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

GB/T 26333—2010

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

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。

目　　次

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。

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。