

---

# **工业控制系统安全指南**

监测控制和数据采集系统、分布式控制系统以及  
可编程逻辑控制器等其他控制系统

---

**Keith Stouffer**

**Victoria Pilliteri**

**Suzanne Lightman**

**Marshall Abrams**

**Adam Hahn**

<http://dx.doi.org/10.6028/NIST.SP.800-82r2>

2015 年 5 月



美国商务部

**Penny Pritzker**, 部长

国家标准和技术研究所

**Willie May**, 商务部副部长兼 NIST 所长

# 目录

## 执行摘要

### 1 介绍

- 1.1 目的和范围
- 1.2 适用对象
- 1.3 篇章结构

### 2 工业控制系统概述

- 2.1 工业控制系统的进化
- 2.2 ICS 工业部门和它们的相互依存性
  - 2.2.1 制造业
  - 2.2.2 配送业
  - 2.2.3 制造 ICS 与输送 ICS 的差别
  - 2.2.4 ICS 与关键基础设施的相互依存性
- 2.3 ICS 的运行和组件
  - 2.3.1 ICS 系统的设计考虑
  - 2.3.2 SCADA 系统
  - 2.3.3 分布式控制系统
  - 2.3.4 基于拓扑结构的可编程逻辑控制器
- 2.4 ICS 与 IT 系统的安全比较
- 2.5 其他类型控制系统

### 3 ICS 风险管理和评价

- 3.1 风险管理
- 3.2 风险管理流程概述
- 3.3 ICS 风险评价的特殊考虑
  - 3.3.1 ICS 信息安全风险评价的安全
  - 3.3.2 ICS 事故的潜在物理影响
  - 3.3.3 ICS 流程物理毁坏的影响
  - 3.3.4 影响评价需涵盖 ICS 的非数字方面
  - 3.3.5 考虑安全系统的影响
  - 3.3.6 考虑影响向相互连接的系统传播的情况

### 4 ICS 安全方案的制定和落实

- 4.1 安全业务案例
  - 4.1.1 好处
  - 4.1.2 潜在后果
  - 4.1.3 建立业务案例的资源
  - 4.1.4 向管理层提交业务案例
- 4.2 组建和训练一个跨职能团队
- 4.3 制定方针并确定范围
- 4.4 制定针对 ICS 的安全策略和规程
- 4.5 执行 ICS 安全风险管理体系
  - 4.5.1 ICS 系统和网络资产分类

4.5.2 挑选 ICS 安全控制

4.5.3 进行风险评价

4.5.4 执行安全控制

## 5 ICS 安全架构

5.1 网络分段和隔离

5.2 边界保护

5.3 防火墙

5.4 逻辑隔离的控制网络

5.5 网络隔离

5.5.1 双宿计算机/双网卡

5.5.2 公司网络与控制网络之间配备防火墙

5.5.3 公司网络与控制网络之间配备防火墙和路由器

5.5.4 公司网络与控制网络之间配备带 DMZ 的防火墙

5.5.5 公司网络与控制网络之间配备成对防火墙

5.5.6 网络隔离小结

5.6 建议的深度防御架构

5.7 ICS 的防火墙总策略

5.8 针对具体服务建议的防火墙规则

5.8.1 域名系统 (DNS)

5.8.2 超文本传输协议 (HTTP)

5.8.3 FTP 和普通文件传送协议 (TFTP)

5.8.4 Telnet

5.8.5 动态主机配置协议 (DHCP)

5.8.6 安全壳 (SSH)

5.8.7 简单对象访问协议 (SOAP)

5.8.8 简单邮件传输协议 (SMTP)

5.8.9 简单网络管理协议 (SNMP)

5.8.10 分布式组件对象模型 (DCOM)

5.8.11 SCADA 和工业协议

5.9 网络地址转换 (NAT)

5.10 ICS 防火墙的具体问题

5.10.1 数据史料库

5.10.2 远程支持访问

5.10.3 组播通信流

5.11 单向网关

5.12 单故障点

5.13 冗余和容错

5.14 预防中间人攻击

5.15 认证和授权

5.15.1 ICS 的执行考虑

5.16 监测、日志记录和审计

5.17 事故检测、响应和系统恢复

## 6 ICS 施用安全控制

## 6.1 为工业控制系统执行风险管理框架

- 6.1.1 步骤 1: 分类信息系统
- 6.1.2 步骤 2: 挑选安全控制
- 6.1.3 步骤 3: 执行安全控制
- 6.1.4 步骤 4: 评价安全控制
- 6.1.5 步骤 5: 授权信息系统运行
- 6.1.6 步骤 6: 监测安全控制

## 6.2 ICS 安全控制实施指南

- 6.2.1 访问控制
- 6.2.2 意识和培训
- 6.2.3 审计和问责
- 6.2.4 安全评价和授权
- 6.2.5 配置管理
- 6.2.6 应急预案规划
- 6.2.7 识别和认证
- 6.2.8 事故响应
- 6.2.9 维护
- 6.2.10 介质保护
- 6.2.11 物理和环境保护
- 6.2.12 规划
- 6.2.13 人员安全
- 6.2.14 风险评价
- 6.2.15 系统和服务采办
- 6.2.16 系统和通信保护
- 6.2.17 系统和信息的完整性
- 6.2.18 方案管理
- 6.2.19 隐私控制

## 附录 A 缩写词和缩略语

## 附录 B 术语表

## 附录 C 威胁源、脆弱性和事故

## 附录 D 工业控制系统安全领域的当前动态

## 附录 E 用于 ICS 的安全能力和工具

## 附录 F 参考文献

## 附录 G ICS 叠加控制

