



中华人民共和国国家标准

GB/T 33009.3—2016

工业自动化和控制系统网络安全 集散控制系统(DCS) 第3部分:评估指南

Industrial automation and control system security—
Distributed control system(DCS)—
Part 3: Assessment guidelines

2016-10-13 发布

2017-05-01 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
1 范围	1
2 规范性引用文件	1
3 术语、定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	4
4 DCS 安全风险评估概述	4
4.1 DCS 系统概述	4
4.2 DCS 安全风险评估流程框架与流程	6
4.3 评估结果	9
5 评估工作准备	11
5.1 概述	11
5.2 确定 DCS 评估目标	11
5.3 确定评估范围	11
5.4 组建评估团队	11
5.5 系统调研	11
5.6 确定评估依据与方法	12
5.7 制定评估方案	12
5.8 获得支持	12
6 DCS 安全要素识别	12
6.1 DCS 资产识别	12
6.2 DCS 脆弱性	13
6.3 威胁识别	14
6.4 工艺特征识别	15
7 DCS 风险分析	16
7.1 风险计算原理	16
7.2 风险处理计划	17
8 安全风险评估文档记录	17
8.1 评估文档记录要求	17
8.2 评估文档	18
附录 A (规范性附录) DCS 生命周期各阶段的安全风险评估	19
附录 B (资料性附录) 风险评估工具和集散控制系统(DCS)常见的测试内容	23
附录 C (规范性附录) 风险的计算方法	26
参考文献	33

前 言

GB/T 33009《工业自动化和控制系统网络安全 集散控制系统(DCS)》和 GB/T 33008《工业自动化和控制系统网络安全 可程序控制器(PLC)》等共同构成工业自动化和控制系统网络安全系列标准。

GB/T 33009《工业自动化和控制系统网络安全 集散控制系统(DCS)》分为 4 个部分：

- 第 1 部分：防护要求；
- 第 2 部分：管理要求；
- 第 3 部分：评估指南；
- 第 4 部分：风险与脆弱性检测要求。

本部分为 GB/T 33009 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量、控制和自动化标准化技术委员会(SAC/TC 124)和全国信息安全标准化技术委员会(SAC/TC 260)归口。

本部分起草单位：浙江中控研究院有限公司、浙江大学、机械工业仪器仪表综合技术经济研究所、重庆邮电大学、中国科学院沈阳自动化研究所、西南大学、福建工程学院、杭州科技职业技术学院、北京启明星辰信息安全技术有限公司、中国电子技术标准化研究院、国网智能电网研究院、中国核电工程有限公司、上海自动化仪表股份有限公司、东土科技股份有限公司、清华大学、西门子(中国)有限公司、施耐德电气(中国)有限公司、北京钢铁设计研究总院、华中科技大学、北京奥斯汀科技有限公司、罗克韦尔自动化(中国)有限公司、中国仪器仪表学会、工业和信息化部电子第五研究所、北京海泰方圆科技有限公司、青岛多芬诺信息安全技术有限公司、北京国电智深控制技术有限公司、北京力控华康科技有限公司、北京和利时系统工程有限公司、中国石油天然气管道有限公司、北京匡恩网络科技有限责任公司、西南电力设计院、广东航宇卫星科技有限公司、华北电力设计院工程有限公司、华为技术有限公司、中国电子科技集团公司第三十研究所、深圳万讯自控股份有限公司、横河电机(中国)有限公司北京研发中心。

本部分主要起草人：施一明、冯冬芹、梅恪、王玉敏、王平、王浩、高梦州、徐珊珊、徐皓冬、刘枫、许剑新、陈平、杨悦梅、陈建飞、还约辉、黄家辉、贾驰千、梁耀、刘大龙、陆耿虹、刘文龙、王芳、孟雅辉、范科峰、梁潇、王彦君、张建军、薛百华、许斌、陈小淙、华镛、高昆仑、王雪、周纯杰、张莉、刘杰、朱毅明、王弢、孙静、胡伯良、刘安正、田雨聪、方亮、马欣欣、王勇、杜佳琳、陈日罡、李锐、刘利民、孔勇、黄敏、朱镜灵、张智、张建勋、兰昆、张晋宾、成继勋、尚文利、钟诚、梁猛、陈小枫、卜志军、丁露、李琳、杨应良、杨磊。

工业自动化和控制系统网络安全

集散控制系统(DCS)

第3部分:评估指南

1 范围

GB/T 33009 的本部分规定了集散控制系统的安全风险评估等级划分、评估的对象及实施流程,以及安全措施有效性测试。

本部分适用于电力、石油、化工、水利、冶金、建材等各领域针对 DCS 系统的进行的安全风险评估活动,也适用于指导 DCS 用户改善和提高生产系统中 DCS 安全能力的系统维护活动。

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 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

3 术语、定义、缩略语

3.1 术语和定义

GB/T 20984—2007 和 GB/T 30976.1—2014 界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出了 GB/T 20984—2007 和 GB/T 30976.1—2014 中的一些术语和定义。

3.1.1

验收 acceptance

风险评估活动中用于结束项目实施的一种方法,主要由被评估方组织机构,对评估活动进行逐项检验,以是否达到评估目标为接受标准。

[GB/T 30976.1—2014,定义 3.1.4]

3.1.2

访问控制 access control

保护系统资源防止未授权的访问;系统资源使用的过程是根据安全策略规定的,并且根据该策略只允许被授权的实体(用户、程序、过程或者其他系统)。

[IEC 62443-1-1,定义 3.2.2]

3.1.3

可用性 availability

数据或资源能被授权实体按要求访问和使用的特性。

[GB/T 20984—2007,定义 3.3]