



工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

分布式能源系统通信协议漏洞挖掘

汇报人：上海电力大学、王勇
汇报日期：2019年9月18日



1

分布式能源系统简介

2

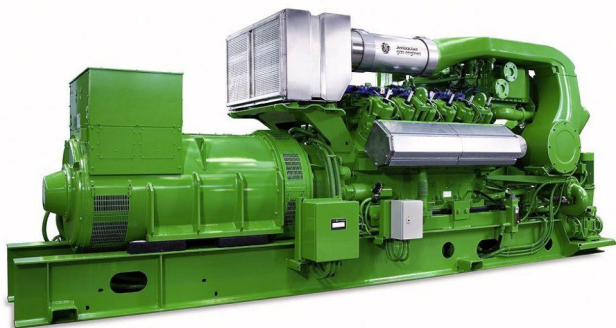
分布式能源系统中的通信协议

3

协议的漏洞挖掘

4

防御措施



燃气内燃机发电机组

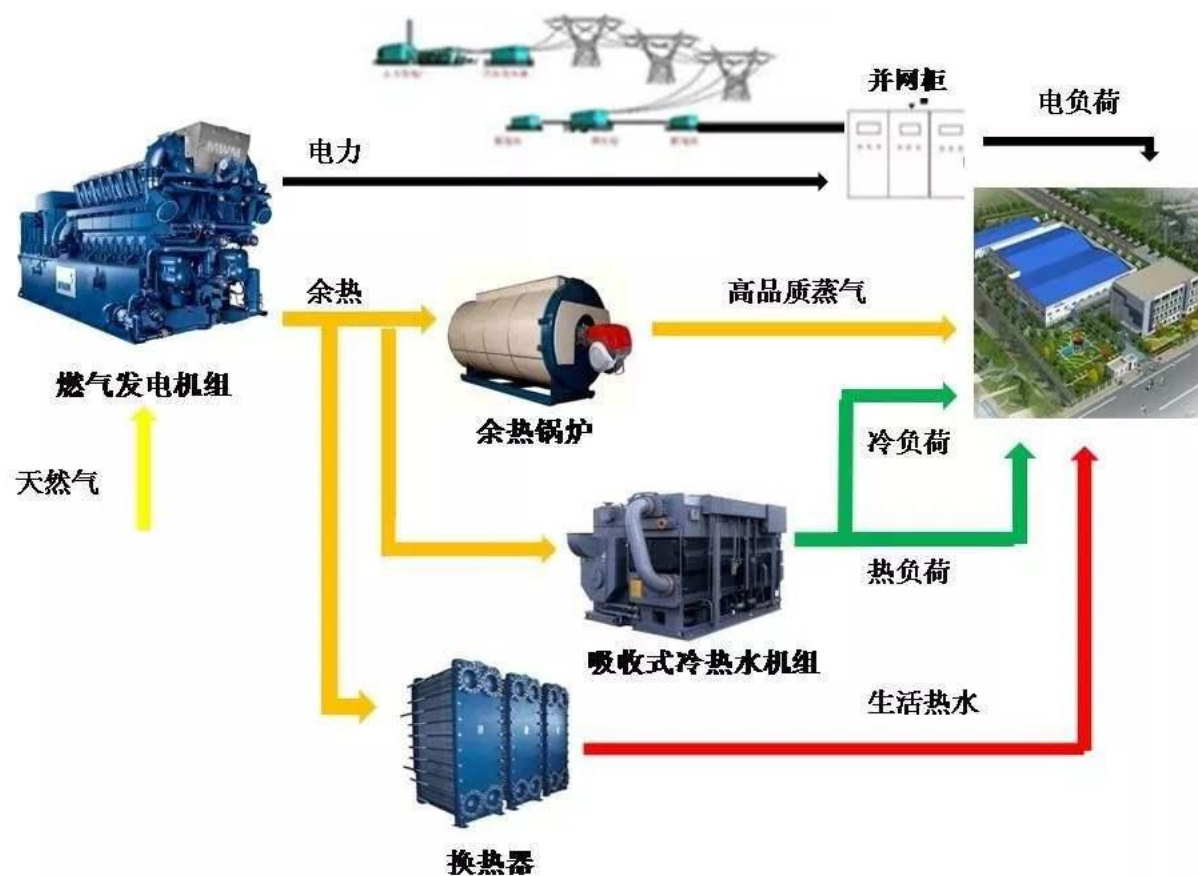


溴化锂吸收式冷热水机组



华电上海迪士尼分布式能源站项目，实现了冷、热、电、压缩空气四联供。

上海迪士尼，分布式利用率达85%以上，比传统模式提高大约1倍。
多联供能源站每年可节约标准煤2万吨，相当于每年少砍伐木材4万吨



分布式能源 热、电、冷三联供

所谓“分布式能源”（Distributed Energy resources）是指分布在用户端的能源综合利用系统。一次能源以气体燃料为主；二次能源以分布在用户端的热、电、冷联产为主，其他中央能源供应系统为辅，实现以直接满足用户多种需求的能源梯级利用。



家用空调



家用热水器



中国华电集团公司是全国性五家国有独资发电企业集团之一，是较早涉足天然气分布式能源行业的发电集团，也是目前国内分布式能源装机规模最大、项目数量最多的发电集团。



国家能源 分布式能源技术研发(实验)中心



1

分布式能源系统简介

2

分布式能源系统中的通信协议

3

协议的漏洞挖掘

4

防御措施



智能电表



智能电表



集中器

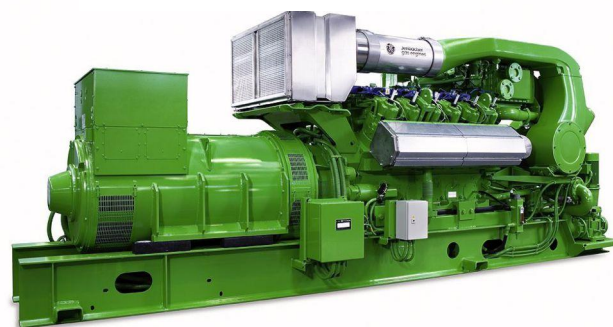
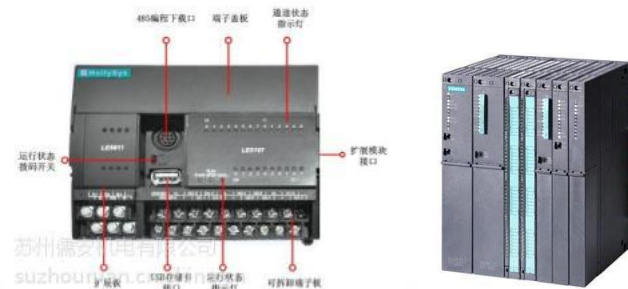
天线



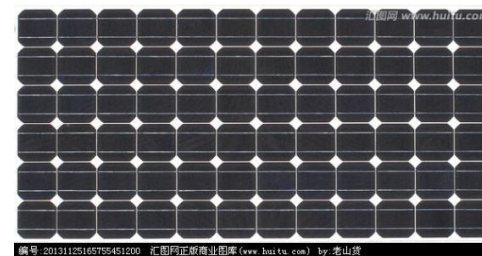
控制箱



溴化锂吸收式冷热水机组



燃气内燃机发电机组



太阳能光伏电板



1MW储能系统逆变器



1500V光伏并网逆变器

储能逆变器

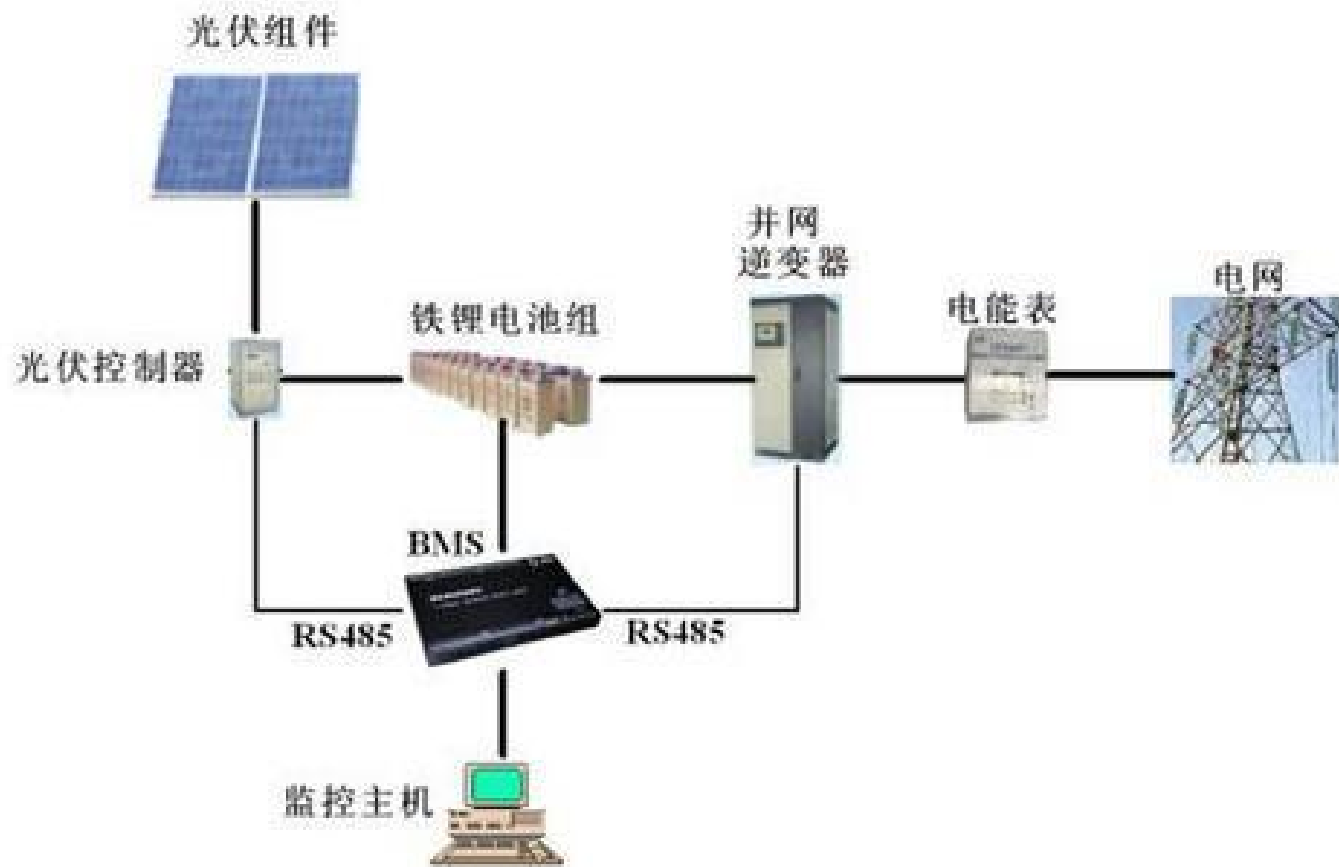


图-4

- a) 智能电表645规约
- b) GDW 374.2-2009 电力用电信息采集协议
- c) Modbus TCP
- d) IEC 61850
- e) TCP/IP
- f) Profinet



智能电表数据采集--645规约



645规约适用于本地系统中**多功能电能表的费率装置与手持单元设备**进行点对点的或一主多从的**数据交换**方式，

Modbus通信协议安全性实例分析

三相四线电子式电能表



单相电子式电能表



使用Modbus通讯协议的智能电表

Modbus协议是应用于电子控制器上的一种通用语言。通过此协议，**控制器相互之间、控制器经由网络（例如以太网）和其它设备之间可以通信。**

此协议支持传统的RS-232、RS-422、RS-485和以太网设备。许多工业设备，包括PLC，DCS，**智能仪表**等都在使用Modbus协议作为他们之间的通信标准。

Modbus通讯协议，可通过RS485通信接口完成**编程和抄表操作。**



1

分布式能源系统简介

2

分布式能源系统中的通信协议

3

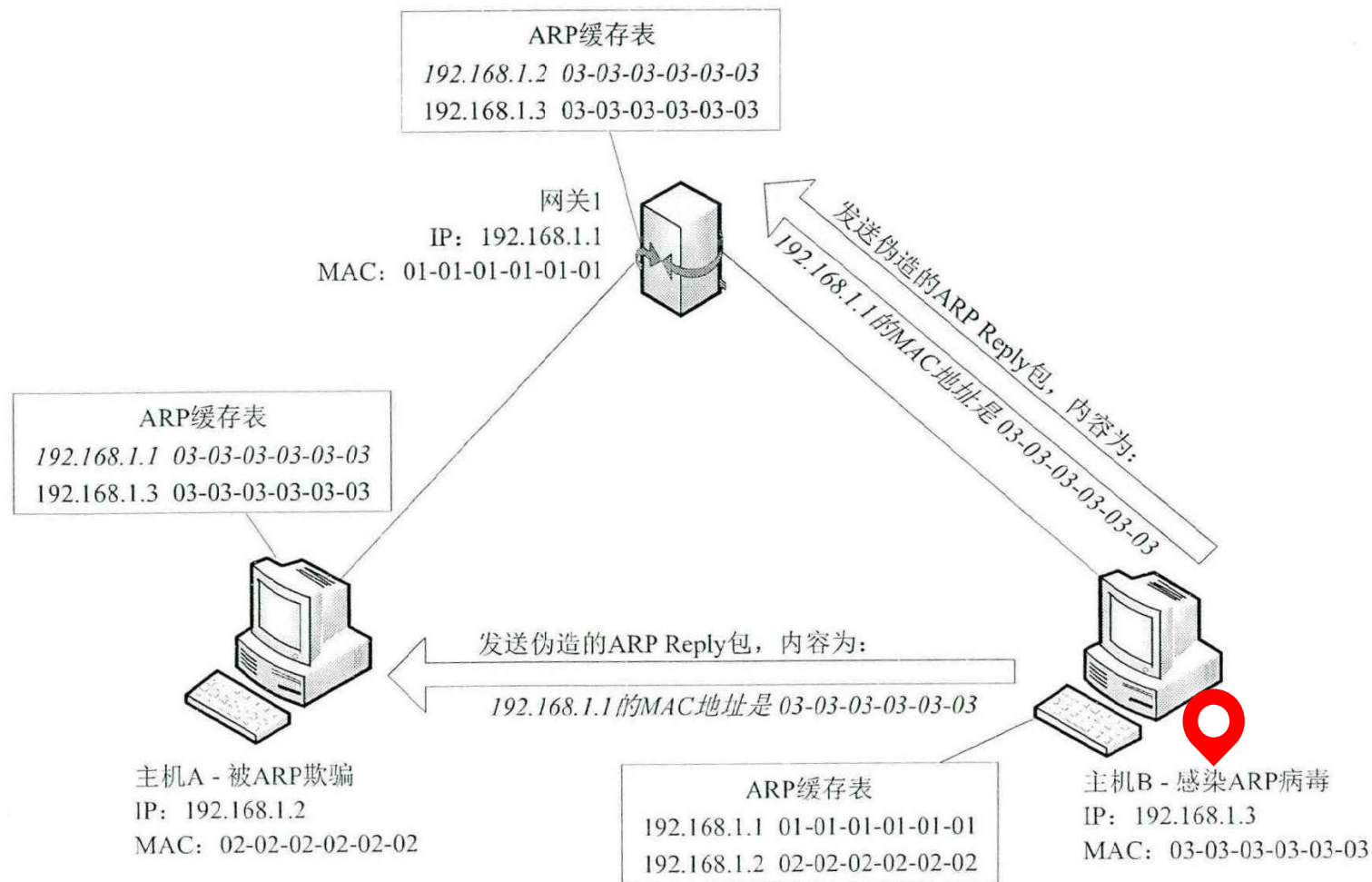
协议的漏洞挖掘

4

防御措施



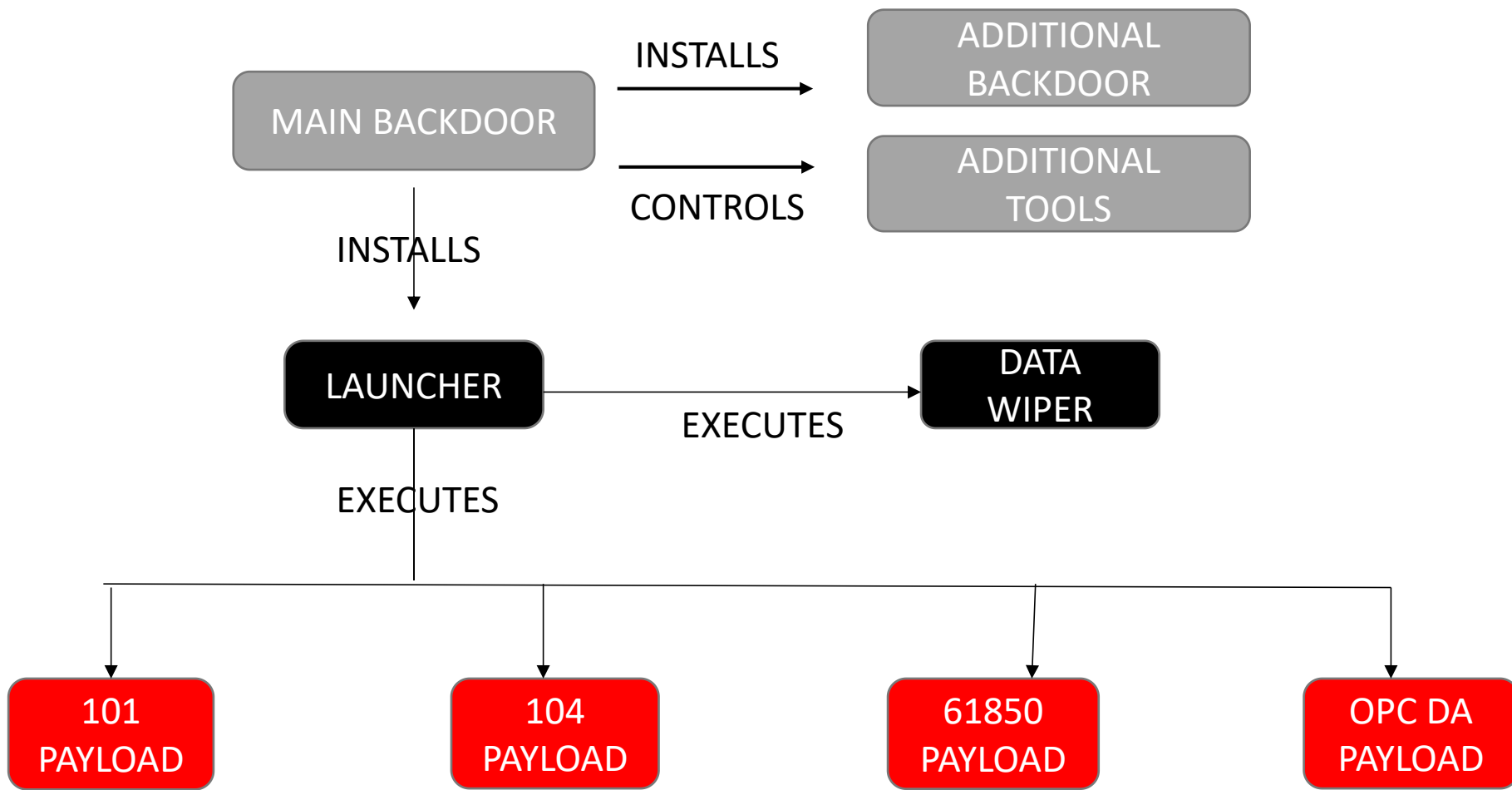
ARP欺骗攻击





TCP协议漏洞攻击

- ◆ 攻击者获取源/目的端口号，即可伪造SEQ符合条件的TCP数据包，发送给TCP连接的任一方。
- 攻击方式一：
 - 伪造RST包复位正常的TCP连接。滑动窗口越大，主机越容易受到RST攻击，若持续发送伪造RST包，则受害者无法进行正常通信
 - RST数据包：连接错误时复位TCP连接
 - 三种原因导致接收到RST数据包：
 - 向不存在的或没有在监听的端口发送SYN，试图建立连接
 - TCP试图主动取消一个连接，主动终止的一方会向另一方发送RST
 - TCP错误地接收到了不属于任何一个连接的数据包

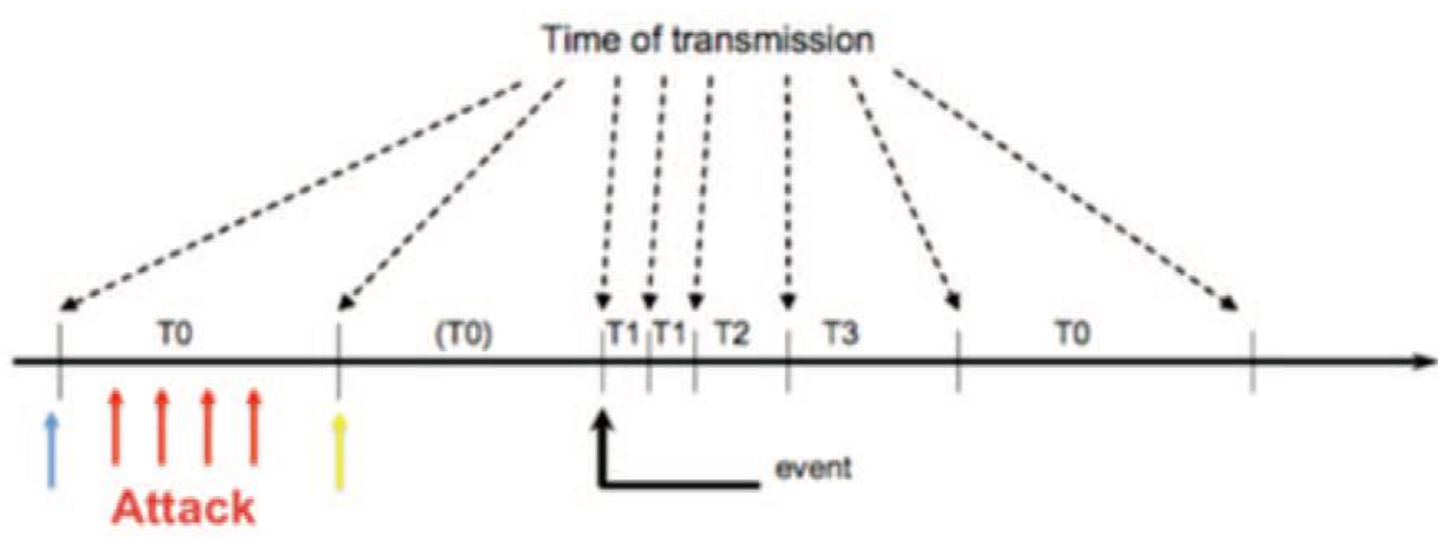


- 面对通用对象的变电站事件（GOOSE）是IEC 61850标准中用于满足变电站自动化系统快速报文的一种机制
- 可以传输开入(智能终端的常规开入等), 开出(跳闸, 遥控, 启动失灵, 联锁, 自检信息等), 实时性要求不高的模拟量(环境温湿度, 直流量)
- 常见传输布尔量, 整型, 浮点型, 位串

- GOOSE采用多播方式传送数据

-以太网传输方式有: 点对点、广播、多播

- GOOSE采用连续多次传送的方式实现可靠传输: T1-2ms T2-4ms T3-8ms To-5s





	GOOSE	
应用层	IEC61850-8-1	
表示层	ASN.1/BER	
会话层		
传输层		
网络层		
数据链路层	以太网/IEC 802.1Q	
物理层	光纤	双绞线

GOOSE消息欺骗步骤:

- 第一，监视物理端口上的数据包，寻找基于以太网类型标识的GOOSE消息。
- 第二，使用抽象语法符号1 (ASN1) 和基本编码规则(BER)[18]解码GOOSE消息。
- 第三，更改每个数据集中的值，保持不同计数器和计时器的顺序。
- 第四，使用BER对数据包进行编码，并通过克隆源MAC地址的物理端口发送数据包。。



GOOSE和SMV 修改攻击

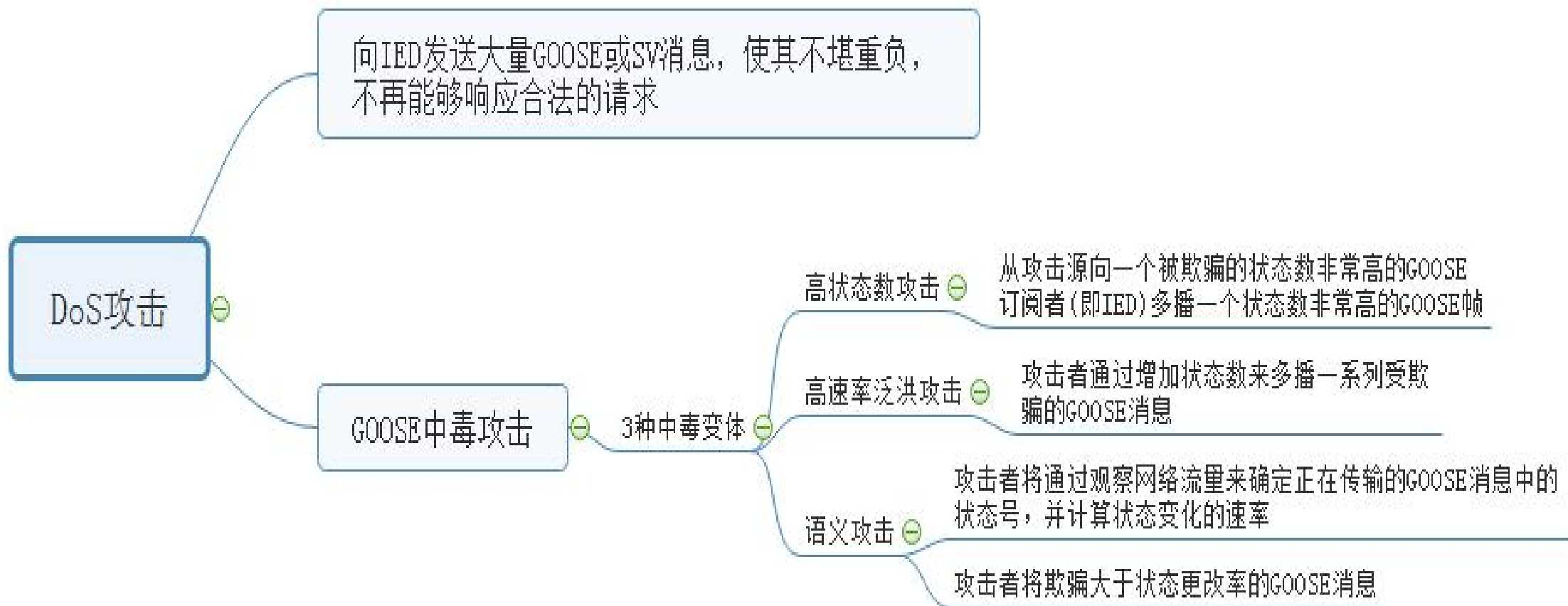
- 用于攻击IED,这种攻击通过在恶意软件中实现进一步扩展，恶意软件可以捕获、修改和重新注入GOOSE消息到网络中。

GOOSE和SMV DoS攻击

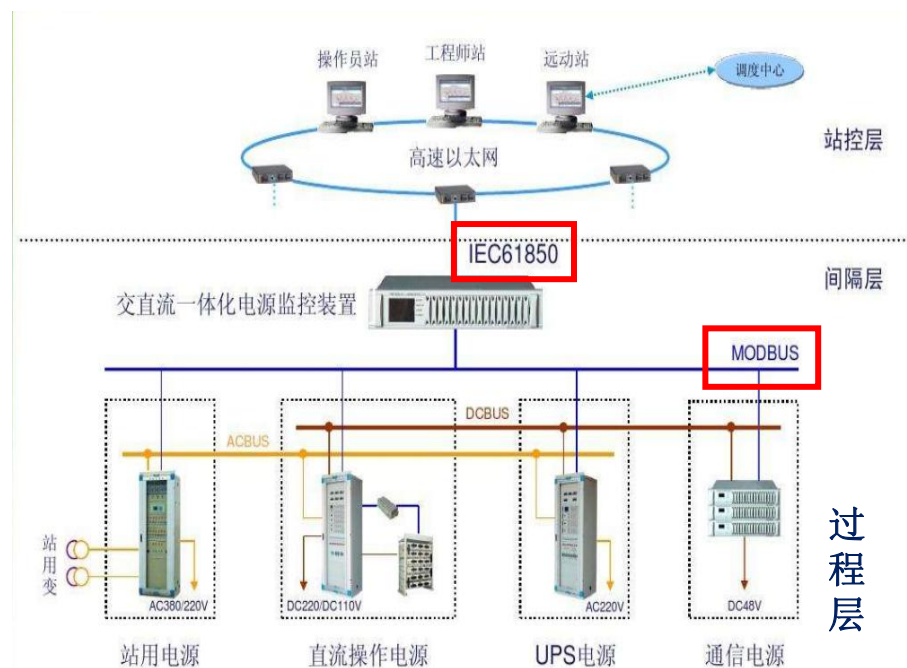
- 发送大量GOOSE或SMV消息来压制IED，这最终将阻止IED为合法GOOSE或SMV消息提供服务
- GOOSE中毒攻击，使合法的GOOSE消息被废弃，随后被IED忽略

GOOSE和SMV 重放攻击

- 获两个主机之间通过网络发送的数据包的行为，其目的是在不进行修改的情况下重放有效负载，以获得相同的结果



IEC61850协议中间人攻击



(1) 在攻击机上执行编写的arp欺骗程序，欺骗client端自己为server端。

(2) 利用iptables的NFQUEUE动作，将数据包从内核空间提取到用户空间。

```
root@kali: ~#  
root@kali: ~# iptables -A FORWARD -s 192.168.1.108 -d 192.168.1.107 -j NFQUEUE  
root@kali: ~#  
(server: 192.168.1.107 b8:27:eb:f1:f4:b6(树莓派))
```

篡改后发给server端。

中间人截获的IEC61850数据包

10	8.180122000	Vmware_8b:e1:	LiteonTe_6b:ae:	ARP	42	192.168.2.100 is at 00:0c:29:8b:e1: (duplicate use of 192.168.2.107 detected!)
11	10.00726700	Vmware_8b:e1:	Raspberr_f1:f4:	ARP	42	192.168.2.107 is at 00:0c:29:8b:e1:
12	10.18036300	Vmware_8b:e1:	LiteonTe_6b:ae:	ARP	42	192.168.2.100 is at 00:0c:29:8b:e1: (duplicate use of 192.168.2.107 detected!)

client端发送给server端的MMS数据包被中间人截获

No.	Time	Source	Destination	Protocol	Length	Info
10	5.588291000	192.168.2.107	192.168.2.100	TCP	74	50325->102 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3434153 TSecr=0 WS=1024
11	5.588346000	192.168.2.107	192.168.2.100	TCP	74	[TCP Out-Of-Order] 50325->102 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3434153 TSecr=0 WS=1024
12	5.589159000	192.168.2.100	192.168.2.107	TCP	74	102->50325 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=8991561 TSecr=3434153 WS=128
13	5.589175000	192.168.2.105	192.168.2.100	ICMP	102	Redirect (Redirect for host)
14	5.589242000	192.168.2.100	192.168.2.107	TCP	74	[TCP Out-Of-Order] 102->50325 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=8991561 TSecr=3434153 WS=128
15	5.590938000	192.168.2.107	192.168.2.100	TCP	66	50325->102 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3434154 TSecr=8991561
16	5.590957000	192.168.2.107	192.168.2.100	TCP	66	[TCP Dup ACK 15#1] 50325->102 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3434154 TSecr=8991561
17	5.591008000	192.168.2.107	192.168.2.100	COTP	88	CR TPDU src-ref: 0x0002 dst-ref: 0x0000

client端发给server端的数据包

目的MAC变为了： 00:0c:29:8b:e1:*，而不是b8:27:eb:f1:f4:* 中间人攻击成功。

0000	00 0c 29 8b e1	b8 ee 65 6b ae	08 00 45 00	..).....ek....E.
0010	00 ef dc 8e 40 00 40 06	d7 5a c0 a8 02 6b c0 a8		@.@. .Z...k..

IEC61850协议攻击效果

在攻击机上设置数据包长度攻击，数据包末尾填充111111.....

```
***** send length attack package *****  
Sent 1 packets.  
time: 0.001201 s
```

wireshark截获数据包显示数据包末尾填充1111....，客户端上没有回显

```
root@kali: ~/桌面/libIEC61850-master/examples/iec61850_client_example3# ./client_example3 192.168.1.107 102  
Connection failed!  
root@kali: ~/桌面/libIEC61850-master/examples/iec61850_client_example3# ./client_example3 192.168.1.107 102  
^C
```

1. flag攻击
2. 数据包长度攻击
3. 功能码攻击
4. 攻击清零

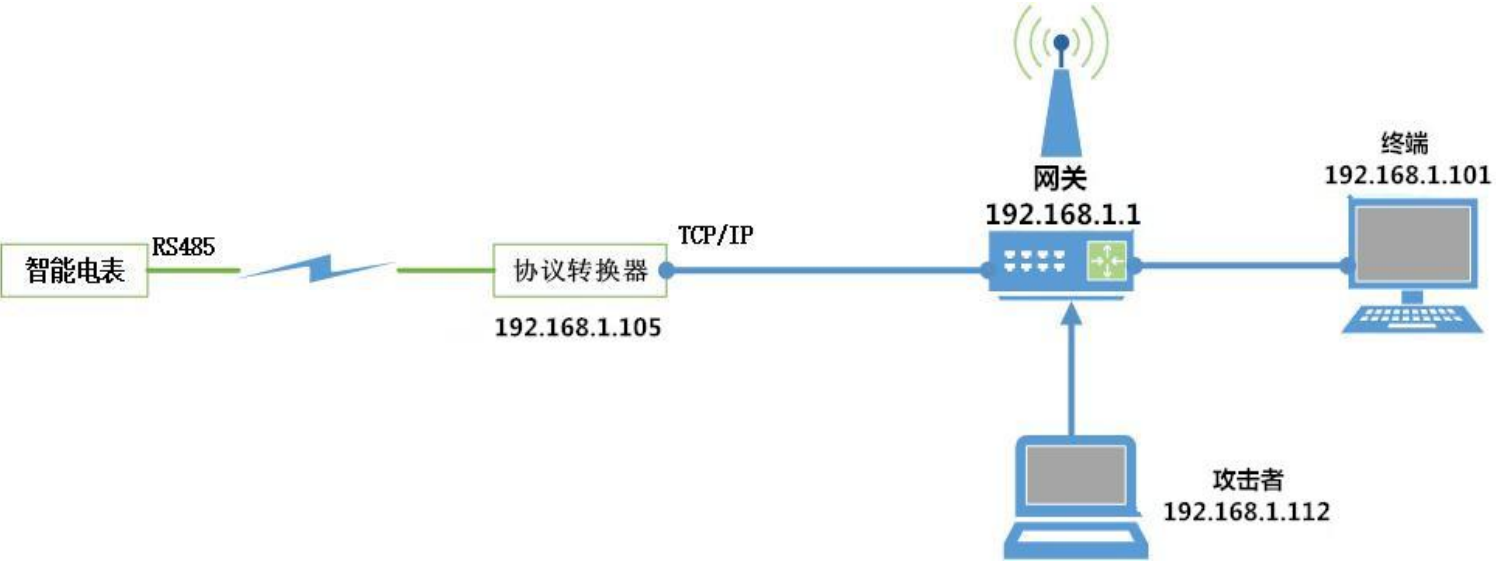
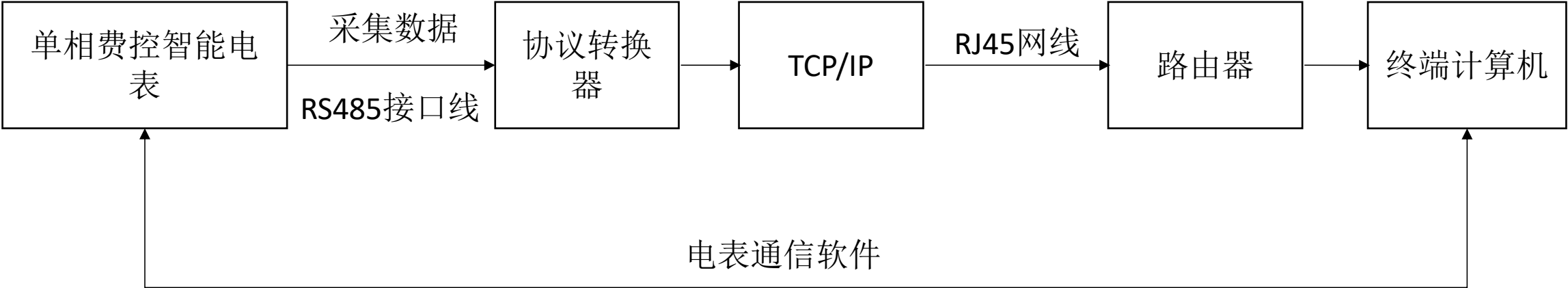
攻击机上设置mms协议的功能码为0xFF

```
***** this is not request mms package *****  
pass  
Sent 1 packets.  
time: 0.001296 s
```

数据包发送后，客户端上回显“段错误”

```
root@kali: ~/桌面/libIEC61850-master/examples/iec61850_client_example3# ./client_example3 192.168.1.107 102  
Connection failed!  
root@kali: ~/桌面/libIEC61850-master/examples/iec61850_client_example3# ./client_example3 192.168.1.107 102  
^C
```

智能电表645规约安全性实例分析



(1) 缺乏身份认证和权限区分

携带控制码满足协议的**格式和规范**，就可以建立起一个合法会话
安全隐患：攻击者很容易利用**网络攻击手段**发动中间人攻击

(2) 未采取加密通信

采用**明文**进行数据传输
安全隐患：通过**抓包软件**就可以截获并解析出里面的数据

(3) 校验方式简单

两种校验方式：传输数据的每一个字节的**偶校验位(P)**
在数据链路层上传输一帧信息的**校验码 (CS)**

安全隐患：**伪造正确的校验码**就可以制造虚假的数据通过协议进行传输

实验过程

<3>登录ZLAN改设备目的ip

攻击者通过运行监听程序实现监听智能电表，使用浏览器搜索攻击者ip加端口号，可以直接登录到ZLAN设备配置界面，更改设备目的ip为攻击者ip（192.168.1.114）。

192.168.1.114:8888/ip.html

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

ZLANWWW.ZLMCU.COM

设备信息

设备名称		固件版本	V1. 518	设备ID	28-4E-BF-03-45-01
------	--	------	---------	------	-------------------

网络设置

设备IP	192.168.1.105	设备端口	13800	网页访问端口	80
工作模式	TCP 客户端	子网掩码	255.255.255.0	网关	192.168.1.1
目的IP/DNS	192.168.1.109	目的端口	4196	IP模式	静态

串口设置

波特率	2400	数据位	8	校验位	奇校验
停止位	1	流控	无		

高级设置

无数据重启	禁用	无数据重启时间	300	5~1270 秒	断线重连时间	12	1~255 秒
-------	----	---------	-----	----------	--------	----	---------

修改网页登录密码

新密码		再次输入新密码			
-----	--	---------	--	--	--

提交修改

Transferring data from 192.168.1.114...

设备信息

设备名称	ZLDEV_LM
------	----------

网络设置

设备IP	192.168.1.105
工作模式	TCP 客户端
目的IP/DNS	192.168.1.114

串口设置

波特率	2400
停止位	1

高级设置

无数据重启	禁用
-------	----

修改网页登录密码

新密码	
-----	--

更改后

实验过程

在目的主机中刷新端口信息，发现目的ip已被篡改

刷新后

刷新前

网络设置

IP模式	静态
IP地址	192 . 168 . 1 . 105
端口	13800
工作模式	TCP 客户端
子网掩码	255 . 255 . 255 . 0
网关	192 . 168 . 1 . 1
目的IP或域名	192.168.1.109 本地IP
目的端口	4196

设备设置

设备信息	网络设置	高级选项
虚拟串口 COM1	IP模式 静态	DNS服务器IP 192 . 168 . 0 . 1
设备型号 ZLSN2003	IP地址 192 . 168 . 1 . 105	目的模式 动态
设备名称 ZLDEV_LM	端口 13800	转化协议 无
设备ID 284EBF034501	工作模式 TCP 客户端	保活定时时间 60 (秒)
固件版本 V1.518	子网掩码 255 . 255 . 255 . 0	断线重连时间 12 (秒)
该设备支持功能	网关 192 . 168 . 1 . 1	网页访问端口 80
☐ 网页下载	目的IP或域名 192.168.1.114 本地IP	所在组播地址 230 . 90 . 76 . 1
☒ 域名系统	目的端口 4196	IO端口配置0x 00
☒ REAL_COM协议	串口设置	无数据重启 ☐ 每隔 300 (秒)
☐ Modbus TCP转RTU	波特率 2400	定时发送参数 ☐ 每隔 5 (分钟)
☒ 串口修改参数	数据位 8	更多高级选项...
☒ 自动获取IP	校验位 偶校验	分包规则
☐ 存储扩展EX功能	停止位 1	数据包长度 1300 (字节)
☒ 多TCP连接	流控 无	数据包间隔 (越小越好) 6 (毫秒)
系统默认参数	保存默认参数	升级固件
加载默认参数		重启设备
		修改设置
		取消

Modbus通信协议安全性实例分析

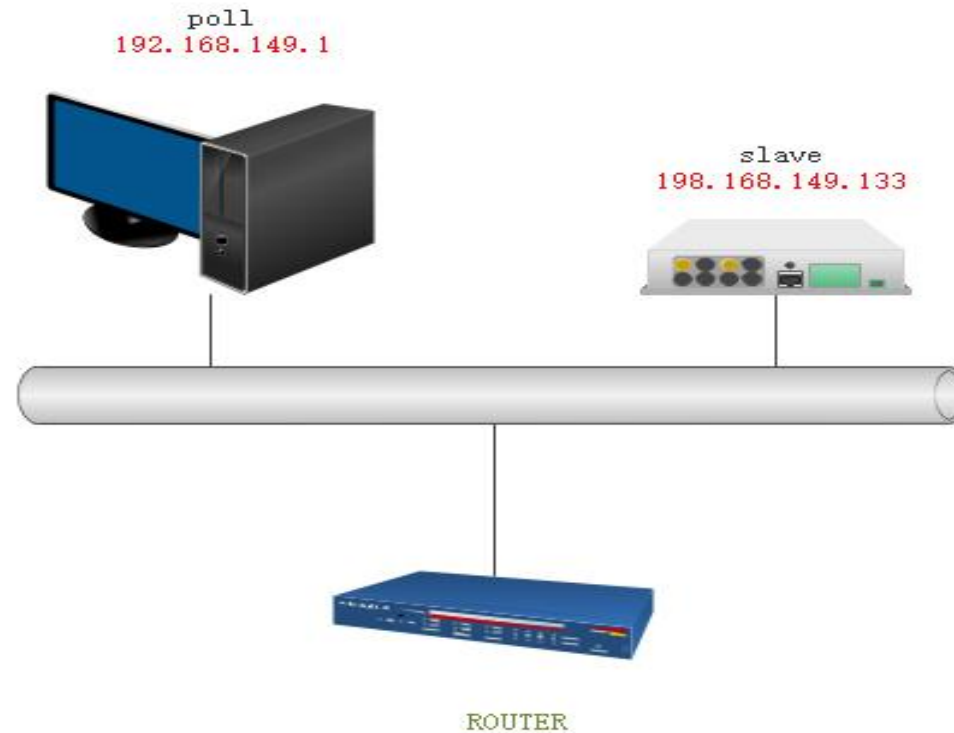
win7虚拟机

物理机IP: 192.168.1.100
虚拟机IP:192.168.149.133

wireshark软件

modbus工具

1. modbus poll
2. modbus slave



攻击实验结果

MODBUS Eth. TCP/IP PLC - Simulator (port: 502)

Connected (1/10) : (received/sent) (1/1) Send write data.

Address: Hex Dec I/O Holding Registers Fmt: decimal Prot: MODBUS TCP/I Clone

Address	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
40001-40010	0	1000	2100	3	4	5090	6000	7	1	1
40011-40020	10	1	1	0	0	0	0	0	0	0
40021-40030	0	0	0	0	0	0	0	0	0	0
40031-40040	0	0	0	0	0	0	0	0	0	0
40041-40050	0	0	0	0	0	0	0	0	0	0
40051-40060	0	0	0	0	0	0	0	0	0	0
40061-40070	0	0	0	0	0	0	0	0	0	0
40071-40080	0	0	0	0	0	0	0	0	0	0
40081-40090	0	0	0	0	0	0	0	0	0	0
40091-40100	0	0	0	0	0	0	0	0	0	0
40101-40110	0	0	0	0	0	0	0	0	0	0
40111-40120	0	0	0	0	0	0	0	0	0	0
40121-40130	0	0	0	0	0	0	0	0	0	0
40131-40140	0	0	0	0	0	0	0	0	0	0
40141-40150	0	0	0	0	0	0	0	0	0	0
40151-40160	0	0	0	0	0	0	0	0	0	0
40161-40170	0	0	0	0	0	0	0	0	0	0
40171-40180	0	0	0	0	0	0	0	0	0	0
40181-40190	0	0	0	0	0	0	0	0	0	0
40191-40200	0	0	0	0	0	0	0	0	0	0

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

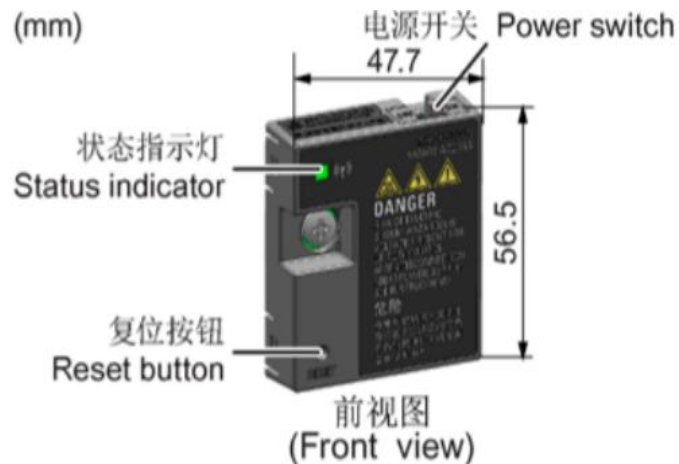
T Comms

西门子变频器Web Socket协议

把电压和频率固定不变的交流电变换为电压或频率可变的交流电的装置称作“变频器”。



西门子V20变频器



SINAMICS V20 智能连接模块

该连接模块是一款集成了 Wi-Fi 连接功能的Web服务器模块。

通过此模块可实现从带无线网卡的传统PC或智能手机对变频器进行web访问，从而对变频器进行快速调试、参数设置、JOG、监控、诊断、备份与恢复等操作。

此款电机具有牢固的零部件连接、高性能防护等级、提高绝缘性能、宽电压宽频、恒可或一定速度范围内可变频调速等特点。



西门子电机1LA7070-4AB10-Z

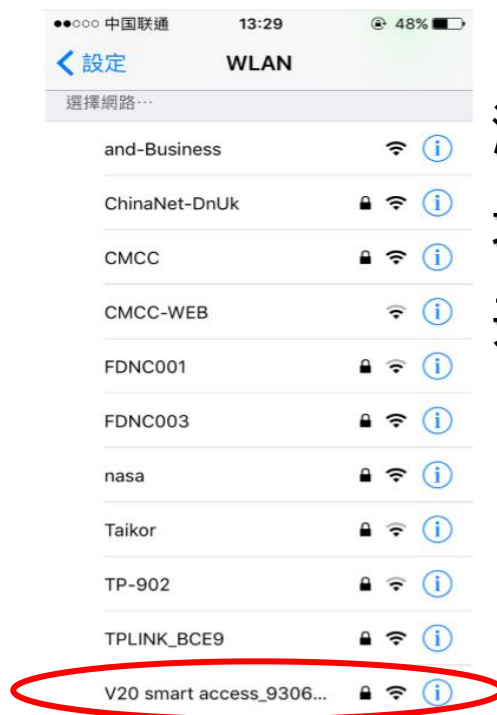


西门子变频器Web Socket协议

(1) 使用无线智能模块控制电机——设备连接



无线模块安装至变频器



该智能模块的无线网络SSID为：
“V20 smart access_9306”

浏览器的地址栏中输入网
址(<http://192.168.1.1>)打
开 V20 网页



控制界面

西门子变频器Web Socket协议

(2) 针对于无线变频器的数据篡改和信号分析的攻击测试:

● Inverter ready		SINAMICS V20
☰ ↑	Monitoring	
Running status		
Setpoint		5.3 Hz
Output frequency		0 Hz
Actual speed		0 rpm
Actual power		2 kW
Motor temperature	1234123123123123123123123	°C
Output voltage	输出电压被篡改	shiep V

监控篡改图

faSum,200,0,0,2

分析出来的websocket控制信号

不管是控制还是显示数据，控制信号的最后一位是最主要的。

通过篡改最后一位后，在输出电压也就是output voltage这一项上面改成了shiep，其实现过程是使用代理机制，主要核心是能够阻断websocket的控制包。



1

分布式能源系统简介

2

分布式能源系统中的通信协议

3

协议的漏洞挖掘

4

防御措施



序号	题目名称	内容要求
1	变电站通信系统设计	1) 构建“变电站”通信系统。 2) 硬件采集数据到计算机, 3) 计算机传递信息到硬件设备 4) 抓取数据包, 分析协议格式
2	配电系统通信系统设	1) 构建“配电”通信系统: 2) 硬件采集数据到计算机, 3) 计算机传递信息到硬件设备 4) 抓取数据包, 分析协议格式
3	变电站3D软硬件协同仿真系统设计	1) Unity 3D 2017 搭建变电站3D实物系统 2) 3D仿真系统与变电站监控系统联动; 3) 硬件获取信号, 传送到3D仿真环境中的监控系统, 4) 监控系统中的操作可以改变硬件的状态信息。
4	配电3D软硬件协同仿真系统设计	1) Unity 3D 2017 搭建配电实物系统: 2) 3D实物系统与变电站监控系统联动; 3) 硬件获取信号, 传送到3D仿真环境中的监控系统, 4) 监控系统中的操作可以改变硬件的状态信息。
5	变电站3D仿真系统与监控系统数据联动	1) 变电站3D仿真软件系统, 不包括硬件 2) 构建组态王或WINCC监控界面 3) 3D仿真系统数据与监控界面数据同步联动。
6	配电3D仿真系统与监控系统数据联动	1) 配电3D仿真软件系统, 不包括硬件 2) 构建组态王或WINCC监控界面 3) 3D仿真系统数据与监控界面数据同步联动。
7	3D仿真系统攻击模拟	1) 攻击方式: 口令破解、网络扫描、注入攻击、数据修改、缓冲区溢出等攻击等 2) 3D 仿真环境应当能够进行攻击模拟, 3D仿真系统的HMI状态会发生相应变化。
8	仿真系统入侵防御系统设计	1) 仿真环境虚拟专用网网络分区、访问控制、 2) 基于开源组件Snort的IDS或IPS等。 3) 当攻击发生时, 能够有效检测出上述各种攻击行为
9	工控协议通信过程仿真	1) 工控通信协议包括: Modbus/TCP通信协议, 西门子Profint协议, IEC104规约 三种。 2) 实现这些协议的通信, 抓取数据包内容3) 动态展示通信数据包
10	工控设备仿真软件设计	1) 西门子PLC-1200、 2) 西门子Logo、 3) 西门子变频器、 4) 变频电机、 5) 远程传输单元RTU、 6) 液压仪器、 7) 流量仪表等。



序号	题目名称	内容要求
1	西门子变频电机的攻击测试	1) 搭建西门子变频电机的通信环境 2) 利用Wfi控制电机转速和转向 3) 破解wif密码 4) 攻击导致西门子电机停机
2	机器臂控制系统攻击测试	1) 构建机器臂的控制系统 2) 利用网络控制机器臂的运行 3) 网络攻击机械臂导致异常 4) 防御机器臂的攻击
3	馈线终端通信系统攻击测试	1) 搭建馈线终端的通信环境 2) 获取馈线终端的传输数据 3) 攻击篡改馈线终端数据 4) 提出可信数字传输防御方法
4	北斗授时系统攻击测试	1) 搭建北斗授时系统实验环境 2) 获取北斗卫星的实时数据 3) 分析传输协议的安全性 4) 北斗授时系统的攻击方法
5	无人机的攻击测试方法	1) 搭建无人机的通信环境 2) 利用手机监控无人机的运行 3) 对通信过程进行攻击测试, 劫持无人机 4) 防御方式
6	智能台灯的红外线攻击测试	1) 搭建红外智能台灯的环境 2) 建立红外通信攻击 3) 改变台灯的正常状态 4) 提出防御措施
7	燃气分布式能源信息安全测评系统设计	1) 设计燃气分布式能源系统的测评内容2) 根据等级保护的相关要求选择测评项目3) 制定测评算法4) 建立信息安全测评系统
8	基于龙芯开发板的可信通信程序设计	1) 在龙芯开发版上运行系统 2) 熟悉编程环境 3) 设计数据的安全传输程序 4) 给出攻击测试与防御方法



工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

Thanks