

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