ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33009.4—2016

工业自动化和控制系统网络安全 集散控制系统(DCS) 第4部分:风险与脆弱性检测要求

**Industrial automation and control system security—
Distributed control system (DCS)—
Part 4:Risk and vulnerability detection requirements**

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 …… 3
4　DCS 风险与脆弱性检测概述 …… 3
4.1　DCS 系统概述 …… 3
4.2　DCS 风险与脆弱性检测的目标 …… 5
4.3　DCS 风险与脆弱性检测基本原则 …… 5
4.4　DCS 风险与脆弱性检测内容 …… 5
4.5　DCS 风险与脆弱性检测基本工作单元 …… 6
4.6　DCS 风险与脆弱性检测的执行 …… 7
4.7　DCS 风险与脆弱性检测结果的处置 …… 7
5　DCS 软件安全风险与脆弱性 …… 7
5.1　服务器和控制站的操作系统 …… 7
5.2　数据库管理系统 …… 8
5.3　OPC 类软件 …… 10
5.4　DCS 监控软件 …… 10
5.5　DCS 组态软件 …… 12
5.6　其他软件 …… 12
6　DCS 网络通信安全风险与脆弱性 …… 13
6.1　商用以太网协议通信机制 …… 13
6.2　工业网络协议通信机制 …… 13
6.3　DCS 通信数据安全 …… 14
6.4　DCS 通信服务 …… 15
6.5　DCS 状态转换 …… 16
参考文献 …… 17

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　可编程序控制器(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4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：浙江大学、浙江中控研究院有限公司、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：冯冬芹、施一明、梅恪、王玉敏、王平、王浩、高梦州、徐珊珊、徐皑冬、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、吴彦彪、王芳、孟雅辉、范科峰、梁潇、王彦君、张建军、薛百华、许斌、陈小淙、华镕、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4部分:风险与脆弱性检测要求

1 范围

GB/T 33009的本部分规定了集散控制系统(DCS)在投运前、后的风险和脆弱性检测,对DCS软件、以太网网络通信协议与工业控制网络协议的风险与脆弱性检测提出具体的要求。

本部分适用于对DCS中的下列对象进行脆弱性检测:

a) 监控软件、组态软件、数据库软件等DCS中的应用软件;

b) DCS操作员站和控制站等操作系统;

c) DCS中的具有网络协议实现和网络通信能力的功能和组件。

本部分不适用于智能仪表和工业无线的脆弱性检测。

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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 28449—2012 信息安全技术 信息系统安全等级保护测评过程指南

GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

GB/T 33009.1—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第1部分:防护要求

GB/T 33009.2—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第2部分:管理要求

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

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]