基于蜜罐的新能源工控协议模糊识别分析*

田学成[1]，赵　谦[1,2]，罗　谢[3]，陈燕峰[1]

（1. 国电南京自动化股份有限公司，江苏　南京　211100；
2. 南京理工大学　网络空间安全学院，江苏　南京　210094；
3. 华电金沙江上游水电开发有限公司，四川　成都　610041）

摘　要：新能源行业是国家可再生能源发展的重要领域，在新能源工业控制系统网络安全研究中需要快速确认工控协议存在的缺陷。分析了新能源风电工业控制系统存在的安全风险问题，实现了基于蜜罐轻量级部署 Modbus 协议，使用模糊测试的方法对协议的安全属性快速测试并进行分析。该研究对新能源工控协议安全发展有重要研究意义。

关键词：工控协议；蜜罐；模糊测试；工控安全

中图分类号：TN915. 08；TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2024. 06. 003

引用格式：田学成，赵谦，罗谢，等. 基于蜜罐的新能源工控协议模糊识别分析［J］. 网络安全与数据治理，2024，43(6)：16 - 22.

Fuzzy identification analysis of new energy industrial control protocol based on honeypot

Tian Xuecheng[1]，Zhao Qian[1,2]，Luo Xie[3]，Chen Yanfeng[1]

（1. Guodian Nanjing Automation Co.，Ltd.，Nanjing 211100，China；
2. School of Cyber Science and Engineering，Nanjing University of Science and Technology，Nanjing 210094，China；
3. Huadian Jinsha River Upstream Hydropower Development Co.，Ltd.，Chengdu 610041，China）

Abstract：The new energy industry is a crucial sector for the advancement of national renewable energy. In the network security research of new energy industrial control systems，it is essential to promptly identify the vulnerabilities in industrial control protocols. This paper examines the security risks present in the new energy wind power industrial control system，deploys the Modbus protocol based on honeypots in a lightweight manner，using the fuzz testing method to quickly test and analyze the security attributes of the protocol. It has important research significance for the security development of new energy industrial control protocols.

Key words：ICS protocol；honeypot；fuzz testing；ICS security

0　引言

随着信息化和工业化的深度融合，新能源风电系统面临越来越多的威胁和挑战。新能源风力发电作为一种分散的能源结构，除了需要应对工控主机和服务的漏洞，还要应对自然灾害引起的物理破坏，未来还面临工控协议的安全威胁。

目前在工控协议安全分析方法上主要有协议的形式化安全分析和基于固件的逆向分析，以及协议的模糊测试方法。其中形式化安全分析只能分析已公开协议规范的工控协议，且因分析工具性能存在差异，导致分析结果存在误差。基于固件的逆向分析对于有加密机制的工控协议很难准确还原协议结构，对于研究分析工控协议的单个具体安全属性并不适用。

本文分析了新能源风电系统的网络安全现状，通过在蜜罐系统上部署轻量级工控协议进行单个协议安全属性的模糊测试，分析了协议的安全属性缺陷，这有助于新能源工控协议高效率分析，且对工控蜜罐的隐藏有重要意义。

*基金项目：江苏省科技成果转化项目（BA 2022011）

1 风电系统网络安全现状

1.1 新能源风电系统概况

我国新能源风力发电系统有独立型风力发电和并网型风力发电两种。其中独立型风力发电规模单机容量10 kW左右，用于解决偏远地区供电；并网型风力发电接入电力系统运行，单机容量在几百KW到MW级别，规模较大且系统安全性要求更高[1]。

目前新能源风电在控制方式上采用四级控制，分别是现场侧、场站侧、集控侧、总控侧。其中现场侧主要包括风机主控系统以及各种PLC和传感器等，边缘控制系统使用了大量的工控协议，如Modbus、DNP3[2]等。工业控制系统重点强调系统的可用性和完整性，在设计之初忽略了安全方面的要求。在现有的新能源集控防护体系中，普遍存在着安全防护措施单一、网络设备资产分散、安全态势监测与预警很难全覆盖、精准防护无法实现等系列问题，尤其在工控协议身份认证、控制指令等关键数据防窃取和防篡改、重要控制类操作指令抗抵赖、通信加密使用等方面没有全备的安全机制，导致新能源风电系统的安全隐患被更多地暴露出来。随着信息化和工业化融合加快投入，实现新能源风电系统网络安全自主化关乎国家电力系统安全。图1是新能源风机控制系统拓扑图。

新能源风力发电现场侧风机主控系统使用了多种控制设备和信号采集设备，导致通信协议在跨地域通信方面面临着诸多安全挑战。攻击者通过边缘网络对新能源系统发起攻击，可对新能源风力发电系统造成严重危害。

1.2 新能源风电系统安全评估现状

等级保护制度是国家提出的关键基础设施保护方案，提供了一种评估新能源系统安全性的框架和方法，可以识别系统的关键资源、威胁和风险，并制定相应的防御措施和应急方案，为新能源系统提供安全防护意见和控制措施的指导，以减轻潜在的威胁和风险[3]。等级保护制度要求建立适当的监测和响应能力，包括入侵检测、安全事件响应和恢复机制等，有助于及时发现和应对网络安全事件，减少对新能源风电系统的损害。新能源风电系统在安全建设和运维以及评估上总体遵循《电力二次系统安全防护规定》（电监会5号令）提出的“安全分区、网络专用、横向隔离、纵向认证”原则[4]，由于新能源风电系统的特殊性，在实际安全评估方面还存在一定的不足，如表1所示。

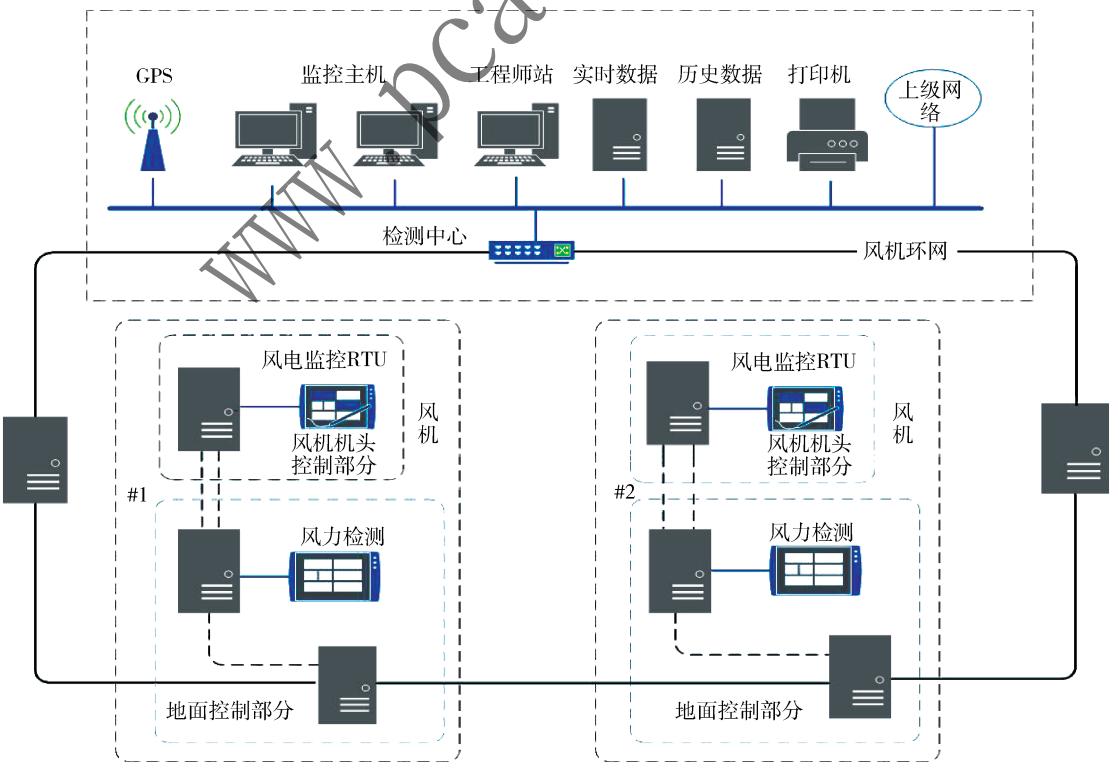

图1 风电场风机控制系统拓扑图

表 1　安全评估不足表现

不足处	具体表现
动态适应性	应对不断演变的安全威胁和攻击技术，可能存在无法及时适应新出现的威胁和漏洞，导致系统在面对新的攻击时缺乏足够的防护能力
检测溯源	较少关注攻击的检测和响应能力，检测和追踪溯源能力不强，对于高级隐蔽的攻击可能无法提供足够的防御能力
人为因素	很大程度上依赖于测评人员的正确理解、遵守和执行，可能存在制度的执行不到位或出现安全检测疏忽
内部威胁	系统内部威胁防御不足，如内部人员的恶意行为或误操作可能绕过具体的防御机制，引发系统安全风险
灵活性扩展	新能源系统存在一定的差别，面对新技术、新业务需求或扩展系统规模时缺乏足够的灵活性和可扩展性
成本和复杂性	新能源系统安全维护复杂、投入大，需要专业的安全人员投入时间和资源来维护和更新防护策略
静态评估	安全评估很难完全预测和适应动态的安全威胁和攻击技术的变化，需要与其他安全机制结合使用

1.3　新能源风电系统安全隐患

大规模的风电、光伏新能源并网后接入电网替代了常规同步机组的发电空间，降低电网系统惯量，在出现故障导致系统频率波动时，极易发生新能源机组大面积脱网事件，引发电力事故，因此需加强对新能源出力占比及系统惯量的监视，确保新能源系统惯量足够，保障电网安全[5]。

2015 年乌克兰伊万诺-弗兰科夫斯克地区电力监控系统遭到“BlackEnergy”恶意代码攻击，攻击者入侵了监控管理系统，导致变电站故障，进而导致大面积停电[6]，引发了各国对电力系统关键基础设施网络安全的高度重视。新能源风电风机主控设备使用 Modbus、DNP3 等控制协议实现风机转舵、收桨等动作。其中 Modbus 协议存在身份认证缺失和明文传输等问题，攻击者通过重放控制指令改变风机运行状态或造成反复启停。大型新能源风电场一旦遭到网络攻击将严重影响大电网的安全。

目前国内工控设备厂家如信捷、汇川、和利时、南大奥拓等相继研发了自己的 PLC 终端控制设备，在产品和市场等层面均取得了显著成果，但仍然大面积依托国外工控协议，使得工控设备依旧存在协议安全引发的威胁[7]。图 2 是某国产 PLC 控制设备的攻击场景，场站侧工程师站下发风机控制指令，依次通过四个节点最终到达风机通信接收端，实现风机启停操作。攻击者可以在接口机和风机主控之间通过部署嵌入式通信设备窃听通信数据。

通过对攻击场景的分析结合实际风电场面临的网络安全问题，本文从不同层面总结了新能源风电系统面临的网络安全隐患，如表 2 所示。

表 2　新能源风电系统面临的安全威胁

威胁类型	具体表现
工控协议漏洞	新能源风电系统使用的工控协议如 Modbus、DNP3 等存在安全隐患，很多工控协议受控于国外技术，缺乏安全防护措施，增加了系统安全风险
供应链攻击	新能源风电系统的供应链环节中存在一定风险，攻击者可能在供应链中引入风险，从而对新能源风电系统进行攻击或渗透
社会工程	通过社会工程技术、钓鱼邮件等方式诱骗系统用户提供敏感信息，从而获取对系统的访问权限或窃取关键信息
媒介攻击	监控系统数据通过公网传输，攻击者可以利用网络漏洞对系统进行攻击、干扰或操纵
身份认证与访问控制	访问控制和身份认证的不足可能导致未经授权的人员或设备进入系统，从而进行恶意活动、篡改数据或破坏系统功能
远程访问漏洞	远程访问接口的安全性不足或配置错误可能使系统易受攻击
物理安全	风机监控不到位可能使之受到物理攻击的威胁，从而对电力系统的正常运行和供电造成影响

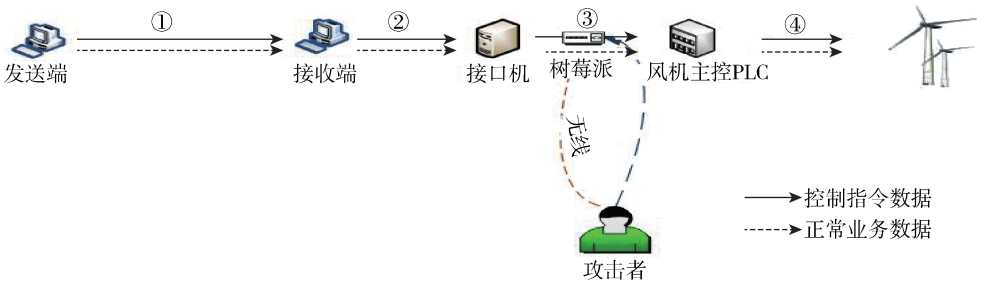

图 2　新能源风电边缘网络攻击场景

2 新能源风电系统蜜罐

2.1 新能源风电系统蜜罐特点

随着网络攻击对抗态势逐渐升级，传统的单向边界防御技术愈发不能满足新能源风电系统应对高级未知危险的防御需求，蜜罐技术的出现及其日益成熟的安全技术发展改变了这个被动的防御局面，然而传统蜜罐存在很多缺点，如不具有高交互性、缺少具体工控业务仿真场景、工控协议未开发部署等，并不适用于新能源风电系统。

新能源风电系统蜜罐被设计为模拟真实的新能源风电系统环境，包括逆变器、发电控制器、风机主控 PLC 等设备，并模拟其行为和功能，实现具体 PLC 的工控协议。这使得蜜罐能够吸引攻击者，并使之相信自己正在攻击真实的工控系统。借此蜜罐可收集到关于攻击行为和策略的信息。

新能源风电系统蜜罐内置了安全监测和响应机制，能够实时监测攻击行为、异常活动和潜在威胁，生成告警或触发响应机制，收集有关攻击方法、技术和工具的信息，提高系统的安全性。利用采集到的攻击者与蜜罐之间的通信、交互和数据流量等信息，进一步开展安全分析和研究，从而识别攻击模式、漏洞利用方式和新的安全威胁。最后通过对新能源风电系统蜜罐的运行和攻击数据的分析，安全团队可以不断学习和改进防御策略，提高系统的安全性，加强对潜在攻击的防范能力。图 3 是一种新能源风电蜜罐部署拓扑。

2.2 新能源风电系统低交互蜜罐和高交互蜜罐

一般情况下，低交互蜜罐用来模拟新能源风电系统网络服务，容易部署且风险较小，但攻击者在低交互蜜罐中能够执行的攻击活动有限，通过低交互蜜罐收集的信息也很少。而高交互蜜罐能够提供更加真实的新能源系统业务，攻击者很难发现模拟痕迹，因此在高交互蜜罐中，能够对攻击者做详细的画像，这对新能源风电系统的安全研究具有重要意义。

（1）低交互蜜罐

低交互蜜罐是一种部署简单、资源占用较低的蜜罐。它们通常模拟一些特定的服务或协议，以吸引攻击者与其进行交互。低交互蜜罐提供有限的功能和模拟服务，通常只模拟目标系统的一部分功能，以限制攻击者与蜜罐的交互程度。如 Conpot、Artillery、GasPot、SCADASim 等，可以模拟某些工控服务端口，但功能通常是受限的，不提供完整的协议通信过程。

Conpot 是工业控制系统低交互蜜罐，模拟具有 Modbus 和 S7comm 协议的西门子 SIMATIC S7 - 200 PLC。传统蜜罐技术对植入性攻击的检测能力较有限，体现在蜜罐对于植入攻击的识别输出较少，以及真实工控协议对工控植入攻击防御能力弱等方面[8]。

（2）高交互蜜罐

高交互蜜罐提供了丰富完整的协议通信，与真实控制设备更接近，可以模拟目标协议的认证、请求、响应、会话过程，提供更高程度的交互。通过记录攻击者的行为和策略，如漏洞利用、命令执行、数据传输等，高交互蜜罐可得到更详细的攻击数据和情报，帮助分析对新能源风电系统造成的危害。

DemonTrace 是一款工业控制系统高交互蜜罐，支持 S7comm、Modbus、BACnet、IEC104、DNP3、HTTP 等协议，可与攻击者进行深度交互，能够模拟真实 PLC 回复攻击者的每一次数据请求，诱导攻击者由低级别的扫描到发起高级别的网络攻击[9]。

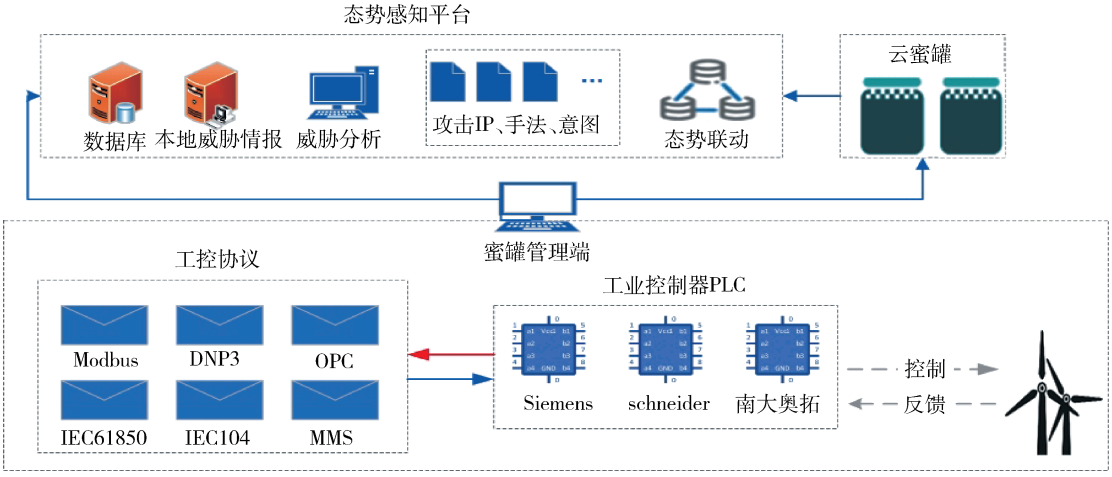

图 3 新能源风电轻量级蜜罐部署拓扑

亚利桑那州立大学网络安全实验室提出的下一代工控蜜罐 Honeyplc 的设计模型，基于开源的 S7 协议通信库 Snap7，Honeyplc 分析工具可以定制，按照需求修改具体 PLC 版本信息，以支持不同品牌和型号的 PLC 设备[10]。

蜜罐遭受攻击可能会失陷，攻击者通过蜜罐网络进而攻击真实的工业控制系统，在蜜罐防御上主要通过将蜜罐部署在云服务器上以避免失陷带来的危害。

在蜜罐系统上研究工控协议的安全性，帮助开发者改进协议安全属性，同时调整新能源风电系统防护策略，能够抵御攻击者轻易地识别工控特征，从而提高蜜罐的隐秘性。本文基于轻量级蜜罐 Conpot 对 Modbus 协议进行模糊安全测试和分析。

3 新能源风电系统工控协议模糊测试

3.1 传统 Fuzzing 测试存在的缺点

Fuzzing 测试称为模糊测试，使用大量构造的数据作为目标程序的输入，通过检测程序出现的异常来发现潜在漏洞[11]。Fuzzing 测试技术应用在工控软硬件的脆弱性分析是当前工控安全领域的重要研究方向，传统的 Fuzzing 测试技术应用于工控系统的测试时，存在未考虑协议交互状态，测试的覆盖率和交互性以及异常监控手段受限等问题，并且很难测试嵌入式的工控设备。协议模糊测试产生误报的主要原因是针对协议安全属性的测试数据覆盖率过大，需要在测试过程中动态调整测试范围，对比输出结果，筛选真实可靠的数据[12]。

工控设备协议模糊测试包括协议解析、测试用例生成、异常捕获和定位三个步骤。协议解析是通过公开的协议规范资料或者对网络数据流量抓包分析，分析待测协议的层次、字段构成、会话过程等信息；测试用例生成是依据上阶段整理出来的字段结构，采用变异的方式生成畸形测试用例发送给待测对象；异常捕获和定位的目的是通过多种探测手段发现由测试用例触发的异常，保存异常相关数据信息，为后续异常的定位和重现提供依据。

3.2 基于 Modbus 协议的 Fuzzing 测试

新能源风电风机主控系统使用的 Modbus 是一种常用的串行通信协议，用于工业自动化和监控系统中的设备通信。在新能源领域 Modbus 常用于逆变器、发电控制器等设备之间的通信。对新能源风电风机主控使用的 Modbus 协议进行模糊测试，有助于发现潜在的安全隐患。

Modbus 协议包括了 TCP、RTU 和 ASCII 三种模式，Modbus ASCII 主要用于传输少量的文本格式数据，Modbus RTU 主要用于传输大量的二进制数据。本文模糊测试基于 Modbus TCP 以太网的数据传输方式进行研究[13]。Modbus 协议的 PLC 从设备每个寄存器内最多存取 250 个字节，超过容量大小的数据包读写操作需要通过多个通信包进行回复。传统蜜罐往往不考虑这个问题。表 3 和表 4 是 Modbus 协议报文 MBAP 结构和对应字段的功能。

表 3 MBAP 报文头结构

事务处理标识	协议标识	长度	单元标识（设备标识）
2 B	2 B	2 B	1 B

表 4 MBAP 报头域对应功能

域	长度/B	描述	客户机	服务器（从设备）
事务元标识符	2	MODBUS 请求/响应事务处理的识别码	客户机启动	服务器从接收的请求中重新复制
协议标识符	2	00 00	客户机启动	服务器从接收的请求中重新复制
长度	2	字节数量	客户机启动请求	服务器（响应）启动
单元标识符	1	串行链路或其他总线上连接的远程从站的识别码	客户机启动	服务器从接收的请求中重新复制

以国产化 PLC 为例，测试 Modbus/TCP 协议，模糊测试引入了 Fuzzowski 测试框架，构造 Modbus/TCP 数据包格式如下：

```
modbus_data = bytearray()
modbus_data.extend(transaction_id.to_bytes(2, byteorder='big'))
modbus_data.extend(b'\x00\x00')
modbus_data.extend((len(data)+2).to_bytes(2, byteorder='big'))
modbus_data.extend(unit_id.to_bytes(1, byteorder='big'))
modbus_data.append(function_code)
modbus_data.extend(data)
```

指定 Modbus 协议标识符为 0x0000，生成模糊测试数据包，每次发送 20 个模糊数据包，生成随机的事务标识符、单元标识符、功能码、数据长度以及数据域内容，构造 Modbus/TCP 数据包发送给模拟的下位机，记录通信报文，检测异常的反馈信息。

```
for_ in range(20):
transaction_id = random.randint(0, 65535)
unit_id = random.randint(0, 255)
```

```
function_code = random.randint(0, 255)
data_length = random.randint(0, 10)
data = bytes(random.randint(0, 255) for_ in range(data_length))
modbus_data = bytearray()
modbus_data.extend(transaction_id.to_bytes(2, byteorder='big'))
modbus_data.extend(b'\x00\x00')
```

表 5 是根据模糊测试生成的测试用例请求 Modbus 从设备得到的具体通信数据报文，根据通信报文分析 Modbus 从设备响应异常。

检测发现 Modbus 通信流量异常，上位机 IP 执行密集读写和探索操作，上位机通过 0x01 读线圈状态、0x03 读保持寄存器、0x04 读输入寄存器等命令执行 PLC 寄存器 ID 全偏移量遍历读取，Modbus 协议存在功能码滥用、通信报文明文传输安全漏洞。模糊测试只针对设计的测试范围，需要全方位对协议的安全属性进行测试，可以有针对性地设计模糊测试的数据域。

表 5 模糊测试请求响应数据包

模糊测试构造请求数据（Rx）	Slave 模拟设备响应数据（Tx）
45 E1 00 00 00 08 A0 98 21 6D 0A AD 51 6D	45 E1 00 00 00 03 A0 18 01
3A C4 00 00 00 02 C5 53	3A C4 00 00 00 03 C5 D3 01
59 91 00 00 00 09 52 A0 56 24 94 08 88 56 97	59 91 00 00 00 03 52 20 01
73 73 00 00 00 02 30 D5	73 73 00 00 00 03 30 55 01
7F F0 00 00 00 03 81 27 06	7F F0 00 00 00 03 81 A7 01
9F A0 00 00 00 02 C0 51	9F A0 00 00 00 03 C0 D1 01
06 8F 00 00 00 04 76 CB 52 58	06 8F 00 00 00 03 76 4B 01
48 B7 00 00 00 05 45 09 C8 99 35	48 B7 00 00 00 03 45 89 01
1C 02 00 00 00 07 97 93 6C B7 9A FE 5F	1C 02 00 00 00 03 97 13 01
A9 F1 00 00 00 09 69 C7 8B 9E A1 43 A4 87 3D	A9 F1 00 00 00 03 69 47 01
26 BF 00 00 00 05 1D B1 84 E5 5B	26 BF 00 00 00 03 1D 31 01
98 AB 00 00 00 0A D2 42 89 60 AB 27 37 EB 84 EF	98 AB 00 00 00 03 D2 C2 01
34 73 00 00 00 03 02 F4 4D	34 73 00 00 00 03 02 74 01
4B B1 00 00 00 03 FA BE 28	4B B1 00 00 00 03 FA 3E 01
90 F9 00 00 00 0B 6E 1B 07 5C 0D 7F CC 81 57 2A A8	90 F9 00 00 00 03 6E 9B 01
AF A4 00 00 00 07 27 EE 41 77 D1 E1 10	AF A4 00 00 00 03 27 6E 01
7E 07 00 00 00 09 2F F0 BB FE 98 19 8B A5 11	7E 07 00 00 00 03 2F 70 01
FB 3D 00 00 00 05 26 13 73 77 B2	FB 3D 00 00 00 03 26 93 01
98 CC 00 00 00 08 23 F4 8A A2 8F 6E 09 DD	98 CC 00 00 00 03 23 74 01
88 A8 00 00 00 09 63 AA 03 FD 82 BD 73 FB AB	88 A8 00 00 00 03 63 2A 01

4 结论

本文分析总结了新能源风电系统安全防护现状和存在的安全缺陷以及未来面临的防御挑战，指出了等级保护在实际安全评估方面的不足之处，介绍了传统的蜜罐研究情况，设计了基于新能源风电系统工控协议研究的蜜罐部署方案，根据 Modbus 协议规范，针对具体安全属性设计了模糊测试方法，通过协议模糊测试分析验证了协议的安全属性问题。新能源工业控制系统中还存在其他广泛的工控协议，通过在蜜罐上快速部署协议进行测试，可加强工控设备的安全防护。这对未来新能源工控安全的研究提供了参考方法。

参考文献

[1] 高靖怡，翁汉琍，林湘宁，等. 全功率型逆变电源侧工频变化量距离保护性能下降机理分析［J/OL］. 电力自动化设备：1－13［2024－03－16］. http://doi.org/10.16081/j.epae.202403002.

[2] 田学成，张五一，江楠，等. 基于 Modbus 协议新能源风电网络通信安全研究［J］. 网络安全与数据治理，2022，41

(8)：61－67.

[3] 余勇，林为民. 基于等级保护的电力信息安全监控系统的设计［J］. 计算机科学，2012，39（S3）：440－442.

[4] 周劼英，张晓，邵立嵩，等. 新型电力系统网络安全防护挑战与展望［J］. 电力系统自动化，2023，47（8）：15－24.

[5] 蔡葆锐，曾丕江，何金定，等. 考虑频率安全约束的云南电网新能源运行边界研究［J］. 云南电力技术，2021，49（5）：17－22.

[6] 杨挺，许哲铭，赵英杰，等. 数字化新型电力系统攻击与防御方法研究综述［J］. 电力系统自动化，2024，48（6）：112－126.

[7] 林浩，杨政厚，霍玉鲜. 国产 PLC 发展现状及展望［J］. 电子技术应用，2023，49（4）：21－27.

[8] MAESSCHALCK S，GIOTSAS V，RACE N. World wide ICS honeypots：a study into the deployment of conpot honeypots［C］// Industrial Control System Security Workshop，2021.

[9] ACKERMAN P. Industrial cybersecurity：efficiently secure critical infrastructure systems［M］. Packt Publishing Ltd，2017：23－56.

[10] LÓPEZ-MORALES E，RUBIO-MEDRANO C，DOUPÉ A，et al. Honeyplc：a next－generation honeypot for industrial control systems［C］//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security，2020：279－291.

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

[12] 张强. 面向工控协议的模糊测试用例生成方法研究［D］. 北京：北京石油化工学院，2023.

[13] RAHMAN A，MUSTAFA G，KHAN A Q，et al. Launch of denial of service attacks on the Modbus/TCP protocol and development of its protection mechanisms［J］. International Journal of Critical Infrastructure Protection，2022，39：100568.

（收稿日期：2024－03－16）

作者简介：

田学成（1991－），男，硕士，工程师，主要研究方向：网络安全、电网工控安全。

赵谦（1985－），男，博士研究生，正高级工程师，主要研究方向：电力工控系统、网络与信息安全。

罗谢（1965－），男，本科，高级工程师，主要研究方向：网络安全及信息化项目规划设计。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部