DOI 10.15302/J-SSCAE-2023.06.008

工业控制系统安全防护技术发展研究

孙彦斌，汪弘毅，田志宏*，方滨兴

（广州大学网络空间安全学院，广州 510006）

摘要：工业控制系统逐渐由封闭隔离走向开放互联，工业控制系统的安全问题进一步凸显；针对工业控制系统的网络威胁呈现出高隐蔽、强对抗、跨域等特点，一旦遭受网络攻击将直接影响工业生产，因而工业控制系统网络安全防护技术备受关注。本文聚焦工业控制系统安全防护问题，分析了工业控制系统安全防护的特殊性及面临的挑战，总结了工业控制系统的主要攻击技术，梳理了以边界防护、纵深防护为代表的“自卫模式”安全防护体系的发展现状。针对工业控制系统面临的安全挑战，从自主可控安全和新型工业控制安全防护体系两个方面提出了今后的重点任务和关键技术攻关路径，即建立自主可控的工业控制系统安全生态和基于“限制器”的底线确保防护机制、探索“自卫模式+护卫模式”的工业控制系统安全防护体系，以为工业控制系统安全防护研究和应用提供参考。

关键词：工业控制系统；安全防护；自主可控；新型防护体系；护卫模式

中图分类号：R-1　　**文献标识码：**A

Development of Security Protection Technologies for Industrial Control System

Sun Yanbin, Wang Hongyi, Tian Zhihong*, Fang Binxing

(Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China)

Abstract: Industrial control system (ICS) is gradually transitioning from being closed and isolated to open and interconnected. The network threats to ICS are becoming highly hidden, strong-confrontation, and cross-domain in nature. Once subjected to cyber-attacks, industrial production will be directly affected. Consequently, network attacks on ICS and corresponding security protection technologies have attracted significant attention. This study focuses on the security protection issues of ICS. First, we analyzed the specific characteristics of ICS security protection, as well as the unclear and uncontrollable security challenges of ICS. The network attacks on ICS are summarized and analyzed, and then the security protection systems with a self-defense mode, such as border protection and defense in depth, are discussed. In view of the security challenges, the development ideas are given from the aspects of security and controllability of ICS and a novel security protection system of ICS, and key tasks and key technology research paths are as follows: establishing an autonomous and controllable ICS security ecology and a security assurance mechanism of foreign devices based on limiters, and exploring the new security protection system of ICS based on a self-defense plus guard mode, such that the security protection ability of ICS can be better improved.

Keywords: industrial control system; security protection; autonomous and controllable; new security-protection architecture; guard mode

收稿日期：2023-07-28；**修回日期：**2023-10-25

通讯作者：*田志宏，广州大学网络空间安全学院教授，研究方向为网络安全；E-mail: tianzhihong@gzhu.edu.cn

资助项目：中国工程院咨询项目“工业互联网安全技术战略研究”(2022-JB-04)；国家自然科学基金项目(62072130)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

随着工业化和信息化的深度融合，工业控制系统逐渐由传统的封闭隔离转为开放互联，并与第五代移动通信（5G）、物联网、工业互联网等技术相结合，有效提升了工业企业的生产效率和灵活性。然而，开放互联场景使工业控制系统的安全问题进一步凸显，增加了工业控制系统的网络安全风险，尤其是在相对封闭环境下的传统工业控制系统。以高级可持续威胁（APT）攻击[1]为代表的网络未知威胁日益增多，呈现出国家间博弈与较量进一步增强的趋势。工业控制系统作为与工业生产直接相关的关键信息基础设施已成为APT攻击的主要目标，面临的攻击威胁呈现持续性、针对性、潜伏性、隐蔽性、未知性等特点，直接影响工业生产过程，范围覆盖军工、民用等多个工业领域，亟需加强工业控制系统安全防护水平。

工业控制系统直接关系工业生产且优先保障可用性，涵盖网络空间、物理空间，场景复杂，受到世界主要国家普遍重视。美国、欧洲等国家和地区在工业控制系统安全防护的战略部署和政策规划方面起步较早，具有一定的优势。美国制定了一系列政策、标准以加强工业控制系统的安全，如出台《关键基础设施信息安全法案》（2001年），将能源等工业关键基础设施列为重要保护对象；美国国家标准与技术研究院（NIST）发布《工业控制系统安全指南》（NIST SP800-82，2011年），为工业控制系统的安全保障提供指导；设立专门的工业控制系统网络应急响应小组和多个国家实验室负责工业控制系统的安全保障和研究工作。德国对工业安全也非常重视，推出了“数字化战略2025”（2016年），明确了工业控制系统安全的重要性，提出了一系列促进相关技术研发和标准制定的措施。欧洲网络安全局发布《工业控制系统网络安全白皮书》（2013年），为工业企业实施安全防御措施提供指导。我国历来重视网络安全问题，坚持底线思维，着力防范化解重大风险，针对工业控制系统的安全威胁，建立有效的工业控制系统安全防护体系和方法以有效应对和化解工业控制系统重大安全风险、保障国家网络空间安全。我国工业控制系统安全的研究与管理虽然起步晚但发展较快。2011年，工业和信息化部发布《关于加强工业控制系统信息安全管理的通知》，明确了工业控制系统安全管理的相关要求。2019年，我国实施《信息安全技术 网络安全等级保护基本要求》（GB/T 22239—2019，简称为等保2.0）[2]，将工业控制系统安全纳入等级保护体系。“十四五”规划纲要提出，维护水利、电力、供水、油气、交通、通信、网络、金融等重要基础设施安全，工业控制系统作为重要关键信息基础设施成为未来安全防护重点。2022年，我国发布《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204—2022），规定了关键信息基础设施在识别分析、安全防护、检测评估等方面的安全控制措施；作为我国首个正式发布的关键信息基础设施安全保护标准，为关键信息基础设施更好开展安全保护工作提供了操作指引。

在工业控制系统安全防护技术及体系研究方面，目前已提出了可编程逻辑控制器（PLC）程序安全分析、工业行为异常检测、工业控制协议安全分析等方法，但主流方法仍沿用传统安全防护技术提出了面向工业控制系统的主机防护、防火墙、入侵检测、蜜罐、可信计算等技术，建立了以纵深防护、主动防护为代表的安全防护体系。现有工业控制系统安全防护面临两方面挑战：一方面，现有安全防护体系难以全面应对隐蔽未知的APT攻击，另一方面，对针对物理空间以及跨信息域和物理域的攻击难以适用，无法直接用于解决工业控制系统安全问题。本文在剖析工业控制系统基本构成和面临的安全防护挑战基础上，梳理工业控制系统安全防护技术的发展现状，厘清工业控制系统安全防护技术的重点任务及关键技术，探索新的安全防护体系、方法及未来发展路线，以期为提升工业控制系统安全防护能力提供参考。

二、工业控制系统的基本构成与面临的安全防护挑战

（一）工业控制系统的基本构成

工业控制系统抽象模型多采用层次架构，包括普渡模型[3]、IEC62264-1标准层次结构模型[4]等。我国等保2.0标准中的工业控制系统相关等级保护要求参考了IEC 62264-1层次结构模型。以该模型为例，工业控制系统自上而下可分为5层（见图1）：企业资源层、生产管理层、过程监控层、现场控制层和现场设备层。企业资源层可为企业提供决策运

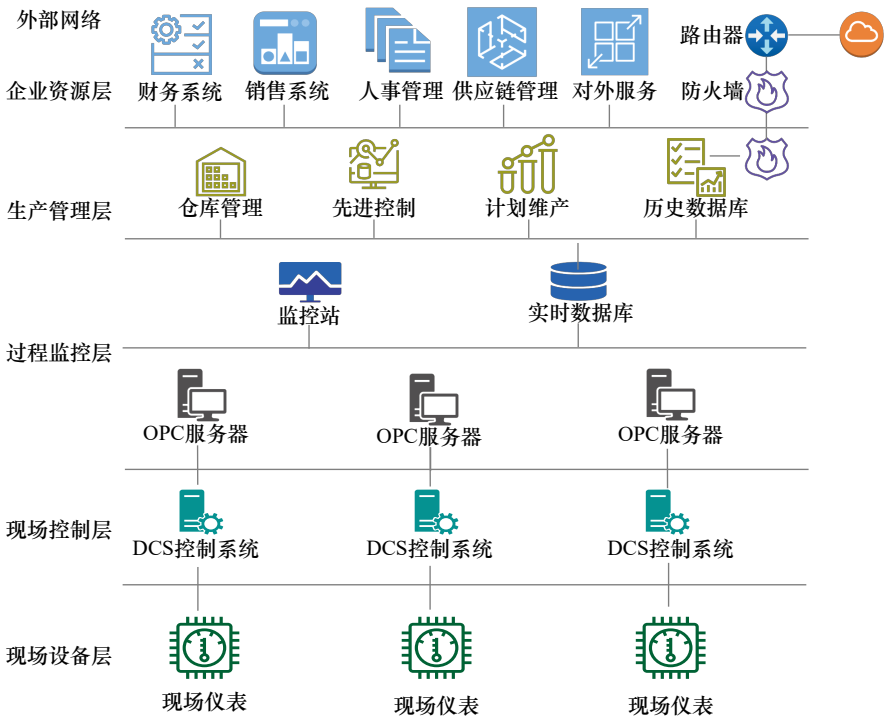

图1　IEC 62264-1工业控制系统层次模型

注：OPC表示开放性过程控制。

行手段；生产管理层可对生产过程进行管理；过程监控层主要对生产过程数据进行采集与监控，并利用人机界面（HMI）系统实现人机交互；现场控制层通过PLC、分布式控制系统（DCS）、远程终端单元（RTU）等控制设备对现场的传感设备、执行设备进行采集和控制；现场设备层主要涉及各类过程传感设备与执行设备单元，对生产过程进行感知与操作。IEC 62264-1层次模型是一种通用的层次模型，尽管电力、冶金、石化等领域的实际工业控制网络架构与其存在一定的差异，如某些层次可能需要扁平化，但该模型仍能覆盖大部分工业控制场景，具有很高的参考价值。

以生产管理层分界，企业资源层、生产管理层多采用信息领域相关的通用技术，其他层多采用工业控制系统特有技术。针对工业控制系统企业资源层和生产管理层的攻击与传统针对信息系统的网络攻击类似，因此，工业控制系统安全可主要关注现场设备层、现场控制层、过程监控层等，而面向这3层的网络攻击通常会给控制设备、工业现场带来严重危害。

区别于传统信息网络，工业控制系统的特殊性主要表现在：① 信息化与自动化融合。工业控制系统融合了信息系统和自动化系统，既需要信息系统提供智能化采集、监测、管理和决策，也需要自动化系统实现对现场工业设备的自动高效控制。② 空间互通。工业控制系统的作用域涵盖网络空间和物理空间，网络空间的决策可影响物理空间的动作，物理空间状态反过来也会影响网络空间的决策。③ 可用优先。工业控制系统在设计之初与外部网络隔离，未考虑安全问题，与工业现场生产关系紧密，设备分散且要求全时段不间断运行，不易通过停产升级以解决安全问题。因此，针对工业控制系统的攻击呈现跨越网络空间和物理空间的特点，与传统网络攻击技术存在较大差异，亟需对安全防护技术进行优化。

（二）工业控制系统安全防护技术面临的挑战

现有工业控制系统安全防护体系在应对网络攻击时呈现出以下特点。① 网络攻防技术的不对称性。网络攻击技术只需突破工业控制系统的某个点，网络防护技术则需要兼顾整个工业控制系统，防守方天然处于不利地位。此外，威胁情报不对称进一步加剧了技术水平的不对称。我国关键工业控制设备大多源自国外供应商，易被恶意植入后门、木马，只能以“黑盒”方式研究工业控制系统的安全问题，在

攻防对抗中不占优势；同时，不同工业控制设备厂商之间存在技术壁垒，攻防技术难以通用。② 攻防过程的强对抗性。针对工业控制系统的攻击呈现有组织、集团化特点，攻击组织往往掌握目标系统的多个零日（0day）漏洞、系统 / 设备后门甚至能够伪造合法凭证，攻击过程较为隐蔽、攻击手段多样、对抗能力较强，致使我国的工业控制系统安全防护疲于应对。③ 安全防护的紧耦合性。工业控制系统所采用的纵深防护、主动防护等措施多以强关联、紧耦合的方式进行设计、研发和部署，是一种“自卫模式”，确保了工业控制系统可以通过自身安全能力建设应对威胁，但这种防护模式在工业控制场景中会对工业控制系统产生一定程度的侵入式影响，对未知攻击难以快速响应。④ 安全更新的高延迟性。工业控制设备和系统要求全时段运行，同时，我国存在大量缺乏维护的老旧工业控制设备，为确保系统稳定运行，不能轻易对此类设备进行改动，以免影响生产。这类工业控制系统在遇到安全问题时，往往无法立即停机更新，更新相对滞后。

工业控制系统安全防护的上述特点使得工业控制系统在攻防对抗中面临“摸不透”和“控不住”两方面的挑战。

1. 工业控制系统面临“摸不透”困境

当前，我国工业领域的核心设备、固件、软件、协议等被国外供应商垂直垄断。在关键工业控制设备 PLC 方面，西门子股份公司生产的 PLC 在大、中型 PLC 市场上具有较强的竞争优势，约占我国 PLC 市场规模的 44%；罗克韦尔自动化有限公司在大型 PLC 产品市场中具有绝对优势[5]。由于工业场景复杂多样、需求不一，不同场景下适用的设备和通信协议各不相同很难形成统一规范，面临中央处理器（CPU）专用、操作系统闭源、协议碎片化等问题，这种封闭性、排他性使我国在某些核心领域很难有所突破。同时，国外供应商为维持各自的市场和技术优势，建立了覆盖硬件、固件、软件、协议的完整垂直生态系统，采用独立、排他且不公开的标准和协议，致使其他厂商的产品很难融入。例如，在工业领域中，仅通信协议就存在多种不同的标准协议，如 RS-232、RS-485、CAN、Modbus、PROFINET、Modbus TCP、UMAS、S7comm、S7comm-Plus、PPI、DNP3、Omron FINS、Melsec 等。以上现状致使我国工业控制领域的核心技术、核心设备长期依赖进口，关键技术被“卡脖子”，易受技术封锁和制裁，产业安全受制于人。

“摸不透”困境也严重影响了工业控制系统的网络安全。我国企业大量的专用软 / 硬件工业控制设备（系统）长期被国外垄断，相关设计方案、运行机理、源码、测试方案、设备维护数据等不对外公开，导致安全分析只能采用“黑盒”操作，很难摸透相关设备（系统）的内部机理，存在较大的安全隐患，不易发现可能存在的漏洞和后门；而国外供应商则完全掌握设备（系统）及设备漏洞，甚至可以预设后门监测通信数据或实施攻击。在攻防对抗中，对安全防护对象“摸不透”致使大量未知威胁难以被发现，甚至可能掉入对方设置的“漏洞陷阱”。

2. 工业控制系统面临“控不住”难题

从攻防对抗角度来看，我国工业控制系统安全防护技术缺乏突破性进展和创新性技术。当前，针对工业控制系统的攻击手段、规模、对象等均体现出鲜明的组织化、规模性和指向性特点，现有工业控制系统安全防护技术难以有效应对，面临“控不住”问题；针对工业控制系统的攻击隐蔽性强、威胁大，攻击方法难以预测，导致工业控制系统面临“未知的未知”网络攻击。同时，工业控制系统设备更新换代慢，存在大量老旧设备，依靠系统自身内在的安全能力难以应对未知安全威胁。现有的内生安全、主动防护、纵深防护等“自卫模式”安全防护体系深入到工业控制系统内部，已为工业控制系统逐步建立起内在的安全防护能力，在一定程度上缓解了我国工业控制安全防护的迫切需求。然而，“自卫模式”安全防护体系从工业控制系统内部构建安全能力会采取一定的侵入式安全措施，影响工业生产，同时针对威胁的防护能力需要一定时间逐步建立，无法快速反应。因此，亟需在不影响工业控制系统原有架构的基础上，在工业控制系统外部形成防护能力，以“护卫模式”安全防护体系弥补现有“自卫模式”体系的不足。

工业控制系统直接关联工业现场，很难直接在工业控制系统上实施安全测试、攻防演练、技术验证，较多依赖工业控制靶场复现以还原工业场景。因此，缺乏可用靶场平台成为制约工业控制系统安全防护发展的重要因素之一。目前，我国工业控制网络靶场的建设、管理、运营缺乏顶层规划，存在重

复建设、资源分散难以共享等问题，未能充分挖掘和发挥其潜力，服务于工业控制系统安全防护。

三、工业控制系统安全防护技术的发展现状

工业控制系统安全防护技术与攻击技术的发展紧密相关，二者在对抗中螺旋上升。在介绍典型工业控制系统攻击技术的基础上，梳理工业控制系统安全防护技术的发展现状。

（一）工业控制系统攻击技术

针对工业控制系统的攻击多为高隐蔽、未知类攻击，极易给工业现场的正常运行带来严重破坏[6]。工业控制系统攻击主要集中在过程监控层、现场控制层、现场设备层。按照层次顺序，工业控制系统攻击可分为上位机攻击、工业控制协议攻击、控制逻辑攻击、虚假数据注入攻击等，主要通过非法地址访问、非法控制命令下发、恶意控制逻辑注入、数据篡改等手段达到窃取数据，实现控制和损害工业生产的目的。

1. 上位机攻击

上位机与工业控制设备（如PLC、DCS）连接，通过控制设备采集工业现场数据，并根据工业现场情况下发控制命令或控制逻辑。一般上位机攻击过程如图2所示。由于工业控制系统处于内网，攻击者通过社工、渗透等手段进入内网，利用已知或0day漏洞对上位机发起攻击，实现对上位机的非法控制。一旦上位机被控制，攻击者可直接向工业控制设备发送控制命令或注入恶意控制逻辑，从而控制或破坏工业生产过程。同时，为达到隐蔽效果，攻击者还可能篡改或采集工业现场数据，使管理者误以为工业现场运行正常。典型的上位机攻击有震网攻击[7]、黑色能量病毒攻击[8]、Triton攻击[9]等。

2. 工业控制协议攻击

工业控制协议（规约）是工业控制系统内部数据或控制命令传输的标准，上位机、控制设备按照协议规范来交换信息。工业控制协议多为工业控制设备厂商的私有协议且缺乏安全考虑，大量工业控制协议缺少有效认证、加密等安全机制。

工业控制协议攻击首先进行协议逆向以获取协议格式及语义，结合漏洞挖掘方法进一步发现工业控制协议的安全漏洞，如缺乏写保护、明文发送密码、小密钥空间和单向认证等[10]。攻击者构造恶意客户端，利用协议漏洞绕过PLC安全校验并与PLC建立连接，从而获取PLC控制权。攻击者也可实施中间人攻击（见图3），通过劫持上位机与PLC间的通信，伪装为上位机、PLC分别与对方建立连接，向PLC下达非法命令或攻击负载，并使用篡改或伪造的协议响应报文隐藏攻击。已有研究[11~16]对S7comm-plus、IEC 60870-5-104、Modbus等工业控制协议进行了安全分析并验证了重放、中间人等攻击。

3. 控制逻辑攻击

控制逻辑指PLC、DCS等工业控制设备上运行的控制程序，由工程师编写、编译后下载至工业控制设备，以工业运行数据作为控制程序输入，按照

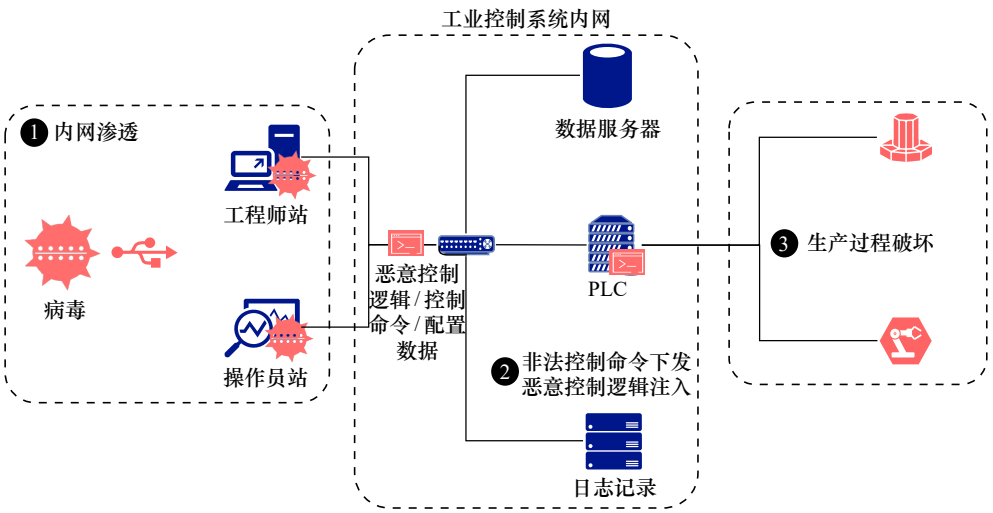

图2　上位机攻击

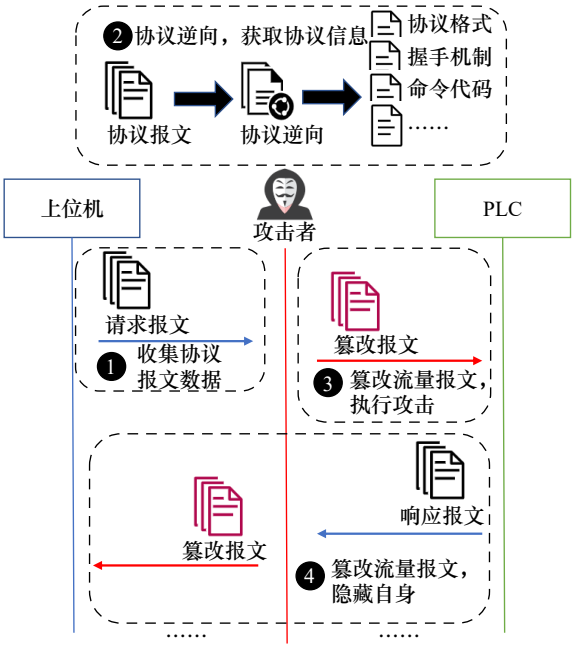

图3 工业控制协议的中间人攻击

一定控制逻辑输出控制动作并下发给工业现场执行设备，进而确保工业生产的稳定运行。控制逻辑攻击一般通过向工业控制设备植入恶意的控制逻辑程序或程序段以篡改其控制过程，典型的如震网病毒、逻辑炸弹[17]、时间中断控制逻辑攻击[18]等。部分恶意控制逻辑具备内网传播功能，采用类似病毒的传播方式，通过控制设备通信模块在内网传播恶意逻辑程序，如借助恶意控制逻辑构造的非法网关[19]、PLC蠕虫病毒[20]等。此外，还有一些攻击方法针对控制逻辑程序本身展开逆向分析和建模研究，通过对控制逻辑的分析找到更多针对工业现场的攻击策略，以增强攻击效果、提高攻击隐蔽性，如控制流攻击[21]、过程感知攻击[22,23]等。

4. 虚假数据注入攻击

虚假数据注入攻击通过篡改工业传感器数据，欺骗上位机或PLC设备以影响工业控制决策。如图4所示，一旦传感器被攻击者攻陷，攻击者即可利用传感器向工业控制系统注入虚假工业现场数据。PLC、上位机均以采集数据作为输入，基于控制逻辑或状态估计算法进行现场控制或决策。若部分工业现场数据被攻击者注入了虚假值，将带来PLC或上位机的控制、决策错误，直接影响工业生产。虚假数据注入攻击效果与攻击者掌握的工业控制系统拓扑及重要数据相关。按照攻击者掌握的工业控制系统信息数量，虚假数据注入攻击可分为全局数据注入攻击[24~26]、局部数据注入攻击[27~29]和盲数据注入攻击[30,31]。

综上所述，工业控制系统攻击技术多以控制或破坏工业生产过程为目的，结合渗透攻击、隐藏攻

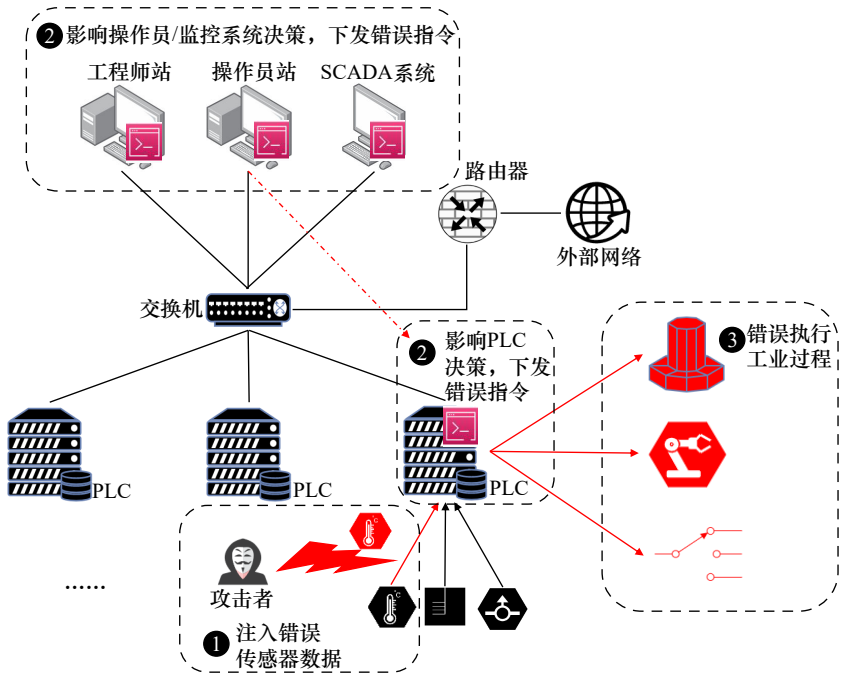

图4 虚假数据注入攻击

击等手段，相关攻击更具有隐蔽性和威胁性。对工业控制系统攻击的前提是需要掌握大量背景知识和安全情报，如网络拓扑、工业控制协议、已知漏洞、0day漏洞、隐藏后门、控制流程等。然而，当前，我国的工业控制生态相对封闭、受国外垂直垄断等不利因素制约了攻击威慑能力、发现潜在攻击威胁能力的提升。

（二）工业控制系统安全防护技术

从已公开的攻击技术来看，针对工业控制系统的攻击技术研究已经深入工业控制系统内部，依靠单一技术层面“一对一”攻防对抗无法应对层出不穷的攻击手段，尤其是攻击组织仍可能掌握大量未公开的攻击手段。因此，工业控制系统安全防护的重点在于构建合适的安全防护体系，综合运用各类防护技术，实现整体防护效果。

1. 工业控制系统安全防护关键技术

工业控制系统安全防护技术沿用并改进了已有的主机防护、防火墙、入侵检测、蜜罐等传统技术。工业控制上位机安全防护的重点是对工业控制组态软件、编程软件的安全运行监测。工业控制系统在运用传统防火墙技术的基础上加入“白名单”、工业控制协议深度包解析等技术，对工业控制专有流量进行解析和过滤；入侵检测主要采用传统或智能化方法展开基于工业控制流量、协议、运行状态的攻击检测[32]；工业控制蜜罐技术主要用于工业控制系统的威胁诱捕，其诱捕效果依赖蜜罐的交互程度，因此，研究重点关注对工业控制协议、工业控制逻辑、工业现场的高逼真仿真以构建高交互工业控制蜜罐[33]。

针对工业控制系统特有设备、软件和场景（如PLC程序、工业现场），已提出了新的工业控制安全防护方法，如工业控制系统攻击图构建[34]、工业控制系统态势感知[35]、PLC程序安全分析[36,37]、工业行为异常检测、工业控制漏洞挖掘（协议、软件及固件）[38,39]等。此外，基于物理系统高保真模型的攻击预测方法[40]，可以通过软件仿真模糊测试，自动发现导致物理系统不安全状态的攻击行为。

针对工业控制系统自身的安全缺陷改进，在协议层面，提出了多种安全工业控制协议，如S7comm-Plus、CIP Security等；在设备层面，研究重点是将可信计算技术与工业控制设备结合，构建安全可信的运行环境。

2. 工业控制系统安全防护体系

工业控制系统安全防护体系的发展态势是从单纯的边界防护、被动防护转变成纵深防护、主动防护等多种防护体系相结合。工业控制系统边界防护的重点是网络边界隔离，利用防火墙、安全网关、网络隔离等设备进行区域隔离，如电力系统安全防护将边界防护作为其防护体系重要部分，实行“安全分区、网络专用、横向隔离、纵向认证”的安全防护策略。工业控制系统边界防护的存在的主要问题是盲目信任边界防护的效果，很难发现以APT为代表的高级可持续攻击。

工业控制系统的纵深防护体系采用多样化、多层次、纵深的安全措施来保障网络安全。在网络架构方面，结合边界防护进行纵向分层、横向分区，根据区域/层次在业务、安全需求的不同，采用不同的安全防护方法；在防护对象方面，根据设备、主机、网络、应用、数据等防护对象的不同，逐层采用差别化的安全防护方法；在防护能力方面，采用保护–检测–响应–恢复（PDRR）、识别–保护–检测–响应–恢复（IPDRR）等安全防护模型，运用识别、保护、检测、响应、恢复等安全能力在不同威胁阶段应对网络攻击。

根据防护方式的不同，工业控制系统防护体系可以分为被动防护和主动防护。被动防护指工业控制系统在遭受网络攻击后，通过采取防护措施加以应对的防护体系，如防火墙、入侵检测、恶意代码扫描等。主动防护则是在攻击实施前，通过威胁诱捕、可信度量、拟态防护等主动防护技术，提前发现安全威胁，并转移、消除潜在威胁。主动防护通常与纵深防护结合，可以构建多样化的安全防护体系。目前，工业控制系统安全防护体系正由被动防护向主动防护与被动防护相结合的方向发展。

四、工业控制系统安全防护技术的重点任务及攻关路径

（一）工业控制系统安全防护的重点任务

1. 确保自主安全可控

目前，我国工业控制系统的相关软硬件具有较大的国产化空间。以PLC设备为例，国内市场主要由西门子、三菱、欧姆龙、罗克韦尔和施耐德等国外品牌主导，实现工业控制系统的自主安全可控成

为亟需。针对工业控制设备不可控引发的“摸不透”困境，可从解决不可控问题本身和应对不可控引发的安全风险两方面展开研究。① 工业领域现有的“烟囱式”纵向垄断现状使我国工业控制系统软 / 硬件核心技术依赖进口，生态垂直垄断，安全问题受制于人。因此，可借鉴计算机系统横向打通的发展历程，在CPU、操作系统、工业控制协议、工业软件等层面建立工业控制系统横向生态模式（见图5），从而创造工业控制领域快速发展机遇，从根本上解决“摸不透”问题。② 建立底线思维和解决方案，针对非自主可控的工业设备，在关键设备受控于人且“不得不用”的情况下，探索非自主可控场景下的应对方法，如在进口设备端口串联“限制器”（如审计盒子、网络靶场等），实时监测取证、访问控制进口设备的“不法”行为。

2. 构建新型工业控制系统安全防护体系

我国工业控制系统安全防护体系多借鉴IPDRR安全防护模型，从工业控制系统内部建立防护能力，属于自卫防护模式，缺乏与工业控制系统的深度融合，缺乏有效手段应对未知攻击，从而引发“控不住”问题。针对“控不住”困境，可从深化现有“自卫模式”和推动新型“护卫模式”安全防护体系两方面展开研究。

深化现有“自卫模式”安全防护体系。工业控制系统安全是信息安全和功能安全的融合，因此，“自卫模式”安全防护体系应将这两方面的安全因素考虑进去，研究黑客、有组织犯罪等人为因素对工业控制系统产生的信息安全威胁；还应考虑工业控制系统的功能结构和运行特点，分析因现场设备、工艺过程破坏导致的功能安全问题以及功能安全威胁和信息安全威胁结合产生的安全问题，从控制网络、控制系统、控制过程等方面进行防护，从工业控制系统全生命周期角度研究信息域和功能域融合的安全问题[41]。

在“自卫模式”基础上，探索构建“护卫模式”安全防护体系。目前，研究人员已构建了“盾立方”护卫模式安全防护体系[42]，并在工业控制场景中应用，有效提升了工业控制系统的防护能力。因此，在此基础上，今后可构建覆盖工业控制系统和物联网的“四蜜”威胁感知体系，建立全流程的威胁感知，实现非侵入、全流程威胁探测；开展跨域的关联研判，通过信息域内部的跨域关联、信息域和功能域的外部跨域关联，从信息安全和功能安全融合角度研究全域攻击研判；探索功能安全和信息安全（双安）冲突消解的“边端网疆”立体管控方法，挖掘功能安全基线，结合功能安全风险评估和人在回路等机制建立双安融合的立体管控能力。

此外，面向工业控制安全技术验证、攻防演练，新型工业控制网络靶场也是工业控制安全发展重要发展方向之一。探索工业控制网络靶场与数字孪生等新技术相结合，利用数字孪生技术构建可复制、高逼真度的网络靶场。

（二）我国工业控制系统安全防护关键技术攻关路径

1. 自主可控安全关键技术的攻关路径

建议行业主管部门加强顶层规划，制定工业领域关键基础设施自主可控发展规划，加强在战略规划、标准规范制定、关键技术突破、平台构建、示

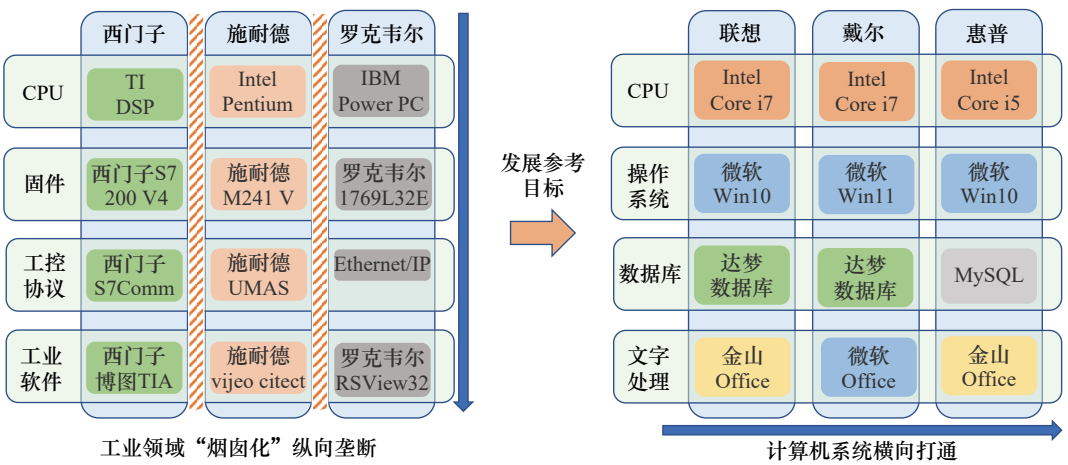

图5　横向打通工业控制系统生态

范应用推广等方面的政策激励和资源引导。积极构建可横向打通的工业控制系统生态体系，聚合科研院所、企业、高校等资源，建立长期稳定的沟通和合作机制，优化科研考核机制，确保自主可控工业控制系统生态研制过程中的智力支持和物质保障。

针对工业控制设备的不可控风险，推动自主可控的开源RISC-V智控芯片与工业制造领域相结合，推动自主安全的工业操作系统（固件）、工业控制协议以及工业软件研究，促进自主安全的横向工业控制系统生态建设。研究工业控制系统的安全性测试与评估技术，实现工控系统级安全性的科学准确量化评估。

探索非自主可控工业控制设备的底线安全确保机制，推进进口设备行为全流程监测和访问控制技术，鼓励为进口设备配备“限制器”，确保进口设备行为全流程可监测、可控制，并逐步形成制度规范。注重从多方面、多渠道对非自主可控的工业控制设备进行安全分析，提升设备掌控能力。

2. 新型工业控制系统安全防护关键技术的攻关路径

建立完善的5G、人工智能融合场景下的工业控制系统安全顶层设计，制定结合“自卫模式”和“护卫模式”的安全防护政策，探索新型工业控制系统安全防护体系及其关键技术。针对工业控制系统双安融合的特点，研究双安融合背景下的威胁感知、攻击检测、响应处置等技术，综合考量通信网络、控制系统、工业现场，构建全生命周期信息域和功能域融合的“自卫模式”安全防护技术体系。研究工业控制场景下的“护卫模式”安全防御体系，深入结合工业控制系统的实际需求，突破全流程攻击感知、信息和功能跨域关联研判、双安冲突消解立体管控，建立跨功能域和信息域的立体式“护卫模式”安全防护体系。结合网络靶场监测和高逼真度仿真能力，重点建立靶场攻击监测、情报收集、全流程攻击感知等能力。推动非侵入式“护卫模式”防护技术的快速落地应用，增强工业控制系统的安全防护能力。

基于数字孪生技术，构建工业控制网络靶场技术及靶场场景还原技术，形成可复制、高逼真度、快速还原的工业控制网络靶场。推进工业控制联邦网络靶场关键技术研究，建立分布式、多点互动的工业控制网络靶场。充分运用网络靶场全流程监测和威胁场景再现的特点，研究基于靶场的安全众测、运维监测、风险评估等应用技术，从多方面提升工业控制系统的安全防护能力。为支持技术验证和人才培养，建议在国家层面统筹重要工业控制网络靶场资源，面向不同应用需求建立公共服务靶场，制定靶场资源共享机制，探索靶场共享技术方法，如分布式靶场技术，实现网络靶场资源的最优化利用。

五、结语

本文围绕工业控制系统安全问题，分析了工业控制系统安全防护面临的“摸不透”“控不住”困境，总结了工业控制系统攻击技术和防护技术的发展现状，发现我国在自主可控安全和应对高隐蔽未知威胁应对方面仍存在不足。因此，针对自主可控安全问题，提出了构建基于开源RISC-V芯片的横向工业控制系统生态和基于“限制器”的进口设备底线确保机制；针对高隐蔽未知威胁，提出了“自卫模式+护卫模式”的新型安全防护体系，分析了相关的重点任务和关键技术攻关路径。

安全是一种持续对抗的过程。随着工业互联网、5G等新技术和应用的推广，工业控制系统将面临攻击面扩大、网络边界模糊化、隔离强度下降、终端海量异构等一系列新问题，安全挑战将进一步加剧。无论如何变化，自主可控都是安全的前提和基础。鉴于工业控制系统的可用性优先特点，安全防护技术研究应始终以不影响工业生产为前提，因此，“护卫模式”网络安全防护技术以其非侵入优势将是未来重要的防护技术体系之一。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: July 28, 2023; **Revised date:** October 25, 2023

Corresponding author: Tian Zhihong is a professor from the Cyberspace Institute of Advanced Technology, Guangzhou University. His major research field is cybersecurity. E-mail: tianzhihong@gzhu.edu.cn

Funding project: Chinese Academy of Engineering project “Development Strategy of Industrial Internet Security Technology” (2022-JB-04); National Natural Science Fund project (62072130)

参考文献

[1] Stojanović B, Hofer-Schmitz K, Kleb U. APT datasets and attack modeling for automated detection methods: A review [J]. Comput-

ers & Security, 2020, 92: 101734.

[2] 马力, 陈广勇, 张振峰, 等. 信息安全技术 网络安全等级保护基本要求: GB/T 22239—2019 [S]. 北京: 中国标准出版社, 2019.
Ma L, Chen G Y, Zhang Z F, et al. Information security technology—Baseline for classified protection of cybersecurity: GB/T 22239—2019 [S]. Beijing: Standard Press of China, 2019.

[3] Williams T J. A reference model for computer integrated manufacturing from the viewpoint of industrial automation [J]. IFAC Proceedings Volumes, 1990, 23(8): 281–291.

[4] International Electrotechnical Commission, International Electrotechnical Commission. IEC 62264-1 enterprise-control system integration—Part 1: Models and terminology [EB/OL]. (2013-05-30)[2023-06-20]. https://www.iso.org/standard/57308.html.

[5] 智研咨询. 2021—2027年中国工业控制系统产业发展动态及投资决策建议报告 [R]. 北京: 智研咨询, 2021.
Zhiyan Kexin Consulting. Report on the development dynamics and investment decision suggestions of China's industrial control system industry from 2021 to 2027 [R]. Beijing: Zhiyan Kexin Consulting, 2021.

[6] 杨婷, 张嘉元, 黄在起, 等. 工业控制系统安全综述 [J]. 计算机研究与发展, 2022, 59(5): 1035–1053.
Yang T, Zhang J Y, Huang Z Q, et al. Survey of industrial control systems security [J]. Journal of Computer Research and Development, 2022, 59(5): 1035–1053.

[7] Falliere N, Murchu L O, Chien E. W32. stuxnet dossier [EB/OL]. (2011-02-20)[2023-06-20]. https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en.

[8] Lee R M, Assante M J, Conway T. Analysis of the cyber attack on the Ukrainian power grid [EB/OL]. (2016-03-18)[2023-06-20]. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/03/Documents_E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[9] Di Pinto A, Dragoni Y, Carcano A. TRITON: The first ICS cyber attack on safety instrument systems [EB/OL]. [2023-06-20]. https://i.blackhat.com/us-18/Wed-August-8/us-18-Carcano-TRITON-How-It-Disrupted-Safety-Systems-And-Changed-The-Threat-Landscape-Of-Industrial-Control-Systems-Forever-wp.pdf.

[10] 黄涛, 付安民, 季宇凯, 等. 工控协议逆向分析技术研究与挑战 [J]. 计算机研究与发展, 2022, 59(5): 1015–1034.
Huang T, Fu A M, Ji Y K, et al. Research and challenges on reverse analysis technology of industrial control protocol [J]. Journal of Computer Research and Development, 2022, 59(5): 1015–1034.

[11] Lei C, Donghong L, Liang M. The spear to break the security wall of S7CommPlus [EB/OL]. [2023-06-20]. https://www.blackhat.com/docs/eu-17/materials/eu-17-Lei-The-Spear-To-Break% 20-The-Security-Wall-Of-S7CommPlus-wp.pdf.

[12] Biham E, Bitan S, Carmel A, et al. Rogue7: Rogue engineering-station attacks on S7 Simatic PLCs [EB/OL]. (2019-08-03)[2023-06-20]. https://i.blackhat.com/USA-19/Thursday/us-19-Bitan-Rogue7-Rogue-Engineering-Station-Attacks-On-S7-Simatic-PLCs-wp.pdf.

[13] Maynard P, McLaughlin K, Haberler B. Towards understanding man-In-the-middle attacks on IEC 60870-5-104 SCADA networks [C]. Swindon: The 2nd International Symposium on ICS & SCADA Cyber Security Research, 2014.

[14] Kleinmann A, Amichay O, Wool A, et al. Stealthy deception attacks against SCADA systems [M]. Cham: Springer International Publishing, 2017: 93–109.

[15] Hu Y, Sun Y Y, Wang Y C, et al. An enhanced multi-stage semantic attack against industrial control systems [J]. IEEE Access, 1809, 7: 156871–156882.

[16] Kalle S, Ameen N, Yoo H, et al. CLIK on PLCs! attacking control logic with decompilation and virtual PLC [C]. San Diego: 2019 Workshop on Binary Analysis Research, 2019.

[17] Govil N, Agrawal A, Tippenhauer N O. On ladder logic bombs in industrial control systems [M]. Cham: Springer International Publishing, 2017: 110–126.

[18] Alsabbagh W, Langendörfer P. Patch now and attack later-exploiting S7 PLCs by time-of-day block [C]. Victoria: 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), 2021.

[19] Klick J, Lau S, Marzin D, et al. Internet-facing PLCs—A new back orifice [EB/OL]. [2023-06-20]. https://www.blackhat.com/docs/us-15/materials/us-15-Klick-Internet-Facing-PLCs-A-New-Back-Orifice-wp.pdf.

[20] Spenneberg R, Brüggemann M, Schwartke H. PLC-blaster: A worm living solely in the PLC [EB/OL]. [2023-06-20]. https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf.

[21] Yoo H, Ahmed I. Control logic injection attacks on industrial control systems [M]. Cham: Springer International Publishing, 2019: 33–48.

[22] Keliris A, Maniatakos M. ICSREF: A framework for automated reverse engineering of industrial control systems binaries [C]. San Diego: 2019 Network and Distributed System Security Symposium, 2019.

[23] Castellanos J H, Ochoa M, Cardenas A A, et al. AttkFinder: Discovering attack vectors in PLC programs using information flow analysis [C]. ZOOM: 24th International Symposium on Research in Attacks, Intrusions and Defenses, 2021.

[24] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids [J]. ACM Transactions on Information and System Security, 2011, 14(1): 1–33.

[25] Sedjelmaci H, Senouci S M, Ansari N. A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48(9): 1594–1606.

[26] Yu J J Q, Hou Y H, Li V O K. Online false data injection attack detection with wavelet transform and deep neural networks [J]. IEEE Transactions on Industrial Informatics, 2018, 14(7): 3271–3280.

[27] Liu X, Li Z Y. Local load redistribution attacks in power systems with incomplete network information [J]. IEEE Transactions on Smart Grid, 2014, 5(4): 1665–1676.

[28] Liu X, Bao Z, Lu D, et al. Modeling of local false data injection attacks with reduced network information [J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1686–1696.

[29] Tajer A. False data injection attacks in electricity markets by limited adversaries: Stochastic robustness [J]. IEEE Transactions on Smart Grid, 2019, 10(1): 128–138.

[30] Bishop A N, Savkin A V. On false-data attacks in robust multi-

sensor-based estimation [C]. Santiago: 2011 9th IEEE International Conference on Control and Automation (ICCA), 2011.

[31] Yu Z H, Chin W L. Blind false data injection attack using PCA approximation method in smart grid [J]. IEEE Transactions on Smart Grid, 2015, 6(3): 1219–1226.

[32] 杨安, 孙利民, 王小山, 等. 工业控制系统入侵检测技术综述 [J]. 计算机研究与发展, 2016, 53(9): 2039–2054.
Yang A, Sun L M, Wang X S, et al. Intrusion detection techniques for industrial control systems [J]. Journal of Computer Research and Development, 2016, 53(9): 2039–2054.

[33] López-Morales E, Rubio-Medrano C, Doupé A, et al. HoneyPLC: A next-generation honeypot for industrial control systems [C]. New York: The 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020.

[34] 黄家辉, 冯冬芹, 王虹鉴. 基于攻击图的工控系统脆弱性量化方法 [J]. 自动化学报, 2016, 42(5): 792–798.
Huang J H, Feng D Q, Wang H J. A method for quantifying vulnerability of industrial control system based on attack graph [J]. Acta Automatica Sinica, 2016, 42(5): 792–798.

[35] 周明, 吕世超, 游建舟, 等. 工业控制系统安全态势感知技术研究 [J]. 信息安全学报, 2022, 7(2): 101–119.
Zhou M, Lyu S C, You J Z, et al. A comprehensive survey of security situational awareness on industrial control systems [J]. Journal of Cyber Security, 2022, 7(2): 101–119.

[36] Zonouz S, Rrushi J, McLaughlin S. Detecting industrial control malware using automated PLC code analytics [J]. IEEE Security & Privacy, 2014, 12(6): 40–47.

[37] Guo S J, Wu M, Wang C. Symbolic execution of programmable logic controller code [C]. Paderborn: The 2017 11th Joint Meeting on Foundations of Software Engineering, 2017.

[38] Zheng Y W, Davanian A, Yin H, et al. FIRM-AFL: High-throughput greybox fuzzing of iot firmware via augmented process emulation [C]. Berkeley: The 28th USENIX Conference on Security Symposium, 2019.

[39] Luo Z X, Zuo F L, Jiang Y, et al. Polar [J]. ACM Transactions on Embedded Computing Systems, 2019, 18(5s): 1–22.

[40] Chen Y Q, Poskitt C M, Sun J, et al. Learning-guided network fuzzing for testing cyber-physical system defences [C]. San Diego: The 34th IEEE/ACM International Conference on Automated Software Engineering, 2019.

[41] 李欣格, 胡晓娅, 周纯杰, 等. 面向工业控制系统全生命周期的脆弱性多维协同分析 [J]. 控制与决策, 2022, 37(11): 2827–2838.
Li X G, Hu X Y, Zhou C J, et al. Multi-dimensional collaborative analysis of vulnerability for full-lifecycle of industrial control systems [J]. Control and Decision, 2022, 37(11): 2827–2838.

[42] BCS 2022 方滨兴: 在冬奥防护中, “四蜜”探查结构塑造了更加强大的防护模式 [EB/OL]. (2022-07-13)[2023-08-18]. https://bcs.qianxin.com/2022 /news/detail?id=55.
BCS 2022 Fang Binxing: In Winter Olympics protection, the “four honey” exploration structure has shaped a more powerful protection mode [EB/OL]. (2022-07-13)[2023-08-18]. https://bcs.qianxin.com/2022 /news/detail?id=55.