ICS 35.040
L 80

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

信息安全技术
工业控制系统网[illegible]险评估实施指南

[illegible]息安全风险评估规范
信息安全风险评估实施指南
[illegible]业控制系统安全控制应用指南
[illegible]制系统综合　第1部分:模型和术语(Enterprise-control system
[illegible]
GB/T 20984—2007　信息安全技术　信[illegible]
GB/T 31509—2015　信息安全[illegible]术　[illegible]
GB/T 32919—2016　信息安全技术
IS[illegible]2264-1:2013　企业控
integration—Part 1:M[illegible]dels and ter
3　术语、定义和缩略语[illegible]
[illegible]
3.1.3
主终端单元 master terminal unit;MTU
用于生产过程信息收集和检测的工业控制系统总站。
注:一般部署在调度控制中心。
3.1.4
远程[illegible]note terminal unit;RTU
用于监测、控制远程工业生产装备的工业控制系统远程站点设备。
3.1.5
[illegible]ble logic controller;PLC
采用可编程存储器,通过数字运算操作对工业生产装备进行控制的[illegible]字设备。

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：一般部署在厂站网络。

3.1.7

人机界面 human-machine interface;HMI

为操作者与控制器之间提供操作界面和数据通信的软件平台。

4 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)

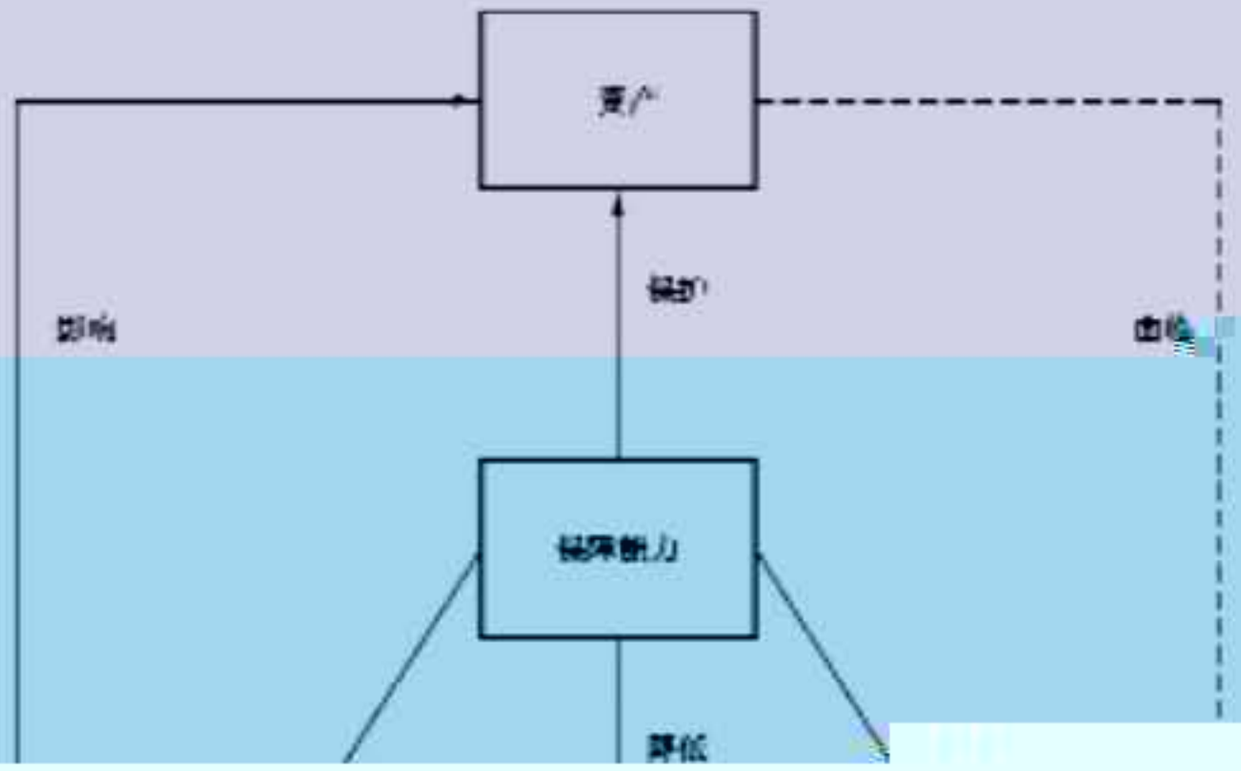
DCOM 分布式组件对象模式(Microsoft Distributed Component Object Model)

OPC 用于过程控制的对象连接与嵌

[illegible]

[illegible]则，包括标准性原则、关[illegible]务原[illegible]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[illegible]方工业控制系统风险评估机构实施。



1) 脆弱性会影响资产安

4.3.2 风险评估流程

图3 风险评估实施流程图

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；

……进行签字确认。

5.4 现场核查

现场核查是……系统现场生产……

以下几种情况可能需要使用现场核查：

a) 对工业控制系统现场物理环境评估；

b) 对工业控制系统配置、系统架构和系统日志等评估；

c) 对工……管理评估；

d) 对已采取安全措施所需的确认。

实施指南如下：

a) 评估方……采用现场核查的方法对工业控制系统现场……生产管理……

……保障人员的安全；

人员和相应的信息安全人员充场，最好由工业控

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

生识别往往需要

测试设备的

或干扰被测试系统的数据库中产

生正效数据。若使用工业控制系统的开发、测试或备用系统作为模拟仿真测试环境，在测试完成后需要经过验证才能将其投入使，以承担其原本的功能。

模拟仿真测试最常用的技术测试方法包括：渗透测试、固件逆向分析、专用嵌入式系统分析、

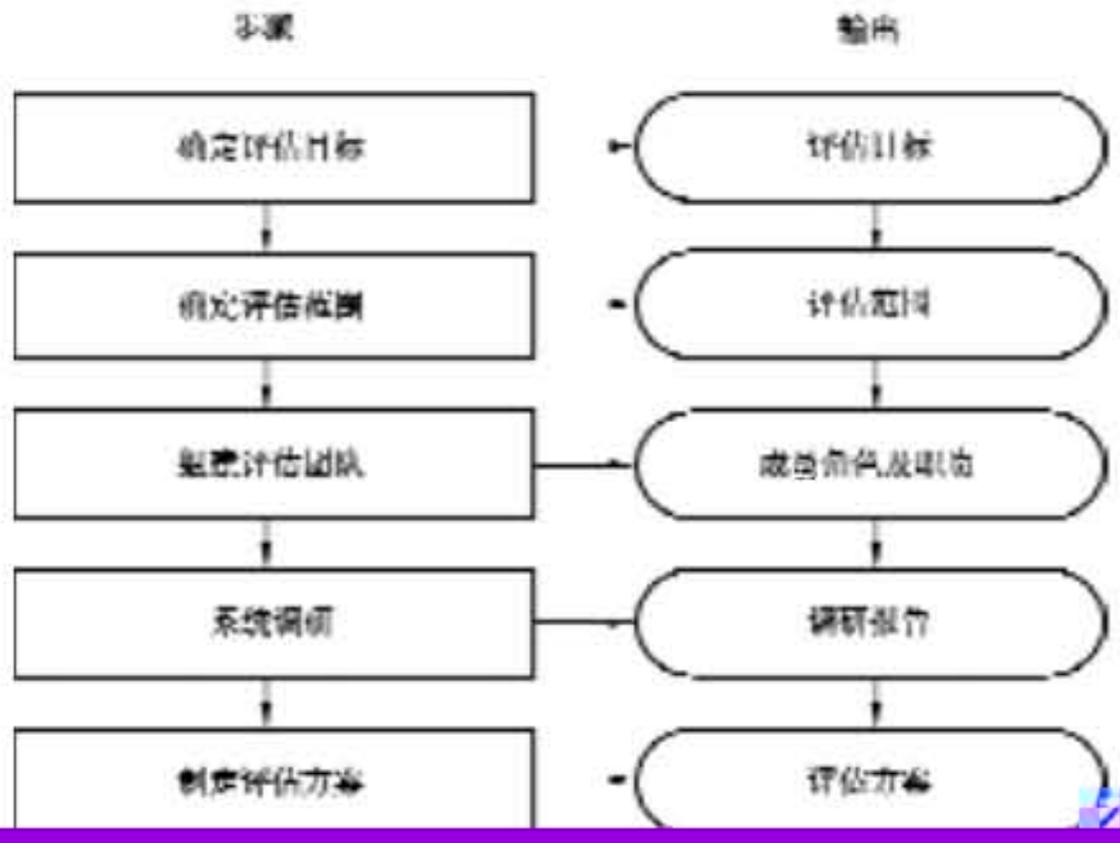
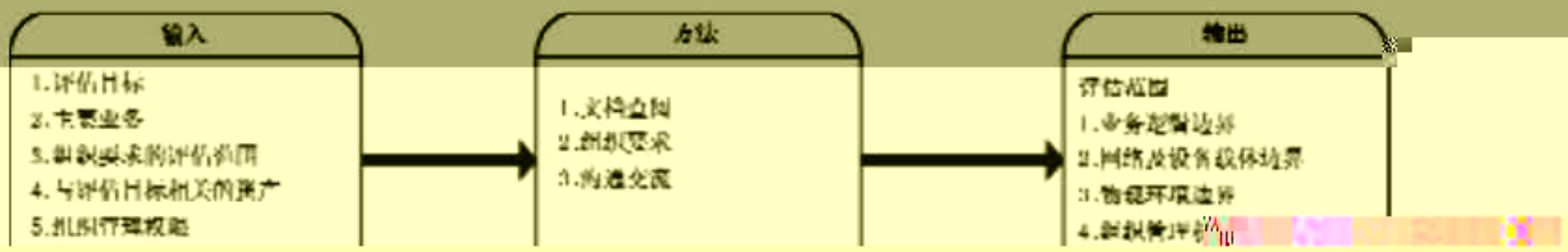


图 5 确定评估目标

实施指南如下：

a) 评估方应根据输入的文档材料及对相关人员的访谈，分析研判出工业控制系统现在所处的生



的是工控系统生态的哪一部分，涉及哪些利益相关方，从而

	7）配合搭建模拟仿真测试环境

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[illegible]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]09—2015 规定的； 2) 参与保密教育及相关技术
质量管控员	1) GB/T 3[illegible]

表 2 被[illegible]

[illegible]方成员职位与职责描[illegible]

表 2（续）

被评估方人员职位	工作职责
人员	2）参与保密教育及相关技术培训；
责包括：	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

系统集成商

专家组由工业控制系统相关领域专家组成，职

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；

具体的业务、网络结构、系统……

……设备、网络边界设备，包括其品牌、型号、……配置、开启的服务等；

b) 关键软件，包括其厂商、版本号、补丁、配置等；

c) 通讯协议；

d) 系统架构及网络架构等；

e) 模拟仿真测试环境的规模……不必与实际系统相同。若被评估方……在工业……的开发、测试环境，评估方需对其进行评判，满足模拟仿真环境的要求后方可在……

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[illegible]
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。

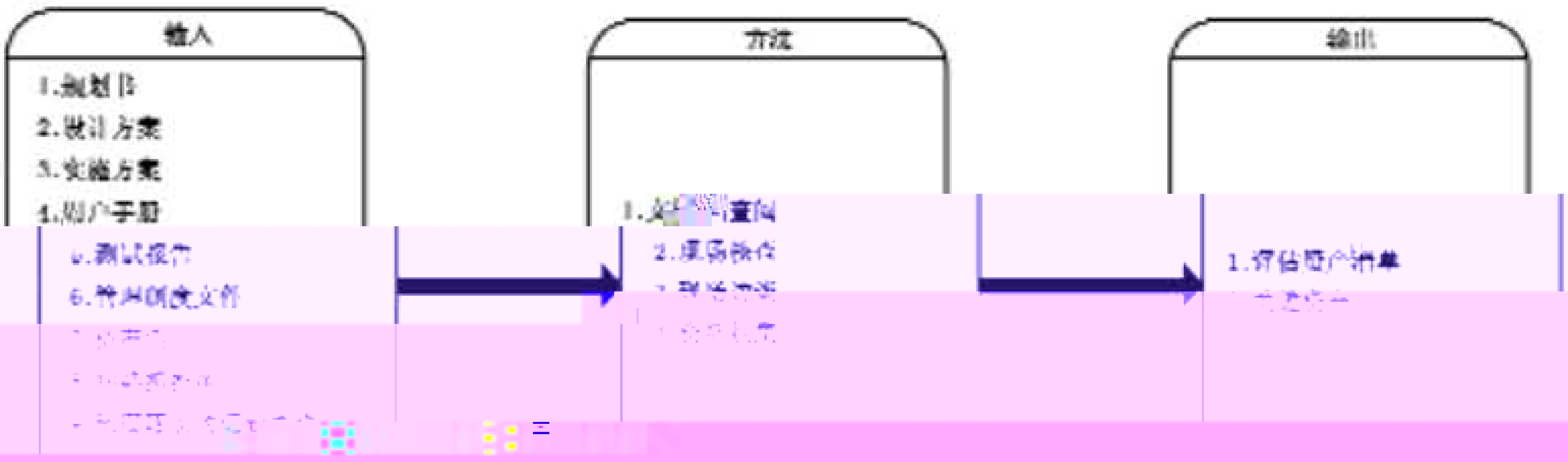
6.2.2 资产分类

在一个组织中，资产有多种存在形式[illegible]对工业控[illegible]

[illegible]		[illegible]器等；
		安全设备：工业防火墙、[illegible]系统、网闸、VPN 等；
	硬资产	计算机设备：服务器、工作站、台式计算机、便携计算机、HMI 等；
		存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等；
		传输线路：光纤、双绞线、无线、CAN 总线[illegible]
		[illegible]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[illegible]系统[illegible]人员、集成人员、关键设备供应商、操作人员、[illegible]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，另一方面要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[illegible]能对所有资产进行全面分析，[illegible]的资产进行分析，资产调查如图 9 所示。



关键资产

6.2.4 资产分析

d) 资产可用性、完整性、保密性对工业控制系统以及相关业务的重要程度。

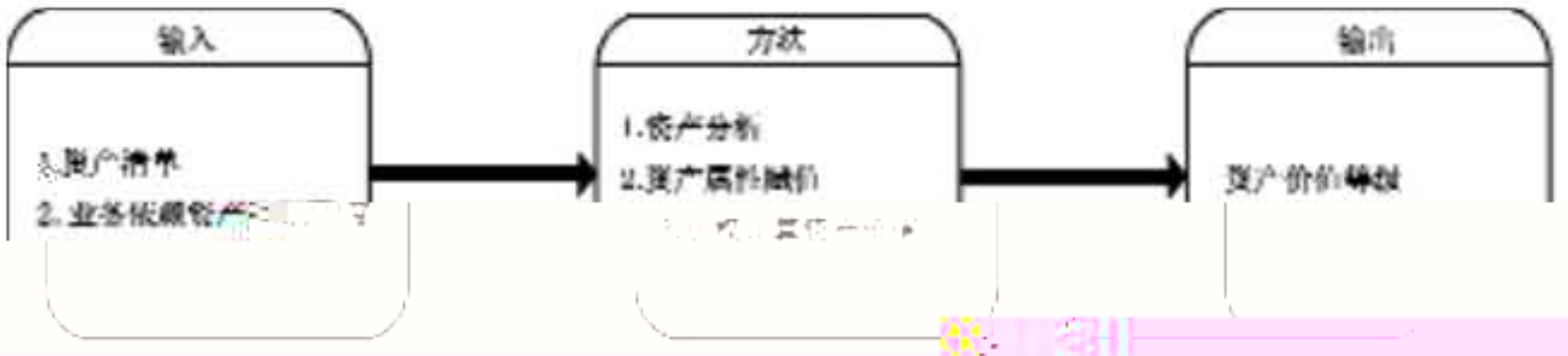

输入
方法
输出
1.资产分析
2.资产属性赋值

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
自然灾害	对工业控制系统的一个或多[illegible]
非法修改	对应用关进行攻击(修改、欺骗、篡改),以修改存储于工业控制系统[illegible]中的敏感信息
非法攻击	对老[illegible]攻击(嗅探、社会活动),用于分析受保护的敏[illegible]
得存储于工业控制系统服务器组 恶意思的。	提升权限	件中的用户凭证,提升工业控制系统[illegible]的权限或[illegible]
统交互式系统中,执行的日常任务没	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[illegible] 有被检测和审计,以[illegible]进一步的分[illegible]和修正
恶意代码造成不必要的系统停机和数据	病毒感染	个人[illegible]关注无意间将感染病毒传入工业控制系统[illegible] 腐败
	非法物理存取	无权限者进行一次物理[illegible]


输出
输入
1.ICS新使物并环境
2.特种ICS的人员
3.管理ICS制度策略
4.资产识别结果
5.故障可被文件
方法
1.文档分图
2.现场检查

实施指南如下：

c) 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宏观节点，并明确

威胁在不同环节的特点，确定威胁路径；

d) 根据威胁途径、攻击能力等判断威胁发生的可能性。

6.3.3 威胁的影响

威胁出现的和

威胁发生的影响较小，有的不能作救或作救代价

影响较大。

6.3.4 威胁分析

在调查威胁的基础

识别威胁发生的概率、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—2

图 12 [illegible]识别

业[illegible]统以往风险评估报告、审计说明、安全需求、安全测试[illegible]单、系统所处

依据

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

、标识、访客人

员登记、专人陪同、

准携带移动介质、相机等管理措施；

e) 评估方查看工业控

系统所在场所是否安装避雷针、安装通风装置、配备灭火器等，各应

源、远离易燃

易爆物品、建筑物漏水渗水等；

f) 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	

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
	对网络设备进行不当的物理访问会导致
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
	无关
	缺少/2、网络接口封堵，是否采用其

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
无线连接客户端与接入点间数据保护不力	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

表 10（续）

脆弱性	描述
不安全的物理端口	不[illegible]的通用接口如 USB [illegible]
不安全的远程访问工业控制系统	未部署安全措施，并[illegible]

[illegible]

表 11（续）

描述	脆弱性
	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

存在已知漏洞

施指南如下：

评估方查看平台中安装的操作系统[illegible]应用软件类型，例如：windows 操作系统、嵌入式系

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

k) 现场核查是否安装入侵检测和防御软件，或是否采用其他替代措施；

l) 现场核查可开启审计功能的软硬件是否开启相关功能，或是否采取替代措施。

6.4.5 [illegible]

[illegible]	2	低
如果被威胁利用，将对资产造成较小损害		
如果被威胁利用，对资产造成的损害可以忽略	1	可忽略

6.5 保障能力评估

6.5.1 保障能力评估概述

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[illegible]措施和[illegible]

弱性。

不同的工业控制系统的保障[illegible]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[illegible]系统的特点、行业要求[illegible]评估[illegible]

[illegible]、B.9 和 B.10 对系统安全管理进行

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

等方面的要求。评估人员可以依据 GB/T [illegible]9—2016 中的 B.

评估。

6.5.4 密[illegible]用管理

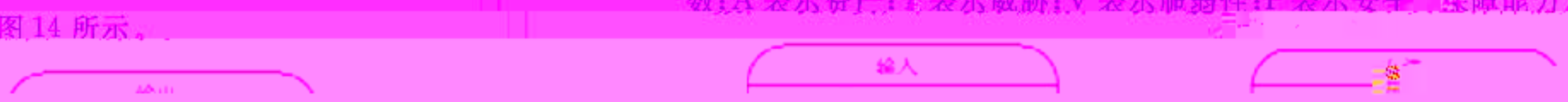
6.6 风险分析

6.6.1 风险分析原

图 13 风险分析原

全风险;F 表示安全风险计算函

险分析如图 14 所示。



工业控制系统各要素的关系,R=F(A,T,V,P)。其中,R 表示安
数,A 表示资产,T 表示威胁,V 表示脆弱性,P 表示安全

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
3	中	一旦发生造成的影响程度不大
2	低	一旦发生造成的
1	很低	

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

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[illegible]关情况	
部署位置	
网络[illegible]结构	
连接[illegible]情况	
主[illegible]名称型号	
系统时[illegible]间段	
数[illegible]中[illegible]	
数[illegible]本[illegible]	
服务[illegible]	

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	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）

	是否保存物理访问记录		9
	是否在需要对访客进行陪同和监视的环境下对访问者的行为进行陪同和监视		10
	是否按照被评估方定义的时间间隔更换访问控制设备的口令，在密码泄露和人员调动或离职时更换访问控制设备的口令		11
			12
	是否采用保护[illegible]的边界设施		19
	是否采用应急设备和备份介质的存储位置与主安全区域保持一个安全距离		20

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	
12	通信协议是否是明文传输	
13	通信协议是否是加密	
14	是否使用密码产品	
30	系统配置是否备份	

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	
[illegible]	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	
[illegible]	[illegible] SNMP 服务的共同	

表 B.3（续）

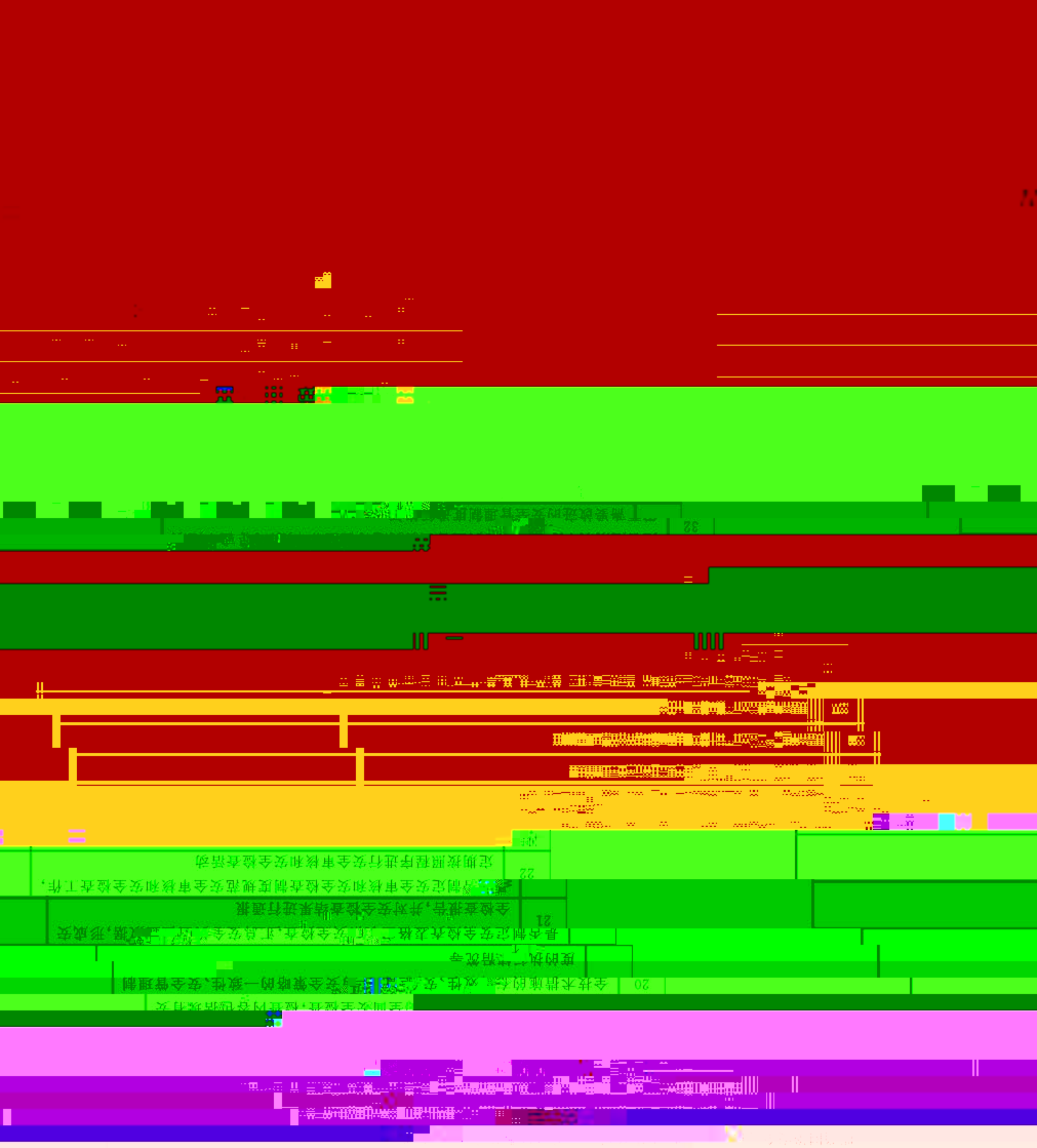
序号	核查项	核查结果
6	[illegible]数据库是否使用通用数据库，是否存在已知漏洞	
14	口令	
15	是否存在	

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[illegible]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	[illegible]	
53	系统日志[illegible]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	

表 B.3（续）

序号	核查项	核
26	[illegible]	
13	互联网接入审批和登记制度，严格控制互联网接入口数	



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/TR 62443-2-3 Industrial communication networks—Network and system security Part2-3:Patch management in the IACS environment

[12] IEC 62443-2-4 Industrial communication networks—Network and system security—Part2-4: Installation and maintenance requirements for IACS suppliers

[16] IEC 62443-4-2 Industrial communication networks—Network and system security Part4-2