ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36466—2018

信息安全技术
工业控制系统风险评估实施指南

Information security technology—
Implementation guide to risk assessment of industrial control systems

2018-06-07 发布　　2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位:国家信息技术安全研究中心、中国电子技术标准化研究院、全球能源互联网研究院、中国电子信息产业集团有限公司第六研究所。

本标准主要起草人:李京春、李冰、刘鸿运、方进社、刘贤刚、范科峰、高昆仑、刘仁辉、葛培勤、王宏、曾珍珍、李健、梁潇、詹雄、李霞、庞宁、姚相振、周睿康、赵婷、刘楠、徐克超、蔡磊。

引　言

随着工业控制系统和信息化技术的融合，工业控制系统广泛应用于冶金、电力、石化、水处理、铁路、航空和食品加工等行业。工业控制系统指应用于工业控制领域的数据采集、监视与控制系统，是由计算机设备、工业过程控制组件和网络组成的控制系统，是工业领域的神经中枢。工业中使用的控制系统包括监视控制与采集系统、分布式控制系统、可编程逻辑控制器系统等。我国把工业控制系统信息安全作为信息安全保障的一个相对独立的体系进行建设，其安全性将直接关系到国家重要基础工业设施生产的正常运行和广大公众的利益。

本标准在对工业控制系统的资产进行整理分析的基础上，从其资产的安全特性出发，分析工业控制系统的威胁来源与自身脆弱性，归纳出工业控制系统面临的信息安全风险，并给出实施工业控制系统风险评估的指导性建议。

本标准主要为第三方安全检测评估机构在工业控制系统现场实施风险评估提供指南，也可供工业控制系统业主单位进行自评估时参考。

信息安全技术
工业控制系统风险评估实施指南

1 范围

本标准规定了工业控制系统风险评估实施的方法和过程。

本标准适用于指导第三方安全检测评估机构对工业控制系统的风险评估实施工作，也可供工业控制系统业主单位进行自评估时参考。

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 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

ISO/IEC 62264-1:2013 企业控制系统综合 第1部分：模型和术语(Enterprise-control system integration—Part 1:Models and terminology)

3 术语、定义和缩略语

3.1 术语和定义

GB/T 31509—2015 和 GB/T 32919—2016 中界定的以及下列术语和定义适用于本文件。

3.1.1

监视控制数据采集系统 supervisory control and data acquisition system;SCADA

在工业生产控制过程中，对大规模远距离地理分布的资产和设备在广域网环境下进行集中式数据采集与监控管理的控制系统。

3.1.2

分布式控制系统 distributed control system;DCS

以计算机为基础，在系统内部(单位内部)对生产过程进行分布控制、集中管理的系统。

3.1.3

主终端单元 master terminal unit;MTU

用于生产过程信息收集和检测的工业控制系统总站。

注：一般部署在调度控制中心。

3.1.4

远程终端单元 remote terminal unit;RTU

用于监测、控制远程工业生产装备的工业控制系统远程站点设备。

3.1.5

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

采用可编程存储器，通过数字运算操作对工业生产装备进行控制的电子设备。