doi:10.11835/j.issn.1000-582X.2017.07.008

智能变电站安全脆弱性评估方法

刘姗梅[1],王　胜[1],柴继文[1],夏晓峰[2]
(1.国网四川省电力公司 电力科学研究院,成都 610000;
2.重庆大学 信息物理社会可信服务计算教育部重点实验室,重庆 400044)

摘要:基于 IEC61850 的智能变电站严重依赖于信息和通信技术,信息安全成为不得不面对的新问题。从智能变电站信息安全脆弱性和传统信息安全评估手段的局限性 2 个方面对智能变电站的安全现状进行分析,提出了可覆盖智能变电站信息系统和控制系统的安全脆弱性评估方法。该方法分别采用已知漏洞扫描技术、未知漏洞挖掘技术以及静态评估方法,分别对智能变电站的各层设备和日常管理进行安全评估工作。通过对智能变电站实验环境的现场实际测试,发现了存在于信息系统、自动化设备中的系统漏洞,验证了该方法评估智能变电站信息安全脆弱性的有效性。应用该方法可以实现对智能变电站信息和控制系统潜在安全漏洞的多方位管控,提升智能变电站的整体安全。

关键词:智能变电站;IEC61850;脆弱性评估;模糊测试
中图分类号:TN914　　**文献标志码**:A　　**文章编号**:1000-582X(2017)07-052-11

The assessment method of cyber-security vulnerability for smart substation

LIU Shanmei[1], *WANG Sheng*[1], *CHAI Jiwen*[1], *XIA Xiaofeng*[2]
(1. Department of Information and Communication Security and Technology, Sichuan Electric Power Research Institute, Chengdu 610000, P.R.China; 2. Key Laboratory of Dependable Service Computing in Cyber-Physical-Society, Ministry of Education, Chongqing University, Chongqing 400044, P.R.China)

Abstract: The cyber security of the IEC 61850-based smart substations has become an inevitable issue since they rely heavily on information and communication technologies. This paper analyzed the current security situation of smart substation from two aspects: cyber security vulnerability of smart substation and limitation of traditional cyber security evaluation methods. It proposed a security analysis and estimation method for information system and automation system, which estimated the security levels of any devices or equipment in substation separately by detecting known or unknown vulnerabilities. The method managed to assess the daily management by using static assessment tool. Through the practical test in the experimental environment for smart substation, several system vulnerabilities were detected towards information system and automation system, where the effectiveness of the cyber security analysis and

收稿日期:2017-03-27
基金项目:重庆市基础科学与前沿技术研究专项资助(cstc2017jcyjB0305),国家自然科学基金面上项目资助(61472054)。Supported by Chongqing Research Program of Basic Science & Frontier Technology (cstc2017jcyjB0305) and National Natural Science Foundation of China(61472054).
作者简介:刘姗梅(1982-),女,高级工程师,主要从事计算机与控制系统研究,(E-mail)harvard2027@sina.com。

estimation method for smart substation was verified. By applying this method, vulnerabilities of substation information system and automation system can be controlled, and the overall security of smart substation thereby can be enhanced.

Keywords: smart substation; IEC61850; vulnerability assessment; fuzz testing

智能变电站是智能电网的关键环节，是“采用先进、可靠、集成、低碳、环保的智能设备，以全站信息数字化、通信平台网络化、信息共享标准化为基本要求，自动完成信息采集、测量、控制、保护、计量和监测等基本功能，并可根据需要支持电网实时自动控制、智能调节、在线分析决策、协同互动等高级功能的变电站”[1]。伴随着信息化程度的提高，智能变电站引入了各种信息安全问题。智能变电站的信息安全脆弱性，包括自动化系统中各个设备的脆弱性、通讯协议的脆弱性、变电站管理规范的脆弱性等[2]。

针对智能变电站存在信息安全问题的现状，国际电工委员会(international electrotechnical commission，IEC)第 57 技术委员会(TC57)制定了若干标准以解决智能变电站自动化系统和附属信息系统的信息安全问题，例如 IEC 62351 标准和 IEC62443 标准[3-4]。IEC 62351 标准通过引入加密和授权机制，为保障智能变电站的通信安全和强化 IEC61850 等通信协议提供了解决方案[5]。IEC62443 标准从电力系统的层面提供了信息安全的指导规范，并为智能变电站的日常运行维护和管理提供了原则性指导意见[6]。目前，对于智能变电站的信息安全脆弱性的研究，特别是设备本身的脆弱性研究，尚在初步阶段，没有统一的标准[7]。针对来自不同厂商的控制设备和系统也缺乏面向信息安全的研究和测试手段[8]。智能变电站的信息安全脆弱性评估方法和测试手段仍需深入研究。

在这个背景下，笔者对智能变电站信息安全脆弱性进行分析，提出了智能变电站信息及控制系统的安全脆弱性评估框架，并给出框架实现方法。该方法通过对智能变电站仿真环境的实际测试，发现智能变电站存在的一些信息安全漏洞和风险，为提升改进智能变电站的信息安全提供了参考和依据。

1　智能变电站安全分析

1.1　智能变电站概述

智能变电站为“三层两网”结构：站控层、间隔层、过程层，站控层网络、过程层网络[9-11]。过程层设备直接面向电力系统的一次设备，主要是智能终端和合并单元。过程层设备采用 IEC61850 协议的通用面向对象变电站事件(Goose)报文和采样值(SV)报文与间隔层设备进行数据通信。间隔层设备包括测控装置、保护装置、故障录波设备、网络报文分析设备。站控层包括时间同步系统、监控站和远动测控站。站控层与间隔层设备之间通过基于 TCP/IP 的 IEC61850 协议的制造报文系统(manufacturing message system，MMS)进行数据通信。

1.2　智能变电站安全脆弱性分析

智能变电站采用以太网方式与控制中心进行远程通信和设备间通信，站内设备采用通用操作系统和应用软件，可能存在系统漏洞、应用软件漏洞、通信协议漏洞和变电站管理漏洞可能被用来对智能变电站进行信息安全攻击和渗透，如图 1 所示。

1.2.1　信息系统脆弱性

信息系统脆弱性指站控层和间隔层设备自身操作系统存在的信息安全漏洞，包括计算机操作系统漏洞、文件漏洞、数据库漏洞等。

1.2.2　控制系统脆弱性

控制系统存在的信息安全漏洞是控制系统信息安全脆弱性的主要来源，从已经公布的工业控制系统漏洞可以发现，主流的工业控制系统厂商的产品均存在的如缓冲区溢出、后门口令等高危漏洞。智能变电站控制系统漏洞主要针对间隔层和过程层的各类设备和终端，包括嵌入式操作系统漏洞、嵌入式应用软件漏洞等。

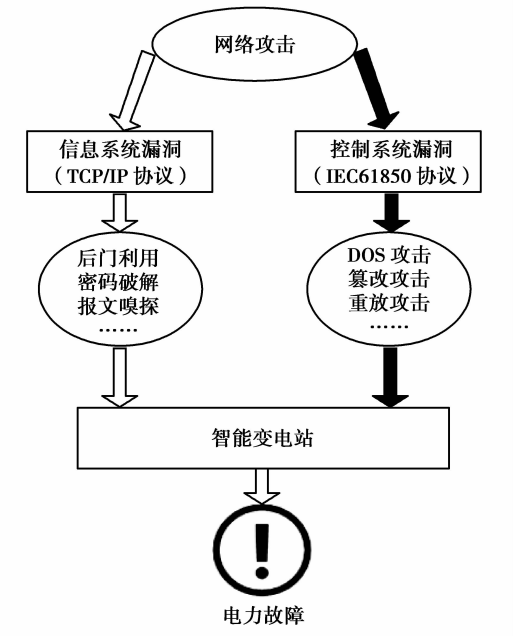

图 1 针对智能变电站的漏洞利用示意图

Fig.1 The schematic diagram for the vulnerability exploitation of smart substation

1.2.3 通信协议脆弱性

智能变电站采用的通信协议如 IEC61850 MMS、Goose、SV 在设计时对信息安全考虑的不够完善，来自站控层一侧的非授权的恶意指令会导致控制系统以及其他连接在网络上的设备不可用，Goose 报文和 SV 报文采用多播消息进行局域网内通信，针对此两类通信的攻击手段至少包括拒绝服务攻击、篡改攻击、重放攻击等[12-15]。

1.3 传统信息安全评估手段的局限性

传统的信息安全脆弱性评估方法和工具主要面向 IT 系统，不能完全满足对智能变电站进行信息安全脆弱性评估的需要：

1)设备是非标准计算机设备。智能变电站设备采用的通用操作系统已被厂商进行了定制化开发，采用普通的工业控制系统信息安全漏洞扫描工具可能产生大量的误报。

2)设备采用定制化的应用软件。由于二次设备采用了非标准的端口、处理方法，所使用的软件为定制开发软件，公开的信息安全漏洞较少，传统信息安全分析评估工具难以对其进行评估。

3)专用通信协议。智能变电站中控制系统部分采用了基于 IEC61850 的网络通信协议，传统信息安全脆弱性评估工具大多不支持这种通讯协议，因此无法进行基于协议的评估和漏洞挖掘。

4)方法和工具缺失。针对 IT 系统的信息安全脆弱性评估工具和方法是基于大量 IT 系统的已知信息安全漏洞和成熟的实践，智能变电站这类控制系统不仅很少有公开的信息安全漏洞，也很少有成功的实践经验，可用的工具也很少。

2 智能变电站安全脆弱性评估方法

针对智能变电站的安全现状，在已有工业控制系统信息安全脆弱性分析的成功实践技术上，笔者设计了一种智能变电站信息系统安全脆弱性评估方法。该方法结合智能变电站现场的特殊软硬件和网络环境，采用了已知漏洞扫描、未知漏洞挖掘、静态安全评估等多种方法。方法实现的框架体系结构如图 2 所示。

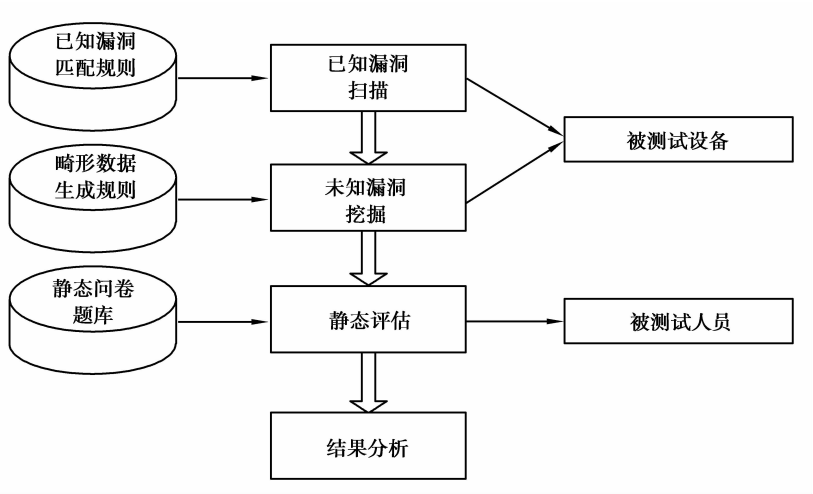

图 2　方法实现框架

Fig.2　The framework of method implementation

2.1　已知漏洞扫描方法

已知漏洞扫描方法采用了基于已知漏洞特征规则匹配的已知漏洞扫描技术,其原理和算法流程如图 3 所示。

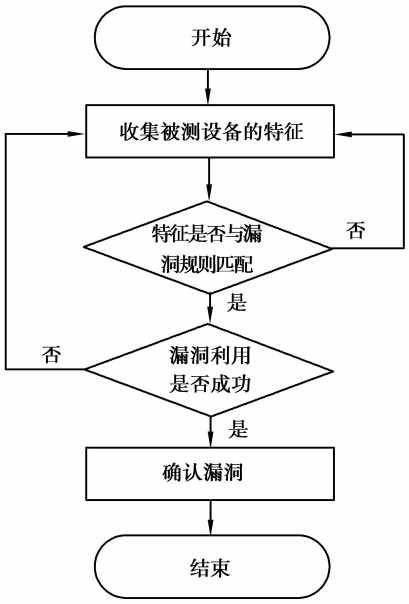

图 3　已知漏洞特征匹配算法流程

Fig.3　The algorithm flow of known vulnerability feature matching

基于已知漏洞的扫描技术的优点是通过使用已知匹配规则,把极为繁琐的手工安全检测,变成程序自动化完成,不仅减轻了测试者的工作,而且缩短了检测时间、拓展了检测范围,使安全问题快速被发现。

针对智能变电站的已知漏洞扫描方法主要用于对智能变电站中信息系统的部分。

2.2　未知漏洞挖掘方法

未知漏洞挖掘引擎利用基于网络协议的模糊测试技术。通过模拟智能变电站信息系统和控制系统相应的通信协议发送机制,向信息系统或控制系统发送变异测试报文,监视被测对象的响应报文以发现错误,进而发现智能变电站信息系统或控制系统的隐患。其测试原理如图 4 所示。

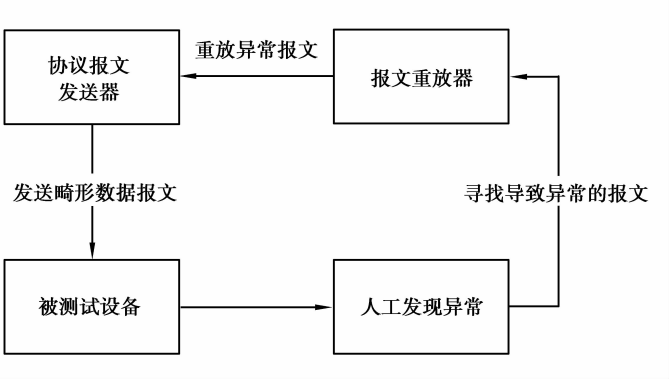

图4 模糊测试原理示意图

Fig.4 Schematic diagram of fuzzy testing

在功能设计中,未知漏洞挖掘需要包括文本分析、协议发送机、测试用例集等功能。其中,测试用例的生成是模糊测试的核心。

测试用例构造的正确度和畸形度直接决定了漏洞挖掘的效率。为了避免在漏洞挖掘过程中产生大量正确度低的测试用例,并减少测试数据构造的复杂度,采用了一种融合了基于生成技术(generation-based)和基于变异技术(mutation-based)的测试用例构造技术。

其中基于生成技术的测试用例构造技术通常基于网络协议知识或者文件格式知识构造测试用例,该技术的优点在于构造的测试用例有效地越过测试目标中对固定字段、校验和、长度的检查,且满足输入数据之间的约束关系,使测试数据的正确度大大提高,从而顺利地覆盖含有潜在漏洞的语句有效性高。

基于变异技术的测试用例构造技术通常基于正常的样本数据(如样本文件、网络数据包),根据一定的漏洞知识(如构造易触发漏洞的畸形数据方法等)变异其中部分数据来生成测试用例。数据畸形的策略如表1所示。该技术的优点在于实现起来简单,自动化程度高。

表1 畸形策略表

Table 1 Deformity strategy

畸形策略类型	实例
大数溢出	0xFF, 0xFE, 0xFD, 0xFFFF, 0xFFFE, 0xFFFD, 0xFFFFFF, 0xFFFFFE,0xFFFFFD 等
小数溢出	0,1,-1,0x00 等
格式化字符串溢出	! @ # MYM%%^ # MYM% # MYM@ # MYM% MYMMYM@ # MYM%^^ * *((), *, ,-, %s, %n, %x 等
字符串超长溢出	AAAAAAAAA…AAAAAAAAAAAAAAA BBBBBBBBBB…BBBBBBBBBBBBBBB ABCCADAFAF…AFFFFCCCCCCCCAAFG 等
字符串分隔符	'",',;,\r,\n,<,>,",/,\,? ' 等

智能变电站采用的是IEC61850协议,针对IEC61850协议的模糊测试是重点。IEC61850协议报文不但包含字符串,而且包含大量的整型数和浮点数,通过对报文中任一或多个字段进行数据变异得到畸形数据。以Goose报文为例,典型的正常报文如图5所示。

在此报文数据的基础上,可以用随机数方法或畸形策略表中的方法更改任一字段的内容,生成畸形的测试用例。例如将Type值0x88B8变换为随机值,得到新的数据包。

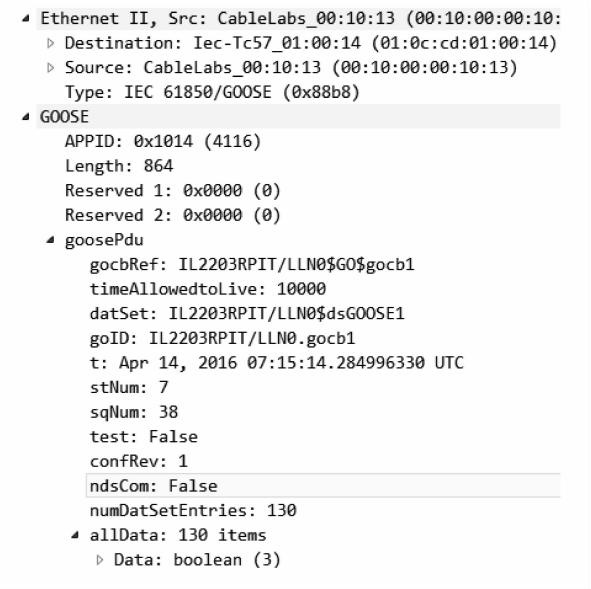

图 5　Goose 报文内容

Fig.5　Goose message content

根据 IEC61850 协议的定义产生的测试用例集包含大量随机或经验性的测试用例。为了提高测试效果,降低测试盲目性和测试成本,文中采用基于遗传算法(genetic algorithm,GA)的启发性测试用例生成算法对测试用例集进行筛选。GA 的形式化描述是

$$\mathrm{GA}=\{n,\ T,\ P,\ R,\ M,\ F,\tau\},$$

式中:n 是测试用例种群的规模;T 是初始种群,$T=\{T_1,\ T_2,\ \cdots,\ T_n\}$,其中 T_i 是种群中的测试用例个体,$1\leqslant i\leqslant n$;P、R、M 分别是 GA 中的基因选择、基因交叉和基因变异 3 个操作,基因采用测试用例字段的二进制位串;F 是评价个体适应度的适应度函数;T_i 的适应度表示为 $f_i=F(T_i)$;τ 是 GA 的终止条件,文中采用最大允许迭代次数。

GA 的核心是选择合适的适应度函数 F,文中参考 Jones 等[16-17]的方法,以测试用例与经验用例或模板用例间的汉明距离构建适应度函数,筛选测试用例,提高测试用例发现漏洞的概率。

2.3　静态评估方法

针对变电站的管理漏洞,采用静态评估问卷的形式对智能变电站的日常管理维护工作方法和流程进行测试评估。

静态评估问卷的设计依据了 IEC 62443、GB/T 30976、GB/T 26333、GB/T 3096 等标准中对信息安全、物理安全、功能安全的相关要求。通过对变电站管理维护工作的责任主体(运行人员、继保人员)进行问卷调查,静态评估方法可以确定被调查的变电站是否具有管理漏洞,并进一步评估信息安全的管理风险等级。

3　应用实践

3.1　测试环境

智能变电站安全脆弱性评估方法被应用于某智能变电站实验环境中。实验环境如图 6 所示。

执行评估方法的测试设备由工业计算机和访问终端构成。测试过程中的设备发现和已知漏洞扫描工作是初步检测,通过接入站控层网络和过程层网络的交换机进行,对三层现场设备进行一次性的测试和评估。

3.2　测试过程

智能变电站安全脆弱性评估包含了对设备的测试以及对现场运维人员的调查,其测试过程如下:

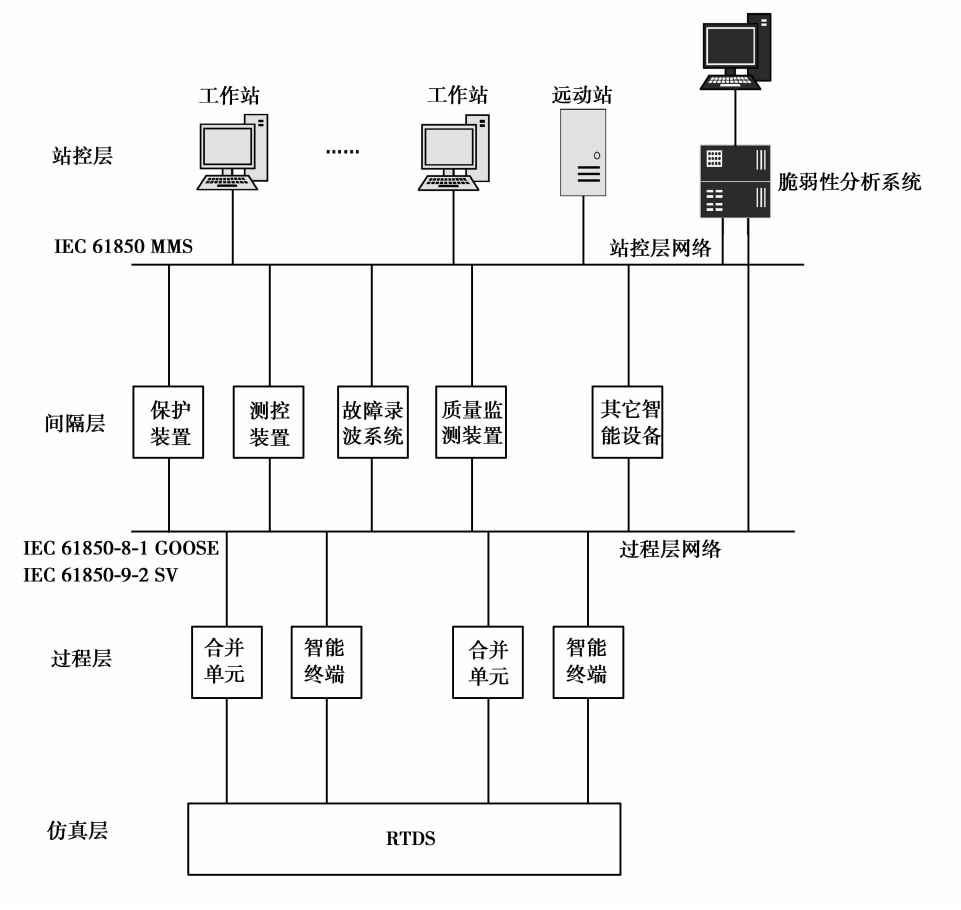

图6 智能变电站安全脆弱性实验环境

Fig.6 The experiment environment of security vulnerability of smart substation

3.2.1 扫描已知漏洞

在确认被测试设备可连通后,执行已知漏洞扫描。扫描对象包括操作系统、数据库和常用应用软件等。扫描的漏洞包括弱口令、用户权限漏洞、访问认证漏洞、系统完整性检查、存储过程漏洞以及与数据库相关的应用程序漏洞等。

3.2.2 挖掘未知漏洞

未知漏洞挖掘是深入检测,需要将被测设备与测试平台进行直连,如图7所示。

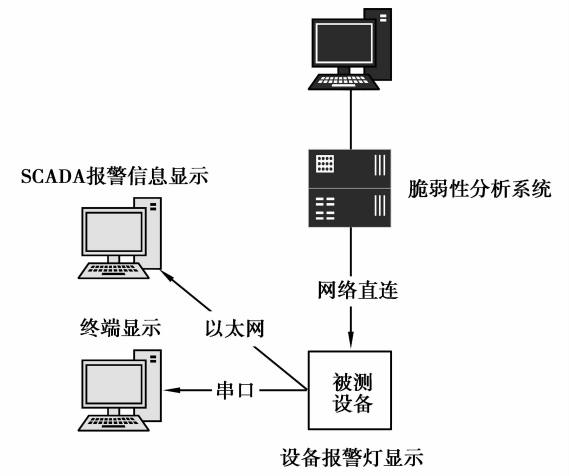

图7 未知漏洞挖掘过程的设备连接方式

Fig.7 The device connection mode of unknown vulnerability mining

智能变电站自动化系统中的设备除了站控层的工作站以外,多数没有屏幕显示的接口。因此,未知漏洞挖掘过程的结果显示方法采用如下方式:

1)设备报警灯显示。所有设备本体上均具备故障报警灯,可简单判断设备是否出现异常,但无法确定异常的具体信息。

2)数据采集与监视控制系统(supervisory control and data acquisition,SCADA)报警信息的显示。运行于站控层的 SCADA 系统对变电站内的所有设备实时采集运行信息。当下层设备出现异常后,SCADA 系统根据网络协议规则、设备历史信息等多个指标对设备运行情况进行判定,报告设备异常信息。但 SCADA 报警信息依赖于 SCADA 系统自身的判断准确性,因此可能出现误报的情况。

3)终端显示。部分设备支持通过串口终端的方式进行远程访问,通过终端可以获得设备自身的详细运行信息,并有可能访问设备内的系统日志等关键文件。

3.2.3　基于标准的静态评估

通过对现场的运行人员和管理人员进行问卷调查,并结合前述步骤中获得现场环境情况,判断现场的日常运维和管理工作是否合法合规,管理流程是否存在漏洞。

3.2.4　确认漏洞

在测试过程中发现被测设备存在异常或被测人员存在不正确行为,则需要对发现的问题进行确认。

3.3　测试结果及分析

文中对某模拟智能变电站进行安全脆弱性评估。该模拟变电站拥有设备共 79 台,使用的操作系统包括 Windows Server 2008、Vxworks、Linux。

3.3.1　已知漏洞扫描

通过对现场设备执行已知漏洞扫描,发现站控层和间隔层的部分设备中有较多漏洞,主要漏洞信息如表 2 所示。

表 2　部分设备已知漏洞信息统计

Table 2　The known vulnerability statistics for some devices

设备类型	漏洞类型	漏洞数量
站控层设备 A	高危险漏洞	5
	中危险漏洞	82
	低危险漏洞	14
间隔层设备 B	高危险漏洞	3
	中危险漏洞	5
	低危险漏洞	1
间隔层设备 C	低危险漏洞	1

3.3.2　未知漏洞挖掘

测试主要对间隔层和过程层设备进行测试,分别采用传统 TCP/IP 类协议和 IEC61850 协议对被测设备发送畸形协议报文。测试中发现多种异常现象:

1)装置报警。通过对间隔层设备发送基于模板和经验值生成的异常数据,SCADA 系统的报警信息报告装置异常,如图 8 所示。

2)非法操作。通过基于模板的异常数据测试,发现过程层的终端设备会响应部分畸形报文,做出分合闸动作,如图 9 和图 10 所示。

1#主变高压侧测控PCS-9705A_PL_GOOSE_A网络风暴报警	通信变位 告警
1#主变高压侧测控PCS-9705A_PL_GOOSE_A网络风暴报警	SOE 告警
1#主变高压侧测控PCS-9705A_PL_GOOSE报警	通信变位 告警
1#主变高压侧测控PCS-9705A_PL_GOOSE报警	SOE 告警
1#主变高压侧测控PCS-9705A_1#主变高压侧测控装置报警	通信变位 由合到分
1#主变高压侧测控PCS-9705A_1#主变高压侧测控装置报警	SOE 由合到分
1#主变高压侧测控PCS-9705A_1#主变高压侧测控装置报警	通信变位 由分到合
1#主变高压侧测控PCS-9705A_1#主变高压侧测控装置报警	SOE 由分到合
1#主变高压侧测控PCS-9705A_2#主变高压智能终端装置告警	通信变位 返回
1#主变高压侧测控PCS-9705A_2#主变高压智能终端装置告警	SOE 返回
1#主变高压侧测控PCS-9705A_2#主变高压智能终端装置告警	通信变位 告警
1#主变高压侧测控PCS-9705A_2#主变高压智能终端装置告警	SOE 告警

图 8 装置报警和网络风暴报警

Fig.8 Equipment alarm and network storm alarm

1#主变高压侧测控PCS-9705A_20160接地刀闸分位	通信变位 由分到合
1#主变高压侧测控PCS-9705A_20160接地刀闸分位	SOE 由分到合
1#主变高压侧测控PCS-9705A_20140接地刀闸分位	通信变位 由分到合
1#主变高压侧测控PCS-9705A_20140接地刀闸分位	SOE 由分到合
1#主变高压侧测控PCS-9705A_20130接地刀闸分位	通信变位 由分到合
1#主变高压侧测控PCS-9705A_20130接地刀闸分位	SOE 由分到合
1#主变高压侧测控PCS-9705A_2012刀闸分位	通信变位 由分到合
1#主变高压侧测控PCS-9705A_2012刀闸分位	SOE 由分到合
1#主变高压侧测控PCS-9705A_2011刀闸分位	通信变位 由合到分
1#主变高压侧测控PCS-9705A_2011刀闸分位	SOE 由合到分

图 9 SCADA 报警信息显示的非法遥控动作

Fig.9 The illegal remote control action from SCADA alarm information

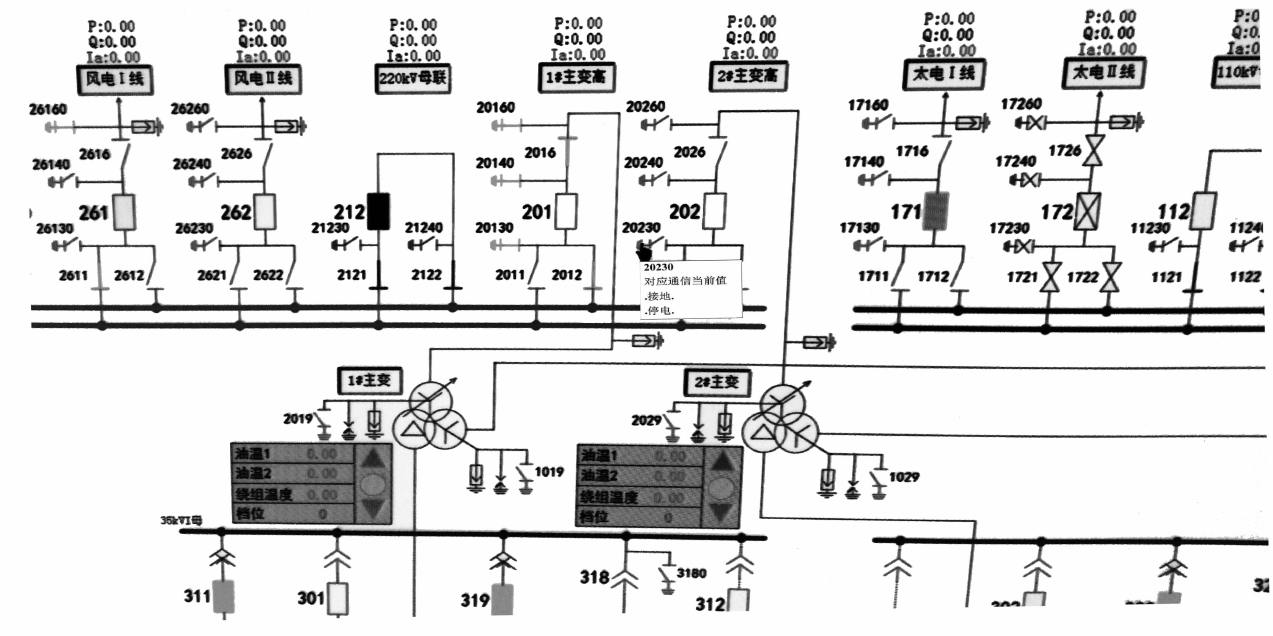

图 10 非法遥控 1＃主变高智能终端动作

Fig.10 The intelligent terminal action of the high side of the first main transformer

3)静态评估。使用调查问卷对现场人员进行测试，发现模拟智能变电站在运维管理中存在漏洞。

由于设备拥有运维接口，按照使用方法，采用串口直连被测设备运维接口，发现终端 root 账户无权限保护，在未授权的情况下直接访问系统后台，并对系统内的文件进行操作，如图 11 所示。

```
/ # ls
bin         hai       linuxrc     proc      sys         var
dev         home      mnt         root      tmp
etc         lib       mountnfs    sbin      usr
/ # rm –rf /hai
/# ls
bin         home      mnt         root      tmp
dev         lib       mountnfs    sbin      usr
etc         linuxrc   proc        sys       var
/ #
```

图 11　非法后台登录和后台操作

Fig.11　Illegal background login and operation

通过以上结果并结合被测设备运行信息分析可以发现：模拟智能变电站的部分设备存在安全漏洞，特别是站控层设备存在大量的高危和中危漏洞；畸形的协议报文可能会导致装置报警，并进一步导致设备重启；部分畸形协议报文可以实现对一次设备的非法操作，带来安全隐患。通过静态评估发现该变电站存在运维过程后台无权限保护的安全隐患，可能为黑客提供了入侵通道。

4　结　论

信息安全问题是智能变电站日常运行中必须关注的重点之一，介绍了一种新的智能变电站信息安全脆弱性评估方法、评估工具和在评估中发现的一些信息安全脆弱性问题，研究了智能变电站信息系统漏洞和控制系统漏洞可能带来的影响。该方法集成了基于特征规则匹配的已知漏洞扫描方法、基于模糊测试的未知漏洞挖掘方法和静态安全评估方法，分别针对智能变电站可能存在的已知漏洞、未知漏洞以及智能变电站可能存在的管理漏洞进行覆盖。研究通过在智能变电站实验环境中的实际测试，发现了实际控制设备和附属信息系统的信息安全隐患，验证了该方法从多个角度评估智能变电站信息安全脆弱性的有效性，为提升智能变电站信息安全防护提供技术支撑和设计依据。

参考文献：

[1] Q/GDW 383—2009 智能变电站技术导则[S]. 国家电网公司，2009.
Q/GDW 383—2009 Technical guide for smart substation[S]. State Grid Corporation of China (SGCC), 2009.

[2] Ten C W, Liu C C, Manimaran G. Vulnerability Assessment of Cybersecurity for SCADA Systems[J]. IEEE Transactions on Power Systems, 2008, 23(4): 1836-1846.

[3] Power systems management and associated information exchange-data and communications security[S]. IEC Std. 62351.

[4] Industrial Communication Networks-Network and System Security[S]. IEC Std. 62443.

[5] Tawde R, Nivangune A, Sankhe M. Cyber security in smart grid SCADA automation systems[C]// International Conference on Innovations in Information, Embedded and Communication Systems. IEEE, 2015: 1-5.

[6] Yang Y, Jiang H T, Mclaughlin K, et al. Cybersecurity test-bed for IEC 61850 based smart substations[C] //Power & Energy Society General Meeting. IEEE, 2015: 1-5.

[7] Drias Z, Serhrouchni A, Vogel O. Analysis of cyber security for industrial control systems[C]//International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications. IEEE, 2015: 1-8.

[8] Ten C W, Hong H J, Liu C C. Anomaly detection for cybersecurity of the substations[J]. IEEE Transactions on Smart Grid, 2011, 2(4): 865-873.

[9] 赵敏，陈红伟.数字化变电站的主要特征和关键技术分析[J].中国电力教育，2012(33)：138-139.

ZHAO Min, CHENG Hongwei. Main features and key technology analysis of digital substation[J]. China Electric Power Education, 2012(33): 138-139. (in Chinese)

[10] 肖静.基于 IEC 61850 规约的智能变电站在线监测系统设计[J].自动化应用,2015(9):107-108.
XIAO Jing. Design of intelligent substation online monitoring system based on IEC 61850[J]. Automation Application, 2015 (9): 107-108. (in Chinese)

[11] 曹楠,李刚,王冬青.智能变电站关键技术及其构建方式的探讨[J].电力系统保护与控制,2011,39(5):63-68.
CAO Nan, LI Gang, WANG Dongqing. Key technologies and construction methods ofsmart substation [J]. Power System Protection and Control, 2011, 39(5): 63-68. (in Chinese)

[12] Elgargouri A, Virrankoski R, Elmusrati M. IEC 61850 based smart grid security[C]. Industrial Technology (ICIT), 2015 IEEE International Conference on. IEEE, 2015: 2461-2465. (in Chinese)

[13] Wang W, Lu Z. Cyber security in the Smart Grid: Survey and challenges[J]. Computer Networks, 2013, 57(5): 1344-1371.

[14] Wu S S, Liu C C, Shosha A F, et al. Cyber Security and Information Protection in a Smart Grid Environment[J]. IFAC Proceedings Volumes, 2011, 44(1): 13696-13704.

[15] Rashid M T A, Yussof S, Yusoff Y, et al. A review of security attacks on IEC61850 substation automation system network[C]// Information Technology and Multimedia (ICIMU), 2014 International Conference on. IEEE, 2014: 5-10.

[16] Jones B F, Sthamer H H, Eyres D E. Automatic structural testing using genetic algorithms[J]. Software Engineering Journal, 1996, 11(5): 299-306.

[17] Jones B F, Sthamer H H, Eyres D E. Generating test data for ADA procedures using genetic algorithms[C]// Genetic Algorithms in Engineering Systems: Innovations and Applications, 1995. IET, 1995: 65-70.

(编辑 詹燕平)