



智能电子设备顽健性测试方法

姜海涛,李斌,王祥,陈锦铭,郭雅娟

(国网江苏省电力公司电力科学研究院,江苏 南京 210011)

摘要:为了检测变电站智能电子设备(intelligent electronic device,IED)通信模块的顽健性,提出了一种基于异常报文的设备顽健性测试方法,并实现了顽健性测试系统。选取部分设备进行顽健性测试实验,验证了测试方法的合理性与测试系统的可行性。实验结果表明,该测试方法能够有效地发现设备无法处理异常报文的问题,并定位导致设备异常的异常报文。

关键词:顽健性测试;智能电子设备;智能变电站

中图分类号:TM774

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2015390

Robustness test method for intelligent electronic device

JIANG Haitao, LI Bin, WANG Xiang, CHEN Jinming, GUO Yajuan

State Grid Jiangsu Electric Power Research Institute, Nanjing 210011, China

Abstract: To detect the robustness of communication module of intelligent electronic devices (IED) in smart station, a device robustness test method was presented based on abnormal messages, and a robustness testing system was achieved. Some devices were selected for robustness test experiment to verify the rationality and feasibility. Results show that the method can effectively detect the robustness of devices and locate the abnormal messages which cause devices' failure.

Key words: robustness test, intelligent electronic device, smart substation

1 引言

智能变电站作为典型的工控系统,是智能电网中的重要组成部分,其信息安全直接关系到整个电力系统的安全性与稳定性^[1]。随着基于TCP/IP的智能电子设备在智能变电站中的广泛应用,在增强设备互操作性和访问能力的同时,也增加了网络安全脆弱性与安全事件发生的可能性^[2]。本文从智能电子设备顽健性测试的角度出发,利用异常报文检测设备的通信模块的容错能力和故障恢复能力,为提高智能变电站的安全与稳定提供支持。

学术界已经提出了许多顽健性测试方法:参考文献[3]

给出了一个基于状态机的构件顽健性测试框架,并实现了原型工具RoTesCo;参考文献[4]中在增加状态、迁移和事件的基础上构造了具有顽健性处理过程的RFSM(robustness finite state machine),并把RFSM模型应用到BGP顽健性测试当中;参考文献[5]使用有限状态机对软件产品进行建模,通过状态扩充和状态对各种异常事件的响应,构建完备的增强有限状态机进行顽健性测试。在商业应用领域,也已经出现了很多顽健性测试工具,如Kali是一个操作系统渗透测试工具;Appscan是一个针对Web应用漏洞的扫描工具。但是在电力工控系统中,设备顽健性测试的研究还相对较少。

传统观念认为智能变电站是一个相对封闭的环境,不存在来自外部的威胁。但是由于U盘等介质和无线设备的普及,工控系统的封闭性已被打破,例如破坏伊朗核电站离心机的震网病毒就是通过U盘带入^[6]。目前针对智能变电站中信息安全的研究已经取得了一定成果:参考文献[7]介绍了智能变电站的特点,探讨了智能变电站的体系架构、智能设备、保护控制策略、测试仿真和信息安全策略等方面的问题,参考文献[8]分析了变电站自动化通信系统的安全性,并提出了一些能有效提高安全强度的方法;参考文献[9]建立了信息安全评估体系,运用D-S证据理论对变电站通信系统的信息安全威胁进行评估。上述研究都是基于工控系统的安全架构或网络安全相关技术,并未关注设备的顽健性。本文提出了一种基于异常报文的设备顽健性方法,在此基础上设计并实现了针对设备顽健性的测试系统。

2 基于异常报文的设备顽健性测试方法

测试设备顽健性的核心思想是基于向设备发送异常报文测试用例,检测设备的通信状态,通过判别设备对异常报文的处理情况,确定设备的顽健性。如果设备出现通信中断、出错、宕机等异常情况,则说明设备对异常报文的抵御能力较差,设备的顽健性有待改善。这是一种仅知道设备支持的通信协议标准,不知道设备内部通信模块具体实现时,采取的黑盒测试方法。以变电站中目前使用最广

泛的 IEC61850^[10]协议为例,设计了图1所示的测试模型,涉及5种设备或系统,分别是:

- 用于测试的间隔层智能电子设备;
- 用于对智能电子设备进行日常运维的机器;
- 用于捕获数据报文的流量采集装置;
- 用于测试设备 IEC61850 通信模块顽健性的测试系统;
- 用于实现以上设备互通的站控层交换机。

上述模型是对变电站实际组织结构的简化,省略了监控后台、过程层网络和设备以及与调度通信的相关设备,只保留了站控层交换机、间隔层智能电子设备和运维机器。同时为了测试设备 IEC61850 通信模块的顽健性,增加了流量采集装置和顽健性测试系统,测试的一般流程如下所述。

(1)运维机器通过 IEC61850 协议选择某个设备执行正常的运维操作,产生 IEC61850 的数据报文。由于 IEC61850 是一种国际通用的通信协议,因此通过任何一个 IEC61850 客户端软件都可以与各个厂商设备进行互操作。

(2)由于所有数据报文都要通过交换机进行转发,流量采集机器可以从交换机捕获运维机器与智能电子设备之间通信的数据报文。目前大部分交换机都设有一个专门的镜像端口,用于将所有经过交换机的数据,从镜像端口做一个备份输出。

(3)对采集到的报文进行预处理,除去非 IEC61850 协

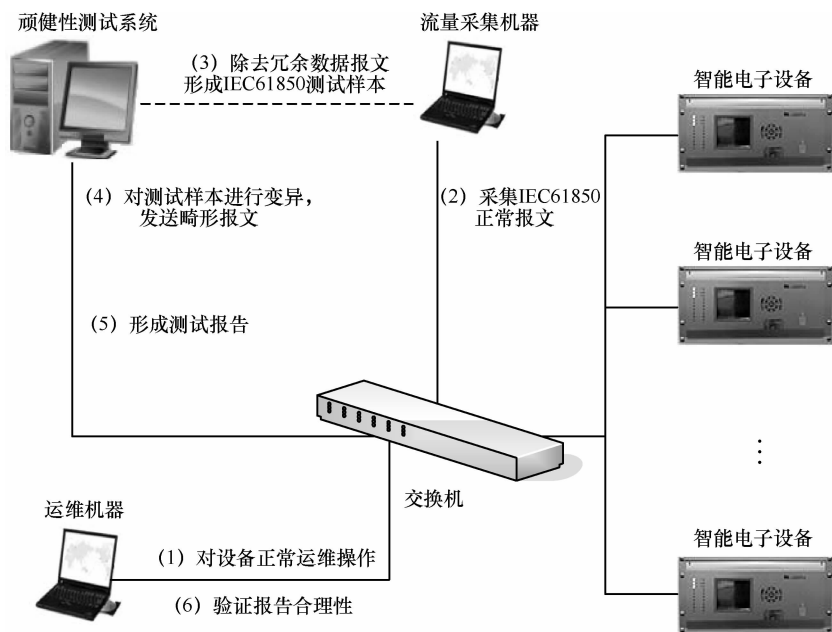


图1 电子设备 IEC61850 通信模块顽健性测试模型

议的冗余数据,形成测试报文样例,导入顽健性测试系统。

(4)顽健性测试系统解析测试样例,对正常的数据报文中的某个或者某几个字段进行变异,选择某个被测设备,并向该设备发送变异之后的异常报文。整个测试过程中,对于每个正常报文,系统产生并向设备发送多个不同的异常报文,同时记录所发送报文以及设备状态等实时信息。

(5)测试结束后,系统根据记录的信息提取设备出现异常时发送的异常报文,统计设备异常时间、发送测试报文数目等信息,根据报告模板生成测试报告。

(6)测试人员根据测试报告中的异常报文,对问题进行排查,确认设备是否出现异常,验证测试结果的合理性,完善测试报告。

在上述流程中,前3个步骤是准备阶段,主要目的是形成 IEC61850 协议的测试报文样例;后3个步骤是测试阶段,主要为了发掘并验证可以导致设备异常的异常报文。图1的5种设备和系统中站控层交换机、智能电子设备、运维机器是变电站已有的设备,利用 Wireshark 等数据分组捕获软件即可实现流量采集,顽健性测试系统成了整个测试模型的核心部分。

3 顽健性测试系统的设计与实现

测试系统的核心功能为读取 IEC61850 测试报文样例文件、生成异常报文测试样本并将其发送给被测设备,检测设备的通信状态,以判断设备对异常报文的抵御能力。

3.1 测试系统的组织模块

图2显示了系统的组织模块以及各个模块之间的关联。系统主要由1个核心调度器、6个功能模块、2个预定义文件和2个数据存储单元组成。

每个模块的主要功能如下所述。

(1)测试样例加载模块

将磁盘上的 IEC61850 测试报文样例文件,去掉 IP 头信息,以字节数组的形式加载到内存中。IP 头信息主要为

报文的 IP 地址、MAC 地址和端口号,并非 IEC61850 协议的内容。

(2)配置文件读取模块

获取 XML 格式的配置文件,该文件包括了系统执行过程中需要的数据,如发送2个报文的时间间隔、判断设备异常的等待时间等。

(3)异常报文产生模块

结合异常报文的历史信息,通过对正常 IEC61850 报文进行变异产生异常报文。

(4)报文发送模块

通过 102 端口(IEC61850 协议使用的标准端口)与设备建立 TCP 连接,向指定设备发送 IEC61850 报文。在通信链路完好的情况下,如果无法与设备建立连接,则说明设备出现异常。

(5)界面展示模块

显示实时测试信息,如发送测试报文数目、测试经历时间等。同时接收用户输入,如被测设备的 IP 地址,测试的开始、停止命令。

(6)报告生成模块

从实时数据存储单元中读取测试产生的结果信息,根据预定义的 HTML 格式的报告模板输出测试报告,报告中主要列举了设备信息和导致设备异常的异常报文。

(7)核心调度器

协调上述6个模块协同工作,调用各个模块的接口,在各个模块之间共享数据,这也符合MVC(model-view-controller)设计模式。其中核心调度模块是 controller,界面展示模块和报告生成模块是 view,其余的模块都是 model。

3.2 基于历史信息的异常报文产生方式

在上述6个模块中,异常报文产生方式决定了测试样例的质量,从而影响了检测的效果。由于同一厂商的设备可能存在相同的问题,并且国内目前 IED 厂商数量有限,因此本文使用基于历史信息的异常报文产生方式,通过已

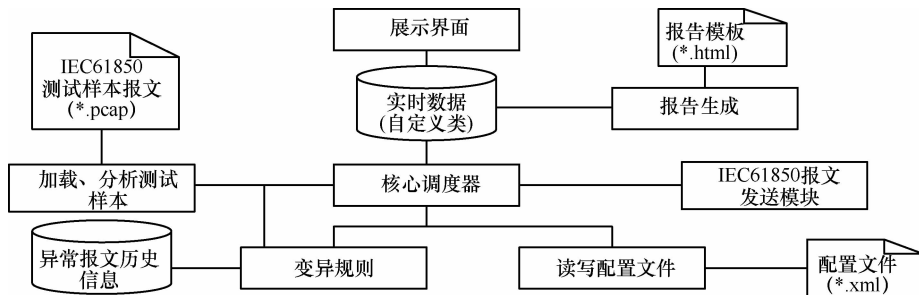


图2 顽健性测试系统组织结构



经确认的异常报文构造测试样例集合,提高异常报文导致设备出现异常的概率。同时不断完善已确认的异常报文信息,提高测试质量。

任意 IEC61850 报文,在去掉 TCP 报文头信息后,都可以根据 IEC61850 协议的语法规则解析得到多个字段,每个字段有相应的名称和长度,字段的值为二进制值或子字段。因此利用正常报文(packet)、字段(field)、异常取值(value)的形式,保存已确认的异常报文。某正常报文的二进制如图 3 所示。

```
03 00 00 16 11 e0 00 00 00 04 00 c1 02 00 01 c2 02 00 01 c0 01 0a
```

图 3 某正常报文的二进制

报文解析之后得到各个字段的名称和值如图 4 所示。

```
TPKT, Version: 3, Length: 22
Version: 3
Reserved: 0
Length: 22
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Length: 17
PDU Type: CR Connect Request (0x0e)
Destination reference: 0x0000
Source reference: 0x0004
0000 .... = Class: 0
.... ..0. = Extended formats: False
.... ..0 = No explicit flow control: False
Parameter code: 0xc1 (src-tsap)
Parameter length: 2
Source TSAP: 0001
Parameter code: 0xc2 (dst-tsap)
Parameter length: 2
Destination TSAP: 0001
Parameter code: 0xc0 (tpdu-size)
Parameter length: 1
TPDU size: 1024
```

图 4 IEC61850 报文解析结果

异常报文保存形式如图 5 所示。

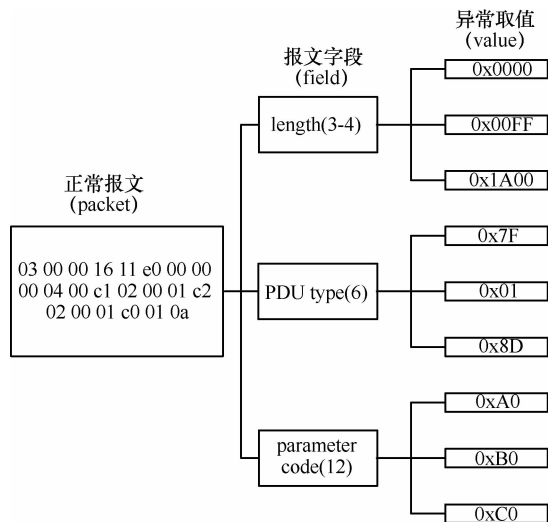


图 5 异常报文保存形式

算法 1 显示了异常报文样例的产生过程。该算法中最外层循环对测试样本的每个字段进行遍历。对于每个字段,如果有历史异常取值,则从历史异常取值中选取一部分,并随机生成一部分异常取值(5~18 行)。在该方法中,选取的历史异常报文数最多为异常报文总数的一半(7~11 行),这样既可以有效利用历史异常报文信息,也能够保证在测试过程中可以发现新的异常报文。

算法 1

```
(1) 初始化异常报文集合;
(2) foreach(字段 in 测试样本) //根据字段产生异常报文
(3) {
(4) 该字段异常报文数 number=len*10; //len 为字段长度
(5) if(该字段有历史异常取值) //获取历史异常取值
(6) {
(7) if(历史异常取值总数 > number/2)
(8) {
(9) 从异常取值中随机选择 number/2 个不同取值;
(10) 加入异常报文集合;
(11) number = number - number/2;
(12) }
(13) else
(14) {
(15) 所有历史异常取值,加入异常报文集合;
(16) number = number-所有异常取值数;
(17) } //随机生成一定的异常字段
(18) }
(19) 随机生成 number 个不同的异常取值,加入异常报文集合; //返回异常报文样例集合
(20) }
(21) return 异常报文集合;
```

3.3 测试系统的执行流程

算法 2 显示了测试的执行流程。该算法中,第 1、2 行为测试的准备阶段,需要读取测试报文样例文件,设置

被测设备的 IP 地址。第 3~20 行的双层循环为测试的执行过程,外层循环遍历样例文件中的测试基准报文,针对每个基准报文生成异常报文样本集合。内层循环遍历异常报文集合,且向设备发送异常报文之后,根据设备的状态记录导致设备出现异常的报文。并且在设备出现异常之后,暂停报文的发送工作直到设备恢复正常(第 12~15 行)。第 21~28 行是异常报文的验证过程,通过再次向设备发送已记录的异常报文,检验设备的状态,验证该报文的有效性,对检测出的异常报文进行验证的目的在于排除网络中断等客观因素造成的误报。最后根据已验证的异常报文信息生成测试报告(第 30 行)。

算法 2

```
(1) 获取 IEC61850 测试样本;    //测试样例加载分析
(2) 输入被测设备的 IP 地址;    //界面展示模块
(3) foreach(测试样本 in 所有测试样本)
(4) {
(5)    变异产生异常报文测试样例集合; //算法 1,
    异常报文产生模块
(6)    foreach(异常报文 in 异常报文样例集合)
(7)    {
(8)        向设备发送异常报文;
(9)        检测设备状态;          //报文发送
    模块
(10)       if(设备状态异常)      //报文发送
    模块
(11)       {
(12)           while(设备状态异常)
(13)           {
(14)               检测设备状态;
(15)           }                //报文发送
    模块
(16)           记录异常报文信息,加入异常报文检
    出集合;
(17)       }
(18)       更新界面;
(19)   }
(20) }
(21) foreach(异常报文 in 异常报文检出集合)
```

```
(22) {
(23)     向设备发送异常报文;
(24)     检测设备状态;          //报文发送
    模块
(25)     if(设备状态异常)      //报文发送
    模块
(26)     {
(27)         加入异常报文确认集合和异常报文历
    史信息中;
(28)     }
(29) }
(30) 生成并显示测试报告;      //报文生成
    模块
```

4 顽健性测试实验及结果分析

为了检验测试方法的有效性,及测试系统的可行性,在智能变电站实验室中执行测试过程。其中测试的前 3 个步骤形成了一个包括 8 个数据报文的 IEC61850 测试样本,接下来使用相同的测试样本,选择了 4 个不同厂商的设备运行测试系统,执行测试的后 3 个步骤。测试系统的执行过程如图 6 所示。

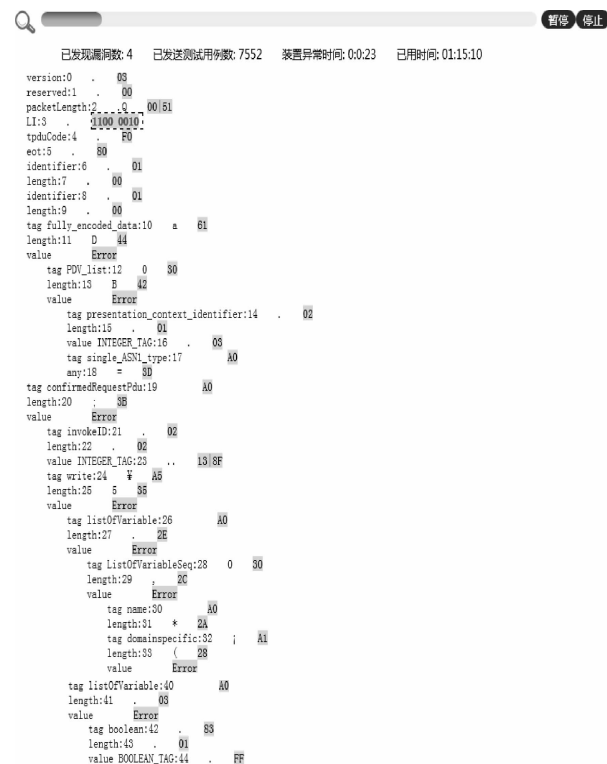


图 6 测试系统执行界面



在测试的执行过程中,会显示当前发送的测试用例数(异常报文数目)、发现的漏洞数(导致设备出现异常的异常报文数目)、装置的异常时间和测试的已用时间。同时显示当前发送的异常报文,其中虚线框出字段为发生变异的字段。图7按照 IEC61850 协议的分层统计了测试结果。

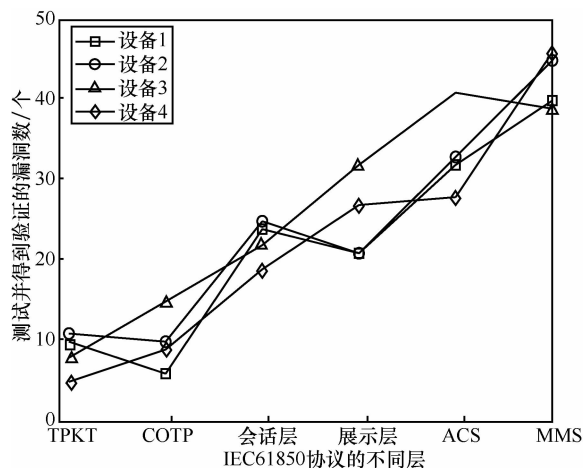


图7 测试结果

从图7中可以看出,执行相同的测试样本,4个设备均存在漏洞。MMS层的漏洞数目要高于TPKT层的漏洞数目,MMS层的报文结构复杂、测试用例多,检测出的漏洞也多。测试过程中的部分漏洞未得到确认,主要原因为设备的某些异常情况并非单个数据报文导致,而是连续几个有关联的报文导致,而测试软件只记录导致设备异常的上一个报文,因此无法验证漏洞是否存在。在下一步的工作中,还将对多个连续报文导致设备异常的情况进行研究。

5 结束语

为了测试变电站中智能电子设备通信模块的顽健性,本文设计了一种测试方法,并实现了对应的测试系统。实验结果表明本文的测试方法可以发掘导致设备出现异常的 IEC61850 异常报文,检测设备针对异常报文的抵御能力。本文仅研究了基于 TCP/IP 的通信模块的顽健性测试方法,可以研究 MAC 层协议通信模块的顽健性测试方法;本文的测试只是对装置的黑盒测试,可通过白盒测试进一步定位装置接收异常报文后出现异常的原因,还需要完善设备的顽健性以提高智能变电站的安全运行水平。

参考文献:

- [1] 庞思睿, 许鸿飞, 杜剑雯, 等. 面向物联网与三维可视化的智能变电站运行辅助管理系统研究与设计[J]. 电信科学, 2015, 31(5): 173-176.
PANG S R, XU H F, DU J W, et al. Research and design of intelligent substation of assist control system based on internet of things and three-dimensional visualization technology [J]. Telecommunications Science, 2015, 31(5): 173-176.
- [2] 吴威, 宋亮亮. 江苏电网 500kV 智能变电站建设技术综述[J]. 江苏电机工程, 2013(6): 51-54.
WU W, SONG L L. Review on 500kV substation construction technology in Jiangsu power grid [J]. Jiangsu Electrical Engineering, 2013(6): 51-54.
- [3] 雷斌, 王林章, 卜磊, 等. 基于状态机模型的构件顽健性测试[J]. 软件学报, 2010, 21(5): 930-941.
LEI B, WANG L Z, BU L, et al. Robustness testing for components based on state machine model [J]. Journal of Software, 2010, 21(5): 930-941.
- [4] 王乐春, 朱培栋, 龚正虎. 基于 RFMS 的顽健性测试技术研究[J]. 通信学报, 2005, 26(9): 21-29.
WANG L C, ZHU P D, GONG Z H. BGP robustness testing based on RFMS [J]. Journal on Communications, 2005, 26(9): 21-29.
- [5] 周章慧, 王同洋, 吴俊军, 等. 基于有限状态机的顽健性测试研究[J]. 计算机工程与科学, 2009, 31(5): 93-97.
ZHOU Z H, WANG T Y, WU J J, et al. Research of robustness testing based on FSM [J]. Computer Engineering & Science, 2009, 31(5): 93-97.
- [6] 郭强. 工控系统信息安全案例 [J]. 信息安全与通信保密, 2012, 33(12): 68-70.
GUO Q. Information security cases of industrial control system[J]. China Information Security, 2012, 33(12): 68-70.
- [7] 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 N, LI G, WANG D Q. Key technologies and construction methods of smart substation [J]. Power System Protection and Control, 2011, 39(5): 63-68.
- [8] DZUNG D, NAEDELE M, VOBHOFF T. Security for industrial communication systems[J]. Proceedings of the IEEE, 2005, 96(6): 1152-1177.
- [9] 曹一家, 姚欢, 黄小庆, 等. 基于 D-S 证据理论的变电站通信系统信息安全评估 [J]. 电力自动化设备, 2011, 31(6): 1-5.
CAO Y J, YAO H, HUANG X Q, et al. Security evaluation of substation communication system based on D-S theory [J]. Electric Power Automation Equipemnt, 2011, 31(6): 1-5.

[10] 潘海萍, 谢狄辉, 储乾旭. 基于 IEC61850 变电站辅助设备信息综合监管系统[J]. 江苏电机工程, 2013, 32(1): 65-67.

PAN H P, XIE D H, CHU Q X. Integrated monitoring system of auxiliary equipment in transformer substation based on IEC 61850[J]. Jiangsu Electrical Engineering, 2013, 32(1): 65-67.

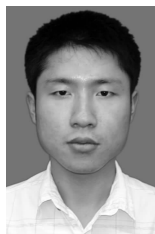
[作者简介]



姜海涛 (1985-), 男, 博士, 国网江苏省电力公司电力科学研究院工程师, 主要研究方向为电力系统信息安全。



李斌 (1983-), 男, 博士, 国网江苏省电力公司电力科学研究院高级工程师, 主要研究方向为电力调度自动化信息系统。



王祥 (1987-), 男, 国网江苏省电力公司电力科学研究院助理工程师, 主要研究方向为电力系统信息化。



陈锦铭 (1985-), 男, 国网江苏省电力公司电力科学研究院工程师, 主要研究方向为电力配网信息系统。



郭雅娟 (1975-), 女, 国网江苏省电力公司电力科学研究院研究员级工程师, 主要研究方向为电力信息管理。