

ICS 25.040
N 10



中华人民共和国国家标准

GB/T 38847—2020

智能工厂 工业控制异常监测工具技术要求

Intelligence factory—
Technical requirements for industrial control abnormal monitoring instrument

2020-07-21 发布

2021-02-01 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	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 工业控制异常监测工具的部署	2
5 工业控制异常监测工具等级划分	2
5.1 技术要求分级	2
5.2 技术要求分类	3
6 技术要求	5
6.1 基本级	5
6.2 增强级	9
附录 A (规范性附录) 环境适应性要求	12

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国机械工业联合会提出。

本标准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。

本标准起草单位:启明星辰信息技术集团股份有限公司、机械工业仪器仪表综合技术经济研究所、中国石油天然气股份有限公司规划总院、北京中油瑞飞信息技术有限责任公司、中车戚墅堰机车有限公司、中国科学院沈阳自动化研究所、北京市自来水集团有限责任公司、重庆信安网络安全等级测评有限公司、上海自动化仪表有限公司、中国网络安全审查技术与认证中心、国家工业信息安全发展研究中心。

本标准主要起草人:孟雅辉、许涛、王玉敏、和曦、杜兰、尚文利、张晨艳、张为群、包伟华、甘杰夫、张哲宇、赵剑明、刘志远、董朋、原真、马俊闯、尚羽佳、王静、周学良、单博、蒋浩然、陈春雨。

引 言

随着工业化与信息化的深度融合,来自信息网络的安全威胁正逐步对工业控制系统造成极大的安全威胁,传统的工业控制异常监测工具在面对工业控制系统的安全监测时因不能识别工业控制系统专用协议、对工业控制系统异常特征分析不足,显得力不从心,因此急需一种能应用于智能工厂中的工业控制异常监测工具对异常行为进行监测和报警。

应用于智能工厂的工业控制异常监测工具与传统工业控制异常监测工具的主要差异体现在:

- a) 智能工厂的工业控制异常监测工具是专门针对工业控制系统的检测系统,支持十几种主流工控协议的深度解析,内置特有的工控网络检测策略;可检测利用工控设备漏洞对工控网络的多种入侵攻击;
- b) 智能工厂的工业控制异常监测工具采用工业级全密闭硬件设计,环境适应能力强;
- c) 智能工厂的工业控制异常监测工具满足工业现场要求的高可靠性和稳定性等需求。

智能工厂

工业控制异常监测工具技术要求

1 范围

本标准规定了智能工厂的工业控制异常监测工具(以下简称:监测工具)的部署、等级划分和技术要求。

本标准适用于工业控制异常监测工具的设计、开发与测试。

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 2423.5—2019 环境试验 第2部分:试验方法 试验 Ea 和导则:冲击

GB/T 2423.10 环境试验 第2部分:试验方法 试验 Fc: 振动(正弦)

GB/T 4208—2017 外壳防护等级(IP代码)

GB 4824 工业、科学和医疗(ISM)射频设备 骚扰特性 限值和测量方法

GB/T 4857.20 包装 运输包装件 碰撞试验方法

GB/T 4857.23—2012 包装 运输包装件基本试验 第23部分:随机振动试验方法

GB/T 9254 信息技术设备的无线电骚扰限值和测量方法

GB/T 13729—2019 远动终端设备

GB/T 15153.1 远动设备及系统 第2部分:工作条件 第1篇:电源和电磁兼容性

GB/T 17214.4 工业过程测量和控制装置的工作条件 第4部分:腐蚀和侵蚀影响

GB/T 17626.2 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 17626.3 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 17626.4 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验

GB/T 17626.5 电磁兼容 试验和测量技术 浪涌(冲击)抗扰度试验

GB/T 17626.6 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度

GB/T 17626.8 电磁兼容 试验和测量技术 工频磁场抗扰度试验

GB/T 17626.10 电磁兼容 试验和测量技术 阻尼振荡磁场抗扰度试验

GB/T 17626.11 电磁兼容 试验和测量技术 电压暂降、短时中断和电压变化的抗扰度试验

GB/T 17626.12—2013 电磁兼容 试验和测量技术 振铃波抗扰度试验

GB/T 17626.16 电磁兼容 试验和测量技术 0 Hz~150 kHz 共模传导骚扰抗扰度试验

GB/T 17626.17 电磁兼容 试验和测量技术 直流电源输入端口纹波抗扰度试验

GB/T 17626.29 电磁兼容 试验和测量技术 直流电源输入端口电压暂降、短时中断和电压变化的抗扰度试验

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

3 术语、定义和缩略语

下列术语和定义适用于本文件。