信息与控制　2022 年　第 51 卷　第 1 期：1 ~ 11

DOI：10.13976/j.cnki.xk.2022.0535　　文章编号：1002 - 0411(2022) - 01 - 0001 - 11

工业测控设备内生信息安全技术研究综述

尚文利[1]，王天宇[2,3,4]，曹　忠[1]，刘贤达[2,3,4]

1. 广州大学电子与通信工程学院，广东 广州　510006；
2. 中国科学院网络化控制系统重点实验室，辽宁 沈阳　110016；
3. 中国科学院沈阳自动化研究所，辽宁 沈阳　110016；
4. 中国科学院机器人与智能制造创新研究院，辽宁 沈阳　110169

基金项目：国家重点研发计划(2018YFB2004200)；国家自然科学基金(62173101，61773368)；之江实验室开放课题(2021KF0AB06)

通信作者：王天宇，wangtianyu@sia.cn　收稿/录用/修回：2020 - 11 - 18/2021 - 06 - 07/2021 - 11 - 19

摘要

工业测控设备是工业控制系统的神经中枢，其信息安全问题直接关系到工业控制系统的安全。传统信息安全防护技术手段具有局限性，网络无法阻断物理介质传输数据和物理设备的接入，即使是物理隔离的工业测控设备，亦可以成为攻击目标，迫切需要增强工业测控设备自身的内生安全防护能力。本文结合相关国际标准和国家标准，将工业测控设备内生信息安全防护技术分为静态加固技术和动态防护技术，对涉及的七类信息安全防护技术进行了逻辑分类，给出了工业测控设备的内生信息安全的术语定义，并具体分析、评价了已有相关理论研究和关键技术的优势和不足之处。最后，对工业测控设备的内生信息安全防护技术的发展趋势进行了展望。

关键词

工业测控设备
信息安全
数据加密
访问控制
完整性保证

中图法分类号：TP393.08

文献标识码：A

Review on Endogenous Information Security Technology of Industrial Measurement and Control Equipment

SHANG Wenli[1], WANG Tianyu[2,3,4], CAO Zhong[1], LIU Xianda[2,3,4]

1. *School of Electronics and Communication Engineering, Guangzhou University, Guangzhou* 510006, *China*;
2. *Key Laboratory of Networked Control System, Chinese Academy of Sciences, Shenyang* 110016, *China*;
3. *Shenyang Institute of Automation, Chinese Academy of Science, Shenyang* 110016, *China*;
4. *Institute for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang* 110169, *China*

Abstract

Industrial measurement and control equipment is the nerve center of an industrial control system, and thus, its information security is directly related to the safety of the industrial control system. The traditional security protection technology has limitations, such as the inability of the network to block the access of physical media transmission data and physical equipment. Even the physically isolated industrial measurement and control equipment can also become the target of attack. Therefore, it is urgent to enhance the endogenous security of industrial measurement and control equipment. According to related international and national standards, the endogenous information security technology of industrial measurement and control equipment is divided into static reinforcement and dynamic protection technologies. In this paper, seven kinds of information security technologies are classified logically. The definition of endogenous information security terminologies in industrial measurement and control equipment is presented, and the research progress of existing key technologies is analyzed and evaluated. Finally, we prospect the development trend of endogenous information security technology of industrial measurement and control equipment.

Keywords

industrial measurement and control equipment;
information security;
data encryption;
access control;
integrity assurance

0 引言

工业控制系统(industry control system, ICS)用于控制关键生产设备的运行,广泛应用在国家关键基础设施中,包括电力、石油化工、轨道交通、航空航天等行业。工业控制系统的脆弱性使其面临信息安全威胁[1-3],工业控制系统信息安全问题已成为国家安全战略的重中之重[4-6]。

工业测控设备是工业控制系统的神经中枢。工业测控设备的范围包括变送器、执行器等过程传感与执行设备,以及 PLC(programmable logic controller)、DCS(distributed control system)等各类控制器,同时包括涉及的上位机系统[7]。工业控制系统信息安全防护长期侧重于网络域的"纵深防御",通过隔离网络保护重要资产,使得传统的外网渗透攻击手段失效。传统防护技术手段具有局限性,网络无法阻断物理介质传输数据和物理设备的接入,随着 APT(advanced persistent threat)攻击愈演愈烈,即使是物理隔离的工业测控设备,亦可以成为攻击目标[8]。增强工业测控设备自身的内生安全防护能力是解决问题的根本途径之一[9]。本文将"内生安全"定义为在程序、系统或设备的设计阶段,将信息安全机制直接设计其中,尽可能减少可利用的缺陷,以抵御攻击。

本文分析了与工业测控设备相关的国际标准、国家标准的信息安全技术要求,从静态加固和动态防护两个角度对工业测控设备信息安全防护设计技术进行分析、评价,并归纳、分类,理清目前国内外相关研究的进展和不足,最后探讨了关键技术和业态的发展趋势。

1 工业测控设备内生信息安全

目前尚未有针对工业测控设备信息安全设计的国际标准、国家标准或规范可查,但是已有针对工业控制系统层面的信息安全技术要求相关国际、国家标准发布或制定中。其中,与工业测控设备信息安全相关的主要有国际标准 IEC62443-4-2-2019《工业自动化和控制系统信息安全第 4-2 部分:IACS 组件的安全技术要求》[10],以及国家标准 GB/T 30976.1-2014《工业控制系统信息安全第 1 部分:评估规范》[11]。

国际标准 IEC62443-4-2-2019 为组成工业自动化和控制系统的组件提供网络安全要求,特别是嵌入式设备、网络组件、主机组件和软件应用程序,定义控制系统组件的安全能力等级[12-13]。

国家标准 GB/T 30976.1-2014 是在信息安全国际标准 IEC62443 的转化工作基础上,制订的符合中国工业应用特点的国家标准。GB/T 30976.1-2014 规定了工业控制系统(DCS, PLC, SCADA(supervisory control and data acquisition), PCS(process control system)等)信息安全评估的目标、评估的内容、实施过程等。适用于系统设计方、设备生产商、系统集成商、工程公司、用户、资产所有人以及评估认证机构等对工业控制系统的信息安全进行评估时使用。

国际标准 IEC62443 系列和国家标准 GB/T 30976.1-2014 为控制系统组件的安全能力等级提供了一个灵活的框架,可以为工业测控设备的内生信息安全能力设计提供指导,工业测控设备的内生信息安全术语定义如表 1 所示。

表 1 工业测控设备的内生信息安全术语定义

Tab.1 Definition of endogenous information security terms for industrial measurement and control equipment

序号	GB/T 30976.1-2014	工业测控设备内生安全设计
1	使用控制	访问控制
2	标识和认证控制	权限控制
3	数据保密性	信息加密
4	限制的数据流	受限数据流
5	系统完整性	完整性保证
6	对事件的及时响应	事件及时响应
7	资源可用性	资源可用性

2 信息安全防护技术分类

本文从国际标准、国家标准的技术要求出发,将工业测控设备信息安全设计技术分为静态加固和动态防护两种。静态加固与固定的配置规则相关,一般依靠网络管理员对设备的人工配置来实现。动态防护则与设备、行为状态等动态信息有关,系统需针对安全态势的变化做出策略响应。静态加固技术包括访问控制、权限控制、信息加密、受限数据流,动态防护技术包括完整性保证、事件及时响应、资源可用性。工业测控设备信息安全防护技术分类如图 1 所示。

3 静态加固技术

3.1 访问控制

GB/T 30976.1-2014 中阐述"使用控制"是为已认证用户分配特权以执行所请求的操作,并进行监

视。本文中针对工业测控设备内生安全设计采用“访问控制”一词，主要包括授权的执行、无线使用控制等技术。

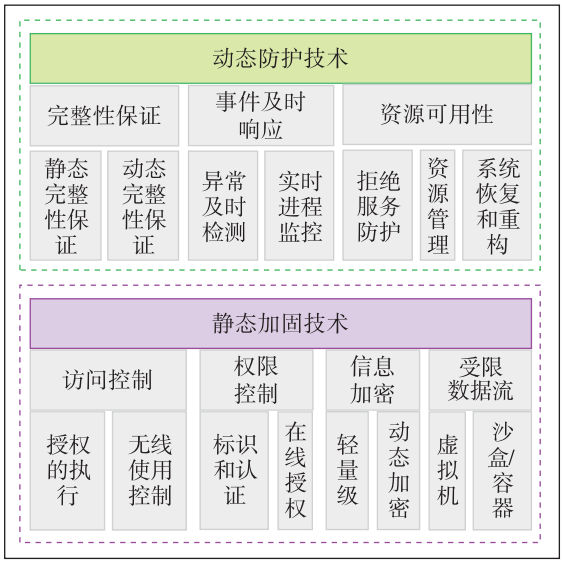

图 1　工业测控设备信息安全防护技术分类

Fig.1　Classification of information security technology for industrial measurement and control equipment

1）授权的执行

文[14]通过实验说明了访问保护可以保护 PLC 免受蠕虫攻击。使用写保护防止修改 PLC 代码，以及使用质询回应身份认证能够防止蠕虫病毒攻击和传播。但是无法针对操作内存、读标识、设置 IP 地址等操作进行有效控制。文[15]提出了一种基于功能码深度检测的 Modbus/TCP 通信访问控制方法，以有效地隔离非法的 PLC 设备通信数据流。但是过滤策略在实际使用中具有优先级，针对过滤策略优先排序的方法还有待讨论。

文[16]分析了几种 PLC 访问控制模型，特别是基于密码的访问控制，展示了如何截获 PLC 存储在内存中的密码并实现了重放、PLC 内存攻击等几种不同攻击，阐述了尚未发布的几种 PLC 版本的漏洞。最后指出在 PLC 和其他设备之间设置一个安全模块可以适当抵御针对 PLC 漏洞的攻击行为。文[17]针对 PLC 系统，设计安全处理单元，为 PLC 控制器提供一种主动防御手段，构造 PLC 硬件和软件安全层。在硬件安全层次，加入部分硬件处理机制支持可信度量、加密算法和签名算法；在软件安全层次，提供透明加解密、完整性验证、备份恢复等功能，能够正确建立 PLC 的可信环境，确保 PLC 经过严格验证的路径引导。设计了全新的星型信任结构，降低信息传递时的损耗，提高信息传递的效率，以期达到安全可靠的目的。文[18]提出一种基于属性加密（attribute-based encryption，ABE）的安全模型，实现客户隐私的数据访问控制机制。将电网网络细分为集群，每个集群都有自己的远程终端单元（remote terminal unit，RTU）和网关智能电表。给定集群中的用户数据被聚合并发送到本地变电站，RTU 和用户拥有由多个密钥分发中心（key distribution center，KDC）分发的属性和密钥。RTU 在一组属性下发送加密数据。拥有有效属性的用户可以解密信息。它允许智能电网不同集群的智能电表在数据/信息交换之前进行相互认证，并在过程中保持低延迟以及相对较少的认证相关消息，但是在属性增加的情况下，计算负载将激增。

2）无线使用控制

文[19]将无线通信技术与 PLC 内核技术集成在一个无线控制器体系结构中。在该架构下，PLC 代码可以通过 PC 机上的人机界面传送给指定的 PLC 组。PLC 代码由远程 PLC 接收并写入其闪存。因此，即使无线通信中断或微芯片复位，无线远程 PLC 仍然可以工作。并建立了 PLC 代码的分组广播和 PLC 之间的数据交换机制。文[20]提出了一种适用于 SCADA 系统的多层安全加固无线远程终端（wireless remote terminal unit，WRTU）。WRTU 基于 ARM Coter-M4 处理器，支持 GSM（global system for mobile communications）和卫星调制解调器、GPS、WiFi 和以太网。WRTU 通过 GSM 或卫星调制解调器连接至监控中心（CMC）。CMC 监控 WRTU 的所有外围设备，维护警报、传感器信息日志、设置关键限制并通过其 GIS 接口提供所有 WRTU 的地理位置。为 SCADA 系统开发的 WRTU 和网络安全框架具有多种好处，从低运营成本和资本的支出到快速的部署和启动时间。但是单一的 CMC 节点有可能成为攻击的目标，CMC 节点的安全等级应该更高。文[21]分析了为 DCS 构建一个更完整、更易于管理的访问控制框架方面的关键挑战，提出了一个 DCS 控制系统模型框架，可用于实现对每个访问都会根据遵循最小特权原则的策略进行检查，所提出的架构有助于集中化、全厂范围的策略管理和保护所有连接的现场设备。文[22]提出一种在电力输送过程中采用单片机装置进行数据采集和控制的方法。采用微控制器代替 PLC，配合 SCADA 系统对整个电网进行控制。它由 3 个单元组成：数据采集/发送单元、接收单元和存储/发送单元。使

用无线通信代替以太网连接可以提高数据传输速率，降低网络电缆成本。设计了单片机与 GSM/GPRS 模块相结合的新型远程传输单元(RTU)。

小结：针对 PLC 等工业测控设备的访问控制方法难度主要集中于如何采用深度协议解析等技术，与控制行为等相结合，实现细粒度的业务逻辑访问控制。PLC 等工业测控设备应具备无线通信功能，同时具有对未授权的无线接入设备进行识别和报告功能。

3.2 权限控制

GB/T 30976.1-2014 中阐述“标识和认证控制”是所有用户在被允许访问控制系统之前，对他们进行标识和认证。本文中针对工业测控设备内生安全设计采用“权限控制”一词。

文[9]从系统架构设计的角度讨论可信计算、加密传输、授权管理、虚拟化等信息安全技术在大型 PLC 应用的可行性以及对于 PLC 实时性和可靠性的影响，提出一种满足日趋严格的工业信息安全要求的 PLC 系统设计思路。文[17]中提出一种基于数字证书和国密 SM2、SM3 算法的双向身份认证方法。设备接入工业测控网络之后，根据证书中指定的数字签名算法来对证书身份进行合法性校验，通信双方均可以根据证书对对方的身份合法性进行验证，实现双向验证。文[23]提出了一种基于状态估计的动态加密认证(SEDEA)方法来保护智能电网中控制中心(control center，CC)和远程终端单元(RTU)之间的通信。采集 RTU 电量参数生成加密密钥。用于生成密钥的功率测量值是不断变化和不可预测的，密钥具有较高安全性。SEDEA 的加密计算功能简单、成本低，例如异或、哈希、轮函数等，适用于电力系统中现有设备。因此，SEDEA 被认为是一种安全性高、轻量级的智能电网方案。文[24]介绍了针对通用工业协议(common industrial protocol，CIP)实现中的身份验证和特权 I/O 攻击。测试环境中 RSLogix 5000 用于支持对 PLC 的远程监控和编程。测试发现了协议漏洞，可被利用绕过身份认证，获得远程 I/O 远程升级特权。最后说明了为 PLC 的每个特权身份验证创建唯一的会话密钥是解决途径之一。文[25]提出了新的交互设备认证方案，包括基于身份的公钥/私钥分发。针对目前大多数电力线系统没有有效的证书颁发机构的情况，作者采用 IBC 的概念，将基于公钥的安全方案应用于大规模电力线网络中。所提出的方案使用 MAC 地址和唯一的小区 ID 来生成公钥/私钥，而不是用户输入。不是所有的设备都有能够进行公钥加密的 CPU。但作者并没有分析方案的安全性和性能开销。

小结：权限控制可以在标识和认证基础上，结合资源审计、在线授权等技术实现增强安全机制。

3.3 信息加密

GB/T 30976.1-2014 中阐述“数据保密性”是确保通信信道和数据仓库信息的保密性，防止未授权泄露。本文中针对工业测控设备内生安全设计采用“信息加密”一词。

文[26]介绍了一种具有自主知识产权的配电自动化远方终端(RTU)的设计与实现方法。基于国产加密算法的安全机制实现数据在 VPN(virtual private network)隧道密文传输和用户认证访问。文[27]提出了 uBUS 协议作为 MODBUS 协议的一种改进。uBUS 协议增强功能包括将地址扩展到 4 079 个地址，增加一个新的通信模式(组广播)。采用非对称加密的 RSA 算法实现通信加密。可以在各种类型的微控制器上实现 uBUS 协议从站功能。通过实验分析，密钥产生时间和加解密时间是可以忽略的，但是密钥长度的增加势必会增加内存的消耗。文[28]对 PLC 最常用的基于密码的访问控制进行了安全性分析。设计实验说明密码如何存储在 PLC 内存中，如何在网络中拦截密码，如何破解密码等，以及利用这些漏洞对控制系统进行重放、PLC 内存损坏等高级攻击。最后设计了安全模块(如 Scalance S)放置于 PLC 和其他设备之间以抵御攻击。文[29]通过研究国际标准 IEC 62443-3-1 部分中所描述的信息安全身份认证技术并进行分析，提出一套信息安全身份认证危害分析和实施策略，为核电厂数字化控制系统(DCS)的信息安全认证方法和策略提供参考。但文章提出的评估方法和认证策略为定性描述，未进行量化处理，执行过程中可能会因人而异。文[30]结合无证书签名和传统信息安全中的群组认证，针对多台 PLC 同时认证场景提出了一种轻量级组认证机制。但文章的机制在对工控终端进行认证时尚且停留在群组认证层面，并未对单一认证进行研究，这在一定程度上影响到了认证机制的完善性。

小结：已有较多针对 PLC、RTU、变送器、执行器等工业测控设备的数据加密算法研究文献可查，研究趋势主要集中在轻量级、动态加密等方向。

3.4 受限数据流

GB/T 30976.1-2014 中阐述“限制的数据流”是

利用区域和管道对控制系统分区，来限制不必要的数据流。本文中针对工业测控设备内生安全设计采用“受限数据流”一词。针对工业测控设备，主要包括虚拟机、沙盒/容器等技术。

1）虚拟机

文[31]提出了在 PLC 虚拟机(VM)中实现 IEC61131-3 标准的方案，该虚拟机是一种以指令表(IL)为中间代码的新型高级语言 VM。PLC 虚拟机使开发人员能够快速地将 IEC-61131-3 应用程序移植到不同的平台上，已经在基于 C51 的嵌入式 PLC 平台上实现了 PLC 虚拟机。文[32]针对 PLC 控制系统设计了一种虚拟机用于运行代码生成器自动生成的 PLC 代码。但虚拟机需要大量的时间来运行其代码，对 PLC 控制循环周期影响较大。文[33]介绍了嵌入式软 PLC 运行系统虚拟机的实现方案和执行过程，包括输入采样程序的实现、指令执行程序的实现和输出刷新程序的实现等软件实现方法。软 PLC 系统由开发系统和运行系统组成。虚拟机是整个软 PLC 系统运行系统的重要组成部分。采用软件技术实现了传统 PLC 微处理器的功能。它具有良好的实时性、准确性和可靠性。特别是在执行速度上，它比传统的硬 PLC 系统要好得多。虚拟机技术能够保证目标代码的独立性和可移植性。文[9]提出采用虚拟化方式在 PLC 中执行用户应用代码，实现对用户应用代码行为的有效监控。离线设定安全边界条件或规则，在线实时检查，发现用户应用代码控制行为异常时可以采取措施降低危险发生的可能性。

2）沙盒/容器

文[34]研究了采用软件沙盒实现资源受限设备的应用程序隔离方法。详细介绍了适用于微控制器的沙盒 eWASM 设计。eWASM 由预编译器 aWsm 和一个运行时组成，运行时程序用于限制内存访问和管理数据流。但沙盒 eWASM 运行时执行性能只有 40%，并且仍会导致大量的内存消耗。文[35]基于轻量级容器解决方案(LXC/Docker)提出了一种多用途控制器的体系结构，并分析了容器技术对 PLC 引擎实时性能的影响。分析结果表明容器开销较低并且性能很稳定，容器内控制程序运行能够满足控制周期延迟要求。已有开发的控制应用程序也可以迁移到容器中。

小结：虚拟机安装时需要为其指定内存和 CPU，不和其他程序共享硬件资源，同时虚拟机消耗系统资源较大，因此，目前基于虚拟机技术实现 PLC 等控制设备内部的业务逻辑数据流分区、隔离难度还较大。与虚拟机相比，轻量级沙盒或容器的应用程序与其他程序共享硬件资源，消耗资源较小，请求响应时间更短[36-37]。同时随着边缘控制器的需求和工业测控设备的资源增加，基于轻量级沙盒或容器技术实现 PLC 应用程序的分区、隔离具有实现的可能。可以在 PLC 等设备上设计多个虚拟化沙盒或容器，工业应用程序运行在每一个沙盒或容器中，沙盒或容器之间独立运行，互不影响。

4　动态防护技术

4.1　完整性保证

GB/T 30976.1-2014 中阐述“系统完整性”是确保工业控制系统完整性，以防止未经授权的操纵。本文中针对工业测控设备内生安全设计采用“完整性保证”一词，可以分为静态完整性保证、动态完整性保证两种方法。

1）静态完整性保证

由于缺乏固件审核功能，SCADA 系统中的可编程逻辑控制器(PLC)特别容易受到攻击，Mcminn 等[38]开发了一种在 SCADA 系统中验证 PLC 固件的工具。该工具在固件加载期间捕获串行数据，并依据正确固件的可执行文件对其进行验证。在没有 PLC 的情况下也可以重放捕获的数据和分析固件，可在多种平台上实现。文[39]采用 Xilinx Zynq-7000 工业级芯片搭建硬件环境，并通过嵌入式系统移植，在可信计算技术基础上，以协同处理的方式实现了快速加解密验证。用哈希(Hash)算法对 PLC 系统启动文件进行了完整性验证，保证了 PLC 系统的可信启动。文[40]设计了基于可信平台模块 TPM(trusted platform module)的嵌入式可信计算平台，并从软件结构和硬件结构，分析了可信平台模块和信任链的传递机制。文[41]针对 PLC 程序的特点，提出了一种实用的 PLC 程序组合检查方法。在定义了 PLC 的工作模式和系统模型的基础上，给出了一个 PLC 程序的状态模型，该模型是 PLC 程序的组合检查框架，可以将一个 PLC 程序映射到输入输出集合，通过分层模块模型和递归状态转移，有效地缩小了状态空间。该形式化验证方法可以用于消除程序错误或验证程序正确性。除此之外，作者还需对这些策略的完备性进行验证，并且提出这些策略在何种条件下使用的选择方法。

2）动态完整性保证

文[42]提出一种在可编程逻辑控制器的控制

逻辑中实现在线验证或入侵检测方法。设计了嵌入式虚拟机监控程序与可编程逻辑控制器共享内存，在 PLC 扫描周期内，将监控对象参数写入临时缓冲区，调用验证库中的函数来验证该值，若该值不违反安全约束，则将临时缓冲区中的值传输到目标缓冲区。这些讨论都是基于 PLC 内部实施，并且缺少与其他算法之间的比较。文[43]通过扩展 Flash 总线实现 PLC 硬件可信启动加载，在出厂初始化阶段通过设计自身固件验证方法进行自身验证，通过读取特定固件信息，进行可信存储区填充；在运行阶段，通过自身固件验证方法，针对特定固件存储区的内容(启动信息和运行的原始程序 MD5 值等)进行数值校验。但是文章对于 PLC 的功能安全防护手段没有研究，并且应该考虑 PLC 信息安全和功能安全的融合增强。

小结：静态完整性保证主要保证系统出厂设置、启动阶段的固件、控制引擎、OS 代码、用户程序等未被篡改。动态完整性保证主要保证系统运行阶段，如何通过内存值校验等方法确保系统运行过程中及时发现系统异常。

4.2 事件及时响应

GB/T 30976.1-2014 中阐述“对事件的及时响应”是当事故发生时，采取推荐方式进行响应，采取及时的纠正行动。本文中针对工业测控设备内生安全设计采用“事件及时响应”一词，主要包括异常及时检测、实时进程监控等技术。

1）异常及时检测

文[44]提出了一种基于单类支持向量机 OCS-VM 的 PLC 异常事件检测方法。采集正常情况下的内存地址值，使用半监督机器学习训练出 PLC 正常行为的模型，对 PLC 事件是否正常运行进行分类。通过模拟交通灯控制系统应用验证了方法的有效性和准确性。文章缺少半监督演算法在集成电路中各种 PLC 应用可行性的评估，应为 PLC 异常检测创建一个通用模型。文[45]使用来自网络和本地访问的程序的执行时间检测单个指令更改，考虑了程序变化对 PLC 扫描周期时间的影响，同时对不常用的源代码执行行为进行评估和白盒建模，能够为低功耗实时设备提供异常检测功能。但是文章还应讨论攻击底层固件的模型，并探索生成白盒模型执行时间的更精确的方法。文[46]通过对 Modbus-ICS 协议的深入分析，提出了一种基于自动学习的恶意入侵检测方法，实验平台多种测试表明了该方法能有效地检测多种网络攻击。该研究还可基于机器学习建立一个更通用的方法。文[47]等提出了一种新的工业以太网 EtherCAT 网络的执行周期异常检测方法，开发了 4 个可编程控制器(PLC)程序，验证了执行周期检测方法的可行性，并实现了执行周期的高精度自动获取。使用特定于协议的操作和字段来检测设备级的执行周期。可以使用不同的采样周期、优先级和延迟时间进行执行周期数据采集。利用执行周期采样发现流量模式，进行了拒绝服务(Denial of Service，DoS)和代码注入攻击测试，验证了入侵检测方法的有效性。文[48]等设计了一个跟踪 PLC 控制系统的输入和输出是否与预期一致的 PLC-PROV 系统，用于检测控制系统的功能安全和信息安全问题。实验表明可以检测攻击行为，包括中间人攻击、拒绝服务攻击和内存损坏攻击(如数组、堆栈和堆溢出、整数溢出和指针损坏等)。

2）实时进程监控

文[49]提出一种新的、与 PLC 兼容的控制流完整性(control flow integrity，CFI)机制 ECFI 来保护 PLC 设备免受控制流劫持攻击。可用于实时 PLC 系统而不影响 PLC 性能，测试表明能够抵御不同类型的攻击。文[50]针对可编程控制器(PLC)控制系统中的故障和行为异常检测与隔离问题，设计了一种 PLC 故障与行为监控工具(Fault and Behavior Monitoring Tool for PLC，FBMTP)，建立 PLC 控制过程的确定性有限状态机模型用于对故障和行为异常进行检测和隔离。文章还应关注具有预测和预测故障查询功能模型。文[51]设计了一种基于符号执行和模型检查的方法用于检测 PLC 恶意代码。通过对 PLC 的功能块、分层寻址、计时器等进行代码映射为时序执行图，构建自动状态机，实现 PLC 代码的控制逻辑建模。文章还应研究接收和处理传感器数据的程序。文[52]提出了一种可编程逻辑控制器(PLC)的输入存储器攻击检测与风险降低机制，并做为 PLC 内部程序进行了实现。响应机制包括优化数据块、在控制策略之间切换以及直接从模拟通道获取传感器读数，通过一个模拟清洁水供应系统的试验台进行了验证。文章还可以将机器学习应用于 PLC 内存的攻击检测，可以将本文算法与机器学习算法进行比较。

小结：异常及时检测和实时进程监控主要针对 PLC 等工业测控设备的内存行为、发包时间、动作执行等进行监控。检测项一般包括硬件故障、固件版本不兼容、由授权程序员或攻击者创建的控制程序错误、停止和启动攻击，以及内存读写攻击等。

4.3 资源可用性

GB/T 30976.1-2014 中阐述“资源可用性”是确保控制系统的可用性，防止拒绝基本服务。本文中针对工业测控设备内生安全设计采用“资源可用性”一词，主要包括资源管理、异常恢复等技术。

1）拒绝服务防护

文[53]以系统的“可用性”为目标，在远程终端单元(RTU)上进行了 DoS 攻击仿真实验。DoS 攻击将在 RTU 与主终端单元(master terminal unit，MTU)之间发送假数据包，使得 HMI/MTU 发出的命令可能无法到达 RTU，从而导致功能异常。实验案例中，MTU 无法从 RTU 获取数据，无法提供监测和进一步决策。该文研究成果说明，针对 RTU 等工业测控设备的信息安全防护，需要结合身份认证、权限控制、入侵检测等多种信息安全防护技术，以及结合“内生”和“外挂”等信息安全防护模式，才能有效抵御拒绝服务攻击等威胁。文[54]使用开源 PLC 设计一种信息嵌入式信息安全机制，独立于所使用的协议，加密 PLC 通过网络发送的所有数据。同时在 PLC 网络堆栈中部署一个基于机器学习的入侵防御系统(intrusion prevention system，IPS)，实验证明了可以抵御拒绝服务(DoS)攻击。文[55]验证了针对 PLC 控制过程的数据包泛洪攻击方法。与一般的 DoS 攻击不同，该实验是针对实际控制过程而不是网络通信。最后说明了设计安全 PLC 架构的重要性。该文的研究成果说明设计安全型 PLC，还需要与 PLC 的控制逻辑相结合，才能实现根本性的 PLC 本体安全防护能力。

2）资源管理

文[56]针对现有 PLC 软件架构中使用全局变量，增加了隐藏的依赖关系，降低了灵活性问题，提出了一种企业服务总线(ESB)类新型服务总线概念，包括解耦软件组件、传输协议转换、消息队列、消息优先级和转换以及服务编排等，以实现对 PLC 资源的灵活管理。文[57]针对用 RS485 建立的 PLC 工业网络存在的故障，提出了一种基于 32 位单片机 LPC2294 的 PLC 接入 CAN(controller area network)总线网络的方案。阐述了给出了作为 CAN 总线智能节点的 PLC 硬件结构和软件设计。文[58]提出了一种多核 CPU 的 PLC 结构，能够实现控制算法的并行处理。控制程序由许多适合并行执行的程序块组成。该体系结构由独立的逻辑和运算单元构成。它们共享各自类型的公共数据存储器。为了实现处理的紧密耦合，提出了一种信号内存概念，将内存和信号控制结合起来，处理器之间的数据流由信号内存控制。通过 FPGA(field programmable gate array)设计验证了提出的体系结构。随着 PLC 异构多核技术的成熟与多核编程方案的成熟，多核 PLC 的应用也会更加广泛。

3）系统恢复和重构

文[59]设计了两级信息安全恢复控制机制：内环基于攻击特征库检测可识别入侵，并对比安全策略库制定安全策略；外环基于系统模型检测不可识别入侵，使用冗余技术进行处理。但是该方法属于 PLC 外部信息安全防护技术，并且没有与 PLC 功能安全技术进行结合。文[60]提出一种基于异构双处理器冗余结构的安全 PLC 结构，阐述了安全 PLC 软件系统工作流程。安全 PLC 执行单元执行编译单元生成的可执行代码，并将输出信号输出给控制装置，根据用户设计的逻辑指令完成对外部仪表等外部部件的操作和安全控制。当主处理器发生故障时，冗余处理器软核将接管实时逻辑的执行，恢复主处理器的执行状态并确保控制程序的准确性和可靠性。但是多处理器冗余结构的安全 PLC 的设计是一个系统工程，任何一个考虑不完备的地方都有可能导致完整性的降低，在测试与应用验证方面还有很多工作需要开展。文[61]提出一种自动生成执行器的运动序列以进行错误恢复方法。将 PLC 中的时序路径用状态流来表示，设计搜索策略寻找从初始状态到最终状态的最优最短路径，实现对 PLC 控制逻辑的恢复。文[62]提出了一种可编程逻辑控制器的四冗余结构，以实现网络抗黑客攻击的能力。传统可编程逻辑控制器冗余方案对物理损坏和随机故障具有鲁棒性，但在软件劫持和其他网络攻击方面表现出严重的脆弱性。提出的四冗余体系结构结合了软件多样化和硬件冗余，被攻击后从预编库中随机抽取二进制文件并随机选择一个内存地址空间程序，自动再生 PLC 软件程序。实验表明该体系结构能够有效检测、阻止和被软件劫持网络攻击后恢复。但该方法的实现与应用比较复杂，系统软硬件成本较高。

小结：系统恢复与重构，一是对原有控制逻辑进行建模，依据模型恢复；二是建立冗余控制逻辑，通过冗余逻辑再生实现系统恢复和重构。从实现角度出发，冗余控制逻辑方法更具有发展前景。

5 趋势分析

前文仅从信息安全功能设计方面进行了研究现

状分析和总结，但是工业测控设备信息安全增加并非“1 +1”的过程，从实际设计角度考虑，工业测控设备信息安全能力的增加，与功能安全存在资源、目标、策略等冲突，如信息安全防护策略有可能会增大系统功能安全方面的风险，功能安全保障措施也有可能给系统引入新的信息安全漏洞等。设计时应将功能安全与信息安全相结合，以业务系统功能安全(safety)的可用性为目标和约束，再考虑信息安全(security)，通过迭代优化设计，消除冲突，实现工业系统的功能安全与信息安全融合，降低信息物理融合带来的信息安全风险。

目前，急需形成工业测控设备的内生信息安全设计规范，以及测试和评估规范，为信息安全型工业测控设备的设计和开发提供指导，满足日益增长的对具有自身抵御攻击能力的工业测控设备的行业需求。

随着边缘服务器、边缘网关、边缘控制器、边缘智能仪器仪表等新型边缘设备的应用，急需从设计层面研究功能安全与信息安全技术的融合理论与方法，以及细粒度的轻量级、可配置、易部署的功能安全与信息安全组件。

6 结束语

本文依据国际标准 IEC62443-4-2-2019 和国家标准 GB/T 30976.1-2014，将工业测控设备内生信息安全设计技术分为静态加固和动态防护两种，并针对涉及的 7 类信息安全技术在工业测控设备内生信息安全方面的应用现状进行了分析、评价。最后，对可能的未来发展趋势和技术研究方向进行了展望。

工业测控设备是工业控制系统的核心，广泛应用于发电、航空航天、交通、化工、石油、供水、天然气、制药、汽车等行业，同时易受多种常见控制系统攻击，包括中间人攻击、拒绝服务攻击和内存损坏攻击等。持续增强工业测控设备内生信息安全能力具有迫切需求，对于保护国家关键基础设施安全，维护国民经济和社会稳定具有重要意义。

参考文献

[1] Parihar V R, DhoteA P. Industrial control system cyber security: Review & recommendations[J]. Journal of Network Security Computer Networks, 2017. http://matjournals.in/index.php/JONSCN/article/view/2055.

[2] Ani U P D, He H M, Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective [J]. Journal of Cyber Security Technology, 2017(1): 32 - 74.

[3] 彭勇，江常青，谢丰，等. 工业控制系统信息安全研究进展[J]. 清华大学学报(自然科学版)，2012，52(10)：1396 - 1408.
Peng Y, Jiang C Q, Xie F, et al. Industrial control system cybersecurity research[J]. Journal of Tsinghua University (Natural Science Edition), 2012, 52(10): 1396 - 1408.

[4] Idrissi O E, Mezrioui A, Belmekki A. Cyber security challenges and issues of industrial control systems - Some security recommendations[C]//2019 IEEE International Smart Cities Conference. Piscataway, USA: IEEE, 2019: 330 - 335.

[5] 陈星，贾卓生. 工业控制网络的信息安全威胁与脆弱性分析与研究[J]. 计算机科学，2012(S2)：188 - 190.
Chen X, Jia Z S. Industrial control network information security threats and vulnerability analysis and research[J]. Computer Science, 2012(S2): 188 - 190.

[6] 赖英旭，刘静，刘增辉，等. 工业控制系统脆弱性分析及漏洞挖掘技术研究综述[J]. 北京工业大学学报，2020(6)：571 - 582.
Lai Y X, Liu J, Liu Z H, et al. Review on vulnerability analysis and vulnerability mining technology of industrial control system [J]. Journal of Beijing University of Technology, 2020(6): 571 - 582.

[7] 尚文利，曾衍瀚，刘贤达，等. 工业测控设备安全技术发展趋势分析[J]. 自动化博览，2021(1)：54 - 56.
Shang W L, Zeng Y H, Liu X D, et al. Analysis on the development trend of safety and security technology of industrial measurement and control equipment[J]. Automation Panorama, 2021(1): 54 - 56.

[8] 徐震，周晓军，王利明，等. PLC 攻防关键技术研究进展[J]. 信息安全学报，2019，4(3)：48 - 69.
Xu Z, Zhou X J, Wang L M, et al. Recent advances in PLC attack and protection technology[J]. Journal of Cyber Security, 2019, 4(3): 48 - 69.

[9] 朱毅明. 可编程控制器原生的信息安全设计[J]. 信息技术与网络安全，2018，37(3)：8 - 10，19.
Zhu Y M. Native security design in PLC[J]. Industrial Control System and Information Security, 2018, 37(3): 8 - 10, 19.

[10] IEC62443-4-2-2019 工业自动化和控制系统信息安全第 4-2 部分：IACS 组件的安全技术要求[S].

IEC62443-4-2-2019 Security for industrial automation and control systems – Part 4-2：Technical security requirements for IACS components[S].

[11] GB/T 30976.1-2014 工业控制系统信息安全第 1 部分：评估规范[S].
GB/T 30976.1-2014 Industrial control system security – Part 1：Assessment specification[S].

[12] 欧阳劲松，丁露. IEC 62443 工控网络与系统信息安全标准综述[J]. 信息技术与标准化，2012(3)：26 – 29.
Ouyang J S，Ding L. Review on IEC 62443 Industrial control network & system security standardization[J]. Security Assurance Level，2012(3)：26 – 29.

[13] 王玉敏. IEC62443 系列标准概述和 SAL 介绍[J]. 仪器仪表标准化与计量，2012(1)：26 – 30.
Wang Y M. Overview of the IEC 62443 serial standards and the introduction of SAL[J]. Instrument Standardization and Metrology，2012(1)：26 – 30.

[14] Spenneberg R，Brüggemann M，Schwartke H. Plc-blaster：A worm living solely in the PLC[J/OL]. OpenSource Security Ralf Spenneberg，2016. https：//www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf.

[15] 万明，尚文利，曾鹏，等. 基于功能码深度检测的 Modbus/TCP 通信访问控制方法[J]. 信息与控制，2016，45(2)：248 – 256.
Wan M，Shang W L，Zeng P，et al. Modbus/TCP communication control method based on deep function code inspection[J]. Information and Control，2016，45(2)：248 – 256.

[16] Wardak H，Zhioua S，Almulhem A. PLC access control：A security analysis[C]//2016 World Congress on Industrial Control Systems Security. Berlin，Germany：Springer，2016：1 – 6.

[17] 尚文利，刘贤达，赵剑明，等. PLC 的安全处理单元及其总线仲裁方法[P]. 2019 – 06 – 04.
Shang W L，Liu X D，Zhao J M，et al. Safety processing unit of PLC and its bus arbitration method[P]. 2019 – 06 – 04.

[18] Mutsvangwa A，Nleya B. Secured access control architecture consideration for smart grids[C]//2016 IEEE PES Power Africa. Piscataway，USA：IEEE，2016：228 – 233.

[19] Yang S K. Design and implementation of wireless PLC with group management[J]. Journal of Physical Chemistry B，2013，117(38)：11091 – 11099.

[20] Durrani S，Jattala I，Farooqi J，et al. Design and development of wireless RTU and cybersecurity framework for SCADA system[C]//5th International Conference on Information and Communication Technologies. Berlin，Germany：Springer，2013：1 – 6.

[21] Huh J H，Bobba R B，Markham T，et al. Next-generation access control for distributed control systems[J]. IEEE Internet Computing，2016，20(5)：28 – 37.

[22] Abdelrassoul R A，Zaghloul M S. Data acquisition and control using microcontroller[J]. International Journal of Scientific & Engineering Research，2015，6(4)：158 – 163.

[23] Liu T，Tian J，Gui Y，et al. SEDEA：State estimation-based dynamic encryption and authentication in smart grid[J]. IEEE Access，2017，5(99)：15682 – 15693.

[24] Grandgenett R，Mahoney W，Gandhi R. Authentication bypass and remote escalated I/O command attacks[C]//Cyber & Information Security Research Conference. New York，USA：ACM，2015：1 – 7.

[25] Heo J，Hong C S，Choi M S，et al. Identity-based mutual device authentication schemes for PLC system[C]//2008 IEEE International Symposium on Power Line Communications and Its Applications. Piscataway，USA：IEEE，2008：47 – 51.

[26] 南亚希，展巍，裴后宣. 自主可控的安全 RTU 设计与实现[J]. 电力系统保护与控制，2016，44(14)：154 – 159.
Nan Y X，Zhan W，Pei H X. Design and implementation of a self-control secure RTU[J]. Power System Protection and Control，2016，44(14)：154 – 159.

[27] Dudak J，Gaspar G，Sedivy S，et al. Serial communication protocol with enhanced properties-securing communication layer for smart sensors applications[J]. IEEE Sensors Journal，2019，19(1)：378 – 390.

[28] Wardak H，Zhioua S，Almulhem A. PLC access control：A security analysis[C]//2016 World Congress on Industrial Control Systems Security. Berlin，Germany：Springer，2016：1 – 6.

[29] 黄鹏，肖鹏，吴志强，等. 基于 IEC 62443-3-1 的核电厂 DCS 身份认证技术方法[J]. 上海交通大学学报，2018，52(S1)：154 – 157.

Huang P, Xiao P, Wu Z Q, et al. DCS authentication technologies of nuclear power plants based on IEC 622443-3-1[J]. Journal of Shanghai Jiao Tong University, 2018, 52(S1): 154 – 157.

[30] 尚文利, 杨路瑶, 陈春雨, 等. 面向工业控制系统终端的轻量级组认证机制[J]. 信息与控制, 2019, 48(3): 344 – 353.
Shang W L, Yang L Y, Chen C Y, et al. Lightweight group authentication mechanism for industrial control system terminals [J]. Information and Control, 2019, 48(3): 344 – 353.

[31] Zhou C, Chen H. Development of a PLC virtual machine orienting IEC 61131-3 standard[C]//2009 International Conference on Measuring Technology and Mechatronics Automation. Piscataway, USA: IEEE, 2009: 374 – 379.

[32] Gasser T. Virtual machine and code generator for PLC-systems[D/OL]. London, UK: University of East London, 2013. [2020 – 02 – 16]. https://doi.org/10.15123/PUB.4018.

[33] Zeng Q, Wu S, Li Z. The design and realization of virtual machine of embedded soft PLC running system[J]. Sensors & Transducers, 2014, 182(11): 276 – 280.

[34] Peach G, Pan R, Wu Z, et al. eWASM: Practical software fault isolation for reliable embedded devices[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39(11): 3492 – 3505.

[35] Goldschmidt T, Hauck-Stattelmann S. Software containers for industrial control[C]//42th Euromicro Conference on Software Engineering and Advanced Applications. Berlin, Germany: Springer, 2016: 258 – 265.

[36] Gupta U. Comparison between security majors in virtual machine and linuxcontainers[J/OL]. Computer Science, 2015. [2020 – 04 – 12]. https://arxiv.org/ftp/arxiv/papers/1507/1507.07816.pdf.

[37] Yadav R R, Sousa E T G, Callou G R A. Performance comparison between virtual machines and docker containers[J]. IEEE Latin America Transactions, 2018, 16(8): 2282 – 2288.

[38] Mcminn L, Butts J. A firmware verification tool for programmable logic controllers[C]//International Conference on Critical Infrastructure Protection. Berlin, Germany: Springer, 2012: 59 – 69.

[39] 乔全胜, 邢双云, 尚文利, 等. 可信 PLC 的设计与实现[J]. 自动化仪表, 2016, 37(12): 76 – 78.
Qiao Q S, Xing S Y, Shang W L, et al. Design and implementation of the trusted PLC[J]. Process Automation Instrumentation, 2016, 37(12): 76 – 78.

[40] 王勇, 尚文利, 赵剑明, 等. 基于 TPM 的嵌入式可信计算平台设计[J]. 计算机工程与应用, 2018, 54(13): 105 – 110.
Wang Y, Shang W L, Zhao J M, et al. Sign of embedded trusted computing platform based on TPM[J]. Computer Engineering and Applications, 2018, 54(13): 105 – 110.

[41] Xiao L, Li M, Gu M, et al. PLC programs′ checking method and strategy based on module state transfer[C]//2015 IEEE International Conference on Information and Automation. Piscataway, USA: IEEE, 2015: 702 – 706.

[42] Garcia L, Zonouz S, Wei D, et al. Detecting PLC control corruption via on-device runtime verification[C]//2016 Resilience Week. Piscataway, USA: IEEE, 2016: 67 – 72.

[43] 尚文利, 尹隆, 刘贤达, 等. 工业控制系统安全可信环境构建技术及应用[J]. 信息网络安全, 2019, 19(6): 1 – 10.
Shang W L, Yin L, Liu X D, et al. Construction technology and application of industrial control system security and trusted environment[J]. Netinfo Security, 2019, 19(6): 1 – 10.

[44] Yau K, Chow K P, Yiu S M, et al. Detecting anomalous behavior of PLC using semi-supervised machine learning[C]//2017 IEEE Conference on Communications and Network Security. Piscataway, USA: IEEE, 2017: 580 – 585.

[45] Formby D, Beyah R. Temporal execution behavior for host anomaly detection in programmable logic controllers[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 1455 – 1469.

[46] Lin C, Wu S, Lee M. Cyberattack and defense on industry control systems[C]//2017 IEEE Conference on Dependable and Secure Computing. Piscataway, USA: IEEE, 2017: 524 – 526.

[47] Akpinar K O, Ozcelik I. Methodology to determine the device-level periodicity for anomaly detection in EtherCAT-based industrial control networks[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 2308 – 2319.

[48] Farooq A A, Marquard J, George K, et al. Detecting safety and security faults in PLC systems with data provenance[C]//2019 IEEE International Symposium on Technologies for Homeland Security. Piscataway, USA: IEEE, 2019: 1 – 6.

[49] Abbasi A, Holz T, Zambon E, et al. ECFI: Asynchronous control flow integrity for programmable logic controllers[C]//33rd Annual Computer Security Applications Conference. New York, USA: ACM, 2017: 437 – 448.

[50] Ghosh A, Qin S, Lee J, et al. FBMTP: An automated fault and behavioral anomaly detection and isolation tool for PLC-controlled manufacturing systems[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017, 47(12): 3397 - 3417.

[51] Zonouz S, Rrushi J, Mclaughlin S. Detecting industrial control malware using automated PLC code analytics[J]. IEEE Security & Privacy, 2015, 12(6): 40 - 47.

[52] Robles A, Moradpoor N, Mcwhinnie J, et al. PLC memory attack detection and response in a clean water supply system[J]. International Journal of Critical Infrastructure Protection, 2019, 26: 1 - 16.

[53] Kalluri R, Mahendra L, Kumar R K S, et al. Simulation and impact analysis of denial-of-service attacks on power SCADA [C]//2016 National Power Systems Conference. Piscataway, USA: IEEE, 2016. DOI: 10.1109/NPSC.2016.7858908.

[54] Alves T, Das R, Morris T. Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers[J]. IEEE Embedded Systems Letters, 2018, 10(3): 99 - 102.

[55] Niedermaier M, Malchow J O, Fischer F, et al. You Snooze. You Lose: Measuring PLC cycle times under attacks[EB/OL]. 12th USENIX Workshop on Offensive Technologies, 2018. https://www.usenix.org/sites/default/files/conference/protected - files/woot18_slides_niedermaier.pdf.

[56] Ashiwal V, Zoitl A, Konnerth M. A service bus concept for modular and adaptable PLC-software[C]// 25th IEEE International Conference on Emerging Technologies and Factory Automation, Piscataway, USA: IEEE, 2020: 22 - 29.

[57] Shi J. The implementation of CAN bus network of PLC based on ARM[C]// 4th International Conference on Intelligent Human-Machine Systems and Cybernetics. Piscataway, USA: IEEE, 2012: 268 - 270.

[58] Milik A, Chmiel M, Hrynkiewicz E. Multiple core PLC CPU with tight thread synchronization[C]//2016 International Conference on Signals and Electronic Systems. Berlin, Germany: Springer, 2016: 253 - 258.

[59] 周浩，黄双，黄雄峰，等. 嵌入式 PLC 的信息安全策略设计与实现[J]. 计算机科学，2013，40(9)：125 - 129.
Zhou H, Huang S, Huang X F, et al. Design and application of information security in EPLC[J]. Computer Science, 2013, 40(9): 125 - 129.

[60] Ma Y, Li M, Yin Z, et al. Design of safety PLC execution unit based on redundancy structure of heterogeneous dual-processor [C]//International Conference on Intelligent Computation Technology & Automation. Piscataway, USA: IEEE, 2017: 364 - 368.

[61] Aoki T, Suzuki T, Matsuzaki M, et al. Automatic generation of motion sequence for error recovery inprogrammable logic control using plant information[C]//8th International Conference on Emerging Technologies and Factory Automation. Berlin, Germany: Springer, 2001: 41 - 46.

[62] Luo J, Kang M, Bisse E. A quad-redundant PLC architecture for cyber-resilient industrial control systems[EB/OL]. IEEE Embedded Systems Letters, 2020. [2020 - 02 - 17]. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9146331.

作者简介

尚文利(1974 -)，男，博士，研究员，博士生导师。研究领域为工业控制系统信息安全，计算智能与机器学习，边缘计算。

王天宇(1990 -)，男，博士，助理研究员。研究领域为工业控制系统信息安全，复杂网络鲁棒性。

曹　忠(1977 -)，男，博士，讲师，硕士生导师。研究领域为人工智能技术，智能控制，工业互联网与信息安全。

刘贤达(1985 -)，男，硕士，副研究员，硕士生导师。研究领域为工业控制系统信息安全。