ICS 35.040
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1390.5—2017

信息安全技术　网络安全等级保护基本要求　第5部分:工业控制系统安全扩展要求

Information security technology—General requirements for classified protection of cyber security—Part 5:Special security requirements for industrial control system

2017-05-08 发布　　2017-05-08 实施

中华人民共和国公安部　　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、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 2
4　概述 …… 2
4.1　安全通用要求 …… 2
4.2　工业控制系统概述提要 …… 3
4.2.1　总则 …… 3
4.2.2　层次模型 …… 3
4.2.3　区域模型 …… 5
4.2.4　安全域划分原则 …… 6
4.3　工业控制系统等级保护原则和要求 …… 6
4.3.1　总则 …… 6
4.3.2　安全域保护原则 …… 6
4.3.3　安全域保护措施实施说明 …… 7
4.3.4　技术要求和管理要求 …… 7
4.4　工业控制系统定级 …… 8
4.5　工业控制系统等级保护通用约束条件 …… 8
4.5.1　概述 …… 8
4.5.2　基本功能支持 …… 8
4.5.3　补偿措施 …… 9
5　第一级基本要求 …… 9
5.1　技术要求 …… 9
5.1.1　物理安全 …… 9
5.1.2　边界防护 …… 10
5.1.3　生产管理层安全要求 …… 10
5.1.4　过程监控层安全要求 …… 12
5.1.5　现场控制层安全要求 …… 15
5.1.6　现场设备层安全要求 …… 16
5.2　管理要求 …… 16
5.2.1　安全管理机构和人员 …… 16
5.2.2　安全运维管理漏洞和风险管理 …… 16
6　第二级基本要求 …… 17

6.1 技术要求 …… 17
6.1.1 物理和环境安全 …… 17
6.1.2 边界防护 …… 18
6.1.3 生产管理层安全要求 …… 18
6.1.4 过程监控层安全要求 …… 21
6.1.5 现场控制层安全要求 …… 25
6.1.6 现场设备层安全要求 …… 27
6.2 管理要求 …… 28
6.2.1 安全管理机构和人员 …… 28
6.2.2 安全运维管理漏洞和风险管理 …… 28
7 第三级基本要求 …… 28
7.1 技术要求 …… 28
7.1.1 物理和环境安全 …… 28
7.1.2 边界防护 …… 29
7.1.3 集中管控 …… 30
7.1.4 生产管理层安全要求 …… 30
7.1.5 过程监控层安全要求 …… 33
7.1.6 现场控制层安全要求 …… 39
7.1.7 现场设备层安全要求 …… 42
7.2 管理要求 …… 42
7.2.1 安全策略和管理制度 …… 42
7.2.2 安全管理机构和人员 …… 42
7.2.3 安全建设管理外包软件开发 …… 43
7.2.4 安全运维管理漏洞和风险管理 …… 43
8 第四级基本要求 …… 43
8.1 技术要求 …… 43
8.1.1 物理和环境安全 …… 43
8.1.2 边界防护 …… 44
8.1.3 集中管控 …… 45
8.1.4 生产管理层安全要求 …… 45
8.1.5 过程监控层安全要求 …… 49
8.1.6 现场控制层安全要求 …… 54
8.1.7 现场设备层安全要求 …… 57
8.2 管理要求 …… 58
8.2.1 安全策略和管理制度安全策略 …… 58
8.2.2 安全管理机构和人员 …… 58
8.2.3 安全管理建设外包软件开发 …… 58
8.2.4 安全运维管理漏洞和风险管理 …… 59
附录 A（资料性附录） 工业控制系统概述详解 …… 60
附录 B（资料性附录） 安全域划分示例 …… 65
附录 C（资料性附录） 基于可信计算技术的工业控制系统安全等级防护 …… 67
参考文献 …… 71

前　言

GA/T 1390《信息安全技术　网络安全等级保护基本要求》已经或计划发布以下部分：

——第1部分：安全通用要求；

——第2部分：云计算安全扩展要求；

——第3部分：移动互联安全扩展要求；

——第4部分：物联网安全扩展要求；

——第5部分：工业控制系统安全扩展要求；

——第6部分：大数据安全扩展要求。

本部分为GA/T 1390的第5部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由公安部信息系统安全标准化技术委员会提出并归口。

本部分负责起草单位：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、公安部第三研究所、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。

本部分参加起草单位：中国电力工程顾问集团西南电力设计院有限公司、北京国电智深控制技术有限公司、西门子(中国)有限公司、施耐德电气(中国)有限公司、工业和信息化部电子第五研究所、北京和利时系统工程公司、东方电气中央研究院、北京市轨道交通设计研究院有限公司、国家信息技术安全研究中心、中国软件测评中心、中石化齐鲁石化公司、中科院沈阳自动化所、中国电子科技集团公司第三十研究所、国家电力投资集团公司、中国电力工程顾问集团华北电力设计院有限公司、国核自仪系统工程有限公司、北京自来水集团。

本部分主要起草人：冯冬芹、刘之涛、贾驰千、陆耿虹、高梦州、梁耀、刘大龙、梅恪、王玉敏、赵艳领、任卫红、袁静、杨悦梅。

本部分参与起草人：张晋宾、朱镜灵、李锐、梁军、刘杰、刘太洪、赵军凯、袁晓舒、梅棋、肖衍、李冰、庞宁、周峰、刘利民、陈秀丽、王爱鹏、孟雅辉、方进社、卜志军、张晨艳、王弢、兰昆、王静、李忠生、王勇、刘志祥、罗安、尚文利、马欣欣、何彦君。

引　言

为了适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下信息安全等级保护工作的开展，需对 GB/T 22239—2008 进行修订，修订的思路和方法是针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域提出扩展的安全要求。

信息安全技术　网络安全等级保护基本要求　第5部分:工业控制系统安全扩展要求

1　范围

GA/T 1390的本部分规定了不同安全保护等级工业控制系统的安全扩展要求。

本部分适用于批量控制、连续控制、离散控制等工业控制系统,为工业控制系统网络安全等级保护措施的设计、落实、测试、评估等提供指导要求。

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 22239　信息安全技术　信息系统安全等级保护基本要求

GB/T 25069—2010　信息安全技术　术语

IEC 62443-1-1　工业通信网络　网络和系统安全　第1-1部分:术语、概念和模型

IEC 62443-3-2　工业通信网络　网络和系统安全　第3-2部分:区域和通道的安全保障等级

3　术语、定义和缩略语

3.1　术语和定义

GB 17859—1999、GB/T 25069—2010和IEC 62443-1-1界定的以及下列术语和定义适用于本文件。

3.1.1

工业控制系统　industrial control system

对工业生产过程安全、信息安全和可靠运行产生作用和影响的人员、硬件和软件的集合。

注:系统包括,但不限于:

1) 工业控制系统包括集散式控制系统(DCS)、可编程逻辑控制器(PLC)、智能电子设备(IED)、监视控制与数据采集(SCADA)系统,运动控制(MC)系统、网络电子传感和控制,监视和诊断系统[在本标准中,不论物理上是分开的还是集成的,过程控制系统(PCS)包括基本过程控制系统和安全仪表系统(SIS)];

2) 相关的信息系统,例如先进控制或多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、制造执行系统(MES);

3) 相关的部门、人员、网络或机器接口,为连续的、批处理、离散的和其他过程提供控制、安全和制造操作功能。

3.1.2

区域　area

站点内划分的物理的、地理的或逻辑的资源分组。

3.1.3

安全域　security zone

具有相同安全要求的逻辑资产或物理资产的集合。