ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36466—2018

信息安全技术
工业控制系统风险评估实施指南

Information security technology—
Implementation guide to risk assessment of industrial control systems

2018-06-07 发布　　2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

引　言

随着工业控制系统和信息化技术的融合，工业控制系统广泛应用于冶金、电力、石化、水处理、铁路、航空和食品加工等行业。工业控制系统指应用于工业控制领域的数据采集、监视与控制系统，是由计算机设备、工业过程控制组件和网络组成的控制系统，是工业领域的神经中枢。工业中使用的控制系统包括监视控制与采集系统、分布式控制系统、可编程逻辑控制器系统等。我国把工业控制系统信息安全作为信息安全保障的一个相对独立的体系进行建设，其安全性将直接关系到国家重要基础工业设施生产的正常运行和广大公众的利益。

本标准在对工业控制系统的资产进行整理分析的基础上，从其资产的安全特性出发，分析工业控制系统的威胁来源与自身脆弱性，归纳出工业控制系统面临的信息安全风险，并给出实施工业控制系统风险评估的指导性建议。

本标准主要为第三方安全检测评估机构在工业控制系统现场实施风险评估提供指南，也可供工业控制系统业主单位进行自评估时参考。

信息安全技术
工业控制系统风险评估实施指南

1 范围

本标准规定了工业控制系统风险评估实施的方法和过程。

本标准适用于指导第三方安全检测评估机构对工业控制系统的风险评估实施工作，也可供工业控制系统业主单位进行自评估时参考。

3.1.6

智能电子设备　intelligent electronic device;IED

用于生产过程的信息采集、自动测量记录和传导,通过网络与 MTU 保持通信的智能化电子设备。

注:一般部署在管网站场。

3.1.7

人机界面　human-machine interface;HMI

为操作者和控制器之间提供操作界面和数据通信的软硬件平台。

3.2　缩略语

下列缩略语适用于本文件。

ICS　工业控制系统(Industrial Control System)

SCADA　监视控制与数据采集系统(Supervisory Control And Data Acquisition)

DCS　分布式控制系统(Distributed Control System)

PLC　可编程逻辑控制器(Programmable Logic Controller)

RTU　远程终端设备(Remote Terminal Unit)

MTU　主终端设备(Master Terminal Unit)

ACL　访问控制列表(Access Control List)

DNS　域名系统(Domain Name System)

DHCP　动态主机配置协议(Dynamic Host Configuration Protocol)

DNP　分布式网络协议(Distributed Network Protocol)

RPC　远程过程调用协议(Remote Procedure Call Protocol)

DCOM　分布式组件对象模式(Microsoft Distributed Component Object Model)

OPC　用于过程控制的对象连接与嵌入(Object Linking and Embedding for Process Control)

DoS　拒绝服务(Denial of Service)

CAN　控制器局域网络(Controller Area Network)

UPS　不间断电源(Uninterruptible Power System)

HMI　人机界面(Human Ma

(Common Vulnerability Scoring Syste

4　概述

4.1　工业控制系统层次结构模型

工业控制系统应用的技术领域、行业特点或者承载的业务类型的差异化导致实际中工业控制系统的架构差别较大。为了就典型的工业控制系统的功能特点和部署形式达成共识,本标准依据 ISO/IEC 62264-1:2013 的层次结构模型,给出了通用的工业控制系统的层次结构模型,如图 1 深色部分所示:

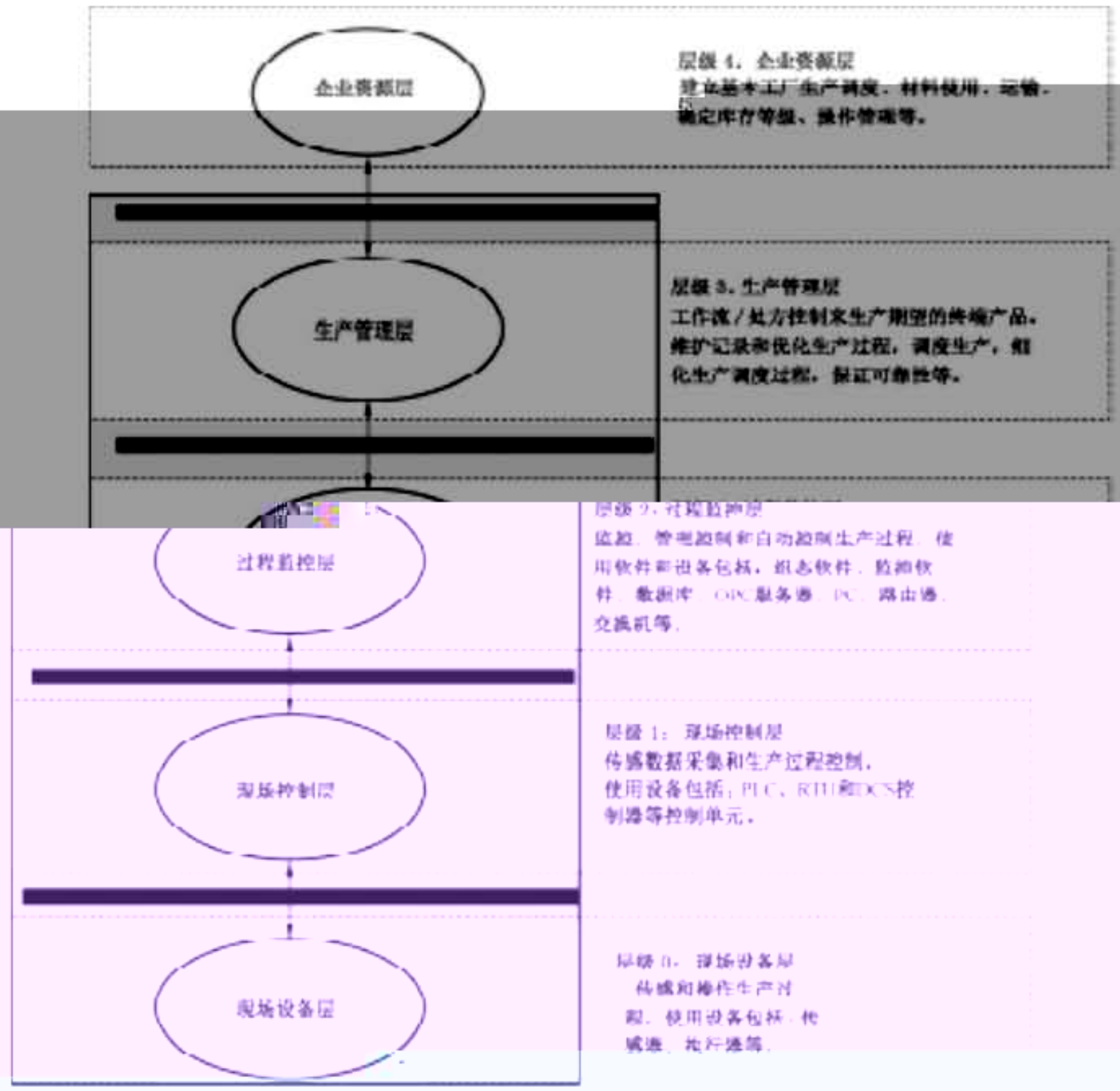


图 1　工业控制系统层次结构模型图

根据层次结构模型图中所述，企业资源层与生产管理层中用到的多为传统信息系统中通用的软件和硬件，GB/T 31509—2015 给出了相应的评估方法。过程监控层、现场控制层和现场设备层是工业控制系统中特有的部分。本标准主要规范这 3 个层面的风险评估的实施工作。

4.2　实施原则及工作形式

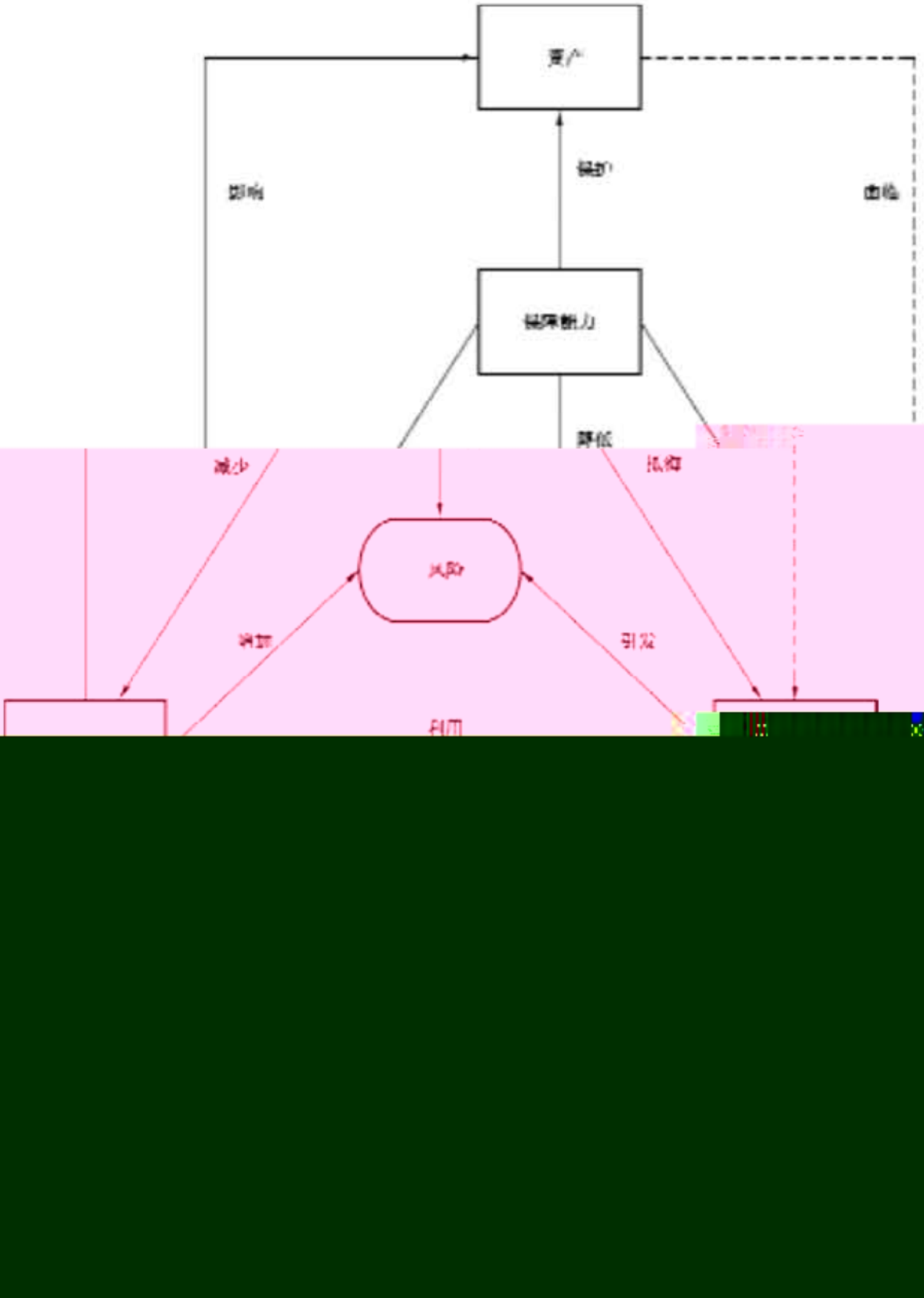
GB/T 31509—2015 规定了风险评估实施的原则，包括标准性原则、关键业务原则、可控性原则及最小影响原则。

GB/T 20984—2007 明确了风险评估的基本工作形式是自评估与检查评估。无论自评估或检查评估均可委托第三方工业控制系统风险评估机构实施。

4.3　框架及流程

4.3.1　风险要素关系

风险评估中各要素及其关系如图 2 所示。


资产
影响
降低
减少
抵御
风险
诱因
引发

4.3.2 风险评估流程

工业控制系统风险评估实施分为3个阶段，包括：风险评估准备阶段、风险要素评估阶段、综合分析阶段。根据工业控制系统风险评估的不同阶段，评估方制定相应的工作计划，保证评估工作的顺利

文件，以确保评估方对其进行全面审查。评估方查阅被评估方的工业控制系统架构设计方案、网络拓扑
图、系统安全防护计划、安全策略、职责、要求、标准作业程序、授权协议、系统互连备忘录、信息安全审核
[illegible]被评估方政策的缺陷、过时内容或不合理
实施指南如下：

a) 评估方在准备阶段编制一份适用的工业控制系统风险评估文档查阅所需文件目录；

b) 被评估方根据文件目录提供相对应的文档；

c) 评估方审查相关文档内容是否完整合规；

d) [illegible]

人员和相应的信息安全人员在场，最好由工业控制系统操作人员对其进行核查操作，评估人员只负责查看并记录结果；

d) 现场核查测试时，评估方不应改动工业控制系统的任何配置；

e) 记录现场核查的结果。若发现不符合项或脆弱项，需对其进行验证。

5.5 现场测试

工业控制系统分为离散型和连续型。某些离散的工业控制系统，如数控机床等，处于非运行状态时可以进行现场测试。现场测试是指直接在待评估工业控制系统现场环境上进行安全性测试，这种测试方法能够更直实的反映工业控制系统存在的脆弱性。现场测试方法包括漏洞扫描、协议分析、设备漏洞挖掘、渗透性测试等。

渗透性测试的目的是为发现和确认工业控制系统的脆弱性，可在被评估方允许的前提下对离散过程的工业控制系统实施。测试前应与相关专家讨论具体的实施方案和评估可能产生的后果，并制定相应的处置计划。评估方应谨慎使用渗透性测试方法。

现场测试完成后，需要对系统进行验证才能再次投入使用。

5.6 模拟仿真环境测试

连续型工业控制系统往往处于不间断运行状态，任何系统故障都可能造成巨大的损失。风险评估过程中脆弱性识别往往需要进行攻击测试或绕过系统的安全机制，若直接在生产系统上实施会带来更大的安全风险，甚至导致工业控制系统崩溃或进入不可控状态。因此需要搭建模拟仿真测试环境并

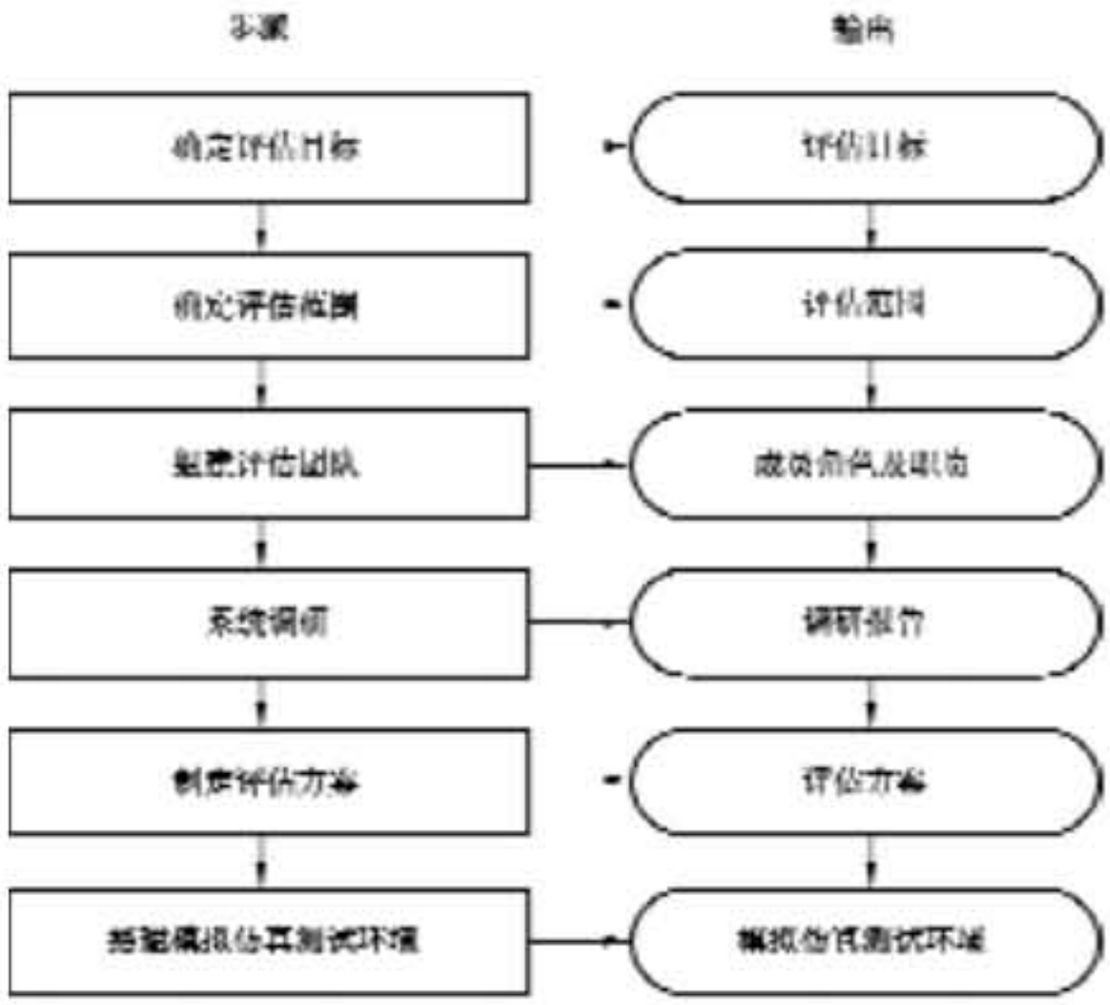


图 4　风险评估准备工作流程

6.1.2　确定目标

风险评估应贯穿于工业控制系统生命周期的各阶段中，由于工业控制系统生命周期各阶段中风险评估实施的内容、对象、安全需求均不同，因此评估方应首先根据当前工业控制系统的实际情况来确定在工业控制系统生命周期中所处的阶段，并以此来明确风险评估目标，如图 5 所示。具体实施过程见GB/T

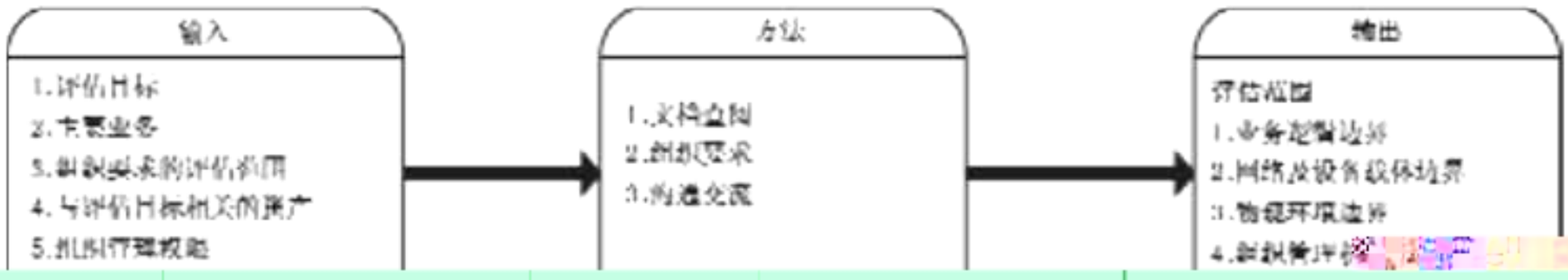


图 6　确定评估范围

指南如下：

评估方应了解工业控制系统所处的工业控制安全基线级别，具体见 GB/T 32919　2016；

评估方应了解被评估方要求评估的范围和实际工业控制系统建设情况；

风险评估实施范围应包括被评估方工业控制系统相关的资产、管理机构、关键业务流程等；

评估方应结合已确定的评估目标、被评估方要求评估的范围和实际工业控制系统建设情况，合理定义评估对象和评估范围边界。

建团队

评估实施团队可由评估方与被评估方的风险评估实施组、专家组共同组成。评估方应由工业专业人员、信息技术评估人员等组成。一个运行的工业控制系统会涉及多个利益相关方，包括产品的厂商、实际销售工控产品的分销商、集成并开发应用系统的集成商、为系统提供运行维护及工控系统的所有者等。在进行工业控制系统的风险评估之前，需要清晰界定评估所针对系统生态的哪一部分，涉及哪些利益相关方，从

实施

a)

b)

c)

d)

6.1.4　组

风险

控制系统

提供工控

护的厂商

的是工控

表 1（续）

评估方人员职位	工作职责
评估人员	是负责风险评估项目中技术方面评估工作的实施人员，应熟悉工业控制系统专用的通信协议（例如：DNP3、ModBus、PROFINET、PROFIBUS 等）；同时应精通编码、逆向工程、协议分析和渗透测试等；部分工业控制系统使用非桌面操作系统，评估实施团队成员应熟悉被检测工业控制系统使用的操作系统。具体工作职责包括： 1) GB/T 31[illegible]39—2015 规定的； 2) 参与保密教育及相关技术培训
	是负责风险评估项目[illegible]

表 2（续）

被评估方 人员职位	工作职责
关键产品供应商人员	是指工业控制系统关键产品（包括软硬件）供应商人员代表。在风险评估项目中的具体工作职责包括： 1）在项目组长的安排下，配合评估方的工作； 2）参与保密教育培训； 3）参与风险评估项目的验收
系统集成商人员	是指工业控制系统的集成商代表，在风险评估项目中具体的工作职责包括： 1）在项目组长的安排下，配合评估方的工作； 2）参与保密教育及相关技术培训； 3）配合搭建模拟仿真测试环境； 4）参与对风险评估项目的验收

专家组由工业控制系统相关领域专家组成，职责包括：

a） 对风险评估实施方案进行评审；

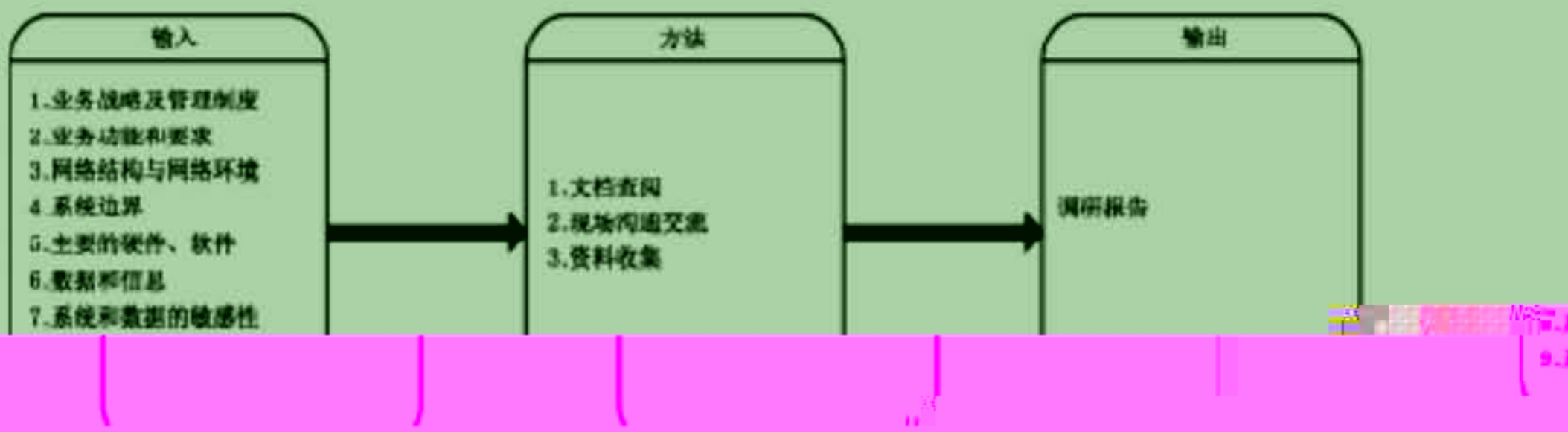
b） 对风险评估报告等项目成果物进行评审；

c） 对评估[illegible]中出现的关键性问题提供指导；

d） 对风险评估整个过程进行监督。

6.1.5 系统调研

系统调研是熟悉了解被评估对象的过程，风险评估组应进行充分的系统调研，修正评估目标跟范围，同时为风险评估依据和方法的选择、评估内容的实施奠定基础。评估方对工业控制系统进行调研可采取文档查阅、资料收集、现场交流和现场查看等方式进行，如图 7 所示。



其承担的业务、网络结构、系统边界等。

b) 评估组查看其设计、使用说明等文档：

1) 在工业控制系统中，若现场设备及其应用软件非被评估方自己开发，评估组需仔细审查供应商提供的所有资料，并与供应商取得联系，以便评估实施时可以进行技术沟通；

2) 查看工业控[illegible]统的安全需求及对应工业控制系统所处安全控制基线级别，采取哪些工业控制系统安全措施。

c) 评估组现场核查工业控制系统的物理环境、操作过程、设备组成等方面的信息并进行资料收集。

d) 评估组根据现场调研整理调研结果，编写调研报告。

6.1.6 制定评估方案

风险评估方案是评估工作实施活动总体计划，用于管理评估工作的开展，使评估各阶段工作可控，并作为评估项目验收的主要依据之一。风险评估方案应得到被评估方的确认和认可。风险评估方案的内容应包括(但不仅限于)：

a) 风险评估工作框架：包括评估目标、评估范围、评估依据、评估工具等，其中评估依据和评估工具可根[illegible]

[illegible]；搭建测试环境，模拟物理测试环境；

e) 风险规避：包括保密协议、评估工作环境要求、评估方法、工具选择、应急预案等；

f) 时间进度安排：评估工作实施的时间进度安排。

6.1.7 搭建模拟仿真测试环境

图 A.1 模拟仿真测试环境

6.2 资产评估

6.2.1 资产评估概述

资产是指，被评估方具有价值的信息或资源，是安全策略的保护对象。资产价值是资产重要程度或敏感程度的表征。资产评估包括识别资产和评估资产价值 2 个方面内容。

6.2.2 资产分类

在一个组织中，资产有多种存在形式。不同类[illegible]

[illegible]对相关的资产进行分类可以提高资产识别的效率。在实际工作中，具体的资产分类方法可以根据[illegible]的评估要求和要求，由评估方灵活把握。根据资产的存在形式，可将资产分为软资产、硬资产和

	防护设备、空调、监控设备、空调、保险柜、文件柜、门禁、消防设施等
人力资产	掌握重要信息和核心业务的人员：信息安全人员、工业控制系统设计人员、集成人员、关键设备供应商、授权人员、运维人员等

6.2.3 资产调查

资产调查是识别被评估方工业控制系统中资产的重要途径。资产调查一方面应识别出有哪些资产，另一方面应识别出每项资产自身的关键属性。工业控制系统结构复杂、资产繁多，为保证风险评估工作的进度要求及质量要求，有时不能对所有资产进行全面分析，应选取其中关键的资产进行分析，资产调查如图 3 所示

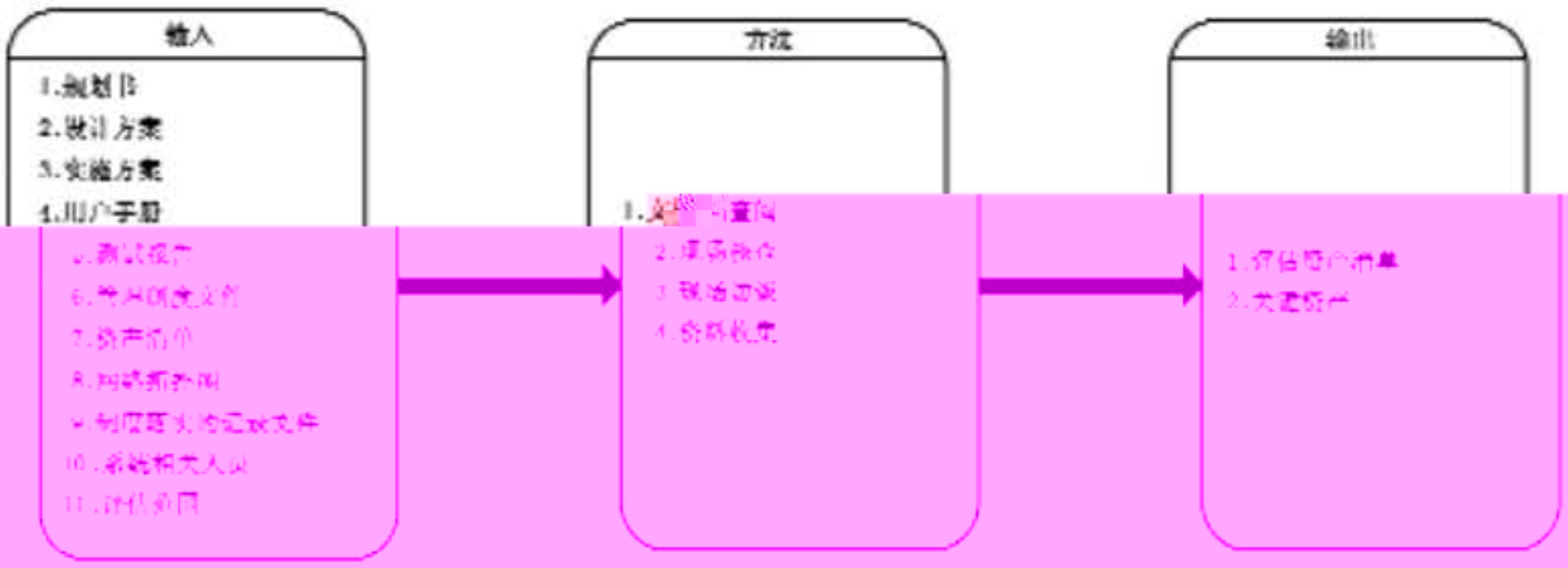


图 9　资产调查

协议通常于系统资产[illegible]工业控制系统广泛使用私有协议，往往会出现许多安全问题。资产调查过程中，应识别出工业控制系统使用的通讯协议并对其进行评估。

实施指南如下：

a) 评估组根据评估目标和范围，确定风险评估对象，并梳理其基本信息，可以参照附录 A 中表 A.1 进行访谈；

b) 评估方根据被评估方提供的规划书、设计方案、用户手册等文档并结合现场访谈相关人员识别出工业控制系统的具体业务；

c) 评估方根据工业控制系统的业务并结合现场访谈相关人员，识别出工业控制系统的工艺需求以及安全需求；

d) 评估方根据工业控制系统的工艺需求和安全需求，结合现场访谈相关人员，识别出关键功能需求及安全需求；

e) 评估方根据识别的关键需求、被评估方提供的资产清单、网络拓扑图等识别出工业控制系统的关键资产。

6.2.4　资产分析

根据工业控制系统承担的业务，判断资产的可用性、完整性和保密性的优先级，评估工业控制系统，将可用性作为首要需求。

进行资产赋值时可[illegible]

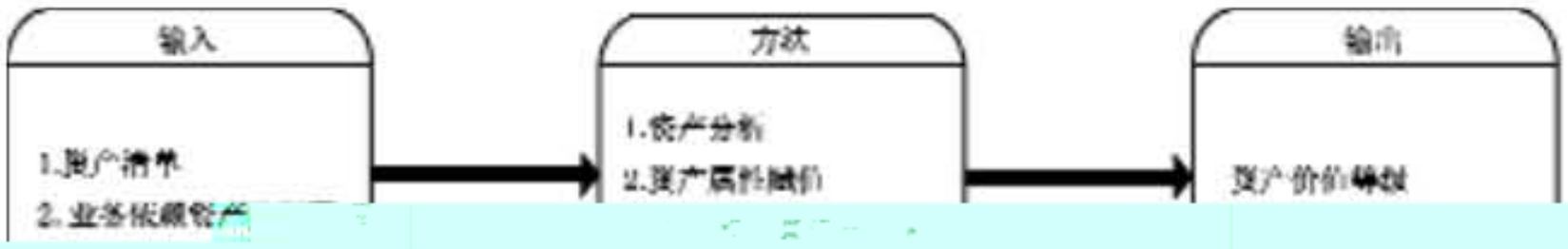


图 6　资产分析

实施指南如下：

a)　根据系统承担的业务，分析评判资产的安全属性可用性、完整性和保密性赋值等级，一般情况下，工业控制系统会将可用性赋值置于首位；

b)　根据资产调查以及资产赋值结果，确定重要资产的范围，并主要围绕重要资产进行下一步的风险评估。

6.3　威胁评估

6.3.1　威胁评估概述

威胁是指可能导致危害系统或被评估方的不希望事故的潜在起因。威胁是客观存在的，不同的资产面临威胁不同，同一个资产不同威胁发生的可能性和造成的影响也不同。全面、准确地识别威胁有利于做好防范措施。威胁评估要识别出威胁源、威胁途径及可能性和威胁影响，并对威胁进行分析赋值。

6.3.2　威胁分类

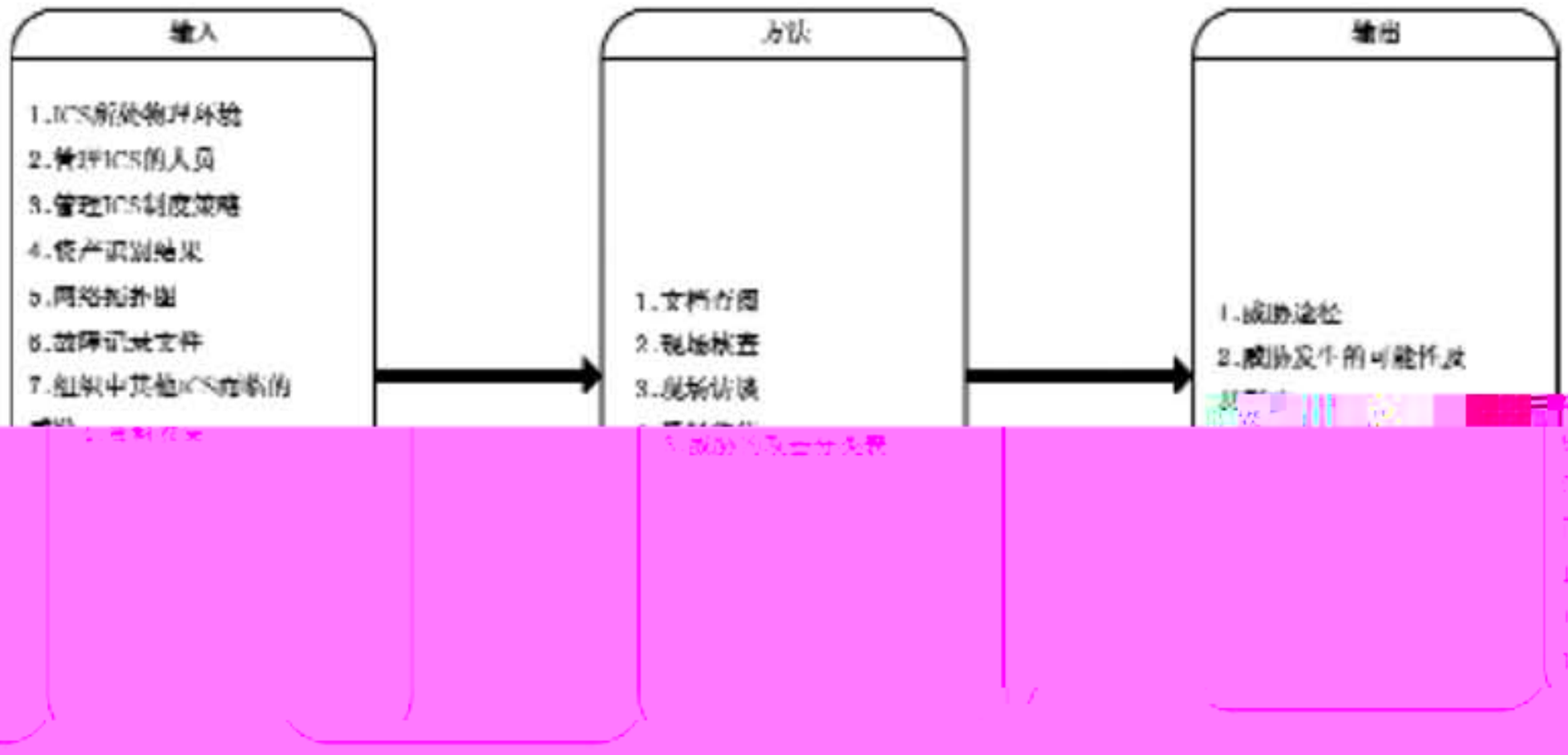
威胁源是产生威胁的主体。不同的威胁源具有不同的攻击能力，会采取不同的攻击方法，利用不同

表 5 中提供了工业控制系统可能存在的威胁。

表 5　工业控制系统可能面临的威胁

威胁名称	描述
灾难	自然灾难使工业控制系统的一个或多个组件停止运行，例如地震、火灾、洪水或其他未预期的事故
停电	自然灾难，恶意或无恶意的个人引起的停电事故，影响工业控制系统一个或多个组件的运行
非法信息披露	无权限者进行攻击(嗅探，社会活动)，以获得储存在工业控制系统组件中的敏感信息
非法分析	无权限者进行攻击(嗅探，社会活动)，用于分析受保护的敏感信息
非法修改	无权限者进行攻击(修改、破坏、嗅探)，以修改存储于工业控制系统
冒充通信	无权限者进行攻击(嗅探、社会活动)，以获得存储于工业控制系统
提升权限	，以获得存储于工业控制系统服务器组件中的用户凭证，提升工业控制系统组件访问的权限，达成恶意目的
故障检测缺失	操作员错误操作和安全违规的系统故障，在工业控制系统交互式系统中，执行的日常任务没有被检测和审计，以作进一步的分析和修正
病毒感染	个人恶意或无意地将病毒传入工业控制系统网络，恶意代码造成不必要的系统停机和数据腐败
非法物理存取	无权限者进行一次物理攻击，以实现对

全威胁日益增长。威胁调查就是要识别被评估方工业
制系统中可能发生并造成影响的威胁，进而分析哪些威胁发生时可能性较大、可能会造成重大影
图 11 所示。



11 威胁调查

业控制网络和外部网络之间进行网络隔离。威胁调查中要

自然环境、相关管理制定策略、资产清单、网络拓扑图、故障

与谈，以识别工业控制系统威胁，如图 11 所示。

工业控制系统大多部署网间设备，在工

着重识别针对网闸等网络隔离设备的威胁。

评估组将被评估的工业控制系统所处的

记录等文件进行汇总，对系统相关人员进行

实施指南如下：

a) 评估

8.3.3.2 威胁途径及可能性

g) 调查威胁攻击路径，要明确威胁发生的起点、威胁发生的中间点以及威胁发生的终点，并明确威胁在不同环节的特点，确定威胁路径；

h) 根据威胁途径、攻击能力等判断威胁发生的可能性。

6.3.3.3 威胁的影响

威胁出现的频率是衡量威胁严重程度的重要要素，因此威胁识别后需要对发生频率进行赋值，以代入最后的风险计算中。

威胁客体是威胁发生时受到影响的对象，威胁影响跟威胁客体密切相关。当一个威胁发生时，会影响到多个对象。威胁客体有层次之分，通常威胁直接影响的对象是资产，间接影响到工业控制系统和组织。

实施指南如下：

a) 识别那些直接受影响的客体，再逐层分析间接受影响的客体；

b) 确定威胁客体的价值，其价值越大，威胁发生的影响越大。

估方计划实施的安全措施、评估范围、常见脆弱性、依据国际或国家安全标准等均可作为评估方评估的资料。评估方通过资料收集、文档查阅、现场访谈、现场核查、模拟仿真环境测试等方法识别工业控制系统存在的脆弱性，如图 12 所示。

实施指南如下：

a) 评估方通过现场访谈和现场核查的方式对物理环境脆弱性进行识别，具体识别过程见 6.4.2；

b) 评估方通过现场访谈、现场核查等方式对网络脆弱性进行识别，具体识别过程见 6.4.3；

c) 评估方通过现场访谈、现场核查、模拟仿真环境测试的方式对平台脆弱性进行识别，具体识别过程见 6.4.4；

d) 评估方通过文档查阅、现场访谈和现场核查的方式对安全管理脆弱性进行识别，具体识别过程见 6.4.5。

6.4.2 物理环境脆弱性识别

物理环境脆弱性识别主要识别工业控制系统物理环境的安全风险，包括场所环境、电磁环境、设备实体、线路等方面。评估方核查已采取物理环境的安全措施及验证其已采取的安全措施有效性，同时查看基于该安全控制级别缺少哪些安全措施。

实施指南如下：

a) 评估方文

表 6（续）

脆弱性	描述
未安装加热/通风、空调等支持系统	需安装加热/通风、空调等支持系统，保证工业控制系统工作环境的稳定
自然灾害	火灾、洪水、地震、雷电和地震等自然灾害引起破坏时，应能备份系统数据，远离易燃易爆材料，配备适当的灭火器
缺少访问登记机制	第三方人员及临时授权人员进入系统场所时应有访问登记记录，防制未授权进入
系统处于复杂电磁环境内	应避免系统暴露于强电磁场 电磁干扰的环境内

6.4.3 网络脆弱性识别

6.4.3.1 网络结构及网络边界脆弱性识别

网络结构及网络边界脆弱性是指工业控制系统网络结构及网络边界存在的脆弱性。表 7 列出了通常工业控制系统可能存在的网络结构和网络边界脆弱性。

表 7 工业控制系统网络结构和网络边界脆弱性

脆弱性	描述
工业控制系统网络入侵及恶意代码攻击	黑客和攻击者设计实施针对工业控制系统网络进行分层隔离，可能会导致多个设备出现异常安全问题或被到整个工业控制系统网络中
缺陷的网络安全策略	由于系统投产需要对工业控制系统网络架构部署及策略进行开发和修改，可能在不经意间将安全漏洞引入网络架构的某一节点中
企业管理网络系统与工控网络中未部署逻辑隔离设备	网络之间未部署网络隔离设备，可直接通信。攻击数据包和恶意软件在网络之间传播，可轻易监测到其他网络上的敏感数据，造成未经授权的访问。
使用双宿主机	双宿主机可以导致数据在两个网络之间传输，若没有适当安全措施的双宿主机将会造成额外的威胁
在控制网中传输非控制数据	控制数据与非控制数据有着不同的要求，比如可靠性程度不同，因此在同一个网络中传输两种流量会导致难以配置网络。例如，非控制流量

核查网络结构和网络边界脆弱性，以及被评估方采取的安全措施的有效性

表 8（续）

脆弱性	描述
无关人员物理访问网络设备	对网络设备进行不当的物理访问会导致： 数据和硬件窃取； 数据和硬件的物理损伤破坏； 对网络安全环境（比如，修改 ACL 允许攻击进入网络）的篡改； 未授权的阻止或控制网络行为； 关闭物理数据链路
没有使用数据流控制	未采用数据流控制机制，如利用访问控制列表（ACL），限制系统或人对网络设备的直接访问
IT 安全设备配置不当	使用缺省配置往往导致主机上运行了不必要的开放端口和可能被威胁所利用的网络服务。不

表 9　通信和无线连接脆弱性

脆弱性	描述
文传输	攻击者可以使用协议分析工具或者其他设备解析 ProfiBus、DNP、Modbus、CAN 等协议传输的数据，实现对工业控制系统的网络监控。使用这些协议也可以使攻击者更容易攻击工业控制系统或控制工业控制系统网络行为
少认证机制	许多工业控制系统协议不具备认证机制，采用此类型的通信协议，存在重放或篡改数据的可能性
整性保护	大部分的工业控制系统协议不具备完整性检查机制。攻击者可以操纵这种没有完整性检查的通信
客户端与接入点间认	无线客户端与接入点之间认证不足，导致客户端访问的是攻击者伪造的接入点，同时非法入侵者可访问工业控制系统无线网络
客户端与接入点间数	无线客户端与接入点间传递的敏感数据未采用加密保护，攻击者监听明文信息造成信息泄露
界不清	无线网络的范围无法精确控制，导致非受控终端的接入

指南如下：

现场对工业控制系统控制柜及机房环境中的无线网络进行搜索，确认企业的无线组网是否采取身份认证措施，是否需要标识和密码验证，是否采取安全监测措施，检查被评估方有无为防止经无线网络进行恶意入侵所采取的其他措施，并分析其有效性；

在模拟仿真环境中对使用的通信协议进行协议分析，分析是否是明文传输；

在模拟仿真环境中使用重放攻击验证是否有数据校验，防篡改的措施；

评估方现场核查无线连接客户端与接入点间的认证方式，评估方在模拟仿真环境中采用相应的测试方法验证其有效性；

评估方现场核查是否有未授权接入无线网络的设备；

在模拟仿真环境中使用相应的工具分析该无线协议是否明文传输。

6.4.4　平台脆弱性识别

6.4.4.1　平台脆弱性识别概述

工业控制系统平台是由工业控制系统硬件、操作系统及其应用软件组成。平台脆弱性是由于工业控制系统中软件本身存在的缺陷、配置不当和缺少必要的维护等问题造成。平台脆弱性包括平台硬件、平台软件和

表 10　[illegible]

脆弱性	描述
开启远程服务的设备安全保护不足	开启远程服务的设备没有配备运行维护工作人员，也没有物理[illegible]
安全变更时未进行充分调试	更换设备时，未对其进行充分的检测

表 10（续）

脆弱性	描述
不安全的物理端口	不安全的通用接口如 USB、[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

表 11（续）

脆弱性	描述
对未定义、定义不明确的错误处理	一些工业控制系统没有充分测试就处理可能包含格式错误或者包含非法域值的数据包
依赖 OPC	不升级系统补丁，RPC/DCOM 的脆弱性可能被利用来攻击 OPC
使用不安全的工业控制系统协议	工业控制系统普遍使用的 CAN、DNP3.0、Modbus、IEC 60870-5-101、IEC 60870-5-104 和一些工业控制系统专用协议的相关信息已公开或被破译。而且这些协议中只有很少或根本不包含安全功能
开启了不必要的服务	不必要的服务未被禁用关闭，可能会被利用
使用明文传输协议	许多工业控制系统的系统协议以明文方式传递信息，导致消息很容易被攻击者窃听
配置和程序软件的认证和访问控制不足	攻击者可以通过非法访问配置和程序软件破坏设备或系统
未安装入侵检测和防御软件	入侵行为会导致系统不可用、数据被截获、修改和删除、控制命令的错误执行
某些软件中存在安全后门	不法供应商为了各种目的，在提供的软件中设置后门，危害性大
通信协议脆弱性	工业控制系统采用的部分通信协议，由于设计原因存在安全脆弱性，这些协议脆弱性可能被攻击者利用，造成系统的不可用，数据被截获、修改和删除，控制系统执行错误的动作等
未安装防护软件	恶意代码会导致系统性能低下、系统不可用和数据被截获、修改和删除
病毒防护软件病毒库过期	病毒防护软件病毒库过期导致系统容易被新的病毒攻击
安装病毒防护软件及其病毒库升级包前未经过仔细的测试	未经测试就安装病毒防护软件及其病毒库升级包可能会影响工业控制系统的正常运行
操作系统存在漏洞	操作系统不升级补丁，存在已知漏洞

实施指南如下：

a) 评估方查看平台中安装的操作系统版本及应用软件类型，例如：windows 操作系统、嵌入式系统、Linux 系统、程序下载软件、数据库软件、远程控制软件等；

b) 必要时在模拟仿真环境中对重要组件进行组件测试，识别其脆弱性；

c) 在模拟仿真环境中查看设备开启的端口，是否开启了不必要的端口服务；

d) 在模拟仿真环境中查找设备存在的系统漏洞；

e) 评估方查看平台是否安装病毒防护软件，病毒防护软件是否经过测试安装，病毒库是否定期更新，查看测试记录及病毒库更新记录；

f) 现场核查系统使用 DCOM 设备是否进行端口限定，是否对 OPC 及时修补升级；

g) 在模拟仿真环境中可以使用恶意代码针对 OPC 进行测试，识别其脆弱性；

h) 查看关键应用软件源代码，若关键应用软件为第三方供应商提供，则需与其联系，取得软件源代码，对其进行分析研判，识别其脆弱性；

i) 现场核查在远程访问控制设备时使用的专用设备及软件，在模拟仿真环境中对其进行技术检测，识别其脆弱性；

j) 现场核查并分析系统运行

络中；

m) 在模拟仿真环境中对使用的工业控制系统协议进行分析，是否是明文传输；

n) 在模拟仿真环境中进行重放攻击，验证是否有数据校验，防篡改；

o) 在模拟仿真环境中进行模糊测试，验证平台是否存在拒绝服务等安全漏洞；

p) 评估方现场查看工业控制系统中重要数据存储是否进行加密或采取其他安

6.4.4.4 平台配置脆弱性识别

平台配置脆弱性是指工业控制系统平台软硬件的配置存在的脆弱性。表 12 列出了工业控制系统的平台配置通常可能存在的

f) 现场核实是否有远程访问记录，远程访问是否经过批准或认证，远程访问数据是否加密，或者采用其他防篡改，防泄密的措施；

g) 现场核查是否使用平台软硬件安装时的预设口令、空口令是否无法登录系统，账户口令是否属于弱口令；

h) 评估方查看工业控制的权限分配，是否责权分离，是否是所需的最小权限，管理员权限是否被评估方指定管理，是否使用缺省访问控制。验证配置访问控制的有效性；

i) 现场核查平台软硬件是否具有限制无效访问次数的能力，对任何用户（人、软件进程和设备）在可配置的时间周期内连续无效访问尝试的次数是否限制为一个可配置的数目，在可配置时间周期内未成功尝试次数超过上限时，在指定时间内是否拒绝其访问直到由最高权限者解锁；

j) 检查控制系统是否提供会话锁能力，在会话不活跃状态超过可配置的时间周期之后，检查会话

弱性。

不同的工业控制系统的保障能力要求不同，本标准提供了一种通用的保障能力评估方法，评估方应根据被评估系统的特点、行业要求等，选取更适合被评估系统的保障能力评估方法，当没有更适用的方法时可以参考本标准进行评估。

6.5.2 网络安全管理

网络安全管理包括对制度建立及落实、责任明确及落实、人员安全管理、资产安全管理、供应链安全管理、外包服务管理、业务连续性管理、宣传教育培训和安全经费保障等方面的要求。评估人员可以依据 GB/T 32919—2016 附录 B 中的 B.1、B.4、B.5 和 B.6 对网络安全管理进行评估。

6.5.3 系统安全管理

工控安全管理通常包括对架构安全、连接安全、组网安全、配置安全、运维安全、数据安全、应急安全等方面的要求。评估人员可以依据 GB/T 32919—2016 中的 B.1、B.9 和 B.10 对系统安全管理进行评估。

6.5.4 密码使用管理

密码使用管理可以依据 GB/T 32919—2016 中的 B.18 进行评估。

6.5.5 宣传教育培训

宣传教育培训可以依据 GB/T 32919—2016 中的 B.11 进行评估。

6.5.6 应急响应

应急响应可以依据 GB/T 32919—2016 中的 B.17 进行评估。

6.5.7 技术防护能力

技术防护能力包括对物理环境安全防护、网络安全防护、网络设备安全防护、安全设备安全防护、服务器安全防护、终端计算机安全防护、存储介质安全防护、应用系统安全防护、门户网站安全防护、电子邮件系统安全防护、重要数据安全防护等方面的要求。评估人员可以依据 GB/T 32919—2016 中的 B.7、B.11、B.12、B.16、B.17 和 B.18 进行评估。

6.5.8 保障能力分析

通过对上述保障能力的识别，综合分析出工业控制系统的保障能力水平。表 14 给出了一种保障能力的等级划分方法。

表 14 保障能力等级划分

等级	标识	定义
4	低	未达到 GB/T 32919—2016 一级基线标准或不满足系统基本安全要求
3	一般	达到 GB/T 32919—2016 一级基线标准或满足系统基本安全需求
2	较高	达到 GB/T 32919—2016 二级基线标准或满足系统大部分安全需求
1	高	达到 GB/T 32919—2016 三级基线标准或几乎满足系统所有安全需求

6.6 风险分析

6.6.1 风险分析原理

完成了资产评估、威胁评估、脆弱性评估，保障能力评估后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对被评估方的影响，即安全风险。风险分析原理如图13所示。

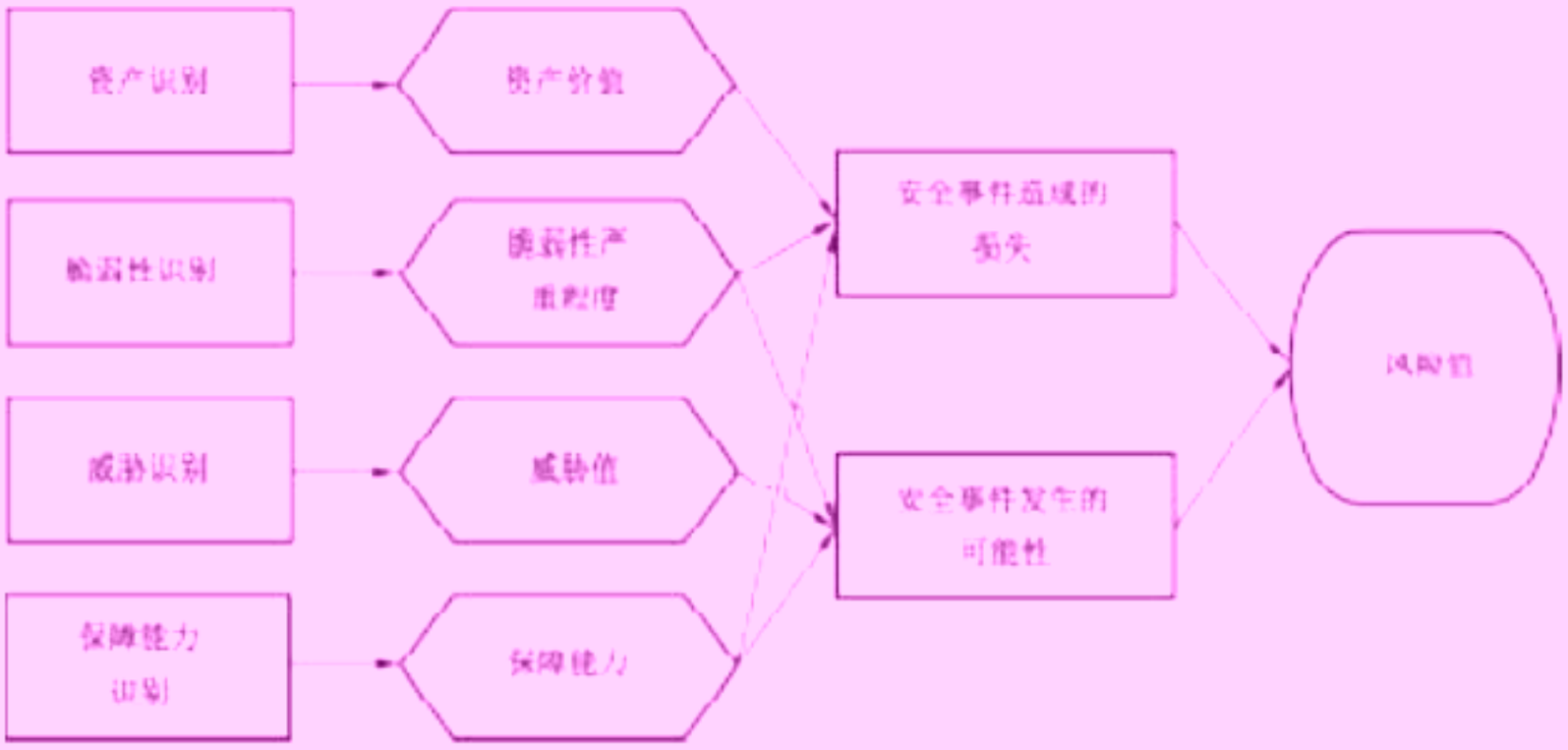


图 13 风险分析原理图

工业控制系统各要素的关系，R=F(A,T,V,P)。其中，R 表示安全风险；F 表示安全风险计算函数；A 表示资产；T 表示威胁；V 表示脆弱性；P 表示安全保障能力。风险分析如图 14 所示。

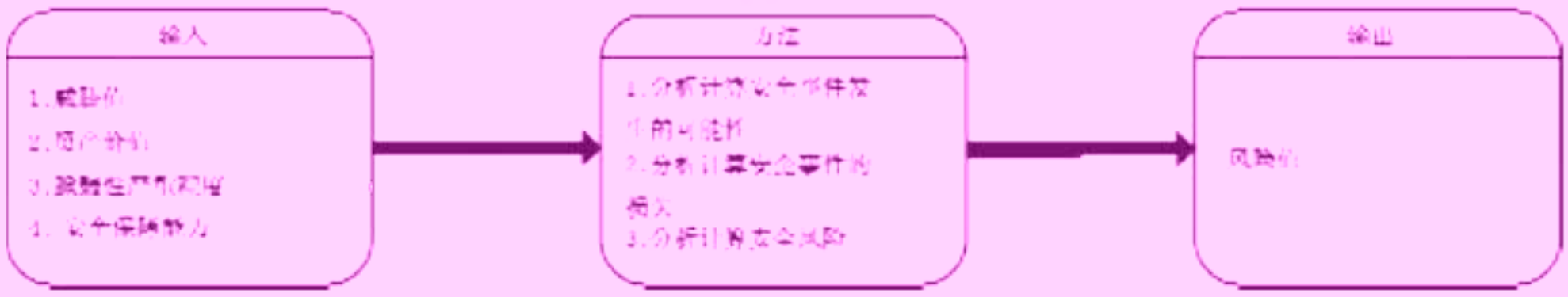


图 14 风险分析

风险计算方法包括定性计算和定量计算，[9]

表 15　风险等级划分表

等级	标识	描述
5	很高	一旦发生将产生非常严重的社会或经济影响，如重大生产事故、系统无法正常运行等
4	高	一旦发生将产生较大的社会或经济影响，如生产事故、在一定范围内影响系统的正常运
3	中等	一旦发生会造成一定的社会或经济影响，但影响面和影响程度不大
2	低	一旦发生造成的影响范围较小，一般很快可被相关方面采取一定手段予以控制
1	非常低	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

被评估方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。对表中资产的风险，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，需要采取一定安全措施以降低、控制风险。另一种的定不可接受的风险的办法是根据等级化处理的结果，设定可接受风险管理基准，选到相应等级的风险都进行处理。

6.7　残留风险控制

风险分析完成后，被评估方需判断风险是否在接受范围内。若风险是可接受的，被评估方应对残留

附 录 A
（资料性附录）
记录表

A.1 工业控制系统基本信息记录表见表 A.1。

表 A.1 工业控制系统基本信息记录表

系统名称	
主要业务	
操作对象	
与危险源关联情况	
部署位置	
网络拓扑结构	
连接互联网情况	
操作系统名称型号	
系统所在网段	
数据集中情况	
数据灾备情况	
服务对象	
用户规模	
业务周期	
业务主管部门	
运维机构	
系统开发商	
系统集成商	
上线运行及最近一次系统升级时间	
系统定级情况	

A.2 工业控制系统资产记录表见表 A.2。

表 A.2 资产记录表

编号	资产名称	品牌和型号	数量	位置	物理控制	业务应用	是否为关键资产
1							
…							
…							
…							

A.3 工业控制系统威胁记录表见表 A.3。

表 A.3 威胁记录表

编号	威胁名称	威胁来源	威胁动机	威胁攻击方法	威胁发生的可能性	威胁发生后造成的影响
1						
…						
…						

附 录 B

（资料性附录）

表 B.2（续）

序号	核查项	核查结果
3	系统网络边界中是否使用网络隔离设备	
4	系统划分 VLAN 是否合理	
5	网络链路是否有冗余设计	
6	网络设备是否有容错能力	
7	控制网络中是否部署企业级应用	
8	控制网络中是否允许 IT 网络服务应用	
9	被评估方是否限制工业控制系统系统访问的数量	
10	网络中存在的通信协议有哪些	
11	控制网络中是否采用专用标准的协议	
12	通信协议是否是明文传输	
13	通信协议是否健壮	
14	是否使用密码产品	
15	是否对产生的密钥进行管理	
16	是否使用无线传输协议	
17	无线	

表 B.2（续）

序号	核查项	核查结果
35	Password 是否加密	
36	是否存在简单口令	
	是否禁用远程管理员权限操作	
38	是否禁用 Telnet 方式访问系统	
39	是否使用 SSH	
40	是否限制 VTY 的数量	
41	是否启用远程访问 ACL 控制	
42	是否开启 SNMP 服务	
43	SNMP 版本	
44	SNMP 服务的共同体字符串是否为默认值	
45	SNMP 是否设置了 ACL 控制	
46	是否禁用 HTTP 配置方式	
47	设备是否定时账户自动退出	
48	是否禁用不使用的端口	
49	是否禁用 AUX 端口(远程配置端口)	
50	是否开启日志功能,能否远程传输保存日志	
51	是否有日志审计功能	
52	是否配置了 SYSLOG	
53	SYSLOG 配置信息	
54	SYSLOG 能否被收集	
55	logging 的配置	
56	是否设置安全访问控制,过滤掉已知安全攻击数据包	
57	当前系统版本是否存在严重的安全漏洞	
58	当前系统版本是否需要升级	

B.3 工业控制系统平台脆弱性核查表示例见表 B.3。

表 B.3 平台脆弱性核查表

序号	核查项	核查结果
1	ICS 是否进行物理或逻辑分区	
2	系统中部署工程师站、操作员站、实时数据库、历史数据库等应用的 PC 和服务器中使用的操作系统是否最新版本,是否存在已知漏洞	
3	HMI、PLC、RTU 和 IED 等控制组件使用的是否是专用操作系统	
4	专业操作系统是否最新版本,是否存在已知漏洞	
5	是否开放的非必要的 TCP 和 UDP 端口	

表 B.3（续）

序号	核查项	核查结果
6	历史数据库是否使用通用数据库，是否存在已知漏洞	
7	实时数据库是否为专用数据库，是否存在已知漏洞	
8	组态软件是否存在已知漏洞	
9	是否进行 MAC 地址绑定	
10	是否禁止控制网络中设备接受邮件	
11	系统中是否使用 TELNET、FTP、TFTP 进行文件传输	
12	用户功能与系统管理功能是否分离	
13	账户类型是否基于角色、设备和属性进行设立	
14	工程师站、操作	

表 B.3（续）

序号	核查项	核查结果
40	是否限制当前会话数量	
41	是否下载控制程序时加密	
42	是否具有防御措施防制非授权用户对设备固件进行更新和维护	
43	固件是否加壳加密	
44	PLC、RTU、DCS 控制器是否存在硬件锁	
45	管理员是否更改默认名称	
46	Administrators 组是否存在可疑账号	
47	端口、进程对应信息检查	
48	检查主机端口限制信息	
49	查看主机磁盘分驱类型	
74	检查注册表中自动启动选项	

表 B.3（续）

序号	核查项	核查结果
75	有无指定当前主机的操作人员	
76	有无指定当前主机的物理接触人员	
77	有无相应的物理损害和其他故障的备份恢复策略	
78	操作人员是否有对应的日志记录	
79	是否安装防病毒软件	
80	防病毒软件厂商	
81	防病毒软件是否自动更新	
82	防病毒软件当前版本	

B.4　工业控制系统保障能力核查表示例见表 B.4。

表 B.4　保障能力核查表

序号	核查项	核查结果
1	是否设立了专门组织机构管理工业控制系统	
2	机构成员角色如何设立	
3	成员职责如何分派	
4	与其他业务部门的关系及如何协调	
5	是否配备一定数量的系统管理员、网络管理员、安全管理员等	
6	是否配备专职安全管理员，不可兼任	
7	查阅相关工作计划、工作方案、规章制度、监督检查记录、宣传教育培训记录等文档，检查网络安全管理机构的履职情况	
8	关键事务岗位是否配备多人共同管理	
9	是否根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等	

表 B.4（续）

序号	核查项	核查结果
17	建立并严格执行外包服务安全管理制度	
18	与网络技术外包服务提供商签订服务合同和网络安全与保密协议，明确网络安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何资产，不得以服务为由强制要求委托方购买、使用指定产品	
19	安全管理员是否定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况	
20	组织或上级单位是否定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	
21	是否制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报	
22	是否制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动	
23	是否建立了[illegible]系统安全事件应急管理策略	
24	是否制[illegible]了移动存储设备的使用与管理策略	
25	是否对系统的配置变更进行安全管理	
26	是否制[illegible]了计算机病毒防治管理制度	
27	是否建立了数据备份管理制度	
28	是否形成由安全策略、管理制度、操作规程和记录组成的全面的管理安全管理制度体系	
29	是否指定或授权专门的部门或人员负责安全管理制度的制定	
30	安全管理制度是否具有统一的格式，并进行版本控制	
31	安全管理制度是否通过正式、有效的方式发布	
32	是否对[illegible]或人员执行安全管理制度的情况[illegible]检查	

参 考 文 献

[1] 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

[2] GB/T 26333—2010 工业控制网络安全风险评估规范

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

[4] ISO/IEC 27005:2008 Information Technology—Security techniques—Information security risk management

[5] IEC 60870-5-101 Telecontrol equipment and systems—Part 5-101:Transmission protocols—Companlon standard for basic telecontrol tasks

[6] IEC 60870-5-104 Telecontrol equipment and systems—Part 5-104: Transmission proto-

[13] IEC/TR 62443-3-1 Industrial communication networks—Network and system security—Part3-1:Security technologies for industrial automation and control systems

[14] IEC 62443-3-2 Industrial communication networks—Network and system security—Part3-2:Security levels for zones and conduits9

[15] IEC 62443-4-1 Industrial communication networks—Network and system security—Part4-1: Product development requirements10

[16] IEC 62443-4-2 Industrial communication networks—Network and system security—Part4-2:Technical security requirements for IACS components11

[17] NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

[18] NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security

[19] NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment