一种基于模糊测试的智能变电站工业控制系统漏洞挖掘方法

姚保明，王紫琦，徐　益，杜江龙

（国网江西省电力有限公司鹰潭供电分公司，江西 鹰潭 335000）

摘　要：随着电网信息化、智能化发展，传统的变电站已不断向智能变电站转变。在变电站的各类技术智能化过程中，智能变电站监控系统面临的安全风险日益增加。网络攻击可能深入到智能电网内部，对智能设施、数据传输安全造成巨大破坏。对智能变电站的各类系统进行渗透测试（Fuzz Testing），以便快速发现其存在的潜在风险显得尤为重要。文中介绍了基于模糊测试的智能变电站工业控制系统漏洞挖掘方法，对智能变电站监控系统进行模糊测试，发现潜在隐患，实现对设备的安全、有效评估，从而加强生产现场的安全管理工作，保证智能变电站系统的安全运行。

关键词：智能变电站；模糊测试；漏洞挖掘；协议栈稳定性

中图分类号：TM 631　　**文献标志码：**B　　**文章编号：**1006-348X（2025）02-0048-04

0　引言

智能变电站技术随着智能电网概念的出现而兴起。由于以往的常规变电站和数字化变电站已经无法适应社会发展的新趋势，不能满足智能电网的新要求，未来的电网发展趋势一定是更趋于智能化。因此，智能变电站作为智能电网的重要环节，在电网运行中处于核心地位。

随着智能化程度的提高，智能变电站网络面临的信息安全形势也越加严峻。尽管智能变电站网络系统相对于传统IT网络更加封闭，但当威胁源以APT（高级持续威胁）的形式出现时，由于其强大的渗透能力和隐蔽性[1]，工业网络内部的HMI、数字化/保护测控装置以及通信协议（如IEC 61850等）的脆弱性将暴露出来，成为主要受攻击面。因此，提高智能变电站的安全运行水平，发现系统脆弱性，并做好安全防护就成为智能变电站信息安全研究的重要方向。

1　现象描述

在智能变电站运行现场中，攻击者可以利用其系统脆弱点进行生产破坏。例如，外部工程师可以软件升级或设备调试为理由，在智能变电站的工程师站注入恶意程序进行攻击，导致变电站设备宕机或拒绝服务。图1、图2分别为注入攻击程序的界面，在注入攻击程序一段时间后，攻击程序运行，导致变电站二次设备工作异常。

图1　攻击程序注入

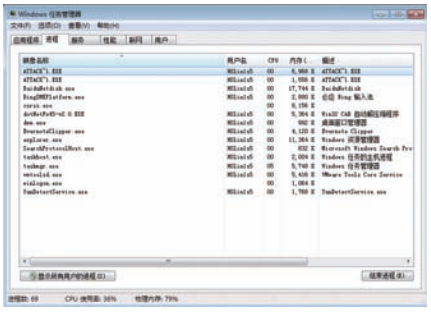

图2　攻击程序运行

通过对智能变电站的工控设备和工控网络的

收稿日期：2024-08-17

作者简介：姚保明（1991），男，硕士，高级工程师，主要从事电网信息安全、网络运行保障相关工作。

安全研究，发现工控网络尽管相对比较封闭，但依然存在着安全隐患：

1）工控设备的研发和生产对于网络安全的关注度比较低，部分软件及系统存在一定脆弱性，因此设备入网时就存在一些安全漏洞[2]；

2）智能变电站生产管理中，一些控制节点防护能力较弱，部分数据传输为明文形式，数据容易被截取、篡改，一旦出现移动设备或无线设备接入的情况，极有可能会被破坏分子利用，导致安全问题；

3）智能变电站协议层存在着安全漏洞，部分核心通信网络未进行认证、加密、授权，访问控制能力弱，导致安全攻击。

因此，对智能变电站工控系统安全问题的研究和漏洞发现，能帮助发现智能变电站系统的安全危机[3]，在实际工作中指导安全管理人员对设备的安全性进行评估，加强生产现场的安全管理工作，保证智能变电站系统的安全运行。

2　基于模糊测试的漏洞挖掘技术

基于模糊测试的漏洞挖掘技术可针对工控系统中常用通讯协议和网络协议，进行风暴测试、语法测试。风暴测试方法使用同一报文，在模糊测试之前进行一次组包，然后通过大量反复发送，实现网络风暴的测试效果；而语法测试则将标准协议的报文特定字段使用自动变化方式，生成大量不同的数据包，然后发送给智能系统和设备[4]。

在系统设计过程中，为了防止语法测试组包过程中占用大量的系统资源和时间，则根据协议分类提前生成测试数据包。在进行语法测试中，通过从文件中读出，可以减少语法测试组包的时间，提高系统运行效率。具体方法如下：

1）构建智能变电站实际运行环境。实验室采用当前主流智能变电站二次设备，配合沙盘模拟主要一次设备，在实验室重建智能变电站的实际运行环境。主要设备如表1和图3所示：

表1　主要模拟设备

序号	设备名称	品牌	型号
1	保护装置	北京四方	CSC-163A/E
2	测控装置	北京四方	CSI-200E/E
3	远动机	北京四方	CSC-1321
4	工程师站PC	北京四方	CSC-2000（V2）

图3　智能变电站主要设备

2）针对智能变电站所使用的设备进行脆弱性测试，包括漏洞扫描以及未知漏洞挖掘等（见图4）。

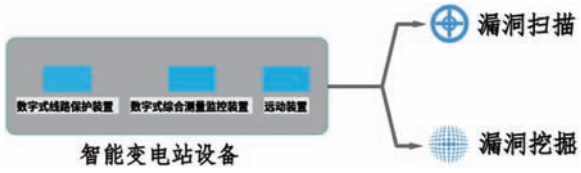

图4　智能变电站漏洞挖掘

漏洞挖掘设备通过Fuzz形式对智能变电站设备进行网络协议栈稳定性测试，根据协议栈的层次，按照由低到高的顺序测试（见图5）。

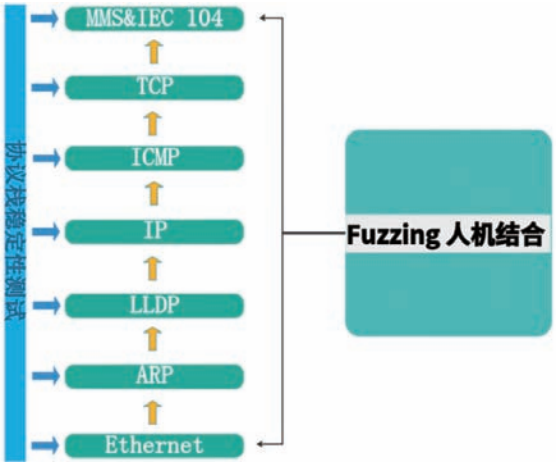

图5　Fuzz协议栈稳定性测试原理

测试通过人机结合的方式进行，由漏洞挖掘设备进行批量自动化测试，再由技术专家根据经验进行复测验证，根据发现的情况输出POC（概念验证程序）。

通过向目标工控系统或设备的应用程序进行Fuzz数据输入实现模糊测试，同时对目标工控设备的输出进行实时监控，Fuzz Testing的漏洞测试对发现智能变电站工业控制系统、设备、协议中存在的安全风险具有重大意义，使得智能变电站工业控制风险

发现不再完全依赖于CVE、CNVD等公开的漏洞库[5]。文中从Fuzz Testing的漏洞测试的原理进行深度研究，并对智能变电站设备进行网络协议栈稳定性测试，应用到智能变电站工业控制系统中，实现测试目标的全方面监控、测试结果的全方位管理。

3 在智能变电站工业控制系统中的应用分析

基于模糊测试的智能变电站工业控制系统漏洞测试方法的核心思想是：通过分析工业控制系统整体架构特点及工控网络协议的协议特征[5]，随机生成测试用例，将其输入实体程序中，并实时监控被测对象的状态，对协议实体异常进行分析。该Fuzz Testing不依赖于被测对象的源代码，通过构建自动化Fuzz Testing应用及可扩展各类漏洞验证POC，可实现智能变电站工业控制系统批量高效的漏洞挖掘和验证[6]。文中Fuzz Testing的一般流程为：

1）向目标系统不断输入可以诱发软件缺陷的测试数据，通过分析被测试应用程序及其使用的数据格式，动态生成测试数据；

2）通过自动化的手段，向被测系统发送数据包、利用被测试程序打开包含测试数据的文件，并进行Fuzz Testing检测；

3）获取一段时间内的测试信息并结合历史测试信息，对异常和错误进行监控；

4）根据发现的情况输出，进行漏洞复验核查。

分析当前智能变电站的工控网络安全整体框架[7]，大致包括智能变电站运行环境仿真、安全漏洞的挖掘及验证、工控安全审计技术研究等内容，如图6所示。

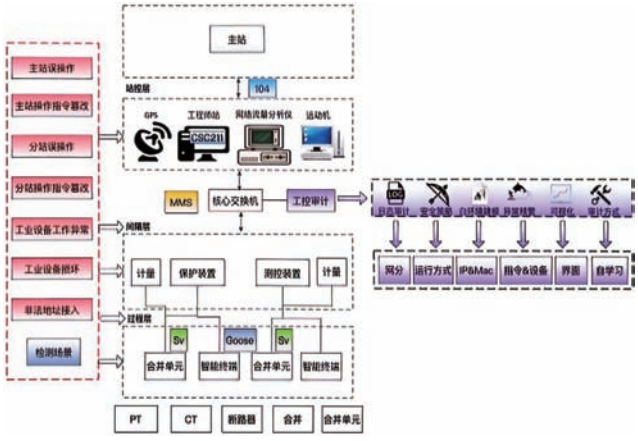

图6 智能变电站安全研究的整体框架图

结合智能变电站的整体架构分析，针对智能电站工控环境下使用的智能设备及应用软件、服务器、设备情况，开发一套软硬件一体的测试系统，对智能变电站综合测量监控装置、数字式线路保护装置、运动装置进行设备安全性和通讯健壮性测试，文中搭建的实验环境如图7所示。

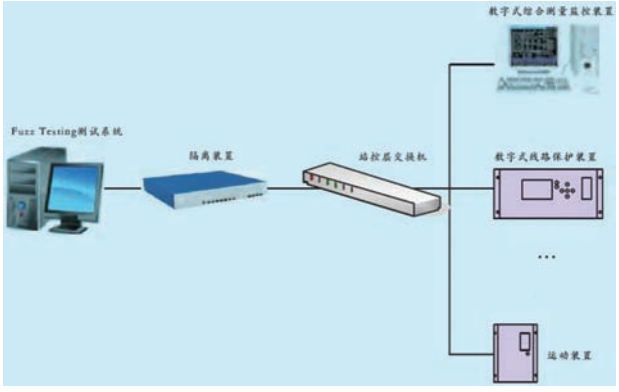

图7 Fuzz Testing实验环境

利用模糊测试方法，对智能变电站内的设备以及网络进行了总计10类、88项安全测试。具体内容为：

1）以太网单播风暴，以太网多播风暴，以太网广播风暴，以太网Fuzzer测试，以太网语法测试（D1），以太网语法测试（D2），Ethernet VLAN语法测试，Ethernet LLC/SNAP语法测试，Ethernet VLAN/LLC/SNAP语法测试，Ethernet数据语法测试；

2）ARP请求风暴，ARP应答风暴，ARP缓存饱和度风暴，ARP语法测试（D1），ARP语法测试（D2）；

3）LLDP风暴测试，LLDP语法测试，LLDP饱和度测试；

4）IP单播风暴，IP多播风暴，IP广播风暴，IP分片风暴，IP错误CheckSum风暴，Ipfuzzer测试，IP语法-头部字段测试（D1），IP语法-头部字段测试（D2），IP语法-分片测试（D1），IP语法-分片测试（D2），IP语法-选项字段测试，IP数据语法，IP语法；

5）ICMP风暴，ICMP Fuzzer测试，ICMP语法（D1），ICMP语法（D2），ICMP TYP/Code语法，ICMP数据语法；

6）IGMPv2查询风暴，IGMPv2应答风暴，IGMPv1语法，IGMPv2语法，IGMPv3请求语法，IGMPv3应答语法；

7）TCP扫描健壮性测试，TCP SYN风暴，TCP

SYN广播风暴，TCP/IP本地风暴，TCP URG风暴，TCP FIN风暴，TCP RST风暴，TCP关闭接收窗口风暴，TCP分片重组风暴，TCP Fuzzer测试，TCP语法测试，TCP语法-头域测试，TCP语法-上下文无效包测试，TCP流量优先级交叉测试，TCP时间戳篡改测试，TCP/IP语法测试，TCP选择性回应测试，TCP接收窗口测试，TCP数据语法，TCP最大连接数测试，TCP初始序列号随机检查测试；

8）UDP扫描健壮性测试，UDP单播风暴，UDP多播风暴，UDP广播风暴，UDP Fuzzer测试，UDP语法测试（D1），UDP语法测试（D2），UDP数据语法测试；

9）IEC 104 APCI语法测试，IEC 104无效ASDU数据单元标识符语法测试；

10）MMS TPKT层语法测试，MMS TPKT层数据段语法测试，MMS-COTP层头语法测试，MMS-COTP层序列语法测试，MMS-COTP层数据语法测试，MMS-COTP层连接耗尽测试，MMS-OSI层会话协议连接SPDU语法测试，MMS-OSI层会话协议非连接SPDU语法测试，MMS-OSI层会话连接用户数据语法测试，MMS-OSI层会话数据传输数据语法测试，MMS-OSI层连接原始会话语法测试，MMS初始化语法测试，MMS Partial初始化语法测试，MMS Full初始化语法测试。

通过上述测试方法在某智能变电站设备的应用，发现了以下安全隐患：

1）拒绝服务类问题

（1）在测控装置上发现WDBrpc接口，可远程导出设备内存数据，通过读取内存数据，攻击者可以得到机器的敏感信息。

在测试测控装置的17185端口时，发现VxWorks的一个WDBrpc端口，该端口使用udp通信，不需要进行认证，通过该调试接口，导出了设备内存信息；

（2）在远动装置上发现rpcbind服务，并伴有拒绝服务漏洞；

（3）保护装置和测控装置的MMS协议栈在处理畸形MMS报文时存在脆弱性，目前现有资料分析时内存溢出，可导致设备宕机或离线。

2）协议栈安全问题

（1）系统协议栈处理风暴不稳定；

（2）协议脆弱性。

通过搭建实验环境，对智能变电站内的设备以及网络进行了总计10类、88项模糊测试，最后构建智能变电站工控漏洞挖掘平台，验证了文中提出检测方法的可行性与测试方法的有效性，其中平台测试结果如图8所示。

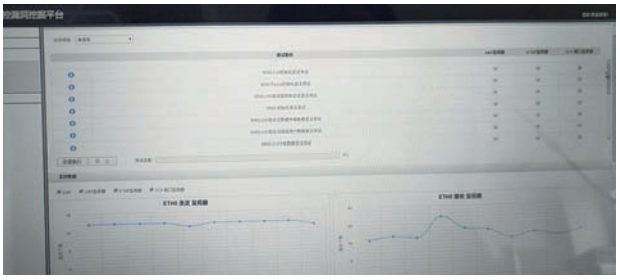

图8　Fuzz Testing测试结果

4　结语

文中提出基于模糊测试的漏洞挖掘方法，通过对智能变电站系统的安全漏洞挖掘，可以发现工控设备在系统层面、应用层面都存在着安全漏洞，有些漏洞是首次发现并验证的，这些安全漏洞一旦被敌对势力或破坏分子利用，将对电网的安全生产构成巨大的危险。这些安全漏洞的发现，将为下一步安全防护技术的研究和利用提供技术基础，在工控网络安全研究领域具有重要意义。

参考文献：

[1] 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，2020，46(6)：571-582.

[2] 车欣.工业控制系统漏洞挖掘技术研究[D].西安：西安电子科技大学，2020.

[3] 赖英旭，杨凯翔，刘静，等.基于模糊测试的工控网络协议漏洞挖掘方法[J].计算机集成制造系统，2019，25(9)：2265-2279.

[4] 冯文倩.基于异常字段定位的Modbus TCP协议漏洞挖掘方法研究[D].北京：北京工业大学，2020.

[5] 任泽众，郑晗，张嘉元，等.模糊测试技术综述[J].计算机研究与发展，2021，58(5)：944-963.

[6] 尤纪鹏.典型工业控制系统私有协议漏洞挖掘技术研究[D].西安：西安电子科技大学，2020.

[7] 宾冬梅，杨春燕，余通，等.基于电力Modbus公开协议的模糊测试方法[J].通信企业管理，2022(2)：77-88.