

**工业控制系统的信息安全防护技术综述**

院 系 自动化学院

专业班级 硕1601班

姓 名 柳 伟

学 号 M201672296

2016年 11月 12日

# 摘 要

工业控制领域正在发生重大的变革，德国和美国相继提出了“工业4.0”、“工业互联网”概念，我国也于2015年5月8日提出“中国制造2025”战略，在两化深度融合的基础上继续进行产业结构调整和升级转型。作为工业控制网络重要的组成部分，工业控制网络安全深刻地影响着工业控制网络及相关产业的发展，具有极强的产业关联度和产业渗透能力，因此工业控制网络安全产业得到了各国极大的关注。

工业控制系统广泛用于电力、石油石化、核能、航空、铁路、公路、水处理、地铁等行业，是这些国家关键基础设施运行的“大脑”和“中枢”，2010年“震网病毒”事件更进一步敲响了工业控制系统信息安全严峻性和现实性的警钟。该文提出了工业控制系统信息安全的内涵，综述了工业控制系统信息安全的现状，讨论了工业控制系统信息安全相关的关键技术，并对工业控制系统信息安全的主要挑战和研究方向进行了展望。

**关键词**：工业控制系统；信息安全；监控和数据采集系统；防护体系

**目 录**

[摘 要 I](#_Toc466753584)

[1 绪论 1](#_Toc466753585)

[2 工业控制系统概述 2](#_Toc466753586)

[3 工业控制网络安全情况总体分析 2](#_Toc466753587)

[3.1 工业控制网络安全情况 2](#_Toc466753588)

[3.2 国际工业控制网络安全政策动态 3](#_Toc466753589)

[4 工业控制系统的威胁 4](#_Toc466753590)

[4.1 工业控制系统面临的威胁 4](#_Toc466753591)

[4.2 工控系统几个重要环节面临的信息安全风险 4](#_Toc466753592)

[5 工业控制系统的信息安全安全防护技术 5](#_Toc466753593)

[5.1 工控系统信息安全防护研究框架安全防护研究框架 5](#_Toc466753594)

[5.2 工业控制系统的安全防护技术 6](#_Toc466753595)

[6 工业控制系统信息安全挑战与展望 8](#_Toc466753596)

[参考文献 10](#_Toc466753597)

# 1 绪论

工业控制系统（Industrial Control Systems，ICS）是指包括计算机设备、自动化控制设备、实时数据采集和检测的过程控制设备在内的自动化控制系统，实现工业设施的自动化运行、过程监测和控制、业务流程的管理和控制。工业控制系统在各个领域都有普遍的应用，如工业、水利、能源等。所以，工业控制系统的安全问题，直接关系到整个工业生产运行、国家经济和人民财产安全。工业控制系统对于目前工业发展的重要性、以及其脆弱的安全现状和日趋严峻的攻击威胁已经引起了世界各国的极大关注，并且从各个方面展开了积极的应对，如政策、技术、标准、方案等。自2013年以来，工业控制系统的安全问题已经成为工业领域和信息安全领域研究的热点。

随着信息化对工业领域的影响越来越深以及物联网的迅速发展，对于传统信息安全领域的威胁（病毒、蠕虫、木马等）正向工业控制领域逐步扩散，工业控制系统的安全问题日渐严峻。近年来，发生了一系列重大的工控系统安全问题，特别是2010年在伊朗爆发的Stuxnet病毒以及其后出现的Flame病毒，都充分体现了工业控制领域所面临的严峻的安全形势。

近年来，工业控制系统安全事件正快速增长，2011年到2014年的统计数据就占了所有统计数据的85%。与传统的IT信息系统软件不同的是，工业控制系统软件的使用较为封闭，开发时主要注重的是系统的功能实现，而对系统安全的关注较少。同时，在基于工控系统组态软件的开发过程中，既没有完善的安全软件开发规范，也没有严格的安全测试流程。这使得工业控制系统必然存在更多的安全缺陷。因此，不仅要完善工业控制系统软件自身的安全性问题，同时工业控制系统的组态软件的安全性问题也不容忽视。

工业控制领域正在发生重大的变革，德国和美国相继提出了“工业4.0”、“工业互联网”概念，我国也于2015年5月8日提出“中国制造2025”战略，在两化深度融合的基础上继续进行产业结构调整和升级转型。作为工业控制网络重要的组成部分，工业控制网络安全深刻地影响着工业控制网络及相关产业的发展，具有极强的产业关联度和产业渗透能力，因此工业控制网络安全产业得到了各国极大的关注。

# 2 工业控制系统概述

工业控制系统是以计算机为基本组件，用于监测和控制物理过程的系统。这类系统包含了大部分网络系统与物理系统连接的网络化系统。根据其应用范围，控制系统又可以分为过程控制系统，监控和数据采集系统（SCADA），或网络-物理系统（CPS）。

控制系统通常由一系列网络设备构成，包括：传感器、执行器、过程控制单元和通信设备。控制系统通常采用分层结构，典型的控制系统网络结构如图2-1所示，第一层为安装有传感器和执行器等现场设备的物理设施，现场设备通过现场总线网络与可编程逻辑控制器（PLC）或远程终端设备（RTU）连接，PLC或RTU设备负责实现局域控制功能。第二层为控制网络，主要负责过程控制器和操作员站之间的实时数据传输。操作员站用于区域监控和设置物理设施的设定值。第三层为企业网，企业工作站负责生产控制，过程优化和过程日志记录。

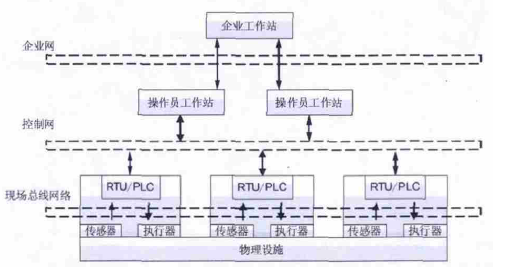


图2-1 典型控制系统的架构

根据控制系统的应用特性，可以分为安全相关的应用和非安全相关的应用。安全相关的应用一旦失效，可能会造成受控制的物理系统发生不可恢复的破坏。如果这类控制系统遭受破坏，将会对公共健康和安全产生重大影响，并导致经济损失。

# 3 工业控制网络安全情况总体分析

## 3.1 工业控制网络安全情况

美国工业控制系统网络应急响应小组（ICS-CERT）发布的2014年关键基础设施安全报告显示，在2014年共收集了167个工控漏洞报告，涉及的设备分布在能源、制造业等多个领域，表3-1中显示了从2012年到2014年工控漏洞报告数量和所涉及到工控设备的数量。

表3-1 工控漏洞及相应的工控产品统计

|  |  |  |  |
| --- | --- | --- | --- |
|  | 2012年 | 2013年 | 2014年 |
| 工控漏洞报告 | 147 | 181 | 167 |
| 涉及的工控产品 | 343 | 285 | 362 |

近几年工业网络安全事件也呈现出稳步增长的趋势，如表2-2所示。

表3-2 工业控制网络安全事件在近几年呈现稳步增长的趋势

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2012年 | 2013年 | 2014年 | 2015年 |
| 网络安全事件 | 197 | 257 | 245 | 295 |

## 3.2 国际工业控制网络安全政策动态

自2005年开始，美国和欧盟就高度重视工业控制网络安全技术的发展，大力推动相关前沿技术研究，相继发布了保护国家关键基础设施的国家战略和政策法规，并牵头建立了多个国家级工业控制网络安全实验室，构建了全维度的工控网络安全国家体系。

美国和欧盟均已发布了关于网络安全和保护关键基础设施的国家战略。美国于2006年专门设立了“国家基础设施保护计划”，并在2010年设立了控制系统安全计划（CSSP），将保护美国国家基础设施的控制系统上升为国家战略。欧盟继美国之后于2013年发布了“欧洲关键基础设施保护项目（EPCIP）”，协调欧盟各个国家保护其关键基础设施，应对日益增加的针对关键基础设施的网络攻击。

美国国防部、国土安全部、能源部、国家标准局、审计署和财政部协调各自职能，为该战略提供相应的资源协助。欧洲则是由欧洲委员会、欧洲高级议会、欧洲对外行动处、欧洲防务局、欧洲网络犯罪中心和欧洲标准机构，协调欧盟各个国家的相关职能，部署各个国家的关键设施保护计划。

同时，美国国土安全部成立了工业控制系统应急响应组（ICS-CERT），作为CSSP的实施部门。欧盟也成立了类似的欧洲网络应急响应组（CERT-EU），同时计划成立针对工业控制网络安全的应急响应组（ICS-CSIRT）。

# 4 工业控制系统的威胁

## 4.1 工业控制系统面临的威胁

工业控制系统面临的威胁可以分为两种：系统相关的威胁和过程相关的威胁。

系统相关的威胁是指由于软件漏洞所造成的威胁。 控制系统从广义上是一种信息系统， 会受到系统相关的威胁， 如协议实现漏洞、操作系统漏洞等。

过程相关的威胁是指工业控制系统在生产过程遭受的攻击。 这种攻击利用过程控制的特点，攻击者非法获取用户访问权限后，发布合法的工业控制系统命令，导致工业过程的故障。 基于工业控制系统用户与工业过程的交互点， 可以将过程相关的威胁分为两类：①影响现场设备的访问控制的威胁；②影响中央控制台的威胁。 前者通常发送错误的现场数据到控制系统状态监测中心，从而导致系统状态分析出现错误。 后者通常在中央控制台执行合法的命令，但该命令对生产过程而言不合理，将对生产或设备产生负面影响。

控制系统的漏洞一旦被攻击者利用，会遭受不同类型的攻击，具体的攻击形式可以分为：

（1）欺骗攻击：在通信过程中伪装成某个合法设备。 例如，使用一个伪造的网络源地址。

（2）拒绝式服务攻击：系统中任意资源的不可用。 例如，设备因忙于应答大量的恶意流量而无法响应其他消息等。

（3）中间人攻击：攻击者从通信的一端拦截所有消息，修改消息后再转发到终端接收设备。

（4）重播攻击：重复发送某个过时的消息，如用户认证或命令等。

## 4.2 工控系统几个重要环节面临的信息安全风险

工控主站系统一般处于相对封闭的专用网络，通过专用隔离装置与外界交互。随着信息化与工业化的深度融合，工控系统正越来越多的使用通用协议、通用操作系统、通用硬件和软件。由于以太网、无线设备无处不在，整个控制系统都可以和远程终端进行互连，病毒、木马、蠕虫等信息网络安全问题直接延伸到工控系统。工控系统几个重要环节面临的信息安全风险如下。

（1）在数据采集环节，工控系统终端设备一般长时间运行在自然条件恶劣的户外或无人值守机房，不仅容易出现物理安全问题，而且受限于设备自身的计算资源，终端设备难以全面应用各种信息安全防护技术，易遭受仿冒、窃听和篡改等攻击。

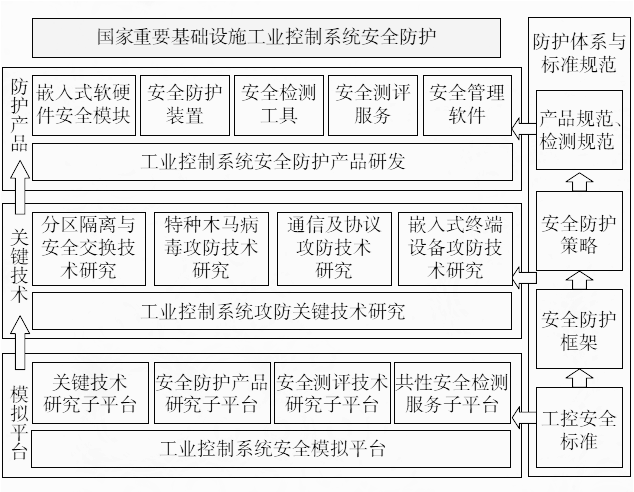
（2）在数据传输环节，绝大部分工控系统都采用国际标准的专有通信协议进行传输，此类协议绝大部分缺乏有效的身份鉴别和访问控制机制，并以明文方式进行传输，导致重要的控制命令、参数设置等信息面临被窃听、篡改的风险。

（3）在数据处理环节，工控系统更多采用标准化的工控机或嵌入式系统，以及通用的数据处理技术，一般信息网络安全问题对工控系统造成日益严重的威胁。

# 5 工业控制系统的信息安全安全防护技术

## 5.1 工控系统信息安全防护研究框架安全防护研究框架

在工控系统信息安全防护需求的基础上，根据国家对工控安全防护的标准规范和政策要求，结合电力、石化等领域多年信息安全防护实践经验，提出由防护体系与标准规范、工控安全模拟平台、攻防关键技术研究、安全防护产品研发等部分组成的工控系统信息安全防护研究框架（见图5-1）。其中防护体系与标准规范研究的成果将直接指导关键技术研究和防护产品研发等工作，模拟平台的建设将为关键技术研究和防护产品研发提供基础环境和设施支撑，关键技术研究的成果将直接转换为研究开发自主知识产权的工控安全专用防护产品，同时为工控产品安全检测和测评服务提供配套技术及工具等方面的有力支撑。



**图5-1 工控系统信息安全防护研究框架安全防护研究框架**

## 5.2 工业控制系统的安全防护技术

为了防止工业控制系统在通信过程中遭受上述各种威胁与攻击，需要使用多层安全措施完成对系统的保护。为了保证工业控制系统的安全性，首先需要增强网络边界的防护，以降低由企业网引入的威胁风险。标准SP800－82《工业控制系统(ICS)安全指南》指出，在处理工业控制系统网络与其他应用网络的连接问题时，需要按照最小访问原则设计，在具体的技术措施上，SP800－82从身份认证、访问控制、审计与核查、系统与通信保护等方面详细介绍了可用的技术措施。

（1）身份认证

通过PIN码或密码验证申请访问的设备或人员。在网络上传输密码时需要对密码进行加密，通过选取合适的加密哈希函数，可以阻止重播攻击。密码认证还可以辅以其他认证措施，如询问／应答或使用生物令牌或物理令牌。紧急情况下，工业控制系统使用密码和生物认证都存在一定危险。因此在不适合使用密码的情况下，可以采用严密的物理安全控制作为替代。

（2）访问控制

基于角色的访问控制（RBAC）可以用于限制用户的权限，使其能以最小的权限完成任务。系统管理员的通讯需要加以认证，并对其保密性和完整性加以保护，如使用SSHv2和HTTPS协议。这两个协议都使用公钥／私钥对进行用户认证。 通信双方产生并使用对称密钥加密数据交互过程。

RADIUS远程认证拨号用户服务式目前使用最多的认证和授权服务。它使用 IEEE802.1x和EAP协议，可以在网络的各个层实现用户认证。例如，防火墙和接入路由可以作为认证代理。当无线设备或中断用户设备需要与其连接时，认证代理向设备发出询问，设备通过认证服务器返回认证信息，从而获得授权和接入许可。

调制解调器经常用于提供备份连接。回叫系统通过存储于数据库中的回叫号码，确认拨号者是否为合法用户。远程控制软件需要使用唯一的用户名和密码，加密和审计日志。链路层的邻居认证需要使用CHAP协议等实现。

（3）审计与核查

工业控制系统需要进行周期性的审计，验证内容包括：测试阶段的安全控制措施在生产系统中仍安装使用；生产系统不受安全破坏，如果受到安全破坏则提供攻击的信息；改动项目需要为所有的变动建立审查和批准的记录。

周期性的审计结果用一定的度量表示，用于显示安全性能和安全趋势。审计需要使用特定工具进行记录维护，需要工业控制系统中的组件支持。审计有利于维护工业控制系统在系统生命周期内的完整性。工业控制系统需要为审计工具提供可靠的同步时间戳。工业控制系统应用中维护的日志可以存储于多个地点，加密或不加密都是可以的。

（4）系统与通信保护

系统与通信的保护可以通过网络防护措施，如防火墙和入侵检测系统等，以及数据加密，如VPN等实现。

网络防火墙控制不同安全等级的网络区域间的数据流量。NIST SP 800-41为防火墙的选择和防火墙策略提供了指导。在工业控制系统环境下，需要在控制网和企业网之间部署防火墙。防火墙包含的特征功能包括：事件记录，入侵检测系统，基于非军事区的路由，访问列表等。

当系统被嗅探或攻击时，入侵检测系统发出警报。入侵检测系统通过在网络的各个关键点收集信息，分析数据包内容发现恶意流量，并发出警报、废弃无效数据、记录事件和活动并触发其他安全响应。对于多种工业控制系统中的应用协议所受到的攻击，如DNP和ICCP，入侵检测系统也会增加相应的攻击特征。

基于IPsec的VPN可以为网络边界的通信提供安全隧道，通常在相应的防火墙上执行。IPsec可以保证完整性、认证和数据保密性。在隧道入口处，IP包外增加额外的数据包头，路由器使用新的包头信息转发数据，到达隧道出口时，将原始 IP 包提取出来。在用户认证过程中，IPsec通常使用私钥和RSA签名。在消息认证和完整性保护时，使用MD5或SHA哈希函数。在数据加密时，使用AES或 3DES。IPsec还使用Diffie-Hellman作为对称密钥推导。IPsec设备使用IKE协议认证其他设备、协商和分配对称加密密钥以及建立IPsec安全连接。

控制系统的安全管理包括检测、分析、提供安全和事件响应。具体内容包括动态调整安全要求，安全漏洞的优先级排序，以及安全要求到安全管理的映射：认证和授权服务器，安全密钥，流量过滤，IDS，登录等。SNMP用于管理IP网络资源，如路由，防火墙和服务器等。SNMP也可用于提供控制系统网络的集中管理。SNMPv3包括的安全特性有消息完整性，认证和加密。SNMPv3使用MD5和 SHA哈希算法和DES以及AES加密算法。

# 6 工业控制系统信息安全挑战与展望

工业控制系统信息安全是多行业、多领域和多学科融合的新兴领域，关于工业控制系统信息安全研究仍然处于起步发展阶段，本文在现有研究分析阐述的基础上简要描述在当前工业控制系统信息安全研究中的主要挑战和展望。

（1）从复杂系统角度来研究工业控制系统的外延，研究工业控制系统信息安全内延和外延的融合，是工业控制系统信息安全理论研究的重要挑战。

将工业控制系统信息安全研究放在更大的关键基础设施的背景中进行研究，研究如何使用复杂网络建模、系统动力学建模等复杂系统理论进行建模，研究工业控制系统之间的相互依赖性、工业控制系统对相互依赖的关键基础设施的影响，研究工业控制系统信息安全事件对所处关键基础设施、相关关键基础设施以及对宏观经济、国家安全的影响和后果，从而支持工业控制系统信息安全宏观管理和决策，是工业控制系统信息安全研究领域中的重大挑战和方向。

（2）从信息物理融合系统（CPS）角度来研究工业控制系统的理论基础和方向，是工业控制系统信息安全理论研究的另一个重大挑战。

信息物理融合系统是多维异构的计算单元和物理对象在网络环境中高度集成交互的新型智能复杂系统，具有实时、鲁棒、自治、高效和高性能等特点。现代工业控制系统是一种典型的信息物理融合系统，如何从工业控制系统是信息物理融合系统这一本质特点出发，深度融合计算、通信和控制领域，实现信息世界和物理世界的完全融合，构建一个可控、可信、可扩展并且安全高效的网络，并最终从根本上改变人类构建工程物理系统的方式是工业控制系统信息安全发展的目标。

（3）进一步深化工业控制系统风险评估技术，深入研究工业控制系统基础平台模拟仿真测试床，工业控制系统漏洞分析和风险评估，建设、部署和管理韧性工业控制系统等方面的技术，都为工业控制系统信息安全理论结合实践的带来了挑战。

# 参考文献

[1] 朱世顺,黄益彬,朱应飞等.工业控制系统信息安全防护关键技术研究. Electric Power ICT, 2013,11(11):106-109

[2] Xin Hao, Feng Zhou, Xi Chen. Analysis on security standards for industrial control system and enlightenment on relevant Chinese standards. 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), 2016: 1967-1971

[3] NIST SP 800-82. Guide to industrial control systems security[S].2011.

[4] 胡冬平. 工业控制系统组态软件安全防护关键技术研究. 哈尔滨工业大学[硕士毕业论文], 2015

[5] Maryna Krotofil, Dieter Gollmann. Industrial control systems security: What is happening? 2013 11th IEEE International Conference on Industrial Informatics (INDIN),2013: 664-675

[6] A. Amrein, V. Angeletti, A. Beitler, M. Német, M. Reiser; S. Riccetti, M. Ph. Stoecklin, A. Wespi. Security intelligence for industrial control systems. IBM Journal of Research and Development, 2016, 60(4): 13:1-13:12

[7] 匡恩网络. 2015年工业控制网络安全态势报告

[8] 何之栋, 裘坤, 钟晨等. 工业控制系统的信息安全问题研究. 工业控制计算机, 2013, 26(10): 1-4

[9] Dacfey Dzung, Martin Naedele, et al． Security for Industrial Communication Systems． Power Delivery, IEEE Transactions on 23．4 (2008): 2628－2629

[10] NIST SP800-82. Guide to Industrial Control Systems (ICS) Security. Gaithersburg, USA: National Institute of Standards and Technology (NIST), 2011

[11] 彭勇, 江长青, 谢丰等. 工业控制系统信息安全研究进展. 清华大学学报（自然科学报）, 2012, 52(10): 1396-1048

[12] 魏可承, 李斌, 易伟文等. 工业控制信息安全防护体系规划研究. 自动化仪表, 2015,36(2): 49-52

[13] 李航, 朱广宇. 建立健全我国工业控制系统信息安全体系. 微型机与应用, 2015,34(1): 13-16

[14] 余勇, 林为民. 工业控制SCADA系统的信息安全防护体系研究. 信息网络安全, 2012,6: 74-77

[15] 张敏, 张五一, 韩桂芬. 工业控制系统信息安全防护体系研究. 工业控制计算机, 2013,26(10): 25-27