ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33008.1—2016

工业自动化和控制系统网络安全 可编程序控制器(PLC) 第1部分:系统要求

Industrial automation and control system security—Programmable logic controller(PLC)—Part 1: System 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 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 2
4　PLC 网络安全概述 …… 3
4.1　总则 …… 3
4.2　网络安全相关内容概述 …… 3
4.3　PLC 系统典型结构 …… 4
4.4　PLC 系统网络安全总体要求 …… 4
5　PLC 系统网络安全技术要求 …… 7
5.1　网络安全技术要求说明 …… 7
5.2　对第 2 层和第 1 层的总体要求 …… 8
5.3　对第 2 层的要求 …… 9
5.4　对第 1 层的要求 …… 17
6　PLC 系统网络安全管理要求 …… 19
6.1　总体要求 …… 19
6.2　PLC 系统设计、开发过程网络安全管理补充要求 …… 19
附录 A（规范性附录）　系统要求和增强要求与安全等级的映射 …… 20
附录 B（规范性附录）　网络安全管理评估列表 …… 24
参考文献 …… 31

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 33008《工业自动化和控制系统网络安全　可编程序控制器(PLC)》计划发布如下部分：

——第1部分：系统要求；

——第2部分：系统评测实施指南；

……

本部分为GB/T 33008的第1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：北京和利时系统工程有限公司、机械工业仪器仪表综合技术经济研究所、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、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、东土科技股份有限公司、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、重庆邮电大学、中国科学院沈阳自动化研究所、西南大学、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、北京启明星辰信息安全技术有限公司、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：王弢、王玉敏、范科峰、梁潇、孙静、冯冬芹、朱毅明、梅恪、王浩、徐皑冬、刘枫、王亦君、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、刘安正、田雨聪、魏钦志、马欣欣、王勇、杜佳琳、陈日罡、丁露、李锐、刘文龙、孟雅辉、刘利民、胡伯良、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、李琳、杨应良、杨磊。

工业自动化和控制系统网络安全 可编程序控制器(PLC) 第1部分:系统要求

1 范围

GB/T 33008的本部分规定了可编程序控制器(PLC)系统的网络安全要求,包括PLC直接或间接与其他系统通信的网络安全要求。

本部分适用于工程设计方、设备生产商、系统集成商、用户以及评估认证机构等。

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 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

可编程序(逻辑)控制器 programmable (logic) controller;PLC

一种用于工业环境的数字式操作的电子系统。这种系统用可编程的存储器作面向用户指令的内部寄存器,完成规定的功能,如逻辑、顺序、定时、计数、运算等,通过数字或模拟的输入/输出,控制各种类型的机械或过程。可编程序控制器及其相关外围设备的设计,使它能够非常方便地集成到工业控制系统中,并能很容易地达到所期望的所有功能。

注:在本部分中使用缩写词PLC代表可编程序控制器(programmable controllers),这在自动化行业中已形成共识。原来曾用PC作为可编程序控制器的缩略语,它容易与个人计算机所使用的缩略语PC相混淆。

[GB/T 15969.1—2007,定义3.5]

3.1.2

可编程序控制器(PLC)系统 programmable controller system or PLC-system

用户根据所要完成的自动化系统要求而建立的由可编程序控制器及其相关外围设备组成的配置。其组成是一些由连接永久设施的电缆或插入部件,以及由连接便携式或可搬运外围设备的电缆或其他连接方式互连的单元。

[GB/T 15969.1—2007,定义3.6]

3.1.3

脆弱性 vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点,可被利用来危害系统的完整性或安全策略。

[GB/T 30976.1—2014,定义3.1.1]