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

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。

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 31509—2015 信息安全技术 信息安全风险评估实施指南

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

ISO/IEC 62264-1:2013 企业控制系统综合 第1部分：模型和术语(Enterprise-control system integration—Part 1: Mo...

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[illegible]rotocol)

DCOM　分布式组件对象模式(Microsoft Distributed Compo[illegible]mt 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[illegible]Interface)

CVSS　通用漏洞评分系[illegible]统(Common Vulnerability Scoring Syste[illegible])

4　概述

4.1　工业控制系统

[illegible]次结构模型

[illegible]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[illegible]。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[illegible]013 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

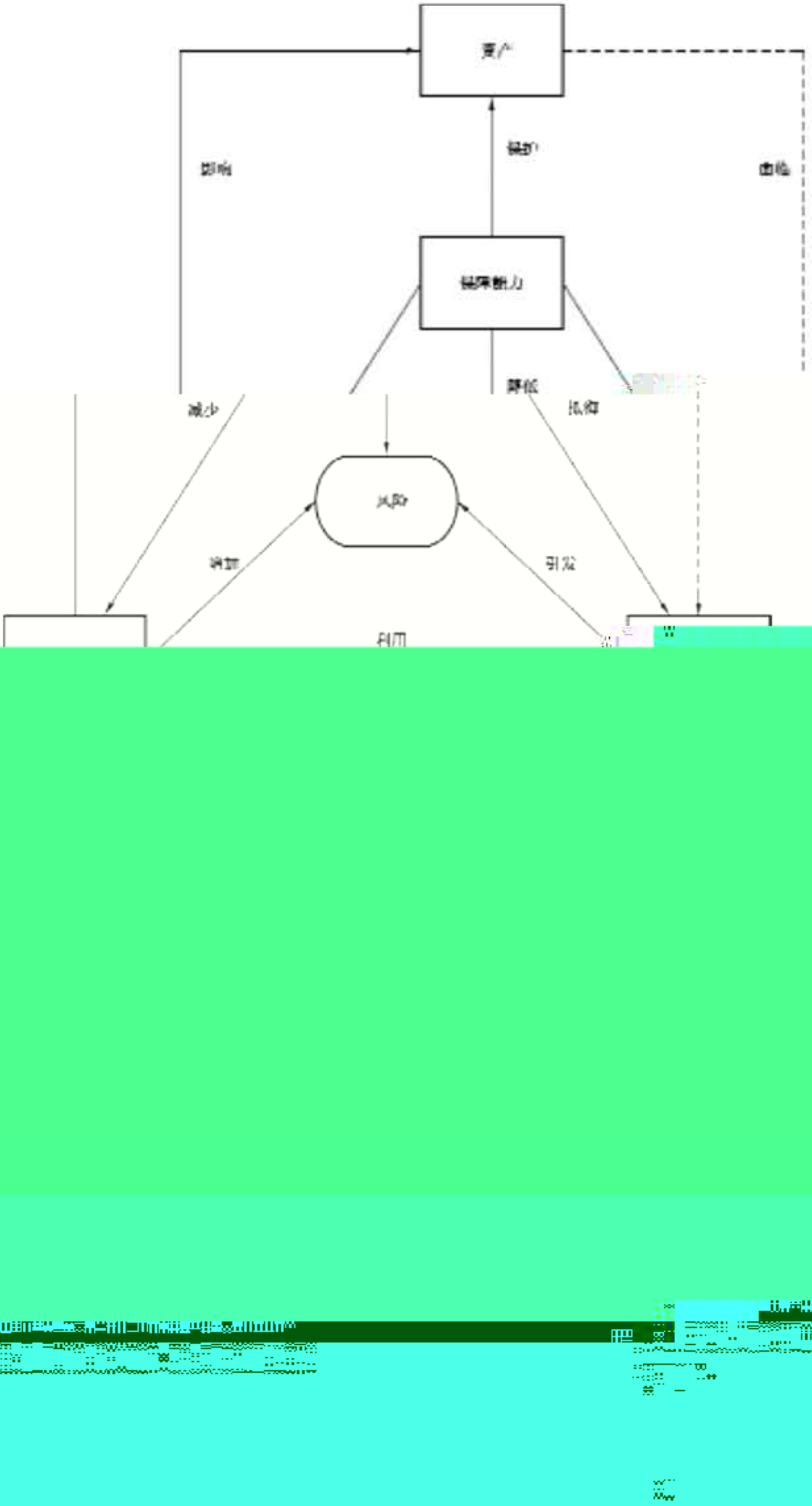
工业控制系统

系统的架构差别较

ISO/IEC 62264-1:

色部分所示:


企业资源层
层级 4，企业资源层


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，评估方需确定可生计划保证评估生产的顺利进行。

风险评估实施过程见第6章，风险评估实施流程如图3所示。

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规划设计方案、网络拓扑

[illegible]人员进行沟通，制定现场核查计划安排。如果工业控制系统分布区域很[illegible]涉及多个部门，需提前做好计划安排，统筹时间和人员等；

b) 对于部分工业控制系统所在的现场环境恶劣的情况，应严格遵守被评估方现场规章制度；必要时，在进入工业控制系统现场前，被评估方可组织评估人员进行安全[illegible]教育培训，保障人员的

人员和相应的信[redacted]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，其中离散型工业控制系统（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，这种测试有[redacted]

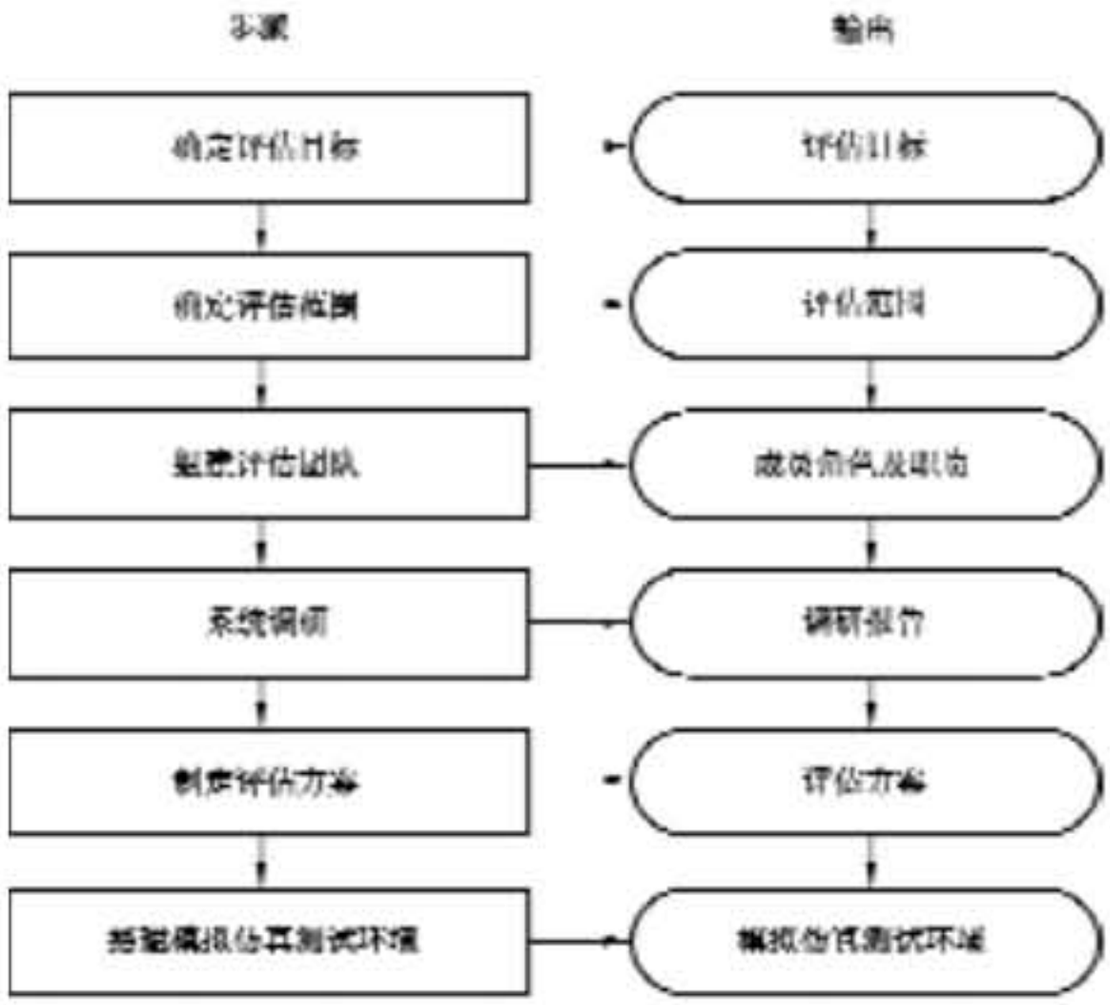


图 4　风险评估准备工作流程

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

[illegible]

[illegible]

[illegible]合评估范围时，应结合评估目标以及工业控制系统的实际建设运行情况合理的确定评估范围边界。确定评估范围如图 6 所示。

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[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]

d） 对风险评估整个过程进行监督

6.1.5 系统调研

系统调研是依据于解被评估对象的过程，风险评估组应进行充分的系统调研，修正评估目标和范围，同时为风险评估依据和方法的选择、评估内容节点确定基础。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

[illegible]

图 7 系统调研

[illegible]

其承担的业务、网络结构、系统重要程度等；

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，以使评估实施时可以进行技术沟通；

2) 查看工业控制系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，用于管理评估工作活动开展，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

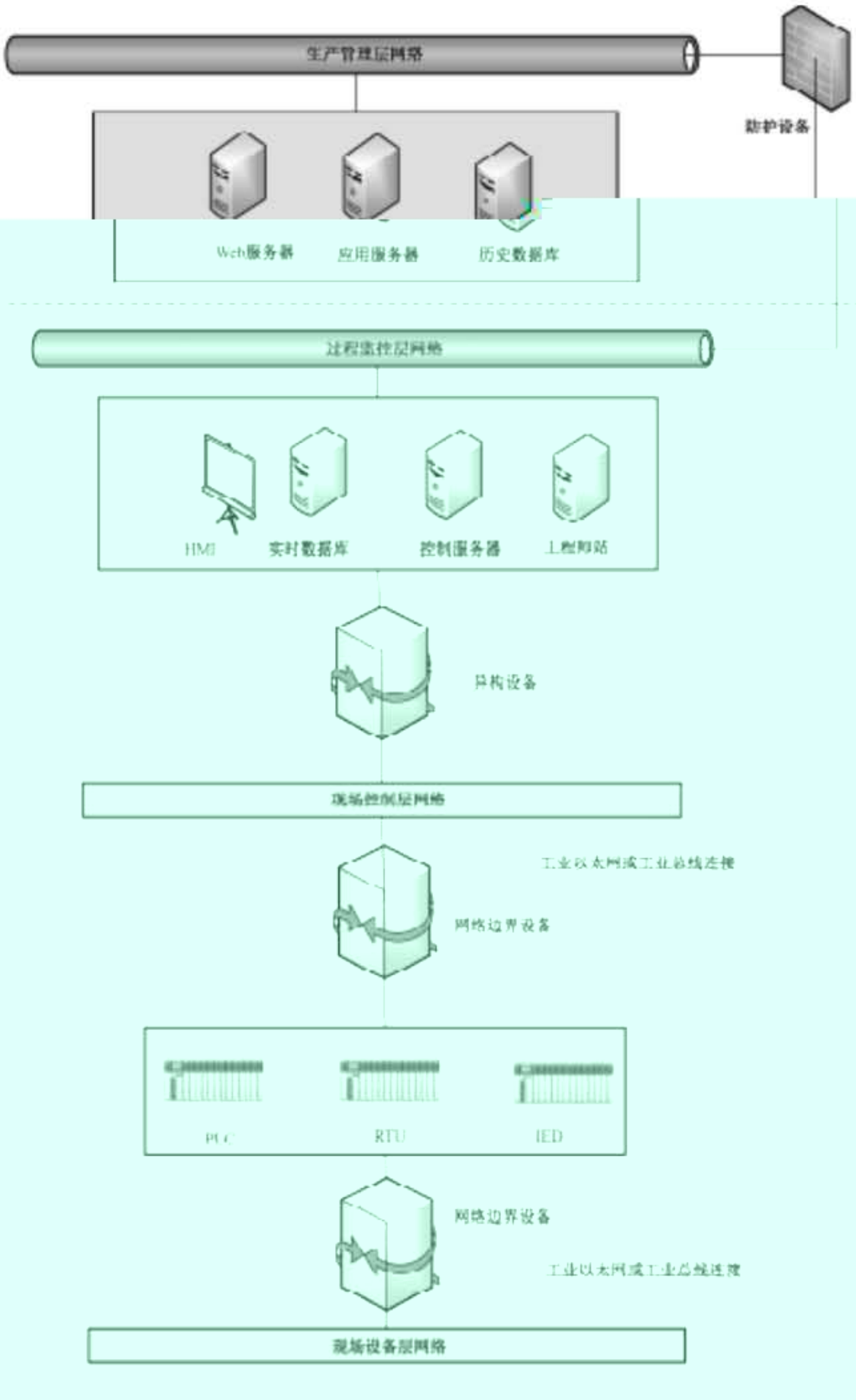

生产管理层网络
防护设备
Web服务器
应用服务器
历史数据库
过程监控层网络
HMI
实时数据库
控制服务器
工程师站
异构设备
现场控制层网络
工业以太网或工业总线连接
网络边界设备
PLC
RTU
IED
网络边界设备
工业以太网或工业总线连接
现场设备层网络

图 8 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。不同类别的资产重要性不同，面临的威胁也不同。对工业控制系统及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具体的评估对象和要求，由评估方灵活把握。根据资产的表现形式，可将资产分为软资产、硬资产和人力资产等，如表 3 所示。

表 3 一种基于表现形式的资产分类实例

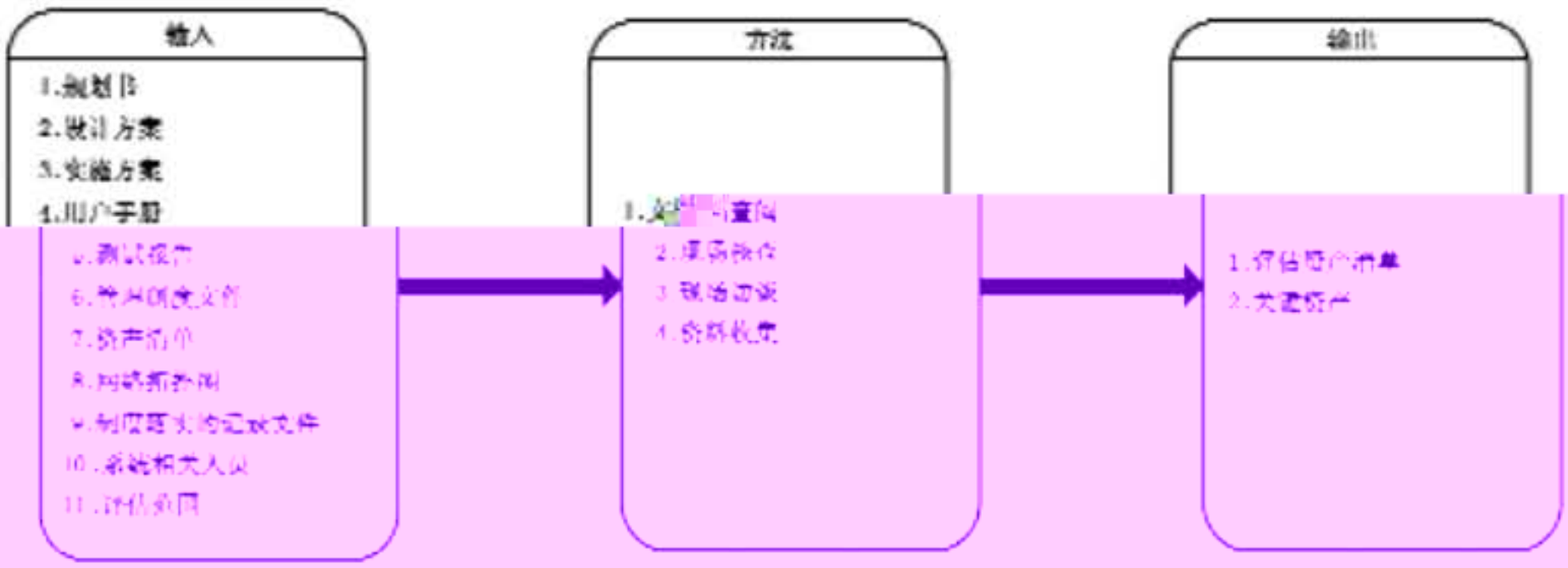


图 9　资产调查

协议也属于系统资产。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) 评估方根据识别出的工业控制系统的关键功能需求及安全需求，确定工业控制系统的关键资产。

5.2.2　资产分析

针对工业控制系统的业务流程，确定工业控制系统的工艺需求，工业控制系统的

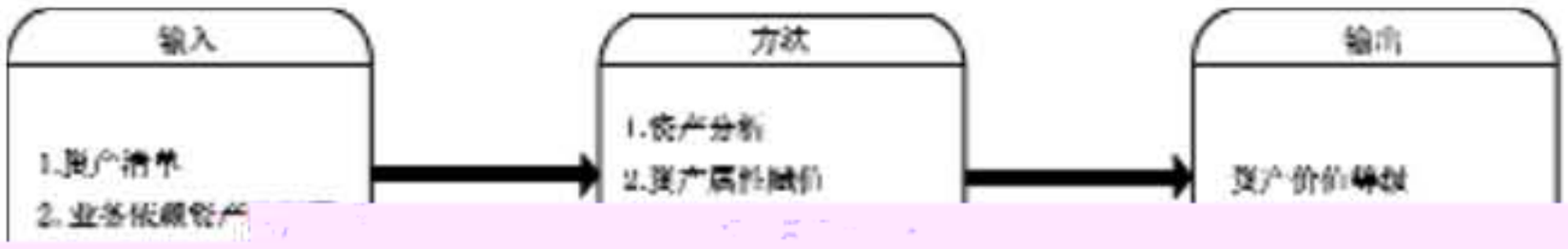


图 E.1 资产分析

实例描述如下：

a) 在完成资产的业务、分析所有资产的安全属性与相关关键性之后，赋值结果；

b) 在完成资产与存在及发现威胁的对应关系之后，对资产的业务、资产价值等级进行下一步的风险评估。

6.3 威胁评估

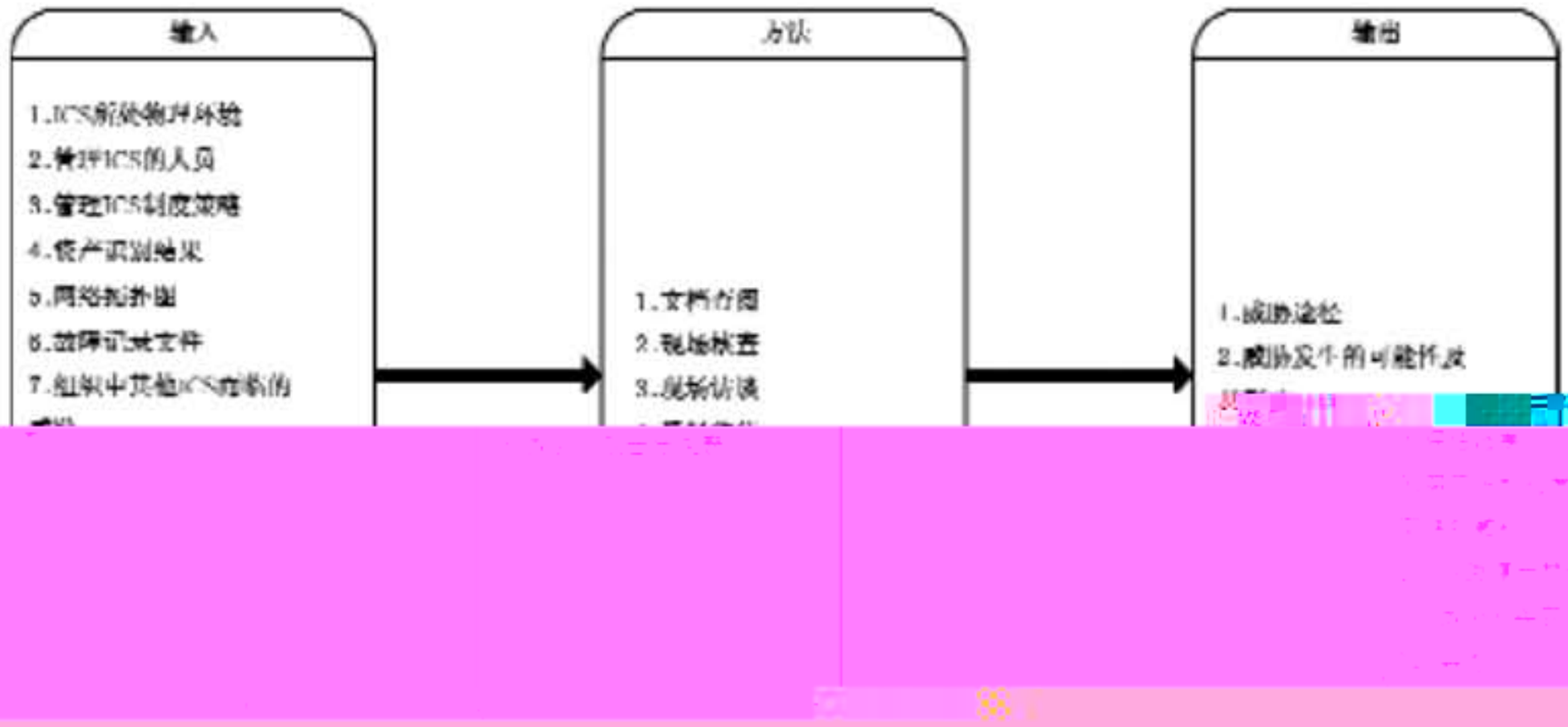
6.3.1 威胁评估概述

威胁是指可能导致危害系统或被评估方某个合理发生的潜在事件，威胁会依赖存在于某个资产的弱

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	自然灾难对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，旁路，嗅探)，以修改存储于工业控制系统组件和


输入
1.ICS所处物理环境
2.管理ICS的人员
3.管理ICS制度策略
4.资产识别结果
5.网络拓扑图
6.故障记录文件
7.组织中其他ICS有关的
方法
1.文档查阅
2.现场核查
3.现场访谈
输出
1.威胁途径
2.威胁发生的可能性及

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；

c) 确定客体范围，其范围越广泛，威胁发生的影响越大；

d) 受影响客体的可补救性也是威胁影响的一个重要方面。遭到威胁破坏的客体，有的可以补救且补救代价可以接受，威胁发生的影响较小；有的不能补救或补救代价难以接受，威胁发生的影响较大。

6.3.4 威胁分析

在调查威胁的基础上，识别威胁发生的概率、威胁影响，分析并确定计算威胁值的方法并对其进行赋值。威胁分析实施见 GB/T 31509—2015。

6.4 脆弱性评估

6.4.1 脆弱性评估概述

脆弱性是资产自身存在的，威胁总是要利用资产的脆弱性才可能造成危害。评估方应考虑工业控制系统脆弱性具有难以修复、原则上需要保密的特点，从物理环境、网络、平台和安全管理 4 个方面对工业控制系统脆弱性进行评估。

脆弱性评估分为脆弱性识别与脆弱性分析两个环节。

生活分析对实施的安禁措施评估范围常见脆弱性依据国际或国家安全标准等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；

标识、访客人

配备应急电

员登记、专人陪同、不准携带移动介质、相机等管理措施；

c) 评估方查看工业控制系统所在场所是否安装避雷针、安装通风装置、配备灭火器源、远离易燃易爆物品、建筑物漏水渗水等；

d) 评估方查看工业控制系统

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
系统处于复杂电磁环境内	应避免系统暴露于强电磁场

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
工业控制系统网络分层	设计和方设计实施无法对工业控制系统网络进行分层隔离，可能会导致多个设备
潜在的网络安全漏洞	由于业务和操作需要对工业控制系统网络架构的开发和修改，可能在不经意间将安全漏洞引入网络架构的某一部分中
企业资源计划（ERP）等非工业控制网络与工业控制网络之间未部署安全防护或者设备	网络之间未部署网络隔离设备，可导致通信、数据泄露和恶意攻击等网络安全事件传播，可轻易渗透到工业控制网络中的敏感区域，造成无法预料的后果
缺少入侵检测/入侵损耗控制机制	流量传输所需要的网络带宽资源，导致工业控制系统的系统功能中
在工业控制网络中被使用	在控制网络中应用 IT 网络服务	IT 网络中使用的服务，如 DNS、DHCP、HTTP、FTP、SMTP 等，用时，可能引入额外的严重安全漏洞
非法的数据流向	控制网络
线路或设备没有冗余	在重要的网络中没有冗余备份链路，可能导致设备遭遇单点故障	重要网络配置
义不清晰	控制网络边界定义不清晰，将难以保证必要的安全措施被合适的实施或配置，会导致对系统和数据的未授权的访问和其他问题	安全边界
设备		

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。

实施指南如下：

a） 查看网络拓扑图及现场核查工业控制系统网络结构是否分层，各层之间是否部署访问控制。

表 8（续）

脆弱性	描述
	对网络设备进行不当的物理访问会导[illegible]
员物理访问网络设备	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
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
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。[illegible]防火墙配置规则和路由器访问控制列表将允许不必要的流量通过
网络设备配置未备份	没有制定和实施网络设备配置备份和恢复规程，偶然或者恶意对网络设备配置进行修改造成系统通信中断时无法及时恢复
口令未加密传输	以明文传输的口令很容易被攻击者窃听，攻击者会利用这些口令对网络设备进行非法访问，通过这种访问，攻击者可以破坏工业控制系统的系统操作或者监视工业控制系统系统网络行为
网络设备口令长期未更改	口令应定期更换，这样，即使未授权用户获得密码，也只有很短的时间段内可以访问网络设备，未定期更换密码可能使黑客破坏工业控制系统的操作或监视器工业控制系统的网络活动
采用的访问控制不足	通过非法访问网络设备，攻击者可以破坏工业控制系统的系统操作或者监视工业控制系统网络行为
专用工业控制系统协议转换设备采用默认设置	将工业控制系统网络中总线协议转换为以太网协议进行数据传输，该设备多为专用设备，管理人员对其内部知之甚少，多采取出厂默认设置，存在一定安全风险

[illegible]

表 9　通信和无线连接脆弱性

脆弱性	描述
明文传输	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
缺少认证机制	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
缺少完整性保护	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
无线客户端与接入点间认证不足	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
无线客户端与接入点间数据保护不足	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
无线网络边界不清	无线网络的范围无法精确控制，导致非受控终端的接入

实施指南如下：

a) 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；

b) 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；

c) 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；

d) 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；

e) 评估方现场核查是否有未授权接入无线网络的设备；

f) 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[illegible]软硬件本身存在的缺陷、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、平台软件和平台配置 3 个方面的脆弱性。

6.4.4.2 平台硬件脆弱性识别

平台硬件脆弱性是指工业控制系统平台硬件设备存在的脆弱性。表 10 列出了工业控制系统的平台硬件通常可能存在的脆弱性。

表 10　平台硬件脆弱性

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

表 11（续）

脆弱性	描述
对未定义、定义不明确或设“非法”情况的错误处理	一些工业控制系统没有进行有效检测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

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必

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

			未设置口令	系统登陆无口令(如果系统有用户账户 系统启动无口令(如果系统没有用户账 系统待机无口令(如果工业控制系统组
一段时间内没被使用)				
能擅自访问机密信息。例子包括：			口令保护不当	缺少适当的密码控制措施，未授权用户 以明文方式将口令记录在本地系统； 与个人账户使用同一的口令； 口令泄漏给第三方； 在未受保护的通信中以明文方式传输口
令				
统用户具有过多或过少的权限。如采用 管理员特权			访问控制不当	访问控制方法不当，可能导致工业控制 缺省的访问控制设置使得操作员具备了
、修改和删除，控制命令的错误执行			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
情况下，实施对工业控制系统的远程访			不安全的工业控制系统组件远程访	系统工程师或厂商在无安全控制措施

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

的脆弱性
赋值时应
处理，不同

赋值方法，例如 CVSS。由于很多脆弱点反映的是同一方面的问题，或可能造成相似的后果
综合考虑这些脆弱点，以确定这一方面脆弱性的严重程度。脆弱性严重程度可以进行等级化

	低	如果被成功利用，对资产造成较小损害
	很低	如果被成功利用，对资产造成的损害可以忽略

6.5 保障能力评估

6.5.1 保障能力评估概述

和对策的能
少系统脆弱性、抵
件发生时，缓解对

、宣传教育培训、应
相关法律、规则和
抵御威胁和减少脆

保障能力是指被评估方在工业控制系统管理、运行、人员和技术等方面提供保障
工业控制系统的安全需求，可以通过安全保障措施的一个或多个层面的安全保障能够
御工业控制系统所面临的安全威胁，从而降低工业控制系统的安全风险；或在安全
被评估方的影响。

保障能力评估包括但不限于对网络安全管理、工控系统安全管理、密码使用管
急响应、技术防护能力等六个方面进行充分性、合规性、有效性的评估。合规性是指
标准的一致性；充分性是指充分覆盖被评估方的安全需求；有效性是指能保护资产

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情况的确认、人员安全管理、资产安全管理、供应链安全

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。

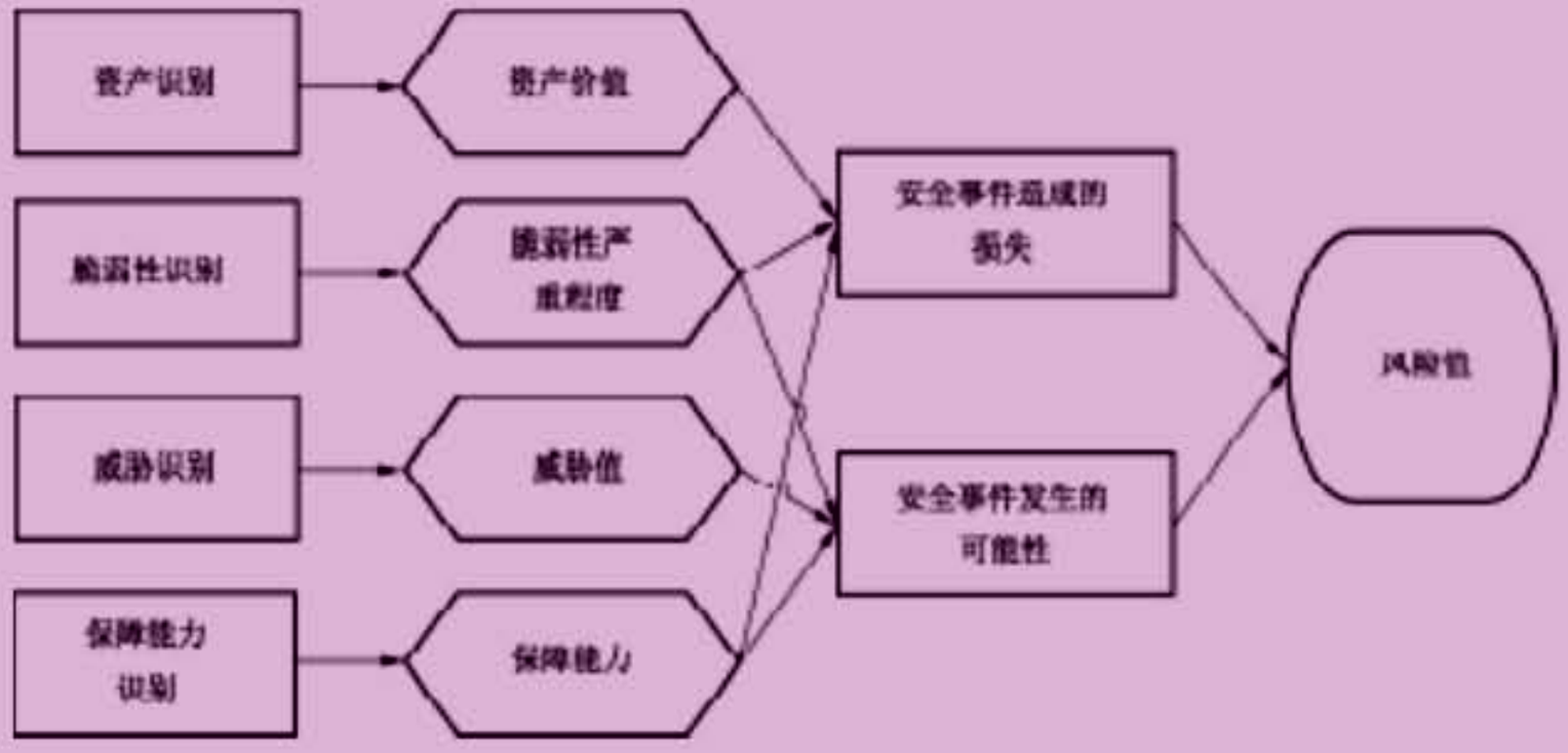


图 13 风险分析原理图

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。

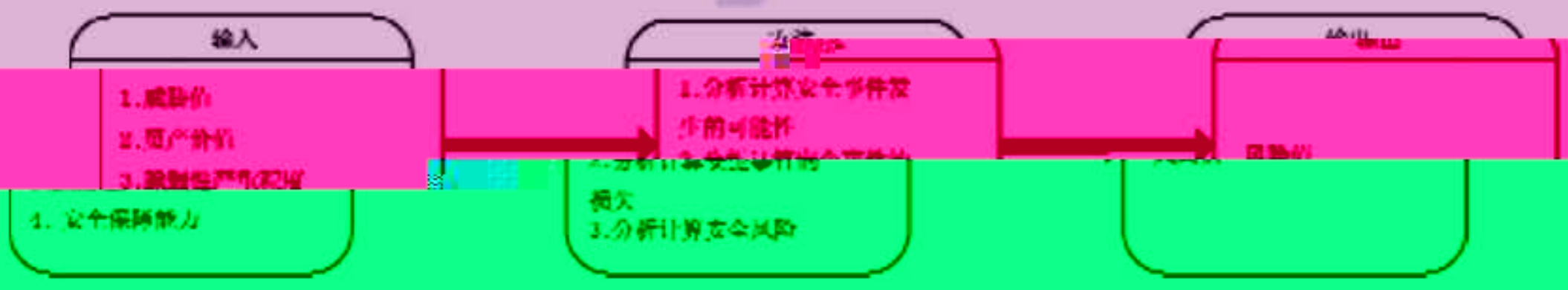


图 14 风险分析

风险计算方法包括定性计算和定量计算，但由于实际工作中定量计算方法的可操作性较差，一般多采用定性计算方法。无论评估方采用何种计算方法，都应对完成协议跨界的设备以及关键设备重点加权。

评估方通过风险计算，完成对风险情况的综合分析与评价。

6.6.2 风险结果判定

为实现对风险的控制与管理，可以对风险评估的

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行等
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程度较低，一般仅限于被评估方内部，通过一定手段很快能解决
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

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。

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，被评估方应对残留风险进行持续的监控。若风险不可接受，需制定风险控制措施并实施风险控制行动。在实施风险控制行动之后，对仍然存在的不可接受安全风险应重新进行评估、控制和管理的活动。残留风险的评估流程及内容可有针对性的适当剪裁。

风险评估报告是综合分析阶段的输出文档，是对整个风险评估过程和结果的总结。

评估方根据评估检测数据和风险计算结果，对被评估对象进行定性、定量分析，明确被评估对象面临的威胁和主要脆弱点，提出相应的整改建议，并在此基础上编制风险评估报告。风险评估报告需要对评估对象进行说明，并阐明采用的风险计算原理及风险评估方法。报告中应对综合分析阶段的结果给予详细说明，主要包括资产、威胁和脆弱性的评估结果，风险对被评估方业务及系统的影响范围、影响程度，风险统计和风险等级，残留风险控制等。评估报告发布后，若需改动或增补，只能采用补充报告的形式，报告上应标明原报告的标题和编号，补充报告的编写要求与原报告相同。

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	IP 地址	物理位置	业务应用	是否为关键资产
1							
2							
3							
4							
5							
6							

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						
2						
3						
4						

附 录 B

资料性

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	

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	
37	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	
50	检查特定目录的权限	
51	审核策略成功还是失败	
52	系统日志覆写规则是否默认	
53	系统日志覆写规则	
54	安全日志存储位置是否默认	
55	安全日志存储位置	
56	最大安全日志文件大小是否默认	
57		

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	
32	需要改进的安全管理制度进行修订	
33	符合性审查	
34	是否对各岗位人员进行了安全意识和基本技能培训	
35	是否与关键岗位人员签署了保密协议	
36	应严格规范人员离岗过程，及时终止离岗员工的所有访问权限	
37	是否有对从事信息安全服务的第三方人员的管控措施	
38	是否对关键岗位的人员进行全面、严格的安全审查和技能考核	
39	是否对考核结果进行记录并保存	
40	是否对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行	
41	建立资产台账(清单)，对资产进行统一分类、分级、编号、标识，及时记录资产状态和使用情况，保证账物相符	
42	专人负责资产的管理	

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-