ICS 35.240.50
CCS J 07

中华人民共和国国家标准

GB/T 41262—2022

工业控制系统的信息物理融合异常检测系统技术要求

Technical requirements for cyber-physical fusion anomaly detection specification of industrial 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

目　　次

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。

本文件由中国机械工业联合会提出。

本文件由全国自动化系统与集成标准化技术委员会(SAC/TC 159)归口。

本文件起草单位：中国科学院信息工程研究所、北京机械工业自动化研究所有限公司、浙江大学、杭州优稳自动化系统有限公司、北京工业大学、上海电力大学、中国科学院声学研究所、奇安信科技集团股份有限公司、中国信息通信研究院、中国科学院沈阳自动化研究所、浙江中控技术股份有限公司、北京东方通科技股份有限公司。

本文件主要起草人：孙利民、石志强、朱红松、闫兆腾、吕世超、陈新、刘俊矫、张雪嫣、孙洁香、王文海、张稳稳、赵璐、赖英旭、孙墨童、谷浩然、王勇、杨军、王勋、陈君、王弢、崔君荣、梁炜、张思超、蒋皓、李艺、倪平、陆卫军、章维、李志、孙玉砚、李红、文辉、路晓、崔婷婷。

工业控制系统的信息物理融合异常检测系统技术要求

1 范围

本文件规定了融合信息空间和物理空间的工业控制系统异常检测技术架构、功能模块、功能要求及性能要求。

本文件适用于工业控制安全厂商、设备生产厂商研制高效的信息物理融合异常检测设备。

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 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 20275—2013 信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 36323 信息安全技术 工业控制系统安全管理基本要求

GB/T 36324—2018 信息安全技术 工业控制系统信息安全分级规范

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统 industrial control system；ICS

一类用于工业生产的控制系统的统称。

注：它包含SCADA、DCS和其他一些常见于工业部门与关键基础设施的小型控制系统(如PLC)等。

3.2

信息物理融合 cyber-physical fusion

将ICS中的指令、状态信息和真实物理系统相结合的过程。

注：具体体现为将ICS中生产控制设备中的物料流、信息流、能量流相结合。

3.3

信息物理系统 cyber-physical system；CPS

一个综合计算、网络和物理环境的多维复杂系统。

注：通过通信技术、计算机技术和控制技术的有机融合与深度协作，实现大型工程系统的实时感知、动态控制和信息服务。

3.4

异常 abnormal

故障、意外或攻击行为导致的系统出现异于正常或已有基线的情况。