工控协议安全研究综述

黄涛[1]，王郅伟[2,3]，刘家池[1]，龙千禧[1]，况博裕[1]，付安民[1]，张玉清[2,3,4]

（1.南京理工大学计算机科学与工程学院，江苏 南京 210094；2.中国科学院大学国家计算机网络入侵防范中心，北京 101408；
3.中关村实验室，北京 100194；4.海南大学网络空间安全学院（密码学院），海南 海口 571835）

摘　要：工控协议安全是保障ICS稳定运行的关键，大量工控协议在设计阶段忽视了对安全性的考量，导致目前大部分主流工控协议普遍存在脆弱性问题。结合ICS架构和工控协议的发展特征，深入解析目前工控协议普遍面临的脆弱性问题和攻击威胁。同时，针对工控协议的潜在漏洞，深入分析基于静态符号执行、代码审计和模糊测试等工控协议漏洞挖掘技术，并从工控协议的规范设计、通信机制以及第三方中间件3个方面全面剖析协议设计的安全防护技术。另外，从沙箱研制、安全防护及漏洞挖掘等方面，对工控协议安全的未来发展趋势进行展望。

关键词：ICS；工控协议；协议脆弱性；安全防护；漏洞挖掘

中图分类号：TP393

文献标志码：A

DOI：10.11959/j.issn.1000−436x.2024104

Survey on industrial control protocol security research

HUANG Tao[1], WANG Zhiwei[2,3], LIU Jiachi[1], LONG Qianxi[1], KUANG Boyu[1],
FU Anmin[1], ZHANG Yuqing[2,3,4]

1. School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
2. National Computer Network Intrusion Protection Center, University of Academy of Sciences, Beijing 101408, China
3. Zhongguancun Laboratory, Beijing 100194, China
4. School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 571835, China

Abstract: The security of industrial control protocol is the cornerstone to ensure ICS's stable operation, a large number of industrial control protocols in the design phase ignore the consideration of security, resulting in most of the mainstream industrial control protocols generally having vulnerabilities. Considering the ICS architecture and the developmental characteristics of industrial control protocols, the various vulnerabilities and attack threats commonly faced by industrial control protocols were systematically summarized. At the same time, for the unknown potential vulnerabilities of industrial control protocols, the vulnerability mining techniques of industrial control protocols were analyzed in-depth, including the static symbolic execution-based, code audit-based, and fuzzing-based. The protocol design security protection technology was comprehensively dissected from the three directions of industrial control protocol specification design, communication mechanism, and third-party middleware. In addition, the future development trend of industrial control protocol security was further prospected from the aspects of sandbox development, security protection, and vulnerability mining.

Keywords: ICS, industrial control protocol, protocol vulnerability, security protection, vulnerability mining

收稿日期：2023−12−08；**修回日期：**2024−05−13

通信作者：付安民，fuam@njust.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2023QY1202）；国家自然科学基金资助项目（No.U1836210, No.62372236）；海南省重点研发计划基金资助项目（No.GHYF2022010）

Foundation Items: The National Key Research and Development Program of China (No.2023QY1202), The National Natural Science Foundation of China (No.U1836210, No.62372236), The Key Research and Development Program of Hainan Province (No.GHYF2022010)

0　引言

工业控制系统（ICS, industrial control system）是由计算机设备与工业过程控制部件组成的自动控制系统[1]，其能够管理、指导和调节自动化工业过程的行为。目前，ICS 已经被广泛应用于工业、能源、交通、水利以及市政等重点领域，并与经济发展、国家安全和社会稳定密切相关[2]。工控协议是 ICS 中各系统和设备之间交换信息时必须遵守的规则集合，是 ICS 的重要组成部分[3-4]。

早期的工控设备计算和存储性能相对较低，并且工控网络相对封闭，面临的网络威胁相对较少，因此早期工控协议的设计重点在于基础功能，较少考虑安全性问题，如数据加密、身份认证等[5-6]。令人担忧的是，由于工控协议的更新迭代速度相对较慢，目前大部分主流工控协议如 Modbus TCP、DNP3/UDP、DNP3/TCP 和 DNPSec[7] 等，都是基于早期工控协议逐步发展或改良而来的，因此，这些工控协议的安全性普遍不高。近年来，随着信息化和工业化不断融合，工控网络逐步从封闭走向开放，工控协议面临的安全威胁也日益严峻，利用工控协议漏洞对 ICS 发起攻击的安全事件也日益频繁[3,8]。

为了提升工控协议的安全性，众多研究学者从不同角度进行了深入研究，主要分为针对已知安全威胁的防护和针对未知安全漏洞的挖掘 2 个方向。其中，针对工控协议缺乏加密、身份认证等已知安全威胁，研究人员分别从协议设计和协议实现等角度进行安全加固，进而提高工控协议自身的安全性。针对工控协议存在的未知安全漏洞，研究学者利用静态符号执行、代码审计、模糊测试等分析技术进行深入挖掘，进而提升工控协议对未知安全威胁的防护能力。

总而言之，工控协议安全是 ICS 安全的重要组成部分[3,9]，利用工控协议的脆弱性或漏洞对 ICS 进行攻击，已经成为攻击者的一种重要攻击手段。因此，本文以工控协议安全为研究目标，从 ICS 框架、工控协议分析、安全威胁、漏洞挖掘、防护技术等方面对工控协议安全进行了全面而深入的探讨和分析，具体如下。

1) 结合 ICS 的 Purdue 架构模型，阐述 ICS 中各分区和各层级的功能与关系，重点分析工控协议分类及其在不同阶段的发展特征，并进一步探讨工业互联网环境下工控协议安全给下层 ICS 的系统、设备与数据带来的安全威胁。

2) 详细梳理了目前主流工控协议在设计与实现方面存在的脆弱性问题，并进一步剖析了由这些脆弱性问题导致的攻击威胁。

3) 针对工控协议存在的潜在漏洞，全面探讨了基于静态符号执行、基于代码审计和基于模糊测试的工控协议漏洞挖掘技术。

4) 针对工控协议存在的脆弱性问题与攻击威胁，分别从工控协议的规范设计、通信机制以及第三方中间件 3 个方面深入剖析了协议设计安全防护技术。

5) 从工控网络沙箱研制、工控协议的安全防护、漏洞挖掘与修复等方面，对工控协议安全的未来发展趋势进行了展望与分析。

1　ICS 框架和工控协议分析

相比于互联网系统，ICS 的网络相对封闭、设备资源相对有限，这些特征深刻影响了 ICS 与工控协议的设计理念和发展方向。

1.1　ICS 框架

ISA-99 采用的 Purdue 参考模型[2] 如图 1 所示，该模型作为 ICS 设计和实施的事实标准，详细地展示了典型 ICS 的所有主要组件之间的互连和依赖关系，并将 ICS 划分为安全区、控制区、隔离区和企业区 4 个区域。其中，控制区和企业区分别采用运营技术（OT, operational technology）和信息技术（IT, information technology）。

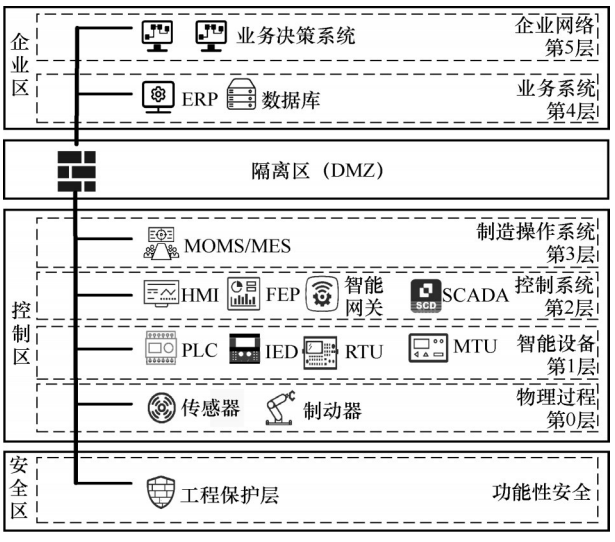


图 1　ICS 的 Purdue 参考模型

1) 安全区：也被称为功能安全层，主要负责监测异常和减少危险事故，以保护ICS设备和系统。该区包括若干工程保护层，当硬件发生故障或其他不确定的不利条件导致整个系统中断时，这些工程保护层能够确保系统不会出现危险故障。

2) 控制区：也被称为OT网络，包括用于监视、控制、维持逻辑或物理过程的自动化操作的系统和设备，该区可以划分为第0层、第1层、第2层和第3层共4个子层。第0层包括直接作用于物理过程的传感器和制动器，如电机、泵、传感器、阀门等。第1层包括可以监控第0层设备的智能设备和系统，如可编程逻辑控制器（PLC, programmable logic controller）、智能电子设备（IED, intelligent electronic device）、远程终端单元（RTU, remote terminal unit）和主终端单元（MTU, master terminal unit）等。第2层包括人机界面（HMI, human machine interface）、前端处理器（FEP）、智能网关和SCADA等控制系统，能够监控和管理系统内的整体过程。第3层包括制造操作系统，通常负责管理控制设备的运行，以生产所需的产品，如批次管理、制造运营管理和制造执行系统等。

3) 隔离区：作为IT和OT网络之间的屏障，负责管理控制区和企业区之间的有限访问，尤其是防止IT网络中的威胁传播到OT网络，实现以安全的方式管理IT网络和OT网络之间的连接。

4) 企业区：即IT网络，包括传统的IT设备和系统，如业务系统和企业网络。虽然此区通常不与ICS直接连接，但是其负责从ICS中收集数据以进行业务决策。企业区可以分为第4层和第5层2个子层。第4层包括每个现场、车间或设施中控制本地设施运行的IT系统，如企业资源规划（ERP, enterprise resource planning）软件、数据库等。该层可以对下层设备和系统进行监控与管理，还能对第5层企业网络进行数据更新。第5层即企业网络，主要负责供应链管理。该层虽然不与ICS直接相连，但是可以从ICS系统中收集数据以进行最终的业务决策。

值得注意的是，虽然理论上隔离区能够有效过滤OT和IT网络之间的所有流量，从而保护OT网络的安全，但是由于现实原因，目前ICS对这些安全防护方面的关注仍不够，ICS的重要设施或系统（即OT网络）容易被潜在的攻击者发现和攻击。

1.2 工控协议

目前，工控协议主要分为传统控制网络协议、现场总线协议、工业以太网协议和工业无线协议4类[4]。

1.2.1 传统控制网络协议

传统控制网络协议主要用于计算机集中控制系统（CCS, centralized control system）、分布式控制系统（DCS, distributed control system）、现场总线控制系统（FCS, fieldbus control system）、过程控制系统（PCS, process control system）和PLC等系统间的通信[5]。CCS作为早期的控制系统结构，可以实现高度集中控制，但其主要缺陷是事故风险集中在主控计算机上，一旦出现问题容易造成大面积瘫痪。DCS基于CCS发展而来，其核心思想是分散控制、集中操作、分级管理、配置灵活以及组态方便。相比于DCS，FCS实现了分散控制，成为近年来迅速发展起来的一种工业数据总线技术。然而，这些早期的传统控制网络协议重点考虑如何在实现ICS功能性需求的基础上对ICS的控制方式进行优化，如由集中控制向分布式控制和现场总线控制的转变，以实现简单、可靠、经济、实用的通信方式为目标。

1.2.2 现场总线协议

现场总线技术通过数字通信替代传统模拟信号及普通开关量信号进行传输，用于解决工业现场中各种智能现场设备和高级控制系统之间的信息传递，具有简单、可靠、经济、实用等优点[10]。在ICS发展初期，常用的现场总线协议主要基于串行链路，包括CAN、DeviceNet、CCL-Link、Modbus (Modbus RTU、Modbus ASCI、Modbus Plus)、DNP3和Profibus (Profibus-DP、Profibus-PA和Profibus-FMS)等。

由于早期工控环境相对封闭且面临的网络威胁较少，同时早期工控设备的计算和存储资源都相对有限，这些早期工控协议设计更加侧重于满足ICS的功能性需求和基本的可靠性需求，没有充分考虑工控协议的安全性需求（如加密机制、身份认证、完整性校验等），因此这些早期工控协议中普遍存在安全脆弱性问题[3]。

1.2.3 工业以太网协议

随着以太网技术的不断进步以及工控硬件性能的逐步提升，为了实现各ICS间的互联互通，ICS

逐渐向互联网开放。在早期基于串行链路的现场总线协议的基础上，逐渐出现了基于以太网的演化版本[4-5]，即工业以太网协议（含TCP/IP之上的某些应用层协议），主要包括Modbus TCP、Profibus (Profinet CBA、Profinet IO)、DNP3 (DNP3/UDP、DNP3/TCP)、EtherNet/IP、EtherCAT、OPC等[11]。

工业以太网协议对传统现场总线协议的功能设计、安全机制等都进行了扩展与完善，不仅能够进一步满足ICS的实时性、稳定性和可靠性等要求，还能对早期工控协议中存在的脆弱性问题进行完善[3]。同时，工业以太网协议还引入了OSI的协议栈模型，能够更好地适用于复杂的互联网环境。然而，这些协议仅解决了自身部分脆弱性问题，由于协议结构更加复杂，还额外引入了更多复杂的互联网相关的安全威胁。目前，大多数现场总线协议和工业以太网协议都已经成为主流工控协议。

1.2.4　工业无线协议

相比于前3类有线协议，无线协议的优势日益凸显，如安装方便、通信成本低、设备布点灵活、监控范围广等，因此，工业界和学术界普遍认为它将是工控网络未来的发展方向[7]。然而，工业无线协议目前仍处于发展的初级阶段，其使用的无线技术包括Wi-Fi、蜂窝网络、蓝牙、WirelessHART和ZigBee等，这些技术主要应用于传感器和测量装置等，常见的工业无线协议主要包括IEEE 802.11 (a/b/g/n)、RFieldbus、ZigBee等。

1.3　工控协议安全

随着互联网技术与制造技术的深度融合，工业互联网应运而生，其本质是在传统ICS架构的基础上引入互联网技术，在不大幅改变传统下层ICS架构的前提下，提升工业设备、数据等资源的全面互联与管理能力。因此，在当前工业互联网环境下，工控协议安全威胁给下层ICS的系统、设备、数据都带来了更加严峻的安全挑战。

在ICS与设备安全方面，ICS的更新迭代速度通常较慢，导致许多系统和设备仍缺乏必要的安全防护措施，如系统设计未充分考虑安全性和工控设备硬件性能的限制等。因此，在当前日益复杂的工业互联网环境下，攻击者可以利用协议安全脆弱性问题对ICS发起更新颖、更复杂的互联网攻击，如分布式拒绝服务攻击、重放攻击、欺骗攻击和中间人攻击等。更严重的是，面对这些互联网攻击，一些传统的工控安全防护技术往往难以有效应对。

在工业数据安全方面，随着工业大数据技术在工业互联网平台的广泛应用，工业数据资源呈现体量大、种类多、关联性强、价值分布不均等特点。在当前工业互联网环境愈发复杂，且ICS仍缺乏充分的安全防护能力的情况下，任何工控协议的安全威胁都容易导致工业敏感信息的泄露。另外，针对这些工业数据的保护，也存在数据分级分类保护难度大、事件追踪溯源困难等问题。

总而言之，Purdue模型作为目前ICS设计与实现的事实标准，通过隔离OT网络与IT网络，构建了相对封闭的早期工控网络，以增强ICS的安全性。同时鉴于工控设备资源的局限性，早期工控协议设计更关注满足ICS基本的功能性与可靠性需求，而忽视了协议安全性，尤其是传统控制网络协议和现场总线协议。随着工控网络逐渐向互联网开放，工控设备的性能也在不断提高，促使部分现场总线协议逐步演化或重新设计出工业以太网协议。这类协议的功能性、安全性等都有所提升，但仅解决了部分自身脆弱性问题，同时还引入了更多复杂的互联网安全威胁。目前传统控制网络协议仍用于ICS下层系统及设备之间的通信，如PCS、FCS、PLC等。现场总线协议和工业以太网协议已成为目前广泛应用的工控协议，而工业无线协议将成为工控协议的未来发展方向。然而，在目前更加复杂的工业互联网环境下，这些工控协议都存在安全脆弱性问题，并严重威胁下层ICS中系统、设备与数据的安全。

2　工控协议安全威胁

工控协议脆弱性问题通常容易引发各类恶意攻击，如窃听攻击、欺骗攻击、重放攻击或拒绝服务攻击等。本节先梳理目前主流工控协议的典型脆弱性问题，再进一步分析针对工控协议的主要攻击方式。

2.1　工控协议脆弱性

网络协议生命周期主要包括协议设计和协议实现2个重要阶段，由于目前工控协议未充分考虑安全性或在实现过程中存在疏忽，工控协议的设计和实现阶段普遍存在较多脆弱性问题。具体来讲，一方面，协议设计者在设计工控协议时未充分考虑安全性，导致这些协议普遍存在如缺乏身份认证、完整性校验等固有的设计脆弱性问题；另一方面，协

议开发者在实现工控协议时存在缺陷，导致这些工控协议存在如缓冲区溢出、命令注入等潜在的实现脆弱性问题。

2.1.1 设计脆弱性

众多研究学者对当前主流的工控协议如Modbus、DNP3、EtherNet/IP、S7Comm等进行了归纳[2]，如图2所示。通过分析发现，这些主流工控协议普遍存在一种或多种设计上的脆弱性问题[9,12]，主要包括弱/缺乏身份认证、缺乏加密机制、缺乏完整性检查、缺乏认证机制、缺乏授权机制等。表1总结了目前主流工控协议的脆弱性问题[7,10,13]，其中，×表示“缺乏”，√表示“具有”，○表示“部分版本具有”，如Modbus-ASCII和Modbus-RTU分别采用纵向冗余校验（LRC校验）和循环冗余校验（CRC），但Modbus-TCP没有完整性校验。

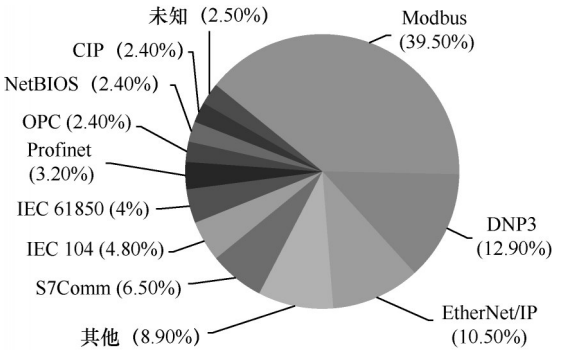


图2 主流工控协议占比

表1 典型工控协议脆弱性

协议	身份认证	加密	完整性校验	可靠性保护	授权
Modbus	×	×	○	×	×
DNP3	×	×	√	√	×
EtherNet/IP	×	×	√	√	×
S7Comm	×	×	×	×	×
IEC 104	×	×	×	√	×
IEC 61850	×	×	×	×	×

为了解决这些典型的脆弱性问题，众多研究学者对部分主流工控协议进行了扩展、改进甚至重新设计。例如，基于Modbus协议衍生出了Modbus-TCP、Modbus-F2009[13]、Modbus-S2015[14]和Modbus-A2018[15]等版本，基于DNP3协议演化出了DNP3/UDP、DNP3/TCP、DNPSec[7]等版本。此外，还有重新定制适用于以太网的EtherNet/IP、IEC 104等协议。

尽管这些工控协议的演化版本有针对性地解决了部分设计脆弱性问题，但是仍存在很多安全漏洞。例如，文献[14,16]指出Modbus/TCP协议缺乏加密机制和身份认证，攻击者可以识别通信设备并篡改数据分组，造成服务器宕机，并容易受到欺骗攻击、洪泛攻击、重放攻击等。DNPSec[7]虽然使用3-DES和SHA-1算法对DNP3进行改进，实现了加密机制和认证机制，但是其所使用的3-DES和SHA-1算法依然存在被破解的风险。IEC 104协议缺乏加密机制、采用明文传输，容易被窃听、伪造及篡改，从而导致源地址欺骗及源路由欺骗[10,17]等攻击。基于OPC改进的OPC UA协议虽然提供了加密、认证、授权、完整性校验等安全机制[18]，但Puys等[19]通过加密协议验证工具ProVerif发现了一些影响协议机密性和身份认证的缺陷，这些缺陷威胁到了协议的安全性。

显而易见，虽然这些主流工控协议及其改进版本解决了早期工控协议的部分设计脆弱性问题，如加密和身份认证的缺失，但是依然面临严峻的安全风险。

2.1.2 实现脆弱性

尽管部分工控协议在设计阶段已充分考虑加密、身份认证等安全机制，但是由于协议开发者的疏忽或其他原因，这些工控协议在实现过程中仍然可能存在潜在的漏洞，使得现有安全机制被攻击者绕过，即工控协议的实现脆弱性。

Biham等[20]发现S7Comm Plus虽然包含加密、认证等安全机制，但是协议认证过程中所有同型号工控设备都采用相同的安全密钥，因此，只要有一款设备的密钥被破解，所有相同版本的设备都不再安全。Kalle等[21]发现UMAS协议实现中会将关键Hash密钥存储在一个固定的地址，攻击者可以通过重写该固定地址的内容以覆盖Hash密钥，从而绕过现有的认证机制。GX Works2[22]软件在接收某个状态消息时未检查协议报文长度，导致出现堆溢出错误。文献[12]指出采用C/C++编码实现的IEC 61850或Modbus协议容易被攻击者利用以破坏计算机程序的内存，包括数组溢出、堆栈溢出、指针损坏、格式化漏洞等。文献[23]指出除了UMAS协议存在关键Hash密钥被覆写的缺陷外[21]，CODESYS-V2协议也存在可能导致未初始化的指针访问或内存越界访问的漏洞。

显然，协议实现过程中的任何疏忽都可能导致实现脆弱性问题，如密钥生成或保存不当、报文长度未检查、协议实现语言存在缺陷等，相比于设计脆弱性，实现脆弱性往往更难以防范。

2.2　工控协议攻击

攻击者可利用工控协议的脆弱性问题对工控协议展开多种网络攻击，破坏ICS的可用性、完整性和机密性等基本安全属性[24]。表2详细梳理了目前针对工控协议的主要攻击方式及其所利用的脆弱性问题[12,25-28]，如窃听攻击、重放攻击、欺骗攻击、中间人攻击、拒绝服务攻击、功能码滥用等。

表2　　主流工控协议的实现漏洞

攻击方式	利用的脆弱性	安全属性危害
窃听攻击	缺乏加密	机密性
重放攻击	缺乏可靠性保护、身份认证	完整性
欺骗攻击	缺乏身份认证、完整性校验	可用性
中间人攻击	缺乏身份认证	完整性
拒绝服务攻击	缺乏身份认证、授权以及漏洞利用	可用性
功能码滥用	缺乏授权、身份认证	可用性

Kang等[25]通过ARP欺骗在智能电网中使用IEC 61850标准的工控设备发起中间人攻击，如图3所示。攻击者首先入侵工控网络内一台工控主机A，并获取光伏逆变器和控制器的IP地址，然后借助被入侵的主机A利用ARP欺骗对光伏逆变器和控制器发起中间人攻击，获取甚至篡改目标设备之间的所有数据包。类似地，Erdődi等[10]通过欺骗攻击伪装成合法的控制站，发送连续的重置消息，并进行数据包注入，进而实现拒绝服务攻击，中断控制站和RTU之间的通信，破坏ICS的可用性。Maynard等[17]通过拦截或篡改IEC 104协议通信报文实现重放攻击和中间人攻击，甚至向SCADA服务器隐藏接地故障，并成功篡改SCADA的核心功能。Kelli等[26]和Hoyos等[27]分别针对DNP3协议、GOOSE协议展开欺骗攻击、中间人攻击、重放攻击、拒绝服务攻击等，严重干扰IED工控设备的正常运行，破坏ICS的机密性、完整性与可用性，而造成这一系列攻击的主要原因是这些协议普遍缺少加密、身份认证等安全机制，这也是其他基于TCP/IP协议栈的工控协议共同面临的问题。此外，Merxell等[28]通过滥用Modbus协议的0x05功能码将所有寄存器置1，打开所有工控设备的阀门。类似地，East等[11]通过滥用DNP3协议功能码重新启动目标设备，导致设备短期内无法使用或恢复到不一致的状态。

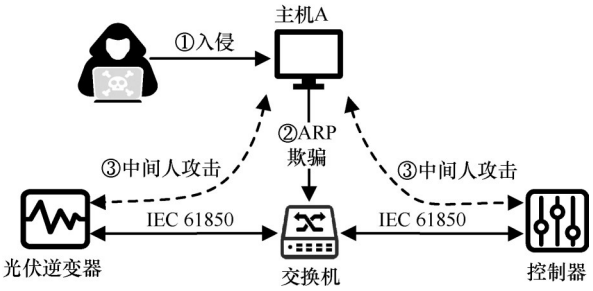


图3　中间人攻击

显然，这些攻击通常利用工控协议存在的多种脆弱性问题展开连续的组合型网络攻击，从而造成范围更大、后果更严重的危害。

总而言之，大多数主流工控协议普遍存在设计脆弱性和实现脆弱性等问题。设计脆弱性主要源自工控协议自身的设计，由于早期工控网络的封闭性与工控设备资源的局限性等现实原因，许多主流工控协议在设计时未考虑加密、身份认证、完整性校验等安全机制，存在设计脆弱性问题。除了工控协议自身的设计脆弱性外，协议在具体实现过程中也存在如密钥保存不当、数据边界未处理等问题，导致存在各种协议实现脆弱性问题，如缓冲区溢出。因此，攻击者可以利用不同的工控协议脆弱性发动不同类型的网络攻击，但通常都是结合工控协议的多种脆弱性，同时展开范围更广、危害更大的组合型攻击。例如，基于窃听攻击进一步实现重放攻击、中间人攻击等，进而破坏ICS的机密性、完整性和可用性。值得注意的是，部分脆弱性问题是导致多种攻击的关键，如表2中缺乏身份认证容易导致重放攻击、欺骗攻击、中间人攻击、拒绝服务攻击等。因此，通过减少工控协议脆弱性问题，尤其是关键脆弱性问题，能够有效降低工控协议被攻击的概率以及相应的危害程度。

3　工控协议漏洞挖掘

针对已知的工控协议脆弱性问题，可以借助各种安全防护技术来增强工控协议的安全性。然而，如何挖掘那些潜在的工控协议漏洞，并达到更多的状态分支以及更深层的探索效果，也是目前的研究热点。针对这一问题，目前主要存在3种技术路

线，包括基于静态符号执行、基于代码审计和基于模糊测试。

3.1 基于静态符号执行

符号执行技术使用符号变量代替具体值作为输入，通过分析程序执行过程中符号变量的状态以及分支跳转时的路径约束条件，以获得程序各个分支的符号化约束关系和各个路径的具体值。符号执行通常分为静态和动态2种方式，目前工业界大多基于静态符号执行进行工控协议漏洞挖掘。

Chau等[29]将符号执行技术应用于针对小型SSL/TLS的X.509实现的漏洞分析中，有效解决了基于黑盒模糊测试的漏洞挖掘无法保证覆盖率而导致严重缺陷被忽略的问题。类似地，Corin等[30]也利用符号执行技术着重分析协议中的重要代码逻辑，采用密码原语重写方式分析WPA2协议，从而更深入地探究工控协议的脆弱性。这些方法虽然能够自动化探索工控协议程序中所有可能的执行路径，通过较少测试用例达到较高覆盖率，进而发现工控协议程序漏洞，但是它们都普遍存在路径爆炸问题。因此，针对路径爆炸问题，部分学者巧妙地将符号执行与其他技术结合，不仅能够尽可能地避免路径爆炸，还能够实现更全面的协议脆弱性分析。

Song等[31]和Cho等[32]将符号执行与具体执行相结合，实现了对程序状态空间广泛而深入的探索，但是模型推断和符号执行的迭代过程十分耗时。Zhang等[33]提出一种以协议状态机指导符号执行的方法，将协议代码中的密码学逻辑与协议交互逻辑分开处理，在保证探索深度的基础上节省开销，避免了密码逻辑的复杂性导致路径约束无法求解的问题。Sun等[23]和谢肖飞等[34]将符号执行与模糊测试相结合，提出了覆盖率度量的导向方式和路径优先级策略，提高了对工控协议漏洞的检测效率，并有效规避了路径爆炸问题。这些技术虽然在一定程度上提高了符号执行在工控协议漏洞挖掘方面的准确率和效率，但是均需要对符号执行技术自身的缺陷进行改进或规避，从而间接增加了使用符号执行进行工控协议漏洞挖掘的复杂程度。

3.2 基于代码审计

代码审计是利用专家经验或者神经网络等人工智能技术，构造访问或者破坏系统的输入，从而对工控协议代码中的脆弱点进行深入分析的过程[35]。

2017年，杜江等[36]将多种代码审计技术搭配使用，并设计了安全属性定义方法，不仅提升了软件安全需求描述的准确度，还保持了代码审计技术自动化程度高的优点，同时提升了审计效率并降低了误报率，深度挖掘了OpenSSL源代码中的脆弱性。2020年，Tang等[37]将传统代码审计技术与RVFL、Bi-LSTM神经网络相结合，显著提高了源代码级程序分析的效率和准确率，为工程师进行漏洞代码审计提供了有价值的指导。2011年，Corin等[30]开发了一种MOSTO工具包，在GNU GPL许可下，使审计人员能够在不干扰ICS工作流程的情况下对Modbus/TCP协议进行安全审计，避免了传统ICS安全性评估方法的临时性以及难以形成具体可预测结果的问题，同时支持结合多种测试框架，可以形式化地测试ICS网络的安全属性。

然而，这类技术通过自动化工具或者人工审查的方式对程序的源代码逐条检查和分析，虽然能够有效识别源代码缺陷引发的安全漏洞及其实例的具体位置等，但是难以识别业务逻辑缺陷和协议设计缺陷等，并且依赖技术人员的专家经验。

3.3 基于模糊测试

模糊测试（即Fuzzing技术）是一种根据一定的规则自动或半自动生成大量随机测试数据，并将其输入目标程序中，通过监控程序是否出现异常来发现潜在漏洞或安全隐患的方法。根据对目标工控协议规范的了解程度，目前主流的工控协议模糊测试可以分为黑盒测试和灰盒测试2种。

3.3.1 黑盒测试

黑盒测试在对目标工控协议规范缺乏具体了解的情况下，向目标协议程序输入大量完全随机或半随机测试数据，通过分析测试过程中输入和输出之间的交互，以发现工控协议的潜在漏洞，通常适用于未知工控协议的漏洞挖掘。

Lee等[38]发布了一款适用于Modbus工控协议的模糊测试工具Sulley，该工具允许测试人员自定义协议消息格式和字段，生成多种变异消息发送到目标服务以检测目标协议的潜在漏洞。此外，Sulley还具有强大的插件功能，能够进一步扩展新的工控协议。然而，该工具主要还是针对多种网络协议进行模糊测试，但对于一些特定的工控协议的测试效果并不好。随后，众多研究学者相继开发出了各类工控协议的专用模糊测试工具。Ta-

cliad 等[39]设计的 EtherNet/IP Fuzzer 在缺乏协议规范的情况下，可以根据自定义的协议格式，通过 Scapy 库生成模糊数据包，并使用启发式算法进行字段结构猜测和数据包字段变异，进而触发 EtherNet/IP 协议程序崩溃，类似的 Fuzzer 还有 LZ[40]、Modbus[41]、ENIP[42]、Prop[43] 等。2018 年，Hu 等[44]提出一种基于生成对抗网络的工控网络协议模糊测试框架 GANFuzz，该框架使用深度学习技术自动生成测试用例，并提出 3 种聚类策略对不同维度的协议消息进行分类，以生成更多样化且高效的测试用例，从而提升代码覆盖率和测试深度。2019 年，Zhao 等[45]提出了 SeqFuzzer，利用长短期记忆网络模型构建和训练 Seq2Seq 模型，学习工控协议报文序列之间的关系，有效提取工控协议格式和状态转换关系，从而高效生成测试用例并监视不规则的 ICS 行为。2023 年，Bytes 等[46]提出一款通过网络流量层面对 ICS 进行模糊测试的黑盒模糊测试工具 FieldFuzz，该模型兼具跨平台适用性。

总体来看，黑盒模糊测试虽然能够有效挖掘未知工控协议的漏洞，但是缺乏对协议规范的了解，导致大量资源被浪费在生成无效测试数据上，因此，黑盒模糊测试普遍效率较低。

3.3.2　灰盒测试

灰盒测试利用目标工控协议的内部信息，如协议格式、字段语义等，生成更具有针对性的测试用例，以达到更深层次和高效的测试效果。因此，该技术适用于公有工控协议，或者需要提前利用未知协议逆向、插桩等技术提取相应的协议内部信息。AFL[47]作为这类工具的典型代表，可用于发现比较复杂的协议漏洞。

Eddington[48]设计了一款智能灰盒模糊测试工具 Peach Fuzzer，该工具允许用户通过定义数据模型和协议语义来描述目标协议或文件格式的结构，并生成大量智能测试用例，以不断发现新的未知漏洞。此外，Peach 具有灵活、易扩展等特性，不仅能够测试 Modbus 工控协议，还能够扩展到其他工控协议。Luo 等[49]在 Peach Fuzzer 的基础上设计了一款开源工控协议模糊测试工具 Peach*，该工具使用 LLVM pass 收集覆盖信息，并以探索路径覆盖率为导向，相比于 Peach Fuzzer，Peach*在模糊测试效率和路径覆盖率方面表现更好，但需要提供待测项目的源码，因此仅适用于开源 ICS 协议项目。Pham 等[50]在 AFL 的基础上提出 AFLNet，通过引入状态机信息对状态码转换过程进行引导，同时使用插桩技术基于覆盖率对模糊测试过程进行引导，从而提高种子有效变异概率。Ba 等[51]对 AFLNet 的状态机进行改进，通过构建状态转换图，使协议报文中的状态转换更清晰，生成更具针对性的工控协议测试样例。Yu 等[52]提出一款针对工业物联网协议的模糊测试框架 CGFuzzer，如图 4 所示。CGFuzzer 设计了一种覆盖引导的生成式对抗网络 Cov-GAN，该网络能够学习工业物联网协议规范，以生成具有高通过率和代码覆盖率的测试用例。

总而言之，基于静态符号执行和代码审计的技术都属于静态分析技术，这些技术都不需要实际运行程序，可以在代码编译或审查阶段发现未初始化的变量、内存泄漏、不安全的函数调用等浅层漏洞或安全隐患，具有较高的执行效率以及较低的开销。但是这类技术普遍存在误报/漏报率高、路径爆炸等问题，导致难以进行复杂工控协议漏洞挖掘，而且严重依赖于工控协议程序的源代码。因此，这类技术主要适用于已知工控协议的漏洞挖掘，而不适用于工控领域目前广泛存在的未知工控协议。而基于模糊测试的技术属于动态分析技术，这类技术通过分析程序运行时的实际行为、执行轨迹和上下文信息，如堆栈跟踪、变量状态和输入数据等，能够发现更深层次的漏洞或安全隐患，不仅对协议源码依赖程度低，而且还具有误报/漏报率低、探索层次深和全面性强等优点。然而，由于需要获取和处理工控协议程序运行时的信息，这类技术往往执行效率低、运行开销高。因此，基于模糊测试的技术主要应用于静态分析技术难以分析的复杂场景或者未知的工控协议漏洞挖掘。

由此可见，静态分析技术和动态分析技术并无优劣之分。目前针对工控协议的漏洞挖掘，通常采用动态、静态结合的漏洞挖掘技术，以弥补各自的缺陷。例如，通过动态分析验证静态分析的结果，从而提高工控协议安全漏洞挖掘的准确性，降低静态分析的漏报率，提升动态分析的代码覆盖率。针对广泛存在的未知工控协议，还可以利用污点分析、插桩等方法提取相应的协议格式，以指导模糊测试更高效地生成测试用例，最终实现更加全面、高效、准确的工控协议漏洞挖掘。

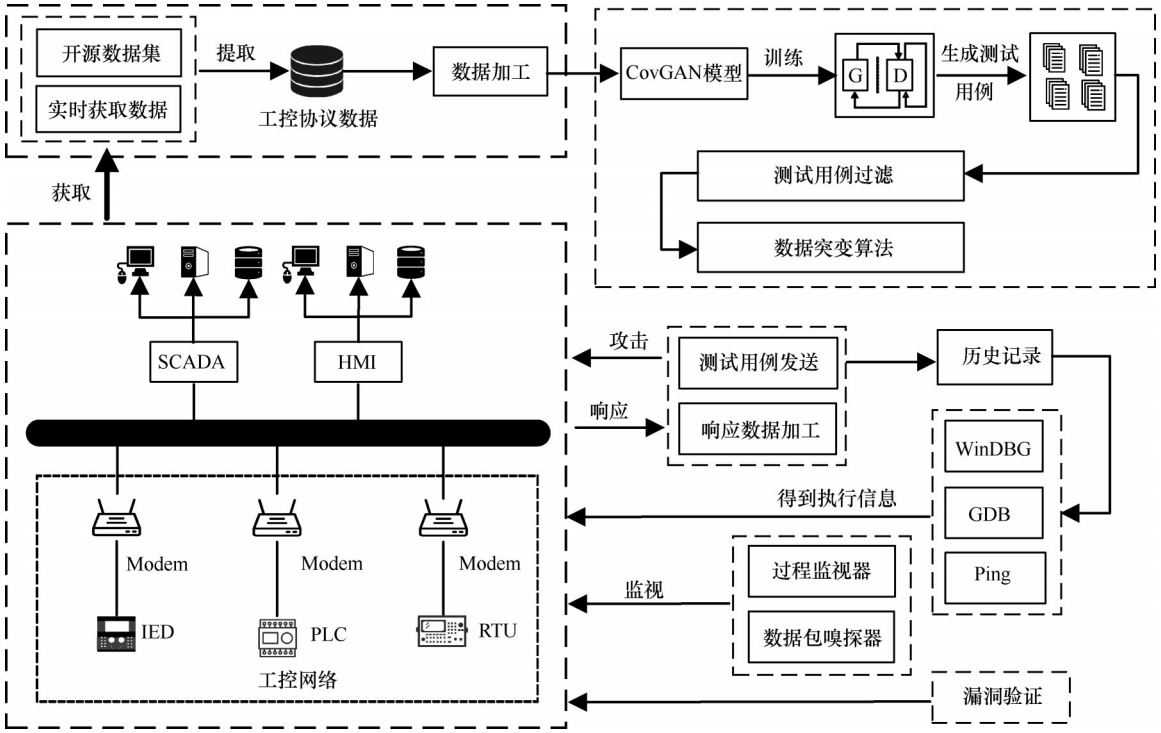


图4　基于CovGAN的工控协议Fuzzing框架

4　工控协议安全防护

针对由工控协议脆弱性引发的各类攻击威胁，众多研究学者研究了相应的安全防护措施。本文按照协议通信的组成结构，将这些措施分为3个研究方向[4]，分别是基于规范设计的防护机制、基于通信机制的防护机制和基于中间件的防护机制。

4.1　基于规范设计的防护机制

由于很多工控协议在设计初期未充分考虑安全性，针对这些工控协议规范进行安全防护（例如，添加必要的安全字段），能够有效提升其安全性。

Shahzad等[14]在Modbus协议的功能字段中添加加密缓冲区，如图5所示，通过此方法能够动态监控Modbus协议的敏感信息，为Modbus协议数据安全传输提供了全面的解决方案。类似地，Fovino等[13]和Al-Shareeda等[53]分别在Modbus协议和SECS/GEM协议中添加时间戳字段，以有效检测和抵抗重放攻击，但是这种方法严重依赖时间精确度。此外，为了进一步帮助协议设计人员从根本上更规范地为物联网协议进行建模，Wang等[54]提出一种基于领域特定语言（DSL, domain specific language）的物联网协议定制系统ProFactory，该系统利用DSL制定各种规范对协议进行建模和组装，从而指示ProFactory生成相应的数据结构和源码，并使用符号检查模型来捕捉协议状态转换中的错误，最终通过工具（如VCC）自动验证代码实现的并发正确性以及内存访问安全性。ProFactory能够消除物联网协议中的消息解析漏洞和基本状态转换错误，从而提高物联网协议的安全性，但是该系统极其依赖于DSL的创建质量。

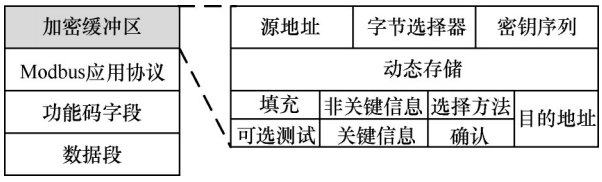


图5　Modbus协议的功能字段

4.2　基于通信机制的防护机制

很多工控协议在规范设计阶段缺乏安全性考量，同时在协议通信机制方面也存在很多脆弱性问题。因此，部分研究学者提出专门针对工控协议通信机制的防护机制，以确保工控协议数据的安全传输，尤其是防止数据被窃取、篡改或未授权访问。

闫爽[55]利用椭圆曲线密码体制（ECC）中的DSA签名验证算法和DH（Diffie-Hellman）密钥交换算法来扩展SSL协议，确保主从设备之间共享密钥的安全传输，并使用AES对称加密和消息认证码运算来解决DNP3协议传输过程中存在的窃听、

篡改等安全隐患，如图 6 所示。Fovino 等[13]和 Luo 等[56]都利用对称密钥算法、数据签名算法和哈希算法确保原 Modbus 协议数据的保密性、可靠性、完整性等，并利用白名单过滤机制对功能码进行基于角色的管理，从而有效防止功能码滥用。Ádámkó 等[15]采用基于 Shamir 秘密共享协议的挑战—响应验证机制和 AES 加密技术来确保 Modbus-RTU 协议的安全性。Lu 等[57]提出了基于 ECC 的数据源认证方案，在严格的时间限制下实现智能电网中协议通信的双向认证和访问控制。Premnath 等[58]提出基于 NTRU（number theory research unit）的轻量级加密验证方案，以解决 SCADA 中协议数据的保密性差、缺乏验证机制和不可否认等问题。

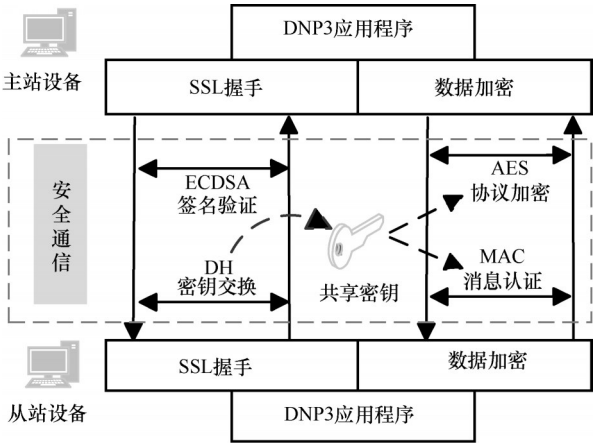


图 6　DNP3 协议安全防护方案

尽管以上方法大多基于预协商密钥的单因素身份进行验证，具有轻量级、易实现等特点，但对于一些通信安全要求较高的 ICS，这些方法的安全防护能力可能存在较大不足。为此，Chan 等[59]提出基于历史数据的可扩展双因素身份验证（CWZT）协议，该协议不仅使用了传统的长期共享密钥作为一种认证因素，还引入了与历史数据相关的动态增长的秘密标签作为第二种认证因素，能够有效避免秘密身份验证信息泄露所带来的危害。Jin 等[60]针对 CWZT 协议提出了标签窃取攻击并成功破坏了该协议的安全机制，又进一步提出了基于历史数据建立多因素认证保密通道（HMACCE），给出了两种 HMACCE 协议（Π_{woFS} 协议和 Π_{FS} 协议）。Π_{woFS} 和 Π_{FS} 协议均采用对称密钥、历史数据和一组与历史数据相关的秘密标签作为认证因素，通过工控边缘设备管理的密钥快速验证历史数据与存储在服务器上的相关标签之间的关系，从而建立协议传输的安全信道。同时，HMACCE 协议也为建立工控协议安全防护信道保留了轻量级的优势。

4.3　基于中间件的防护机制

由于并非所有基于协议规范或通信机制的防护措施都能确保不对 ICS 造成影响，尤其是在中大型 ICS 中。因此，部分研究学者提出在协议通信实体间加入额外的软/硬件（即中间件），用于增强协议的安全性，以保护工控协议通信数据安全。此外，该方案还具有跨网络、跨平台和跨设备等特点[61-64]。

安全代理和安全隧道是典型的软件型中间件应用。GoProxy[61]通过创建代理服务器，为工控协议通信提供 TLS 加密传输、协议转换以及负载均衡等安全防护功能，有效解决了工控协议数据的隐私保护、访问限制以及安全加密等问题。Goldy[62]通过 TLS 证书和密钥建立通信双方的安全隧道，为通信双方提供透明的加密验证服务。然而，这些软件型中间件没有考虑网络带宽、服务器性能等对工控协议通信造成的时延问题，而且软件自身也存在被攻击的风险。因此，Poddar 等[63]和 Duan 等[64]基于 Intel SGX 硬件分别实现了可信中间件 SafeBricks 和 LightBox，能够显著提高中间件的性能。SafeBricks 能够保护网络功能流量、云服务器流量以及网络功能源码的安全，而 LightBox 通过设计安全、高效和可用的虚拟网络接口，以及针对安全隔离环境优化的流状态管理方案来保护敏感协议数据，并维持高性能运行。但是 SafeBricks 不支持多播网络，LightBox 对原始设备不透明，因此这 2 种方式仅适用于少量工控协议实现场景。Zhan 等[62]提出一种高性能、安全、易于集成的中间件 GuardBox，采用商用可信硬件来确保密钥安全性，为工控协议数据包提供高效的机密性和完整性服务。虽然硬件型中间件的安全性高于软件型中间件，但需要增加额外的硬件成本，并且无法抵抗侧信道攻击、重放攻击等。

本节分别从工控协议自身规范设计、通信机制以及第三方中间件 3 个角度分析了工控协议安全防护技术，表 3 详细对比了这些防护方法的防护目标、原理以及特点。

基于规范设计的防护主要针对工控协议自身的协议规范，通过添加额外安全字段的方式，能够从

表3 工控协议安全防护方法对比

类型	方法	目标脆弱性或缺陷	防护机制原理	特点
基于规范设计的防护	文献[13, 53]方法	无法抵御重放攻击	添加时间戳字段	轻量级，但改进空间较小、安全防护性能提升有限，且对ICS运行影响较大，适用于轻量级或新的ICS
	文献[14]方法	缺乏加密机制	在功能字段中添加加密缓冲区	
	文献[54]方法	消息解析和状态转换漏洞	基于DSL的协议定制方法	
基于通信机制的防护	文献[55]方法	缺乏加密、完整性校验等	基于椭圆曲线密码体制、非对称加密算法和MAC等实现	基本都是利用加密、签名和身份认证等密码学技术对工控协议的通信机制进行改进，不仅具有较大改进空间，还能够更大限度地提高安全防护能力，但也会带来较高的性能开销、密钥安全管理和协议兼容性等问题，属于目前的研究热点
	文献[13, 56]方法	缺乏加密、可靠性、完整性校验、身份认证等	基于对称密钥算法、数据签名算法和哈希算法等进行改进	
	文献[15]方法	缺乏验证机制、加密功能	基于Shamir秘密共享协议和AES算法进行改进	
	文献[57]方法	缺乏身份认证、授权等	基于ECC的数据源认证	
	文献[58]方法	缺乏加密、身份认证等	基于NTRU加密验证	
	文献[59]方法	秘密身份验证信息泄露	基于历史数据的可扩展双因素身份验证	
	文献[60]方法	针对文献[59]方法的标签窃取攻击	基于历史数据的多因素认证和保密通道	
基于中间件的防护	Goproxy	缺乏加密、身份认证等	基于安全代理（软件型）	兼容性高，其中，软件型中间件具有易实施、适用范围广、成本低等优点，但是防护性能较低；硬件型中间件防护性能较高，但是成本也较高
	Goldy	缺乏加密	基于安全隧道（软件型）	
	文献[63]方法	缺乏敏感协议数据保护	基于可信硬件（硬件型）	
	文献[64]方法	缺乏敏感协议数据保护	基于可信硬件（硬件型）	
	文献[62]方法	缺乏机密性、完整性保护	基于可信硬件（硬件型）	

根本上解决工控协议的脆弱性问题。但是这种方法的改进空间较小，安全防护性能提升有限，通常需要协议运行机制同步改进。最重要的是，该方案可能对现有ICS的运行产生影响，主要适用于轻量级或新的ICS。

基于通信机制的防护主要针对工控协议的通信过程，利用加密、签名和身份认证等密码学技术来提升安全性。这种方法具有较大改进空间，能够更大限度地提高安全防护能力，但可能带来较高的性能开销，且需要考虑密钥安全管理、协议兼容性等问题。因此，该方法主要适用于对防护性能要求较高且设备资源充足的ICS，属于目前的研究热点。

鉴于工控协议的规范设计或通信机制的防护都对现有ICS的兼容性或工控设备性能提出一定要求，因此，基于中间件的防护具有更明显的优势。该方案以第三方角色为工控协议通信提供额外的安全层，不仅具有较高的兼容性，还不会额外占用过多工控设备的资源。其中，软件型中间件通常具有易实施、适用范围广、成本低等优点，但是防护性能较低，主要适用于防护要求低的ICS；硬件型中间件的防护性能通常较高，但是其成本也较高，主要适用于防护要求较高的ICS。此外，中间件自身也有可能成为攻击者的新目标，并为ICS引入新的安全风险。

5 未来展望

针对工控协议目前所面临的各种设计、实现脆弱性问题以及攻击威胁，尽管现有研究已经提出了相应的安全防护和漏洞挖掘技术，但是在工控协议的脆弱性检测、安全防护性能、漏洞挖掘效果与智能化等方面仍存在不足。因此，本文从以下5个要点对工控协议安全的未来发展进行展望。

1) 全面、专业的工控网络沙箱体系

目前，工控协议的脆弱性、安全防护性能等测试大多基于网络沙箱环境进行，然而现有的网络沙箱技术主要针对IT环境下的恶意攻击，未充分考虑工控协议与工控设备，尤其是难以模拟一些具有特殊功能的工控组件，导致这些网络沙箱技术无法高效检测工控协议的脆弱性问题以及专门针对ICS的恶意攻击。因此，结合工控协议、设备及组件的特点，开发能模拟真实工控网络环境的更全面、专业的工控网络沙箱体系，为工控协议及ICS的攻防演练与更深层次的安全性测试提供近乎真实的环境基础，将成为未来重要的研究方向之一。

2) 轻量级工控协议安全增强与加固技术

相比于互联网系统，ICS在系统、设备和协议等方面的更新迭代速度都相对较慢，尤其是早期的一些中大型ICS，依然运行着大量计算和存储资源相对有限的工控设备，并使用安全脆弱性问题较多的工控协议，从而更易遭受网络攻击，且危害较大。因此，借助资源更丰富、安全性更高的第三方硬件设备来提高现有工控协议安全防护技术的防护性能，或者基于资源有限的工控设备设计更加安全且轻量的工控协议安全防护方案，将是一个具有研究价值的方向。

3) 工控协议安全威胁感知与分析技术

随着工业网络开放程度的增加，ICS因其重要性正在遭受更加复杂的安全威胁。目前，工控协议的传统安全防护技术在硬件、软件等方面都远远落后于互联网协议，导致其更加难以抵抗复杂的安全威胁。因此，防护理念需要从被动防护转为主动防御，结合工控环境的特点，深化其他安全防护技术在工控协议安全领域的应用与结合。例如，利用态势感知、蜜罐等分析技术，基于协议深度解析及事件关联分析机制，分析工业互联网当前运行状态并预判未来安全走势，并在安全威胁出现时通过协同联动机制及时介入，阻止安全威胁的蔓延，进而提高对更加复杂、新颖的安全威胁的安全感知能力。此外，借鉴零信任安全架构的理念，提升工控协议通信在全域和全时的安全防护性能，也是目前亟须研究的方向。

4) 高效、精准的工控协议漏洞挖掘技术

目前，大多数工控协议漏洞挖掘工具都是基于理想环境探讨工控协议的漏洞挖掘，具有利用复杂度高、兼容性较差等缺点。在真实工控环境下，协议漏洞挖掘普遍面临目标更复杂、状态反馈更多样等问题。因此，利用静态符号执行、代码审计和模糊测试等技术，研制适用于真实工控环境下的高效、精准的工控协议漏洞挖掘工具，以提高工控协议漏洞挖掘的效率和准确度，是目前非常值得研究的一个方向。

5) 工控协议漏洞自动发现与智能修复技术

随着工业互联网的不断发展，工控协议变得更为复杂，这不仅体现在协议结构和种类上，还体现在报文响应频次和时效性等方面，这些因素加剧了潜在漏洞的复杂性、隐蔽性和难修复性，导致传统工控协议漏洞挖掘技术已经难以及时发现漏洞，进而影响漏洞修复的时效性和难度。因此，利用人工智能技术或者通过多个自动化漏洞挖掘工具的协同配合，再结合人工审核和测试以提高漏洞发现与修复的准确性，进而实现工控协议漏洞的自动发现与智能修复，这也是未来的一个研究热点。

6　结束语

由于早期工控环境的封闭性以及工控设备性能的局限性，大多数工控协议都侧重考虑基础功能性和可靠性等需求，而忽略了安全性需求，导致目前大量主流工控协议在设计和实现方面普遍存在较多的脆弱性问题。攻击者可以利用这些工控协议脆弱性问题对ICS展开各种网络攻击。因此，针对这些协议脆弱性与攻击等安全威胁，众多研究学者提出各种安全应对措施，如针对已知的工控协议脆弱性问题，分别从工控协议的规范设计、通信机制和中间件等角度制定相应的安全防护方案，同时针对未知的工控协议漏洞，利用静态符号执行、代码审计、模糊测试等技术进行深度挖掘。本文分别从工控协议的安全威胁、安全防护和漏洞挖掘3个方面进行深入分析，再对工控协议未来的发展趋势进行展望，以推进工控协议安全发展。

参考文献:

[1] 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.

[2] CONTI M, DONADEL D, TURRIN F. A survey on industrial control

system testbeds and datasets for security research[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2248-2294.

[3] ANTON S D D, FRAUNHOLZ D, KROHMER D, et al. The global state of security in industrial control systems: an empirical analysis of vulnerabilities around the world[J]. IEEE Internet of Things Journal, 2021, 8(24): 17525-17540.

[4] 方栋梁, 刘圃卓, 秦川, 等. 工业控制系统协议安全综述[J]. 计算机研究与发展, 2022, 59(5): 978-993.
FANG D L, LIU P Z, QIN C, et al. Survey of protocol security of industrial control system[J]. Journal of Computer Research and Development, 2022, 59(5): 978-993.

[5] VOLKOVA A, NIEDERMEIER M, BASMADJIAN R, et al. Security challenges in control network protocols: a survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(1): 619-639.

[6] JAVADPOUR A, SANGAIAH A K, JAFARI F, et al. Toward a secure industrial wireless body area network focusing MAC layer protocols: an analytical review[J]. IEEE Transactions on Industrial Informatics, 2023, 19(2): 2028-2038.

[7] MAJDALAWIEH M, PARISI-PRESICCE F, WIJESEKERA D. DNPSec: distributed network protocol version 3 (DNP3) security framework[C]// Advances in Computer，Information, and Systems Sciences, and Engineering. Berlin: Springer, 2007: 227-234.

[8] 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.

[9] 冯涛, 鲁晔, 方君丽. 工业以太网协议脆弱性与安全防护技术综述[J]. 通信学报, 2017, 38(S2): 185-196.
FENG T, LU Y, FANG J L. Research on vulnerability and security technology of industrial Ethernet protocol[J]. Journal on Communications, 2017, 38(S2): 185-196.

[10] ERDŐDI L, KALIYAR P, HOUMB S H, et al. Attacking power grid substations: an experiment demonstrating how to attack the SCADA protocol IEC 60870-5-104[C]//Proceedings of the 17th International Conference on Availability, Reliability and Security. New York: ACM Press, 2022: 1-10.

[11] EAST S, BUTTS J, PAPA M, et al. A taxonomy of attacks on the DNP3 protocol[C]//Critical Infrastructure Protection III: third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. Berlin: Springer, 2009: 67-81.

[12] RRUSHI J L. SCADA protocol vulnerabilities[M]. Berlin: Springer, 2012.

[13] FOVINO I N, CARCANO A, MASERA M, et al. Design and implementation of a secure modbus protocol[C]//International Conference on Critical Infrastructure Protection. Berlin: Springer, 2009: 83-96.

[14] SHAHZAD A, LEE M, LEE Y K, et al. Real time MODBUS transmissions and cryptography security designs and enhancements of protocol sensitive information[J]. Symmetry, 2015, 7(3): 1176-1210.

[15] ÁDÁMKÓ É, JAKABÓCZKI G, TAMÁS S P. Roposal of a secure modbus RTU communication with ADI Shamir's secret sharing method[J]. International Journal of Electronics and Telecommunications, 2018, 64(2): 107-114.

[16] NARDONE R, RODRÍGUEZ R J, MARRONE S. Formal security assessment of Modbus protocol[C]//Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). Piscataway: IEEE Press, 2016: 142-147.

[17] MAYNARD P, MCLAUGHLIN K, HABERLER B. Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks[C]//Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014. New York: ACM Press, 2014: 30-42.

[18] SCHWARZ M H, BÖRCSÖK J. A survey on OPC and OPC-UA: about the standard, developments and investigations[C]//Proceedings of the 2013 XXIV International Conference on Information, Communication and Automation Technologies (ICAT). Piscataway: IEEE Press, 2013: 1-6.

[19] PUYS M, POTET M L, LAFOURCADE P. Formal analysis of security properties on the OPC-UA SCADA protocol[C]//International Conference on Computer Safety, Reliability, and Security. Berlin: Springer, 2016: 67-75.

[20] BIHAM E, BITAN S, CARMEL A, et al. Rogue7: rogue engineering-station attacks on S7 simatic PLCs[C]//Conference of. Black Hat 2019. San Francisco: CMP, 2019: 1-21.

[21] KALLE S, AMEEN N, YOO H, et al. CLIK on PLCs! attacking control logic with decompilation and virtual PLC[C]//Proceedings 2019 Workshop on Binary Analysis Research. Reston: Internet Society, 2019: 1-12.

[22] 董一帆, 熊荫乔, 王宝耀. 智能电网通信协议安全威胁与防御技术[J]. 计算机技术与发展, 2019, 29(2): 1-6.
DONG Y F, XIONG Y Q, WANG B Y. Security threat and defense technology of smart grid communication protocol[J]. Computer Technology and Development, 2019, 29(2): 1-6.

[23] SUN Y, LI Z, LYU S C, et al. Spenny: extensive ICS protocol reverse analysis via field guided symbolic execution[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 4502-4518.

[24] LI Y, WU S H, PAN Q. Network security in the industrial control system: a survey[J]. arXiv Preprint, arXiv: 2308.03478, 2023.

[25] KANG B, MAYNARD P, MCLAUGHLIN K, et al. Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations[C]//Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). Piscataway: IEEE Press, 2015: 1-8.

[26] KELLI V, RADOGLOU-GRAMMATIKIS P, LAGKAS T, et al. Risk analysis of DNP3 attacks[C]//Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR). Piscataway: IEEE Press, 2022: 351-356.

[27] HOYOS J, DEHUS M, BROWN T X. Exploiting the GOOSE protocol: a practical attack on cyber-infrastructure[C]//Proceedings of the 2012 IEEE Globecom Workshops. Piscataway: IEEE Press, 2012: 1508-1513.

[28] MERXELL B, FORNER E. Out of control: demostrasting scada exploitation[C]//Conference of Black Hat 2013. San Francisco: CMP, 2013: 1-7.

[29] CHAU S Y, CHOWDHURY O, HOQUE E, et al. SymCerts: practical symbolic execution for exposing noncompliance in X.509 certificate validation implementations[C]//Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2017:

503-520.

[30] CORIN R, MANZANO F A. Efficient symbolic execution for analysing cryptographic protocol implementations[C]// International Symposium on Engineering Secure Software and Systems. Berlin: Springer, 2011: 58-72.

[31] SONG J, CADAR C, PIETZUCH P. SymbexNet: testing network protocol implementations with symbolic execution and rule-based specifications[J]. IEEE Transactions on Software Engineering, 2014, 40(7): 695-709.

[32] CHO C Y, BABI D, POOSANKAM P, et al. MACE: model-inference-assisted concolic exploration for protocol and vulnerability discovery[C]// 20th USENIX Security Symposium (USENIX Security 11). Berkeley: USENIX Association, 2011: 1-16.

[33] ZHANG X L, ZHU Y F, GU C X, et al. Security protocol code analysis method combining model learning and symbolic execution[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 93-104.

[34] 谢肖飞, 李晓红, 陈翔, 等. 基于符号执行与模糊测试的混合测试方法[J]. 软件学报, 2019, 30(10): 3071-3089.
XIE X F, LI X H, CHEN X, et al. Hybrid testing based on symbolic execution and fuzzing[J]. Journal of Software, 2019, 30(10): 3071-3089.

[35] RODRÍGUEZ R J, MARRONE S, MARCOS I, et al. MOSTO: a toolkit to facilitate security auditing of ICS devices using modbus/TCP[J]. Computers & Security, 2023, 132: 1-12.

[36] 杜江, 罗权. 基于代码审计技术的OpenSSL脆弱性分析[J]. 计算机系统应用, 2017, 26(9): 253-258.
DU J, LUO Q. Vulnerability analysis of OpenSSL based on code audit technology[J]. Computer Systems & Applications, 2017, 26(9): 253-258.

[37] TANG G G, MENG L X, WANG H Q, et al. A comparative study of neural network techniques for automatic software vulnerability detection[C]//Proceedings of the 2020 International Symposium on Theoretical Aspects of Software Engineering (TASE). Piscataway: IEEE Press, 2020: 1-8.

[38] LEE H R, SHIN S H, CHOI K H, et al. Detecting the vulnerability of software with cyclic behavior using Sulley[C]//Proceedings of the 2011 7th International Conference on Advanced Information Management and Service (ICIPM). Piscataway: IEEE Press, 2011: 83-88.

[39] TACLIAD F, NGUYEN T D, GONDREE M. DoS exploitation of Allen-Bradley's legacy protocol through fuzz testing[C]//Proceedings of the 3rd Annual Industrial Control System Security Workshop. New York: ACM Press, 2017: 24-31.

[40] BRATUS S, HANSEN A, SHUBINA A. LZfuzz: a fast compression-based fuzzer for poorly documented protocols[J]. Computer Science, 2008, 9(1): 1-22.

[41] VOYIATZIS A G, KATSIGIANNIS K, KOUBIAS S. A modbus/TCP fuzzer for testing internetworked industrial systems[C]//Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). Piscataway: IEEE Press, 2015: 1-6.

[42] TACLIAD F. ENIP fuzz: a scapy-based EtherNet/IP fuzzer for security testing[D]. California: Naval Postgraduate School (Monterey), 2016.

[43] NIEDERMAIER M, FISCHER F, VON B A. PropFuzz—an IT-security fuzzing framework for proprietary ICS protocols[C]//Proceedings of the 2017 International Conference on Applied Electronics (AE). Piscataway: IEEE Press, 2017: 1-4.

[44] HU Z C, SHI J Q, HUANG Y H, et al. GANFuzz: a GAN-based industrial network protocol fuzzing framework[C]//Proceedings of the Proceedings of the 15th ACM International Conference on Computing Frontiers. New York: ACM Press, 2018: 138-145.

[45] ZHAO H, LI Z H, WEI H S, et al. SeqFuzzer: an industrial protocol fuzzing framework from a deep learning perspective[C]//Proceedings of the 2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST). Piscataway: IEEE Press, 2019: 59-67.

[46] BYTES A, RAJPUT P H N, DOUMANIDIS C, et al. FieldFuzz: in situ blackbox fuzzing of proprietary industrial automation runtimes via the network[C]//Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. New York: ACM Press, 2023: 499-512.

[47] YU X J, WU Y B, ZHANG Y Q. Research on the design of cloud security architecture[J]. Netinfo Security, 2020, 20(9): 62-66.

[48] EDDINGTON M. Peach fuzzing platform[J]. Peach Fuzzer, 2011, 34: 32-43.

[49] LUO Z X, ZUO F L, SHEN Y H, et al. ICS protocol fuzzing: coverage guided packet crack and generation[C]//Proceedings of the 2020 57th ACM/IEEE Design Automation Conference (DAC). Piscataway: IEEE Press, 2020: 1-6.

[50] PHAM V T, BÖHME M, ROYCHOUDHURY A. AFLNet: a greybox fuzzer for network protocols[C]//Proceedings of the 2020 IEEE 13th International Conference on Software Testing, Validation and Verification (ICST). Piscataway: IEEE Press, 2020: 460-465.

[51] BA J S, MARCEL B, ZAHRA M, et al. Stateful greybox fuzzing[C]// 31st USENIX Security Symposium (USENIX Security 22). Berkeley: USENIX Association, 2022: 3255-3272.

[52] YU Z H, WANG H L, WANG D, et al. CGFuzzer: a fuzzing approach based on coverage-guided generative adversarial networks for industrial IoT protocols[J]. IEEE Internet of Things Journal, 2022, 9(21): 21607-21619.

[53] AL-SHAREEDA M A, MANICKAM S, LAGHARI S A, et al. Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications[J]. Sustainability, 2022, 14 (23): 1-15.

[54] WANG F, WU J, NAN Y, et al. ProFactory: improving IoT Security via formalized protocol customization[C]//31st USENIX Security Symposium (USENIX Security 22). Berkeley: USENIX Association, 2022: 3879-3896.

[55] 闫爽. 智能电网DNP3协议安全机制研究与实现[D]. 长沙: 国防科学技术大学, 2016.
YAN S. The research and implementation of security mechanism for smart grid DNP3[D]. Changsha: National University of Defense Technology, 2016.

[56] LUO X, LI Y Z. Research and implementation of modbus TCP security enhancement protocol[J]. Journal of Physics: Conference Series, 2019, 1213(5): 1-12.

[57] LU X, WANG W Y, MA J F. Authentication and integrity in the smart grid: an empirical study in substation automation systems[J]. International Journal of Distributed Sensor Networks, 2012, 8(6): 1-17.

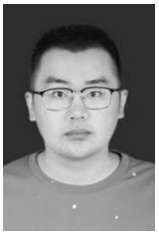
[58] PREMNATH A P, JO J Y, KIM Y. Application of NTRU cryptographic algorithm for SCADA security[C]//Proceedings of the 2014 11th International Conference on Information Technology: New Generations. Piscataway: IEEE Press, 2014: 341-346.

[59] CHAN A C F, WONG J W, ZHOU J, et al. Scalable two-factor authentication using historical data[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2016: 91-110.
[60] JIN C L, YANG Z, XIANG T, et al. HMACCE: establishing authenticated and confidential channel from historical data for industrial Internet of things[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 1080-1094.
[61] MIYAZAWA H. A latency-aware container scheduling in edge cloud computing environment[C]//Proceedings of the 2023 Congress in Computer Science, Computer Engineering & Applied Computing (CSCE). Piscataway: IEEE Press, 2023: 1728-1731.
[62] ZHAN M Q, LI Y, YU G X, et al. GuardBox: a high-performance middlebox providing confidentiality and integrity for packets[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2413-2426.
[63] PODDAR R, LAN C, POPA R A, et al. SafeBricks: shielding network functions in the cloud[C]//Proceedings of the 15th USENIX Conference on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2018: 201-216.
[64] DUAN H Y, WANG C, YUAN X L, et al. LightBox: full-stack protected stateful middlebox at lightning speed[C]//Proceedings of the Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 2351-2367.

[作者简介]

黄涛（1988– ），男，江苏扬州人，南京理工大学博士生，主要研究方向为工控系统安全和协议逆向等。

王郅伟（2000– ），男，河南信阳人，中国科学院大学博士生，主要研究方向为工控协议模糊测试、APT攻击与防御技术等。



刘家池（2000– ），男，河南安阳人，南京理工大学硕士生，主要研究方向为工控协议安全和协议逆向等。

龙千禧（2000– ），女，湖北咸宁人，南京理工大学硕士生，主要研究方向为工控系统安全和协议逆向等。

况博裕（1994– ），男，四川绵阳人，南京理工大学在站博士后，主要研究方向为物联网安全和隐私保护等。

付安民（1981– ），男，湖北通城人，博士，南京理工大学教授、博士生导师，主要研究方向为物联网安全、密码学和隐私保护等。

张玉清（1966– ），男，陕西宝鸡人，博士，中国科学院大学博士生导师，主要研究方向为网络攻防与系统安全、大数据与智能安全、物联网系统安全。