相关文档是否需要以及详略程度由组织的管理者来决定。

8.2 评估文档

评估文档是指在整个 DCS 安全风险评估过程中产生的评估过程文档和评估结果文档，包括(但不仅限于此)：

a) 安全风险评估方案：阐述评估的目标、范围、人员、评估方法、评估结果的形式和实施进度等；

b) 安全风险评估程序：明确评估的目的、职责、过程、相关的文档要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据；

c) DCS 设备识别清单：根据组织在评估程序文件中所确定的分类方法进行 DCS 设备识别，形成 DCS 设备识别清单，明确资产的责任人/部门，并对关键部位标注名称、描述、类型、重要程度；

d) 工艺特征识别文件，根据组织在评估程序文件中所确定的分类方法对生产工艺的重要性、影响性和复杂性进行识别赋值，形成 DCS 系统的生产工艺特征识别文件，其中要包括生产工艺过程、工艺环节和工序进行具体说明，明确工艺特征赋值的判断依据；

e) DCS 威胁列表：根据威胁识别结果，形成威胁列表，包括威胁名称、种类、来源、动机及出现的频率等；

f) DCS 脆弱性列表：根据脆弱性识别结果，形成脆弱性列表，包括具体弱点的名称、描述、类型及严重程度等；

g) DCS 已有安全措施确认表：根据对已采取的安全措施确认的结果，形成已有安全措施确认表，包括已有安全措施名称、类型、功能描述及实施效果等；

h) DCS 风险评估报告：对整个风险评估过程和结果进行总结，详细说明被评估对象、风险评估方法、资产、威胁、脆弱性的识别结果、风险分析、风险统计和结论等内容；

i) DCS 风险处理计划：对评估结果中不可接受的风险制定风险处理计划，选择确定适当的控制目标，选择适当的安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性；

j) DCS 风险评估记录：根据风险评估程序，要求风险评估过程中的各种现场记录可复现评估过程，并作为产生歧义后解决问题的依据。

附 录 A
（规范性附录）
DCS 生命周期各阶段的安全风险评估

A.1 网络安全等级生命周期

安全风险评估应贯穿于 DCS 系统生命周期的各阶段中。DCS 系统生命周期各阶段中涉及的安全风险评估的原则和方法是一致的，但由于各阶段实施的内容、对象、安全需求不同，使得安全风险评估的对象、目的、要求等各方面也有所不同。具体而言，在规划设计阶段，通过风险评估以确定系统的安全目标；在建设验收阶段，通过安全风险评估以确定系统的安全目标达成与否；在运行维护阶段，要不断地实施风险评估以识别系统面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现。因此，每个阶段安全风险评估的具体实施应根据该阶段的特点有所侧重地进行。有条件时，应采用安全风险评估工具开展评估活动。

图 A.1 描述了网络安全等级生命周期。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应审计和/或测试并升级对抗措施。

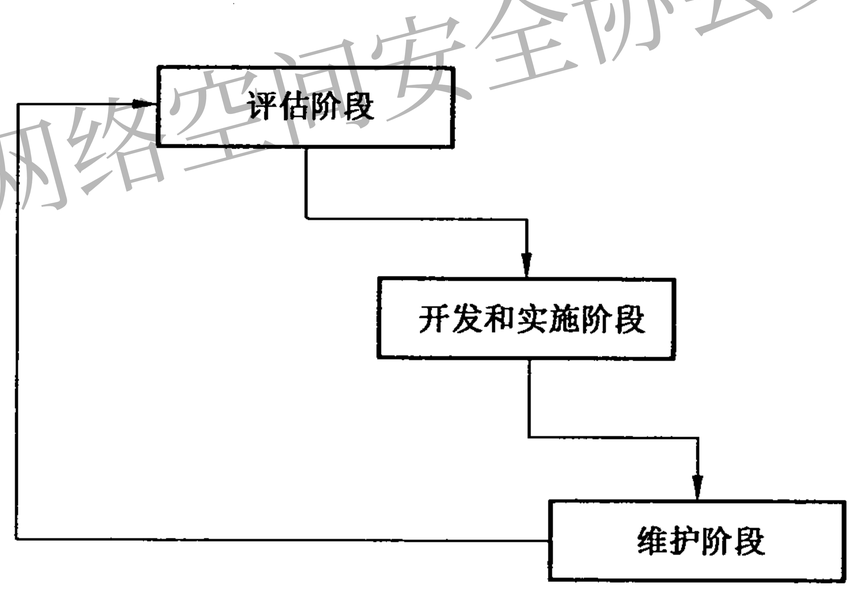


图 A.1 网络安全等级生命周期

A.2 评估阶段

DCS 安全生命周期的评估阶段包括图 A.2 所示的活动。在给区域分配安全目标前，应建立以下内容：

a) 区域边界；

b) 组织的风险容忍准则。

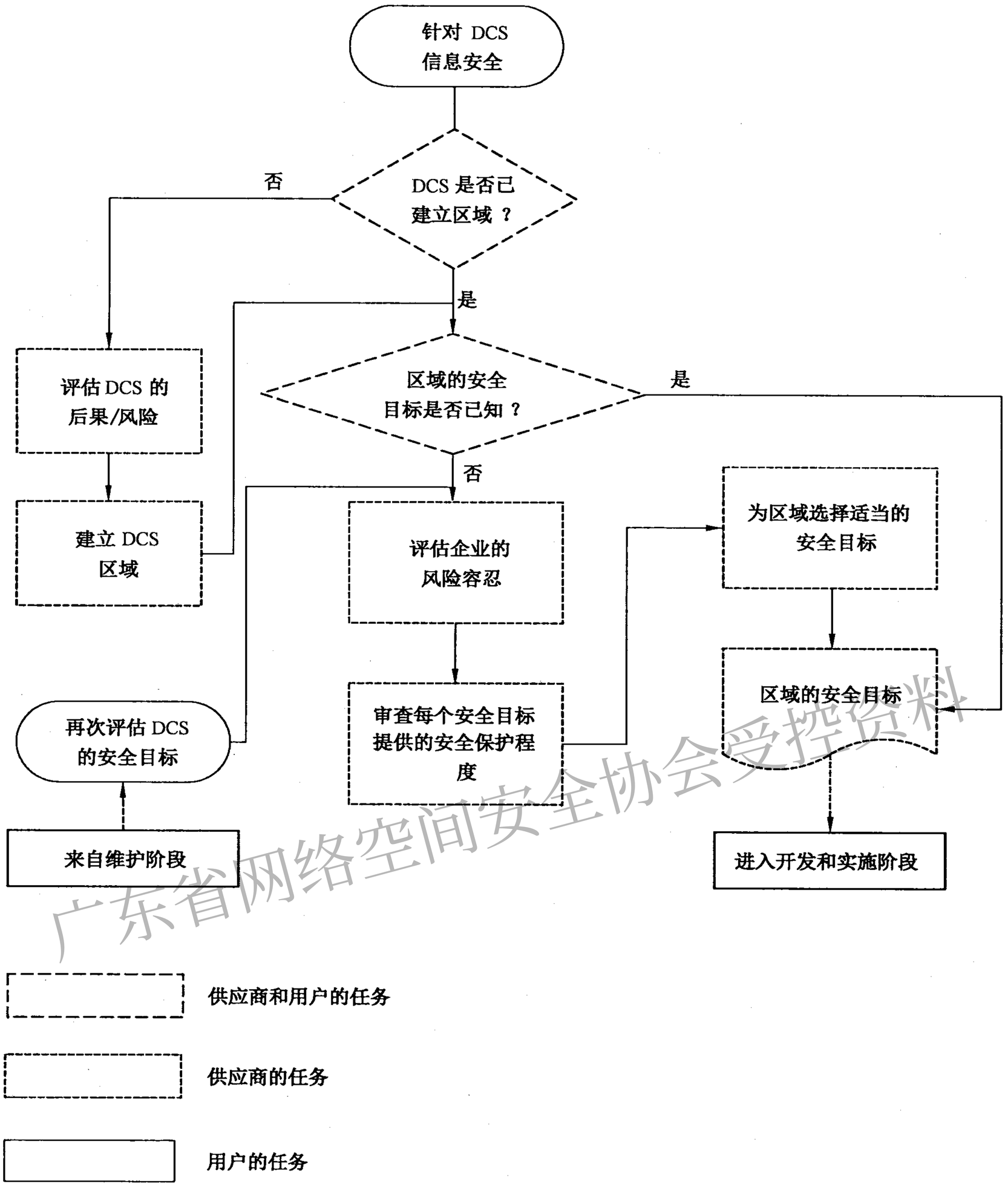


图 A.2　网络安全等级生命周期——评估阶段

A.3　开发和实施阶段

一旦在评估阶段给区域分配了安全目标，就应执行对抗措施以验证区域的安全目标大于或等于设定的安全目标。图 A.3 描述了在网络安全等级生命周期的实施阶段，有关新建或现有 DCS 区域的所有活动。在根据区域的安全要求确认系统后，其对应的安全目标就已确定。

与实施阶段相关活动的细节见 IEC 62443-2-1 的部分。

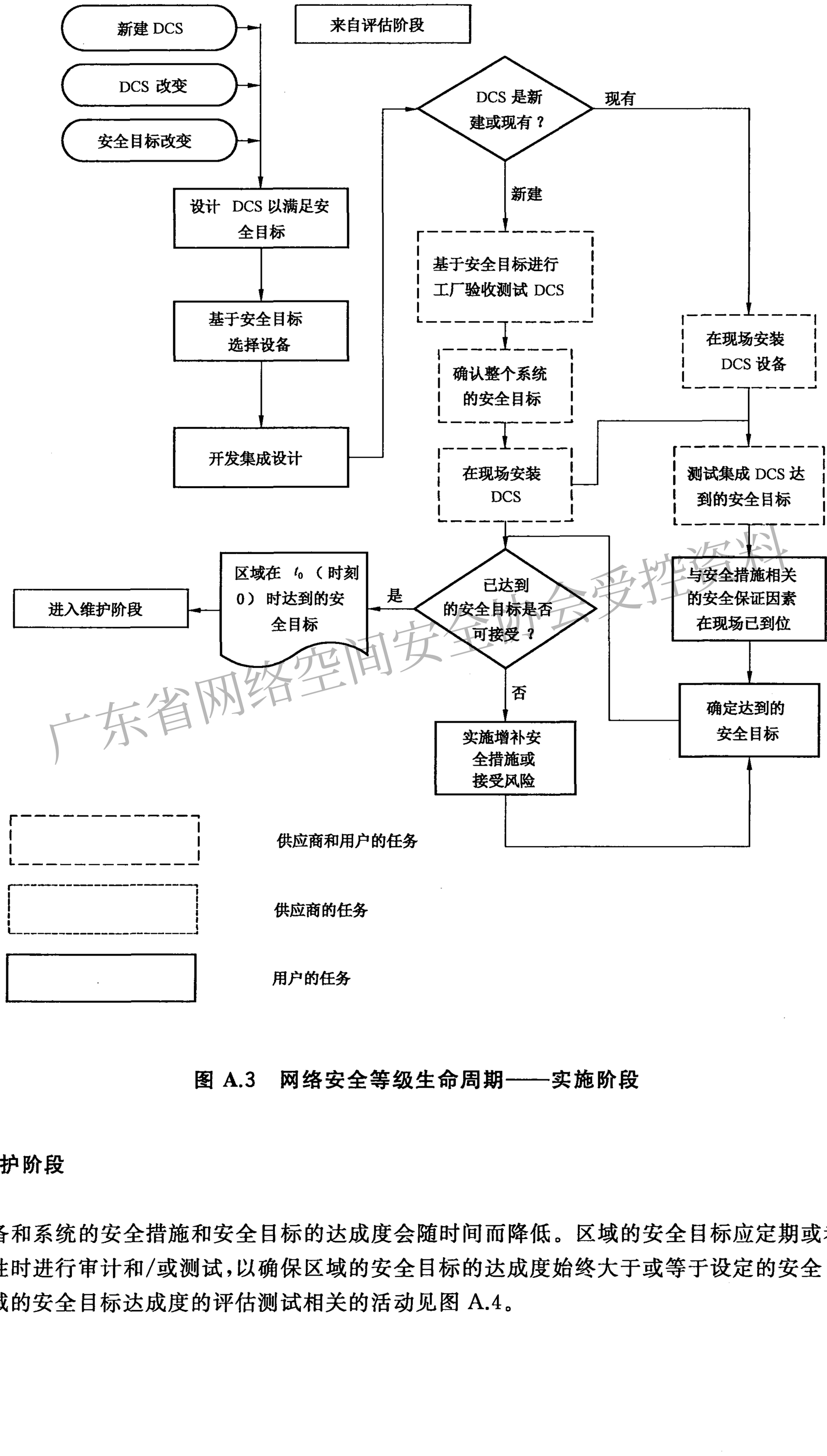
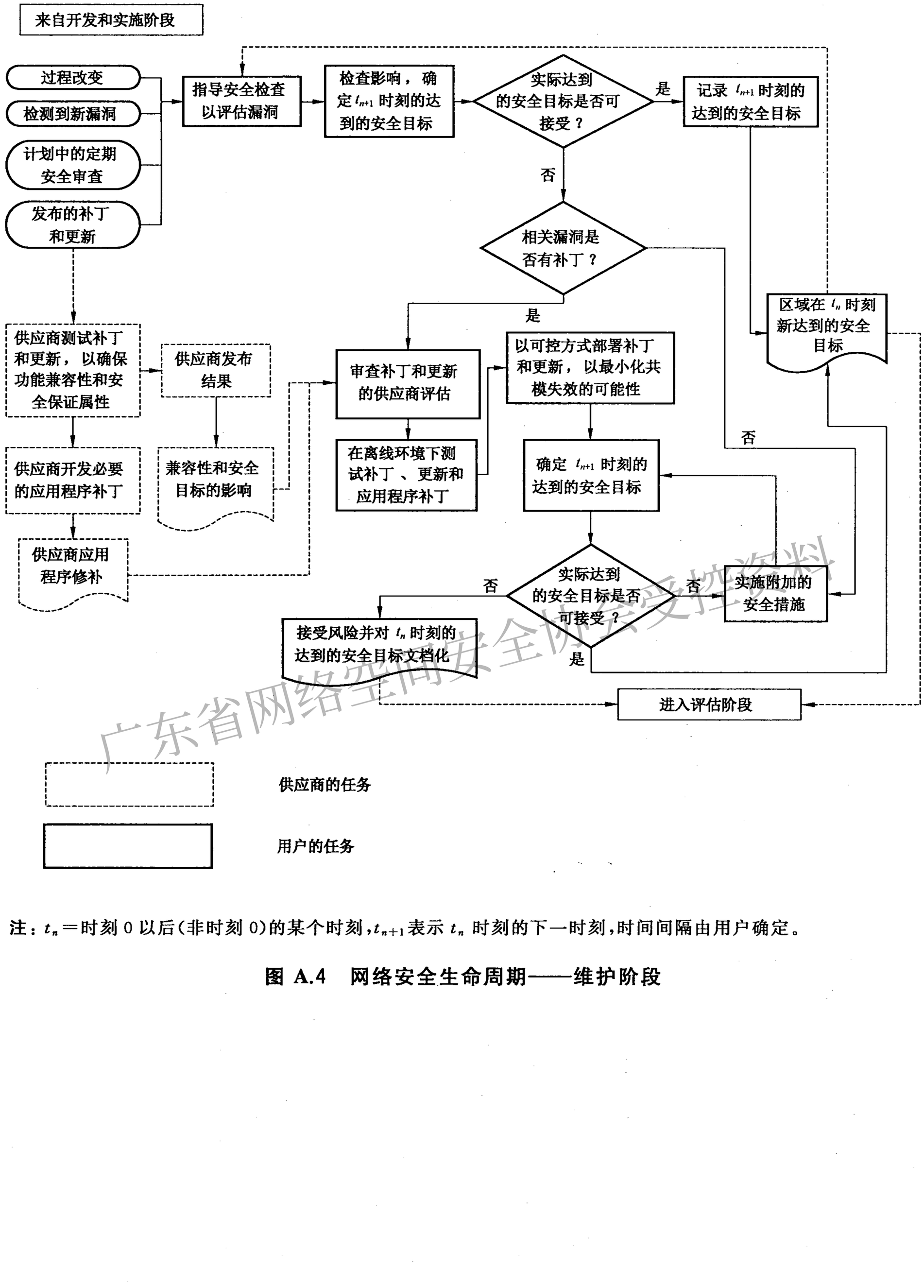


图 A.3　网络安全等级生命周期——实施阶段

A.4　维护阶段

设备和系统的安全措施和安全目标的达成度会随时间而降低。区域的安全目标应定期或者当发现新脆弱性时进行审计和/或测试，以确保区域的安全目标的达成度始终大于或等于设定的安全目标。与维护区域的安全目标达成度的评估测试相关的活动见图 A.4。



注：t_n＝时刻 0 以后(非时刻 0)的某个时刻，t_{n+1}表示 t_n 时刻的下一时刻，时间间隔由用户确定。

图 A.4　网络安全生命周期——维护阶段

附 录 B
（资料性附录）
风险评估工具和集散控制系统(DCS)常见的测试内容

B.1 风险评估工具概述

B.1.1 风险评估与管理工具

风险评估与管理工具大部分是基于某种标准方法或某组织机构自行开发的评估方法，可以有效地通过输入数据来分析风险，给出对风险的评价并推荐控制风险的安全措施。

风险评估与管理工具通常建立在一定的模型或算法之上，风险由重要资产(如 SIS 系统、SLC 系统等)、所面临的威胁以及威胁所利用的脆弱性三者来确定；也有的通过建立专家系统，利用专家经验进行分析，给出分析结论。这种评估工具需要不断进行知识库的扩充。

此类工具实现了对风险评估全过程的实施和管理，包括：被评估信息系统基本信息获取、重要系统获取、脆弱性识别与管理、威胁识别、评估过程与评估结果管理等功能。评估的方式可以通过问卷的方式，也可以通过结构化的推理过程，建立模型，输入相关信息，得出评估结论。通常这类工具在对风险进行评估后都会有针对性地提出风险控制措施。

根据实现方法不同，风险评估与管理工具可以分为三类：

a) 基于网络安全标准的风险评估与管理工具

目前，国际上存在多种不同的风险分析标准或指南，不同的风险分析方法侧重点不同，例如 ISA Secure、NIST SP800-30、BS 7799、ISO/IEC 13335 等。以这些标准或指南的内容为基础，分别开发相应的评估工具，完成遵循标准或指南的风险评估过程。

b) 基于知识的风险评估与管理工具

基于知识的风险评估与管理工具并不仅仅限于某个单一的标准或指南，而是将各种风险分析方法进行综合，并结合实践经验，形成风险评估知识库，以此为基础完成综合评估。他还涉及来自类似组织机构(包括规模、商务目标和市场等)的最佳实践，主要通过多种途径采集相关的信息，识别组织机构的风险和当前的安全措施；与特定的标准或最佳实践进行比较，从中找出不符合的地方；按照标准或最佳实践的推荐选择安全措施以控制风险。

c) 基于模型的风险评估与管理工具

基于标准或基于知识的风险评估与管理工具，都使用了定性分析方法或定量分析方法，或者定性与定量相结合。定性分析方法是目前广泛采用的方法，需要凭借评估者的知识、经验和直觉，或者业界的标准和实践，为风险的各个要素定级。定性分析法操作相对容易，但也可能因为评估者经验和直觉的偏差而使分析结果失准。定量分析则对构成风险的各个要素和潜在损失水平赋值，通过对度量风险的所有要素进行赋值，建立综合评价的数学模型，从而完成风险的量化计算。定量分析方法准确，但前期建立系统风险模型较困难。定性与定量结合分析方法是将风险要素的赋值和计算，根据需要分别采取定性和定量方法完成。这类工具是在对系统各组成部分、安全要素充分研究的基础上，对典型系统、威胁、脆弱性建立量化或半量化的模型，根据采集信息的输入，得到评价的结果。

B.1.2 系统基础平台风险评估工具

系统风险平台风险评估工具分析包括脆弱性扫描工具和渗透性测试工具。脆弱性扫描工具又称为安全扫描器、漏洞扫描仪等，主要用于识别网络、操作系统、数据库系统的脆弱性。通常情况下，这些工具能够发现软件和硬件中已知的脆弱性，以决定系统是否易受已知攻击的影响。

脆弱性扫描工具是目前应用最广泛的风险评估工具，主要完成操作系统、数据库系统、网络协议、网络服务等的安全脆弱性检测功能，目前常见的脆弱性扫描工具有以下几种类型：

a) 基于网络的扫描器：在网络中运行，能够检测如防火墙错误配置或连接到网络上的易受攻击的网络服务器的关键脆弱性；

b) 基于主机的扫描器：发现主机的操作系统、特殊服务和配置的细节，发现潜在的用户行为风险，如密码强度不够，也可实施对文件系统的检查；

c) 分布式网络扫描器：由远程扫描代理、对这些代理的即播即用更新机制、中心管理点三部分构成，用于企业级网络的脆弱性评估，分布和位于不同位置、城市甚至不同的国家；

d) 数据库脆弱性扫描器：对数据库的授权、认证和完整性进行详细分析，也可以识别数据库系统中潜在的脆弱性。

渗透性测试工具是根据脆弱性扫描工具扫描的结果进行模拟攻击测试，判断被非法访问者利用的可能性。这类工具通常包括黑客工具、脚本文件。渗透性测试的目的是检测已发现的脆弱性是否真正会给系统或网络带来影响。

集散控制系统评估中，如果进行任何渗透测试，要慎重使用攻击性测试手段，并且测试系统的性能需要注明额外的渗透测试结果。最有可能有一些系统或组件由于渗透测试而性能退化。这些性能衰减应该被注明供今后使用。通常渗透性工具与脆弱性扫描工具一起使用。

B.1.3 风险评估辅助工具

科学的风险评估需要大量的实践和经验数据的支持，这些数据的积累是风险评估科学性的基础。风险评估过程中，可以利用一些辅助性的工具和方法来采集数据，帮助完成现状分析和趋势判断，如：

a) 检查列表：检查列表是基于特定标准或基线建立的，对特定系统进行审查的项目条款。通过检查列表，操作者可以快速定位系统目前的安全状况与基线要求之间的差距；

b) 入侵检测系统：入侵检测系统通过部署检测引擎，收集、处理整个网络中的通信信息，以获取可能对网络主机造成危害的入侵攻击事件；帮助检测各种攻击试探和误操作；同时也可以作为一个警报器，提醒管理员发生的安全状况；

c) 安全审计工具：用于记录网络行为，分析系统或网络安全现状；其审计记录可以作为风险评估中的安全现状数据，并可用于判断被评估对象威胁信息的来源；

d) 病毒和恶意代码检测工具：该工具如同一个主动的侦查代理者，对上述迹象的非正常的活动目录进行侦查。病毒和恶意代码检测工具能够监查并运行在有恶意代码活动的主机上，或是网络服务器的层面上，如同一个邮件服务器。未来方向包括启发式、统计以及神经网络技术的病毒和恶意代码检测系统；

e) 资产信息收集系统：通过提供调查表形式，完成被评估信息系统数据、管理、人员等资产信息的收集功能，了解到组织机构的主要业务、重要资产、威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况。此类系统主要采取电子调查表形式，需要被评估系统管理人员参与填写，并自动完成资产信息获取；

f) 拓扑发现工具：通过接入点接入被评估网络，完成被评估网络中的资产发现功能，并提供网络资产的相关信息，包括操作系统版本、型号等。拓扑发现工具主要是自动完成网络硬件设备的识别、发现功能。

B.2 集散控制系统(DCS)网络安全常见评估对象及测试

B.2.1 离线的安全测试

离线测试要包括系统的安全性测试设备的安全测试，以确保评估工作的完整性和健壮性。

如果被评估对象 DCS 是一个新系统，应该在系统脱机环境下进行安全测试。系统应该在供应商的位置或最终工厂场地分步骤进行离线测试。位置并不重要，重要的是执行的安全测试步骤。虽然这对安全测试的所有设备和应用于最后设备状态的对策很有意义，但是这也许支付不起且不适用。所以测试的设计应该更关注 ICS 设备的能力和不局限于安装位置的对策。安全测试应该不仅仅包括评估受试者遇到了典型的安全威胁的抵抗能力，也应该包括进行的系统安全支持的测试。这些包括但不限于：

a) 测试操作系统修补补丁和升级；

b) 测试 DCS 供应商的补丁和升级过程；

c) 测试离线系统的开发环境；

d) 测试恶意软件的部署和更新恶意软件的签名。

B.2.2 现场测试

被评估对象如果是新安装的 DCS，应该在 DCS 上线之前进行这些测试。如果新系统是用于改造和替换现有的 DCS 设备或者扩展现有生产过程或控制功能，可能无法进行全面的系统安全功能和安全策略的现场测试。如果新安装的 DCS 是全新的系统，则可以在其上线之前对其系统安全功能和安全策略进行全面的现场测试，不必担心 DCS 安全功能和策略的现场测试对的 DCS 基本控制功能造成的影响。

需要牢记的是系统性能测试应包括系统对正常和异常的工业操作类型事件和安全事故类型事件的反应。结合这些才能全面衡量系统的鲁棒性和完整性。由于每个工业操作稍有不同，你可能确定一个测试流程手册。他将需要大量的设计工作去决定最好的方法来保证测试，从而使得安全功能满足目标安全等级。

B.2.3 集散控制系统(DCS)的测试类型

B.2.3.1 组件测试

组件测试应该由供应商和系统拥有者来完成。组件可以是软件、硬件或任何组合情况。组件需要被测试以验证他满足特定的操作和安全要求。组件测试是正常的工作台测试，要保证当组件集成到系统中，每个组件都能按预期运行。

B.2.3.2 集成测试

集成测试应该由集成商和系统拥有者来验证。该测试包括可能来自不同供应商的各种组件的操作和安全测试，这些组件是和工作台或辅助测试平台相连接，来检查所有的组件在投入 DCS 生产环境之前是否能一起正常的工作。集成测试可能需要使用额外的测试工具，如网络管理工具。

B.2.3.3 系统测试

系统测试应该由拥有者验证。验证的目的是证明 DCS 安全功能和安全策略的有效性。确保新的安全功能在 DCS 运行过程中满足其安全要求，且不影响其性能和生产运行。

系统测试可能包括系统的渗透测试来保证安全组件的能力，从而保护系统受到各种威胁满足每个区域的安全等级。渗透测试时一个已知的人尝试在系统中渗透安全防御，寻找脆弱性，并利用脆弱性来获得访问或控制系统的权限。

常用的测试工具主要包括用于可以协助实际的测试的测试脚本、数据库变量、度量标准和标定工具和可以进行路由、网关、连接设备模拟和诊断的软件。

进行任何渗透测试时，应在测试中记录渗透测试对系统性能的影响。一些系统或组件会因渗透测试而造成性能退化。记录数据有助于后期的系统改进。

附 录 C
（规范性附录）
风险的计算方法

C.1 风险计算概述

对风险进行计算，需要确定影响风险要素、要素之间的组合方式以及具体的计算方法，将风险要素按照组合方式使用具体的计算方法进行计算，得到风险值。

本附录首先说明矩阵法和相乘法的原理，然后基于正文第 8 章风险计算原理中指出的风险要素和要素组合方式，以示例的形式说明采用矩阵法和相乘法计算风险值的过程。

在实际应用中，可以将矩阵法和相乘法结合使用。

C.2 使用矩阵法计算风险

C.2.1 矩阵法原理

矩阵法主要适用于由两个要素值确定一个要素值的情形。首先需要确定二维计算矩阵，矩阵内各个要素的值根据具体情况和函数递增情况采用数学方法确定，然后将两个元素的值在矩阵中进行比对，行列交叉处即为所确定的计算结果。

即 $z=f(x,y)$，函数 f 可以采用矩阵法。

矩阵法的原理是：

$x=\{x_1,x_2,\cdots,x_i,\cdots,x_m\}$，$1\leqslant i\leqslant m$，$x_i$ 为正整数；

$y=\{y_1,y_2,\cdots,y_i,\cdots,y_n\}$，$1\leqslant j\leqslant n$，$y_j$ 为正整数。

以要素 x 和要素 y 的取值构建一个二维矩阵，如表 C.1 所示。矩阵行值为要素 y 的所有取值，矩阵列值为要素 x 的所有取值。矩阵内 $m\times n$ 个值即为要素 z 的取值，$z=\{z_{11},z_{12},\cdots,z_{ij},\cdots,z_{mn}\}$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$，$z_{ij}$ 为正整数。

表 C.1 二维计算矩阵赋值表

	y	y_1	y_2	…	y_j	…	y_n
x	x_1	z_{11}	z_{12}	…	z_{1j}	…	z_{1n}
	x_2	z_{21}	z_{22}	…	z_{2j}	…	z_{2n}
	…	…	…	…	…	…	…
	x_i	z_{i1}	z_{i2}	…	z_{ij}	…	z_{in}
	…	…	…	…	…	…	…
	x_m	z_{m1}	z_{m2}	…	z_{mj}	…	z_{mn}

对于 z_{ij} 的计算，可以采用以下计算公式，

$z_{ij}=x_i+y_j$，或 $z_{ij}=x_i\times y_j$，

或 $z_{ij}=\alpha\times x_i+\beta\times y_j$，其中 α 和 β 为正常数。

z_{ij} 的计算需要根据实际情况确定，矩阵内 z_{ij} 值的计算不一定遵循统一的计算公式，但应具有统一

的增减趋势，即如果 f 是递增函数，z_{ij} 值应随着 x_i 与 y_j 的值递增，反之亦然。

矩阵法的特点在于通过构造两两要素计算矩阵，可以清晰罗列要素的变化趋势，具备良好灵活性。在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值等，同时需要整体掌握风险值的确定，因此矩阵法在风险分析中得到广泛采用。

C.2.2 计算示例

C.2.2.1 条件

共有三个重要设备，设备 A1、设备 A2 和设备 A3；其中包含两个生产业务工艺，工艺 P1，工艺 P2；

设备 A1 属于工艺 P1；

设备 A2 属于工艺 P1；

设备 A3 属于工艺 P2；

工艺 P1 的重要性 Ps1，复杂性 Pc1，影响性 Pi1；

工艺 P2 的重要性 Ps2，复杂性 Pc2，影响性 Pi2；

设备 A1 面临两个主要威胁，威胁 T1 和威胁 T2；

设备 A2 面临一个主要威胁，威胁 T3；

设备 A3 面临两个主要威胁，威胁 T4 和 T5；

威胁 T1 可以利用的设备 A1 存在的两个脆弱性，脆弱性 V1 和脆弱性 V2；

威胁 T2 可以利用的设备 A1 存在的三个脆弱性，脆弱性 V3、脆弱性 V4 和脆弱性 V5；

威胁 T3 可以利用的设备 A2 存在的两个脆弱性，脆弱性 V6 和脆弱性 V7；

威胁 T4 可以利用的设备 A3 存在的一个脆弱性，脆弱性 V8；

威胁 T5 可以利用的设备 A3 存在的一个脆弱性，脆弱性 V9；

工艺 P1 的重要性 Ps1＝3，复杂性 Pc1＝2，影响性 Pi1＝4；

工艺 P2 的重要性 Ps2＝1，复杂性 Pc1＝2，影响性 Pi1＝3；

设备价值分别是：设备 A1＝2，设备 A2＝3，设备 A3＝4；

威胁发生频率分别是：威胁 T1＝2，威胁 T2＝1，威胁 T3＝2，威胁 T4＝3，威胁 T5＝4；

脆弱性严重程度分别是：脆弱性 V1＝2，脆弱性 V2＝3，脆弱性 V3＝1，脆弱性 V4＝4，脆弱性 V5＝2，脆弱性 V6＝4，脆弱性 V7＝2，脆弱性 V8＝3，脆弱性 V9＝4。

C.2.2.2 计算重要设备的风险值

三个设备的风险值计算过程类似，下面以设备 A1 为例使用矩阵法计算风险值。

设备 A1 属于工艺 P1，面临的主要威胁包括威胁 T1 和威胁 T2，威胁 T1 可以利用的资产 A1 存在的脆弱性包括两个，威胁 T2 可以利用的资产 A1 存在的脆弱性包括三个，则资产 A1 存在的风险值包括五个。五个风险值的计算过程类似，下面以设备 A1 面临的威胁 T1 可以利用的脆弱性 V1 为例，计算安全风险值。

a） 计算安全事件发生可能性

工艺重要性 Ps1＝3，复杂性 Pc1＝2。

威胁发生频率：威胁 T1＝2；

脆弱性严重程度：脆弱性 V1＝2。

首先构建工艺下的威胁发生频率矩阵，如表 C.2 所示。

表 C.2　工艺下的威胁发生频率矩阵

	工艺的重要性	1	2	3	4
威胁发生频率	1	2	4	6	10
	2	3	5	9	12
	3	4	7	11	15
	4	5	8	14	20

根据工艺的重要性和威胁发生频率值，确定工艺下的威胁发生频率＝9。

然后构建工艺下的脆弱性严重程度矩阵，如表 C.3 所示。

表 C.3　工艺下的脆弱性严重程度矩阵

	工艺的复杂性	1	2	3	4
脆弱性严重程度	1	2	3	5	11
	2	3	4	8	14
	3	4	6	10	16
	4	5	7	13	20

根据工艺的复杂性和脆弱性严重程度，确定工艺下的脆弱性严重程度＝4。

接着构建安全事件发生可能性矩阵，如表 C.4 所示。

表 C.4　安全事件发生可能性等级矩阵

	工艺下脆弱性严重程度	1～5	6～10	11～15	16～20
工艺下威胁发生频率	1～5	2	4	7	11
	6～10	3	6	10	13
	11～15	5	9	12	16
	16～20	7	11	14	20

然后根据工艺下威胁发生频率值和工艺下脆弱性严重程度值在矩阵中进行对照，确定安全事件发生可能性等级＝3。

由于安全事件发生可能性将参与风险事件值的计算，为了构建风险矩阵，对上述计算得到的安全风险事件发生可能性进行等级划分，如表 C.5 所示，安全事件发生可能性等级＝1。

表 C.5　安全事件可能性等级矩阵

安全事件发生可能性值	1～5	6～10	11～15	16～20
发生可能性等级	1	2	3	4

b)　计算安全事件的损失

工艺影响性 Pi1＝4

设备价值：设备 A1＝2；

脆弱性严重程度:脆弱性 V1＝2;

首先构建安全事件损失矩阵,如表 C.6 所示。

表 C.6　安全事件损失矩阵

	脆弱性严重程度	1	2	3	4
设备价值	1	2	4	6	10
	2	3	5	9	12
	3	4	7	11	15
	4	5	8	14	19

根据设备价值和脆弱性严重程度值在矩阵中进行对照,确定安全事件损失值＝5。

然后构建工艺影响性和安全事件损失值矩阵,如表 C.7 所示。

表 C.7　工艺下的安全事件损失矩阵

	安全事件损失值	1～5	6～10	11～15	16～20
工艺影响性	1	2	4	6	10
	2	3	5	8	11
	3	5	7	11	14
	4	6	9	13	19

根据工艺影响性和安全事件损失值在矩阵中进行对照,确定工艺下的安全事件损失值＝6。

由于安全事件损失将参与风险事件值的计算,为了构建风险矩阵,对上述计算得到的工艺下的安全事件损失进行等级划分,如表 C.8 所示,安全事件发生可能性值＝2。

表 C.8　工艺下的安全事件损失等级划分

工艺下的安全事件损失值	1～5	6～10	11～15	16～20
安全事件损失等级	1	2	3	4

c)　计算风险值

工艺下的安全事件发生可能性＝1;工艺下的安全事件损失＝2。

首先构建风险矩阵,如表 C.9 所示。

表 C.9　风险矩阵

	可能性	1	2	3	4
损失	1	3	6	9	12
	2	5	8	11	15
	3	6	9	13	17
	4	7	11	16	20

然后根据安全事件发生可能性和安全事件损失在矩阵中进行对照,确定安全事件风险＝5。

按照上述方法进行计算,得到资产 A 的其他的风险值,以及资产 A2 和资产 A3 的风险。然后再进

行风险结果等级判定。

C.2.2.3 结果判定

确定风险等级划分，如表 C.10 所示。

表 C.10 风险等级划分

工艺下的安全事件损失值	1～5	6～10	11～15	16～20
安全事件损失等级	1	2	3	4

根据上述计算方法，以此类推，得到三个重要资产的风险值，并根据风险等级划分表，确定风险等级，结果如表 C.11 所示。

表 C.11 风险结果

设备	工艺	威胁	脆弱性	风险值	风险等级
设备 A1	工艺 P1	威胁 T1	脆弱性 V1	5	1
		威胁 T1	脆弱性 V2	8	2
		威胁 T2	脆弱性 V3	5	1
		威胁 T2	脆弱性 V4	9	2
		威胁 T2	脆弱性 V5	5	1
设备 A2		威胁 T3	脆弱性 V6	9	2
		威胁 T3	脆弱性 V7	5	1
设备 A3	工艺 P2	威胁 T4	脆弱性 V8	6	2
		威胁 T5	脆弱性 V9	6	2

C.3 使用相乘法计算风险

C.3.1 计算原理

相乘法主要用于两个或多个要素值确定一个要素值的情形。即 $z=f(x,y)$，函数 f 可以采用相乘法。

相乘法的原理是：

$z=f(x,y)=x\otimes y$。

当 f 为增量函数时，$\otimes$可以为直接相乘，也可以为相乘后取模等，例如：

$z=f(x,y)=x\times y$，

或 $z=f(x,y)=\sqrt{x\times y}$，

或 $z=f(x,y)=\left[\sqrt{x\times y}\right]$，

或 $z=f(x,y)=\left[\dfrac{\sqrt{x\times y}}{x+y}\right]$等。

相乘法提供一种定量的计算方法，直接使用两个要素值进行相乘得到另一个要素的值。相乘法的特点是简单明确，直接按照统一公式计算，即可得到所需结果。

在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如由威胁和脆弱性确定安

全事件发生可能性值、由设备和脆弱性确定安全事件的损失值，因此相乘法在风险分析中得到广泛采用。

C.3.2 计算示例

C.3.2.1 条件

共有三个重要设备，设备 A1、设备 A2 和设备 A3；其中包含两个生产业务工艺，工艺 P1，工艺 P2；
设备 A1 属于工艺 P1；
设备 A2 属于工艺 P1；
设备 A3 属于工艺 P2；
工艺 P1 的重要性 Ps1，复杂性 Pc1，影响性 Pi1；
工艺 P2 的重要性 Ps2，复杂性 Pc2，影响性 Pi2；
设备 A1 面临两个主要威胁，威胁 T1 和威胁 T2；
设备 A2 面临一个主要威胁，威胁 T3；
设备 A3 面临两个主要威胁，威胁 T4 和 T5；
威胁 T1 可以利用的设备 A1 存在的两个脆弱性，脆弱性 V1 和脆弱性 V2；
威胁 T2 可以利用的设备 A1 存在的三个脆弱性，脆弱性 V3、脆弱性 V4 和脆弱性 V5；
威胁 T3 可以利用的设备 A2 存在的两个脆弱性，脆弱性 V6 和脆弱性 V7；
威胁 T4 可以利用的设备 A3 存在的一个脆弱性，脆弱性 V8；
威胁 T5 可以利用的设备 A3 存在的一个脆弱性，脆弱性 V9；
工艺 P1 的重要性 Ps1＝3，复杂性 Pc1＝2，影响性 Pi1＝4；
工艺 P2 的重要性 Ps2＝1，复杂性 Pc1＝2，影响性 Pi1＝3；
设备价值分别是：设备 A1＝2，设备 A2＝3，设备 A3＝4；
威胁发生频率分别是：威胁 T1＝2，威胁 T2＝1，威胁 T3＝2，威胁 T4＝3，威胁 T5＝4；
脆弱性严重程度分别是：脆弱性 V1＝2，脆弱性 V2＝3，脆弱性 V3＝1，脆弱性 V4＝4，脆弱性 V5＝2，脆弱性 V6＝4，脆弱性 V7＝2，脆弱性 V8＝3，脆弱性 V9＝4。

C.3.2.2 计算重要设备的风险值

三个设备的风险值计算过程类似，下面以设备 A1 为例使用矩阵法计算风险值。

设备 A1 属于工艺 P1，面临的主要威胁包括威胁 T1 和威胁 T2，威胁 T1 可以利用的资产 A1 存在的脆弱性包括两个，威胁 T2 可以利用的资产 A1 存在的脆弱性包括三个，则资产 A1 存在的风险值包括五个。五个风险值的计算过程类似，下面以设备 A1 面临的威胁 T1 可以利用的脆弱性 V1 为例，计算安全风险值。其中计算公式使用：

$z=f(x,y)=\sqrt{x\times y}$，并对 z 的计算值四舍五入取整得到最终结果。

a） 计算安全事件发生可能性

工艺重要性 Ps1＝3，复杂性 Pc1＝2；
威胁发生频率：威胁 T1＝2；
脆弱性严重程度：脆弱性 V1＝2。
计算安全事件发生可能性，安全事件发生可能性＝$\sqrt{3\times2\times2\times2}=\sqrt{24}$。

b） 计算安全事件的损失

工艺影响性 Pi1＝4；
设备价值：设备 A1＝4；
脆弱性严重程度：脆弱性 V1＝2。

计算安全事件的损失，安全事件损失$=\sqrt{4\times4\times2}=\sqrt{32}$。

c) 计算风险值

安全事件发生可能性$=\sqrt{24}$；

安全事件损失$=\sqrt{32}$。

安全事件风险值$=\sqrt{24}\times\sqrt{32}=\sqrt{768}\approx27$。

按照上述方法进行计算，得到资产 A1 的其他的风险值，以及资产 A2 和资产 A3 风险值。然后再进行风险结果等级判定。

C.3.2.3 结果判定

确定风险等级划分，如表 C.12 所示。

表 C.12 风险等级划分

工艺下的安全事件损失值	1～20	21～40	41～80	81～128
安全事件损失等级	1	2	3	4

根据上述计算方法，以此类推，得到三个重要资产的风险值，并根据风险等级划分表，确定风险等级，结果如表 C.13 所示。

表 C.13 风险结果

设备	工艺	威胁	脆弱性	风险值	风险等级
设备 A1	工艺 P1	威胁 T1	脆弱性 V1	27	2
		威胁 T1	脆弱性 V2	29	2
		威胁 T2	脆弱性 V3	7	1
		威胁 T2	脆弱性 V4	28	2
		威胁 T2	脆弱性 V5	14	1
设备 A2		威胁 T3	脆弱性 V6	48	3
		威胁 T3	脆弱性 V7	24	2
设备 A3	工艺 P2	威胁 T4	脆弱性 V8	25	2
		威胁 T5	脆弱性 V9	39	2

参 考 文 献

[1] GB/T 15851—1995 信息技术 安全技术 带消息恢复的安全技术要求

[2] GB/T 17901 信息技术 安全技术 密钥管理 第1部分:框架(GB/ T 17901—1999,idt ISO/IEC 11770-1:1996)

[3] GB/T 17902—1999 信息技术 安全技术 带附录的数字签名

[4] GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则

[5] GB/T 19011—2003 质量和(或)环境管理体系审核指南(ISO 19011:2002,IDT)

[6] GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

[7] ISO/IEC 9798 Information technology—Security techniques—Entity authentication

[8] ISO/IEC 20009-2 Information technology—Security techniques—Anonymous entity authentication—Part 2: Mechanisms based on signatures using a group public key

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

[10] IEC 62443-1-3 Security for industrial automation and control systems—Part 1-3: Cyber security system conformance metrics

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

[12] IEC 62443-3-2 Security for industrial automation and control systems—Part 3-2: Security risk assessment and system design

[13] IEC 62443-4-1 Security for industrial automation and control systems—Part 4-1: Secure Product Development Lifecycle Requirements

[14] IEC 62443-4-2 Security for industrial automation and control systems—Part 4-2: Technical security requirements for IACS

中华人民共和国
国家标准
工业自动化和控制系统网络安全
集散控制系统(DCS)
第3部分:评估指南
GB/T 33009.3—2016
*
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.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.5 字数 69 千字
2016年10月第一版 2016年10月第一次印刷
*
书号:155066·1-54798 定价 36.00元

GB/T 33009.3-2016