ICS 35.240.50
CCS J 07

# 中华人民共和国国家标准

GB/T 41263—2022

# 工控系统动态重构主动防御体系架构规范

**Industrial control system dynamic reconfiguration active defense technical architecture specification**

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：中国人民解放军信息工程大学、北京机械工业自动化研究所有限公司、北京四方继保自动化股份有限公司、北京众享比特科技有限公司、中国工程物理研究院计算机应用研究所。

本文件主要起草人：魏强、宋涛、王红敏、陈鸿刚、员天佑、张雪嫣、周立东、王凯、陈红、黄辉辉、麻荣宽、杨永辉。

# 工控系统动态重构主动防御体系架构规范

## 1 范围

本文件规定了工控网络的信息安全体系架构，描述了过程监控层异构编译环境多态部署、工控网络信息安全传输模式、现场控制层异构运行逻辑及智能判决和工程文件安全存储验证机制，规定了信息安全体系评价指标参数。

本文件适用于旨在构建具有内生安全防护能力的所有工业控制系统参与者，为相关参与者设计动态重构主动防御的工控网络提供指导要求。

## 2 规范性引用文件

本文件没有规范性引用文件。

## 3 术语和定义

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**

由计算机和工业过程控制部件构成的自动化控制系统。

注 1：工业控制系统简称“工控系统”。该系统通过工业通信线路，根据专用的工业通信协议将控制器、传感器、执行器和输入/输出接口等部分连接起来，构建一个具有自动控制能力的工业制造系统。

注 2：ICS 是一个通用术语，它包括多种工业生产中使用的控制系统，包括 SCADA、DCS 和其他较小的控制系统，如 PLC，现已广泛应用在工业部门和关键基础设施中。对这一概念更多的讨论见 GB/T 32919—2016。

3.2

**工业控制网络 industrial control network**

一种利用各种通信设备将所有工业生产设备和自动化控制系统连接起来的通信网络。

注：工业控制网络是 ICS 中的网络部分，简称“工控网络”。

3.3

**可编程逻辑控制器 programmable logic controller；PLC**

一种用于工业环境的数字式操作的电子系统。

注 1：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。PLC 及其相关外围设备的设计，使它能够非常方便地集成到 ICS 中，并能很容易地达到所期望的所有功能。

注 2：对这一概念更多的讨论见 GB/T 33008.1—2016。

3.4

**分散控制系统 distributed control system；DCS**

采用计算机、通信和屏幕显示技术，实现对生产过程的数据采集、控制和保护功能，利用通信技术实现数据共享的多计算机监控系统。

注 1：分散控制系统的主要特点是功能分散、操作显示集中、数据共享。根据具体情况也可以是硬件布置上的分散。