ICS 25.040
N 10

中华人民共和国国家标准

GB/T 26333—2010

工业控制网络安全风险评估规范

Evaluation specification for security in industrial control network

2011-01-14 发布　　2011-06-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 2
4　符号和缩略语 …… 3
5　风险评估要点 …… 3
6　特性 …… 6
7　确定评估目的 …… 8
8　评估设计和规划 …… 8
9　制定评估计划 …… 11
10　评定技术 …… 11
11　评估的实施 …… 12
12　编写评估报告 …… 12
附录A（规范性附录）　工业控制网络安全网关的安全风险评估 …… 13
附录B（规范性附录）　工业控制网络现场设备层安全风险评估 …… 15

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准中的一些内容可能涉及某些专利，本标准对任何这样的专利权均不负有鉴别责任。

本标准由中国机械工业联合会提出。

本标准由全国工业过程测量和控制标准化技术委员会归口。

本标准起草单位：重庆邮电大学、浙江大学、浙江中控技术股份有限公司、机械工业仪器仪表综合技术经济研究所、中国科学院沈阳自动化研究所、大连理工大学、上海工业自动化仪表研究所、上海自动化仪表股份有限公司、中国四联仪器仪表集团有限公司、西南大学、天津天仪集团仪表有限公司、北京华控技术有限公司。

本标准起草人：王浩、王平、金建祥、冯冬芹、欧阳劲松、梅恪、徐皑冬、仲崇权、缪学勤、包伟华、刘进、张庆军、秘明睿、刘杰、刘枫、杨彬、周勇。

引　言

随着各种通信技术在工业控制网络中的广泛应用，在实现更多功能的同时，工业控制网络的安全问题日益凸显。

本评估标准是一种针对工业控制网络的安全风险评估方法。通过对工业控制网络的安全风险评估可以发现网络的安全隐患，通过采用相应的安全措施弥补安全漏洞，从而增强工业控制网络的安全。

本标准规定了工业控制网络安全风险评估的一般方法和准则，描述了工业控制网络安全风险评估的一般步骤，侧重于评估对象的分析和评估计划的设计。

工业控制网络安全风险评估规范

1 范围

本标准规定了评估的步骤，对评估方法给出了建议。

本标准适用于工业控制网络的安全风险评估，定义了评估的要点。

本标准讨论工业控制网络的通信安全，它主要取决于系统所采用的防护措施。

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 9361—1988 计算机场地安全要求

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 17903.1—2008 信息技术 安全技术 抗抵赖 第1部分：概述

GB/T 17965—2000 信息技术 开放系统互连 高层安全模型(idt ISO/IEC 10745:1995)

GB/T 18272.1—2000 工业过程测量和控制 系统评估中系统特性的评定 第1部分：总则和方法学

GB/T 18272.2—2000 工业过程测量和控制 系统评估中系统特性的评定 第2部分：评估方法学

GB/T 18272.3—2000 工业过程测量和控制 系统评估中系统特性的评定 第3部分：系统功能性评估

GB/T 18272.7—2006 工业过程测量和控制 系统评估中系统特性的评定 第7部分：系统安全性评估

GB/T 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型(ISO/IEC 15408-1:2005，IDT)

GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求(ISO/IEC 15408-2:2005，IDT)

GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求(ISO/IEC 15408-3:2005，IDT)

GB/T 19715.1—2005 信息技术 信息技术安全管理指南 第1部分：信息技术安全概念和模型

GB/T 20000.4—2003 标准化工作指南 第4部分：标准中涉及安全的内容

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 20270—2006 信息安全技术 网络基础安全技术要求

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20275—2006 信息安全技术 入侵检测系统技术要求和测试评价方法

GB/T 20278—2006 信息安全技术 网络脆弱性扫描产品技术要求

GB/T 20281—2006 信息安全技术 防火墙技术要求和测试评价方法

GB/T 20945—2007 信息安全技术 信息系统安全审计产品技术要求和测试评价方法

GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求

GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

ISO/IEC TR 13335 Guidelines for the Management of IT Security(IT 安全管理指南)

ISO/IEC TR 13335.1 Information technology—Guidelines for the management of IT Security—Part 1:Concepts and models of IT Security

ISO/IEC 15408 Evaluation Criteria for IT Security(IT 安全评估准则)

ISO/IEC 17799:2000 Information technology—Part 1:Code of practice for information security management

ISO/IEC 17799:2005 信息技术 安全技术 信息安全管理实践规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全 safety

不存在不可接受的风险。

3.2

安全状态 safe state

不存在不可接受风险的状态。

3.3

资产 asset

对组织具有价值的信息资源,是工业安全策略保护的对象(参见 ISO/IEC 13335-1:2004)。

3.4

信息安全 information security

保护信息的机密性、完整性和可用性及其他属性,如防抵赖性、可靠性等(参见 ISO/IEC 17799:2005)。

3.5

工业控制网络安全风险评估 security risk assessment in industrial control network

依据有关信息安全技术与管理标准,考虑工业控制网络的特殊性,对工业控制网络及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性,并结合资产价值来判断安全事件一旦发生对工业企业造成的影响。

3.6

机密性 confidentiality

使控制信息不泄露给未授权的个人、实体、过程或不使信息为其利用的特性。

3.7

完整性 integrality

保证控制信息及控制系统不会被有意地或无意地更改或破坏的特性。

3.8

可用性 availability

数据或资源的特性,被授权实体按要求能访问和使用数据或资源(参见 ISO/IEC 13335-1:2004)。

3.9

安全事件　security event

指系统、服务或网络的一种可识别状态的发生，它可能是对信息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。

3.10

安全需求　security requirement

为保证组织业务战略的正常运作而在安全措施方面提出的要求。

3.11

安全措施　security measure

保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制的总称。

3.12

证书　certificate

用于证明相关威胁、漏洞针对于特定网络的相对安全性。

3.13

威胁　threat

可能对资产或组织造成损害的潜在原因。威胁可以通过威胁主体、资源、动机、途径等多种属性来刻画。

3.14

工业以太网　ethernet for plant automation

EPA

我国第一个拥有自主知识产权的现场总线国家标准。同时，该标准被列入现场总线国际标准IEC 61158(第四版)中的第十四类型，并列为与IEC 61158相配套的实时以太网应用行规国际标准IEC 61784-2中的第十四应用行规簇(Common Profile Family 14，CPF14)。

4　符号和缩略语

ICS	工业控制系统(Industrial Control Systems)
PLC	可编程逻辑控制器(Programmable logic Controller)
SCADA	监控和数据采集(Supervisory Control and Data Acquisition)
DCS	分布式控制系统(Distributed Control System)
RTOS	实时操作系统(Real-time operating system)

5　风险评估要点

工业控制网络安全风险评估的目的是定性和(或)定量地确定其完成某一特定使命的能力。

评估一个工业控制网络就是根据各种数据判断其是否适用于某一特定的使命或者某一类使命。

要想获取全部数据，就需要在各种影响条件下，评定与工业控制网络的特定使命或一类使命相关的各种网络性能，但实施难度极大。因此，工业控制网络评估的基本原理是：

——确定与完成网络使命有关的网络的临界状态；

——通过研究评定各种特性的成本效益制定评定有关工业控制网络特性的计划。

工业控制网络安全风险评估的关键是必须考虑以允许的经费和时间，尽可能地提高工业控制网络适用性的置信度。

5.1 评估范围

对工业控制网络的安全风险评估必须是一个整体考虑、充分规划、持续运作的过程，从系统结构方面，评估范围包括了工业控制网络的各个逻辑层(现场设备层、过程监控层、企业管理层)；从评估要素方面，评估范围包括技术、管理、运行等各层面；从系统生命周期方面，工业控制网络的安全评估过程必须贯穿于整个网络设计、开发、建设和维护的各个阶段。

工业控制网络中比较有代表性的 EPA 网络，结构一般如图 1 所示(参照 GB/T 20171—2006 中 6.3.1的定义)。

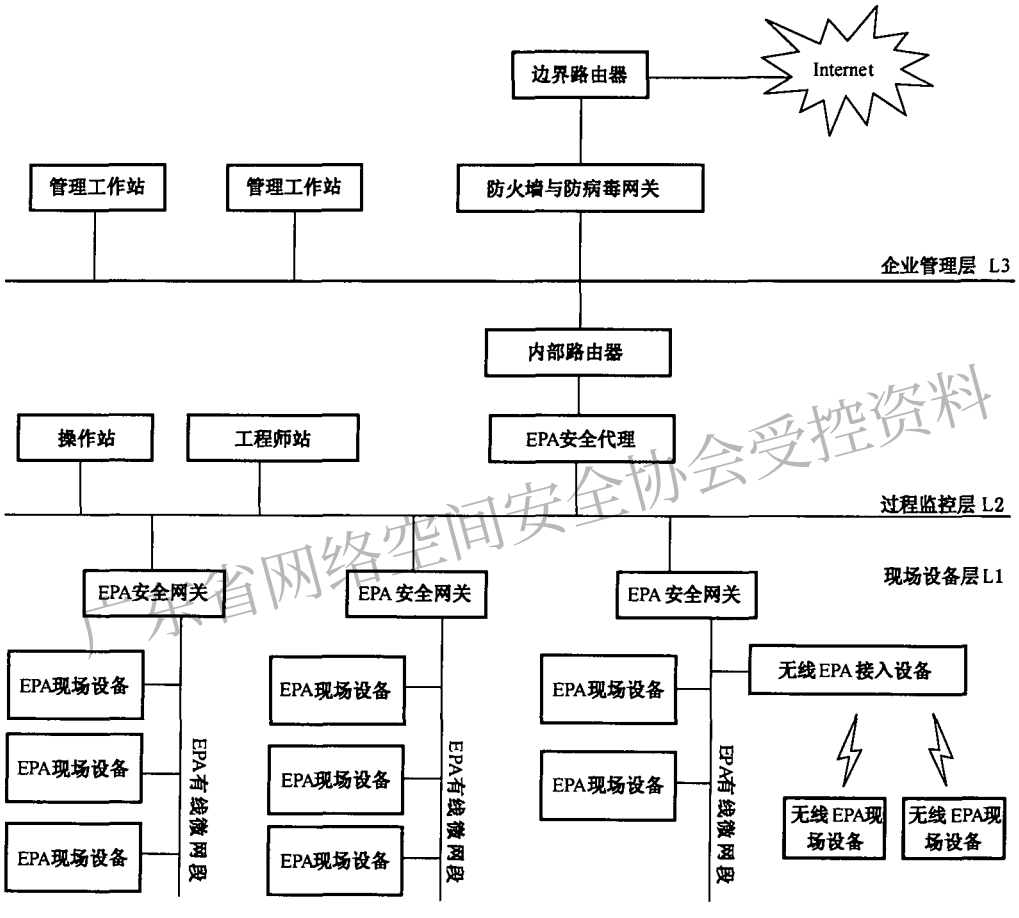

图 1 EPA 网络结构

在定义评估范围时，要对控制系统边界和机构责任进行分析，可以通过一组进程、通信、存储、资源等来确定。

在控制系统的边界范围内的每个要素必须满足：

——处于相同的直接管理控制下；

——具有相同的功能或使命目标；

——有本质上相同的运行特性和安全需求；

——位于相同的通用运行环境中。

5.2 评估对象

工业控制网络的安全风险评估，是为了保护控制系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证控制网络系统能够连续、正常、可靠的运行。因此，工业控制网络的安全风险评估对象，包括了网络中的各种关键信息资产、应用系统、实物资产、设施和环境，以及

人员、管理规程等。

对于一个具体的工业控制网络，安全风险评估主要涉及到该控制系统的关键和敏感部分。因此，根据实际控制系统不同，安全风险评估的对象也有所不同。

5.3 评估目的

工业控制网络的拥有者在进行安全设备选型、控制系统安全需求分析、系统网络建设、系统网络改造、应用系统试运行、内网与外网互联等业务之前，进行安全风险评估会帮助系统拥有者在一个安全状态下进行组织活动。安全状态应包括机密性、完整性和可用性，即在威胁产生安全事件的情况下，安全措施所能起到的相应保护作用。

工业控制网络安全评估的目的通常包括以下几个方面：

——确定可能对工业控制网络资产造成危害的威胁，包括入侵者、罪犯、不满员工、恐怖分子和自然灾害等；

——通过对历史资料和专家的经验确定威胁实施的可能性；

——对可能受到威胁影响的资产确定其价值、敏感性和严重性，以及相应的级别，确定哪些资产是最重要的；

——对最重要的、最敏感的资产，确定一旦威胁发生其潜在的损失或破坏；

——准确了解工业企业的网络和系统安全现状；

——明晰工业企业网络的安全需求；

——制定工业安全策略；

——制定工业控制网络和系统的安全解决方案；

——指导工业企业网络未来的建设和投入；

——通过项目实施和培训，培养用户自己的安全队伍。

根据实际控制系统不同，安全风险评估的目标有所不同。

5.4 影响条件

在评估工业控制网络之前有必要确定在安全风险评估执行期间所有的可能。

工业控制网络的影响条件一般包含下列几种：

——工业控制网络承担的任务；

——相关的操作人员；

——工业控制网络所连接的工业过程；

——工业控制网络连接的外部系统；

——为工业控制网络提供支持的公用设施气电等；

——工业控制网络自身的一些特性。

5.5 评估原则

工业控制网络安全评估原则包括以下内容：

5.5.1 可控性原则

包括人员可控性、工具可控性和项目过程可控性。

所有参与工业控制网络安全风险评估的人员均应进行严格的资格审查和备案，明确其职责分工，并对人员工作岗位的变更执行严格的审批手续，确保人员可控。

相关评估人员必须持有国际、国家认证注册的信息安全从业人员资质证书，确保具备可靠的职业、道德素质。

如果根据项目的具体情况，需要进行人员调整时，必须经过项目变更程序，得到双方的正式认可和签署。

所有使用的安全风险评估工具均应通过多方综合性能对比、挑选，并取得有关专家论证和相关部门的认证。

5.5.2 完整性原则

严格按照委托单位的评估要求和指定的范围进行全面的评估服务。

5.5.3 最小影响原则

从管理层面和工具技术层面，力求将风险评估对工业控制网络的正常运行的可能影响降低到最低限度。一般评估采用分析法(和)或比较法，进行安全风险评估。在采用试验法进行风险评估时，实施在备份网络上，或是分部门、分段在非生产周期/生产低峰期进行实施。

5.5.4 保密原则

与被评估单位签署保密协议和非侵害性协议。

5.6 评估程序

工业控制网络的风险评估程序分为五个阶段：

——第一阶段为准备阶段，确定评估目的；

——第二阶段为评估设计和规划；

——第三阶段为制定评估计划；

——第四阶段为评估的实施；

——第五阶段为编写评估报告。

6 特性

本标准中的特性，特指与工业控制网络安全相关的特性，所讨论、涉及的都是与工业控制网络安全直接或间接相关，对于工业控制网络安全是不容忽视的特性。

安全风险评估时，应根据特性考虑采用合适的国家标准、国际标准和有关法规。

工业控制网络安全特性可以包含很多种类，但 6.1 所述特性必须包括。

6.1 与安全相关特性

6.1.1 功能性

工业控制网络完成其既定使命的能力。

功能性取决于：

——提供功能的范围；

——实时完成功能的能力；

——必要时选择和完成所需功能的灵活性。

6.1.2 性能

在规定的工作条件和环境条件下能够执行所提供功能的程度。

对于每一种功能有必要规定对其性能进行物理测量，其中可包括精确度、重复性、响应速度、分辨

力等。

6.1.3 机密性

工业控制网络上传输、处理的数据所具有的特性，即表示数据所达到的未提供或未泄露给未授权的个人、过程或其他实体的程度。

6.1.4 完整性

保证工业控制网络上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。

6.1.5 可用性

工业控制网络上数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

6.1.6 身份认证

认证、鉴别设备或设备使用者的合法性。

6.1.7 不可抵赖性

不可抵赖性包括行为的不可抵赖和行为发生时间的不可抵赖。

6.1.8 授权

防止未授权用户访问或使用系统，即规定了用户对数据的访问权限。

6.1.9 安全审计

对用户行为的合法性、安全性进行审核和记录。

6.1.10 第三方安全

单个服务或设备的失效不应引起对其他组件的损害。

6.2 威胁的种类

威胁可能影响安全特性，甚至导致特性失效。

工业控制网络可能受到入侵、毁坏或重放攻击等威胁。这些威胁可分为恶意和非恶意两类。在工业控制网络中，至少应考虑下列安全威胁。

6.2.1 非法设备的物理接入

非法设备的物理接入可能影响网络的可用性、机密性、第三方安全。

6.2.2 访问授权的非法获取

访问授权的非法获取可能影响网络的可用性、机密性、身份认证、不可抵赖性、授权、安全审计。

6.2.3 控制信息的非法获取

控制信息的非法获取可能影响网络的机密性、第三方安全。

6.2.4 控制信息的篡改和破坏

控制信息的篡改和破坏可能影响网络的可用性、完整性、机密性。

6.2.5 未授权的网络连接

未授权的网络连接可能影响网络的可用性、机密性、授权。

6.2.6 数据包重放攻击

数据包重放攻击可能影响网络的可用性。

6.2.7 拒绝提供服务

拒绝提供服务可能影响网络的可用性。

6.2.8 病毒感染,引起系统崩溃和数据损坏

病毒感染,引起系统崩溃和数据损坏可能影响网络的可用性、第三方安全。

6.2.9 抵赖

抵赖将影响不可抵赖性。

7 确定评估目的

7.1 明确评估目的

在实施评估之前,应详细阐明评估的目的,以此作为编制评估计划的依据,评估目的对于评估的性质和深度具有很大的影响。

一个工业控制网络可能是相当复杂的,以至于对其进行全面的评定,将是得不偿失甚至是不可能的。通过仔细考虑评估目的、网络结构、体系结构、影响条件、评估申请方要求等,可以将评估项目减少到只包括那些对工业控制网络应用最敏感的项目上。在制定评估计划之前,应该认真地将评估目的编制成文,并将其作为整个评估过程中的指导原则的依据。

7.2 生成系统要求文件

系统要求文件由第5章,第6章和7.1共同生成。

是将评估对象所必须的性能、功能等文档化。

对评估对象使命的描述应该说明所要达到的目标,而不必说明为什么和如何达到。确定目标所涉及的安全特性,并按一定的方法将其归类。

对于目标进行分类。如:基本目标,重要目标,期望目标等。

必须考虑到影响条件。

8 评估设计和规划

8.1 概述

在此阶段将评估目的转化成与目标有关的观察和测量试验。

为了有效地完成这一任务应考虑第5章至第6章所述的各个方面。

8.2 评估对象

计划评估的一个重要步骤是确定被评估工业控制网络的评估对象。由于工业控制系统的类型很

多，包括了集中式数字控制系统、分布式控制系统(DCS)、多种现场总线控制系统等，为了帮助评估者全面了解控制网络的特点、业务、结构等，在评估前期需要先进行对象识别与描述。

对工业控制网络的概要描述，用来帮助评估者理解安全评估目标、安全需求是否准确合理，有利于评估者对开发者提交的报告进行评估，评估报告内容是否属实，与所提交的其他材料是否具有一致性。

在对象识别和描述中，调查和统计组织的全部对象。明确其现有状况、配置情况和管理情况。

8.3 网络边界

应根据评估目标和申请方要求，通过区分哪些属于、哪些不属于被评估的网络，认真确定网络的边界。

一个工业控制网络具有若干截然不同的边界：

——企业内网与外网；

——现场设备层、过程监控层与企业管理层；

——控制系统与办公网络；

——各个部门间的网络；

——网段与虚拟局域网。

每一个边界都应做出明确的选择。

内网指评估申请方所拥有的能够完全进行管理、控制的网络，包括工业控制网络和办公自动化网络等，外网指除内网之外的，评估申请方无力或不能完全进行管理、控制的网络，如 Internet。

8.4 评估项目

评估项目的分类，条目的生成不做任何硬性规定，参考标准亦只作为推荐之用。评估者可根据实际情况自行选择，但是，国家、国际规章制定机构要求进行的评估项目必须按这些规章规定的规则进行评估和评定。

以下罗列一些经常的评估项目。

8.4.1 物理安全评估

评估工业控制系统基础设施的物理安全对整个系统安全的影响。具体从车间场地、车间防火、车间供配电、车间防静电、车间接地与防雷、电磁防护、环境与人身安全、通信线路的保护、设备本身安全、设备管理、监控系统等物理安全相关技术措施方面进行测试。

具体测试要求、方法、条目等可参考以下标准：

GB/T 9361—1988 计算机场地安全要求

GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求(idt ISO/IEC 15408-3：2005)

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 21052—2007 信息安全技术 信息安全等级保护 信息系统物理安全技术要求

8.4.2 体系结构安全评估

评估系统网络体系结构是否合理，是否符合安全目标的要求。具体包括通讯协议、操作系统、网络隔离与边界控制策略、网络层次结构等。

具体测试要求、方法、条目等可参考以下标准：

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构

GB/T 18272.7—2006 工业过程测量和控制 系统评估中系统特性的评定 第7部分：系统安全性评估

GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求(ISO/IEC 15408-2:2005,IDT)

GB/T 19716—2005 信息技术 信息安全管理实用规则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

8.4.3 安全管理评估

从管理的角度,判断与信息控制、处理相关的各种技术活动是否处于有效安全监控之下。包括:安全方针、人员安全、安全组织、接入控制、系统管理、运行维护管理、业务连续性、符合性等。

具体测试要求、方法、条目等可参考以下标准:

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则

ISO/IEC TR 13335:Guidelines for the Management of IT Security(IT安全管理指南)

ISO/IEC 17799:2005 信息技术 安全技术 信息安全管理实践规范

8.4.4 安全运行评估

基于控制系统的业务应用,对控制系统实际运行的安全性进行测试。应具体有业务运行逻辑安全、业务交往的不可抵赖性、操作权限管理、故障排除与恢复、系统维护与变更、网络流量监控与分析、系统软件和协议栈软件、应用软件安全、数据库安全等。

具体测试要求、方法、条目等可参考以下标准:

GB/T 20270—2006 信息安全技术 网络基础安全技术要求

GB/T 17903.1—2008 信息技术 安全技术 抗抵赖 第1部分:概述

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 22019—2008 信息安全技术 信息系统安全等级保护基本要求

ISO/IEC 17799:2000 Information security management —Part 1:Code of practice for information security management

8.4.5 信息保护评估

基于工业控制网络业务信息流分析,对信息处理的功能、性能和安全机制进行测试;具体有访问控制、数据保护、通信保密、识别与鉴别、网络和服务设置、审计机制等测试内容。

具体测试要求、方法、条目等可参考以下标准:

GB/T 18336.3—2008 信息技术安全性评估标准 第3部分:安全保证要求(ISO/IEC 15408-3:2005,IDT)

GB/T 18336.2—2008 信息技术安全评估标准 第2部分:安全功能要求(ISO/IEC 15408-2:2005,IDT)

GB/T 20000.4—2003 标准化工作指南 第4部分:标准中涉及安全的内容

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20945—2007 信息安全技术 信息系统安全审计产品技术要求和测试评价方法

ISO/IEC 15408 Evaluation Criteria for IT Security(IT安全评估准则)

8.5 对评估计划的制约

规定了评估对象的评估范围、指定了先后顺序、确定了试验项目以后,应仔细审查每项试验,确定试验是否会妨碍或阻止其他试验项目的正确实施,以至于影响或降低工业控制网络的性能或威胁其安全性。

这些问题应编成文件，以指出其对评估工作顺序安排的制约作用。

由于工业控制网络的特殊性，评估方式一般选择分析法评定技术。只有当分析法评定技术得出的结果不能保证工业控制网络的安全或是不能达到申请方的要求时，才采用试验法评定技术。而试验法评定技术一般也只在备份网络上使用。任何在实际运行的工业控制网络上的测试，必须征得申请方及相关主管部门的许可，在制定完备的意外方案后方可实施。

实施评估计划的周期、经费都是必须考虑的重要因素。

9 制定评估计划

经第6章至第8章分析做出的决定，落实于评估计划的制定工作中，按时间表列出评估活动及其顺序，同时订出充足的复查点，使评估工作得到有效控制。

评估工作应以能反映出各种主要制约的逻辑顺序排列。应规定评估协议，说明改变和发布评估计划的主管机构、评估规范和评估报告需遵循的评估程序，以及在发生意外事故致使评估不能按计划进行时，不需征求上级主管机构意见允许采取的应急措施。

时间表的确立，评估时机的选择，根据具体情况及与申请方的协商结果而定。

制定评估计划时，必须考虑到实施周期、资金、人员等限制。

最终的评估计划至少应规定和(或)列出下列要点：

——7.1所得出的评估目的；

——考虑的原则；

——7.2所述的系统要求文件；

——8.4所述的评估项目；

——要求达到的安全水平；

——评估进度表；

——要考虑到试验可能产生的永久性影响。

10 评定技术

10.1 总则

应选择可以将评定结果与工业控制网络系统要求文件提出的要求作定性和(或)定量比较的评定技术。

所选择的评定技术可能只需利用文件进行分析，也可能需要接触实际系统以实验为依据，亦可能两者兼有，或数种并存。评定技术产生的结果可以是定量的或者是定性的，也可以是定性定量结合的。其选择依据，以评估工业控制网络的特点及评估申请方的需求为主要依据，以评估时间、评估内容、评估资金等为约束条件。

本标准推荐了几种评定技术。也可以采用其他方法，但在任何情况下评估报告都应该提供描述所用技术的文件出处。

10.2 分析法评定技术

工业控制网络的安全性评定技术主要是分析法评定技术。

对每一个测评项目应采取下列步骤：

a) 在系统要求文件所述或强制性规章规定的工作条件下检查是否存在威胁、漏洞等，每种存在的危险是否有证书，证书是否有效。

b) 如果没有符合要求的证书，就应进行相应的风险分析。为支持这种分析，可以采用10.3所述

的评定技术。

10.3 试验法评定技术

试验法评定技术是分析法评定技术的补充。

每当分析法技术不能保证系统的安全性等级时，就应该进行试验法评定，以便对缺乏数据的那些方面进行评估。

对照评测对象的功能、安全要求、安全目标等进行相应的测试，试验法评定技术是一个不断发展、种类繁多的技术，并且针对性十分强，每一种方法适用范围十分有限，故在此不做赘述。评估机构可根据具体对象、申请者的需求、资金、评估时间等选择合适的测评工具、测评方法。本标准在此不做任何硬性规定，但所选工具或方法必须是安全的，符合国家、国际一般性准则的。

以下列出一些参考标准：

GB/T 20278—2006　信息安全技术　网络脆弱性扫描产品技术要求

GB/T 20275—2006　信息安全技术　入侵检测系统技术要求和测试评价方法

GB/T 20281—2006　信息安全技术　防火墙技术要求和测试评价方法

11 评估的实施

安全风险评估实施时应严格按照评估计划和规定的协议开展工作。

评估应由专业或专门人员实行。

如必须做出更改时，除预先商定的可采取的应急措施以外，应将变动内容写成报告并与有关主管机构磋商。

所有的观察、测量、测试、计算等工作均应随时记录在案，所有的记录都应妥善保管并加以保密。最后随评估报告一并交予评估申请方。

12 编写评估报告

所有的观察、测量、测试、计算等工作均应随时记录在案，并随评估报告一起交予评估申请方。

评估实施情况和评估结果均应列入综合评估和(或)评定报告。该报告应准确、清楚、明确和客观地陈述评估的目的、结果和全部的有关内容。

安全风险评估报告至少应包含下列内容：

——一个合适的标题；

——负责评估的机构和/或人员；

——评估的目的；

——评估对象的基本特征；

——评估计划及必要的变动；

——汇总收集到的所有信息；

——评估使用的方法、工具；

——评估的具体项目，结果；

——评测中遇到的问题；

——建议做进一步分析和/或试验的评估项目清单。

评估报告应附封面，封面注明报告标题、统一编号、评估的机构和日期。

评估报告发布后若需做改动或增补，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
（规范性附录）
工业控制网络安全网关的安全风险评估

A.1 概述

工业控制网络中安全网关是现场设备层网络与过程监控层网络之间的唯一入口。提供对现场设备层的边界保护，防止可能存在的非法设备接入和未授权的访问等。保护现场设备层的安全网关在实现上采用访问控制、设备鉴别、数据加密、数据校验和包过滤等技术。

A.2 确定评估目的

本示例针对工业控制网络中安全网关的安全风险评估，主要检测是否达到本身的性能指标和预期的在网络中的安全性功能。在本阶段，收集、整理资料是主要任务，生成系统要求文件，为后续工作提供指导、帮助。

A.3 评估设计和规划

A.3.1 评估对象

评估对象为某工业控制网络中的安全网关。

A.3.2 网络边界

安全网关位于现场设备层与过程控制层之间，属于企业内部网络。因此，本示例涉及的评估范围为现场设备层与过程控制层。

A.3.3 评估项目

通过前期收集、整理的资料，对安全网关设备的性能和功能进行检测。由于工业生产的特点及工业控制网络的高实时性要求等，评估方式宜采用分析法或者通过对比产品说明书来验证。必须测试时，可选择同型号产品，搭建测试平台，进行相关测试。

其他如网络性能，安全管理等具可参照相关标准进行评估。

针对工业控制网络中安全网关所应具有的一些功能和要求设计评估项目见表 A.1

表 A.1 作为评估项目示例，只涉及部分评测项目，为信息安全相关条目，完整的评估项目是所有 8.4、具体网络要求和评估申请方请求等的综合，其内容、项目均应根据具体情况设计。

表 A.1 评估项目示例表

评估项目	评估内容	评估方式
身份鉴别	应对登录网络设备进行身份鉴别	分析法/试验法
	应对网络上的对等实体进行身份鉴别	分析法/试验法
	身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等	分析法/试验法

表 A.1（续）

评估项目	评估内容	评估方式
报文校验	防止对报文的非法篡改和破坏	分析法/试验法
访问控制	实现网络边界访问控制	分析法/试验法
	禁止未通过鉴别的设备与上层的全部通信	分析法/试验法
	通过鉴别的设备与上层网络间之间通信的访问控制	分析法/试验法
	应依据安全策略允许或者拒绝便携式和移动式设备的网络接入	分析法/试验法
	禁止外部网络访问现场层设备	分析法/试验法
	支持适当的 VPN 服务	分析法/试验法
入侵防范	安装防火墙　软□　硬□	分析法/试验法
	安装 IDS 入侵检测系统	分析法/试验法
	应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等入侵事件的发生	分析法/试验法
	当检测到入侵事件时，应记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警	分析法/试验法
抗抵赖	应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能	分析法/试验法
	应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能	分析法/试验法
报文加密	实现报文加密保证控制信息安全	分析法/试验法
包过滤	基于一定规则过滤包	分析法/试验法
协议转换	进行相应的协议转换	分析法/试验法

A.4　制定评估计划

根据评估项目等，在与相关部门、责任人进行协商后，制定相应的评估计划。

评估计划的制定原则等见本标准第 9 章。

A.5　评估实施

应严格遵照评估计划实施，将各种信息随时记录在案，妥善保管并严格保密。

A.6　编写评估报告

评估报告的撰写见本标准第 12 章。

附 录 B
（规范性附录）
工业控制网络现场设备层安全风险评估

B.1 概述

现场设备层网络由现场设备互联而成，以实现现场控制为主要目的。

现场设备层安全涉及各种现场设备，交换机和（或）集线器，物理链路，供电，协议栈，通信安全和管理制度等众多方面。明确评估目标，确定评估项目显得极其重要。

现场设备层网络上的设备对实时性要求高，而设备资源又有限。因此，对现场设备的安全防护（包括其本身安全和通信安全）既是现场设备层网络安全的重要目的，又是现场设备层网络安全的主要衡量标准。应将重点放在对现场设备的评估。

B.2 确定评估目的

本示例针对工业控制网络现场设备层进行安全风险评估，主要检测在各种情况下评估对象是否能完成预期的任务。

在本阶段，收集、整理资料是主要任务，生成系统要求文件，为后续工作提供指导、帮助。

B.3 评估设计和规划

B.3.1 评估对象

评估对象为某工业控制网络的现场设备层网络。

B.3.2 网络边界

现场设备层位于工业控制网络三层结构中的第一层，通过安全网关与过程控制层相连，属于企业内部网络。

B.3.3 评估项目

B.3.3.1 物理安全风险评估

从工业控制系统基础设施的物理安全方面，评估对整个现场设备层网络安全的影响。

包括场地安全，通信线路安全，防火、防雷、防静电，设备本身安全，供电及其冗余，电磁防护等方面。鉴于具体现场设备层环境、设备的复杂多样，详细评估项目视实际情况而定。

B.3.3.2 体系结构安全评估

分析测试系统网络体系结构是否合理，是否符合安全目标的要求。

具体包括通讯协议、操作系统、网络隔离与边界控制策略、网络层次结构等。

详细评估项目视具体工业控制网络的特性而定。

B.3.3.3 安全管理评估

从管理的角度，判断与信息控制、处理相关的各种技术活动是否处于有效安全监控之下。

包括:安全方针、人员安全、安全组织、接入控制、系统管理、运行维护管理、业务连续性、符合性等。

详细评估项目据评估申请方要求和具体工业控制网络的特性等综合确定。

B.3.3.4 安全运行评估

基于控制系统的业务应用,对控制系统实际运行的安全性进行测试。

应包括业务运行逻辑安全、业务交往的不可抵赖性、操作权限管理、故障排除与恢复、系统维护与变更、网络流量监控与分析。

其他项目,见本标准 8.4.4 及相应参考标准。

B.3.3.5 信息保护评估

基于业务信息流分析,对信息处理的功能、性能和安全机制进行测试。

可包括访问控制、数据保护、通信保密、识别与鉴别、网络和服务设置、审计机制等内容。

详细项目根据具体的工业控制网络安全等级和评估申请方的要求,综合确定。

B.4 制定评估计划

根据评估项目等,在与相关部门、责任人进行协商后,制定相应的评估计划。

评估计划的制定原则等见本标准第 9 章。

B.5 评定技术的选择

本示例是对某工业控制网络的现场设备层网络进行评估。现场设备层的高实时性,工业生产的连续性以及试验法的复杂性,推荐使用本标准 10.2 所述分析法。

分析法基于系统要求文件和(或)强制性规章,采取对比分析的方法,对评估对象的安全性进行分析、评估。

当分析法技术不能保证系统的安全性等级时,可采用试验法评定,以便对缺乏数据的那些方面进行评估。或作为分析法的支持。

B.6 评估实施

应严格遵照评估计划实施,将各种信息随时记录在案,妥善保管并严格保密。

B.7 编写评估报告

评估报告的撰写见本标准第 12 章。

中 华 人 民 共 和 国
国 家 标 准
工业控制网络安全风险评估规范
GB/T 26333—2010
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
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 1.5 字数 34 千字
2011年6月第一版 2011年6月第一次印刷
*
书号:155066·1-42825 定价 24.00 元

GB/T 26333-2010