ICS 25.040.40
CCS N 18

中华人民共和国国家标准

GB/T 41274—2022

可编程控制系统内生安全体系架构

Endogenous safety architecture of programmable control system

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件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)归口。

本文件起草单位：浙江大学、杭州优稳自动化系统有限公司、上海电气集团股份有限公司、北京机械工业自动化研究所有限公司。

本文件主要起草人：王文海、高慧、贾廷纲、张益南、许志正、张晓东、嵇月强、张稳稳、曹剑、范鹏鹏、袁超、周伟、徐斌、王秋婷、何萍、邵舒婷、赵璐、张雪嫣、王凯。

可编程控制系统内生安全体系架构

1 范围

本文件规定了可编程控制系统内生安全体系架构，描述了可编程控制系统内生安全的目标和各单元模块的相关安全需求，规定了可编程控制系统的内生安全要求。其中，可编程控制系统内生安全的目标为保障可编程控制系统的完整性；各单元模块的相关安全需求包括全生命周期安全保护、综合诊断与高可用实现等。

本文件适用于工程设计商、设备生产商、系统集成商、用户以及评估认证机构等，主要应用于化工、石化、电力等行业。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15969.3—2017 可编程序控制器 第3部分：编程语言

3 术语和定义

下列术语和定义适用于本文件。

3.1 安全术语

3.1.1

伤害 harm

人身损伤、人的健康损害、财产或环境的损害。

[来源：ISO/IEC GUIDE 51：2014，3.1]

3.1.2

危险 hazard

伤害的潜在根源。

注：这个术语包括短时间对人身的伤害（如着火和爆炸），以及那些对人身健康长时间的损害（如有毒物质释放）。

[来源：ISO/IEC GUIDE 51：2014，3.2]

3.1.3

风险 risk

伤害发生的概率与该伤害严重程度的组合。

[来源：ISO/IEC GUIDE 51：2014，3.9]

3.1.4

安全 safety

免于不可接受的风险。