国家电网
STATE GRID
国网河南省电力公司
STATE GRID HANAN ELECTRIC POWER CORPORATION

从stuxnet到industroyer
--从工控病毒看电网信息安全

国网河南电科院
郭志民

国家电网
STATE GRID
国网河南省电力公司
STATE GRID HANAN ELECTRIC POWER CORPORATION

目录 Contents

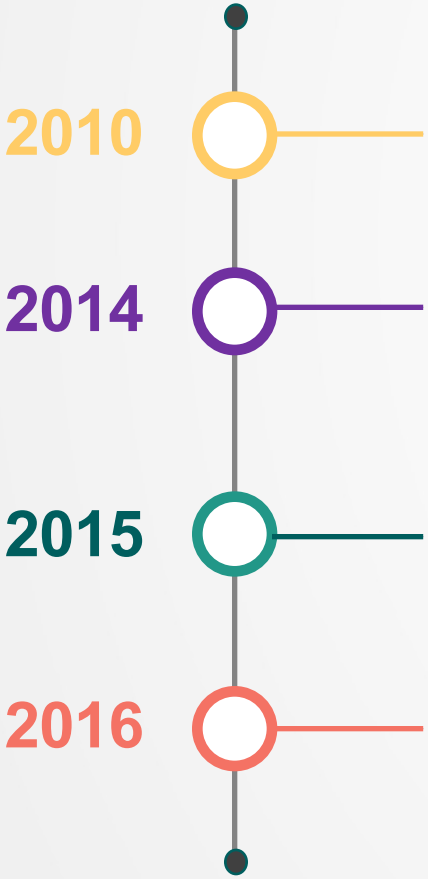
01 从病毒开始

02 一些思考

03 几点建议

一. 从病毒开始

目前现实世界当中出现过四例针对工业控制系统的恶意程序肆虐案例，分别为最为知名的美国政府开发之Stuxnet（即震网病毒）、BlackEnergy、Havex、以及新出现的Industroyer病毒。



“震网”病毒，导致伊朗布什尔核电站遭攻击，实现两个功能，一是使伊朗的离心机运行失控，二是掩盖发生故障的情况

“Havex”病毒，欧洲蔓延，使用OPC Da协议收集网络和联网设备。

“BlackEnergy”病毒，乌克兰至少三个区域的电力系统被攻击导致大规模停电。通过Office 文件攻击，删除文件系统，实现SSH远程访问。

“Industroyer”病毒，直接控制断路器，可导致变电站断电，目前支持四种工控协议：IEC 60870-5-101、IEC 60870-5-104、IEC 61850以及OLE for Process Control Data Access（简称OPC DA）。

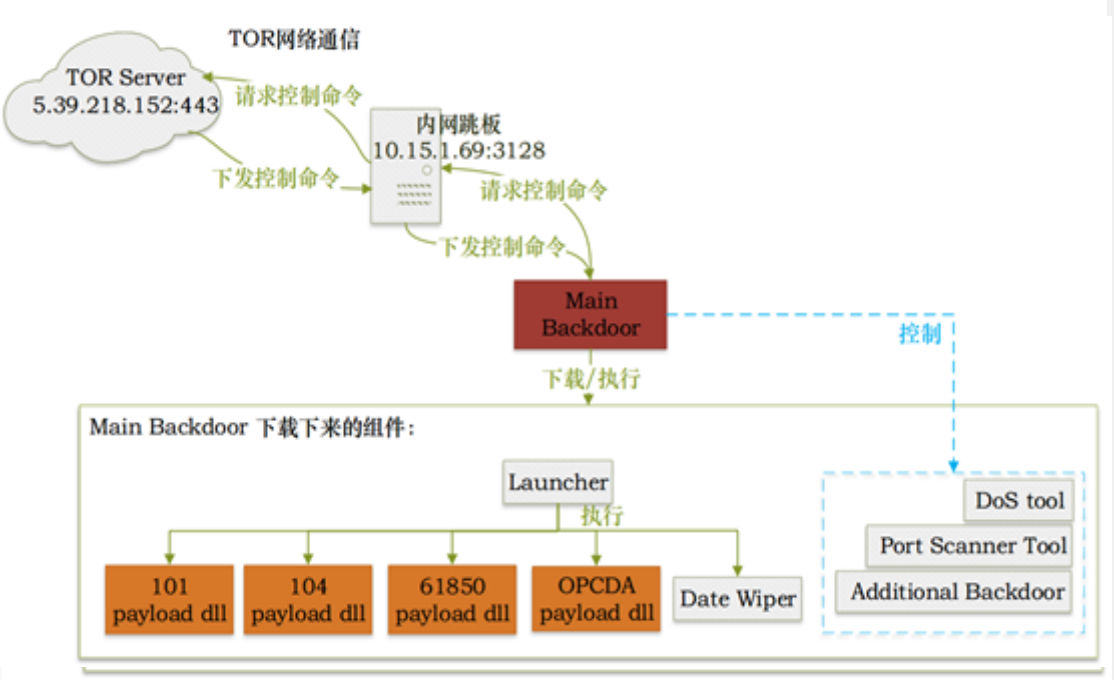
Industroyer病毒简况

Industroyer恶意软件目前支持四种工控协议：IEC 60870-5-101、IEC 60870-5-104、IEC 61850以及OLE for Process Control Data Access（简称OPC DA）。其中IEC 60870-5-101、IEC 60870-5-104、IEC 61850都是在我国调度、配电自动化和智能变电站中广泛适用的协议。

一. 从病毒开始

Industroyer执行过程

Industroyer恶意软件由一系列攻击模块组成，其中存在一个主后门模块，用于连接C&C下载另一批模块执行，这些模块分别为：实现DLL Payload模块执行的加载器模块（Launcher）、实现数据及痕迹清理的haslo模块、实现IP端口扫描的port模块以及实现西门子SIPROTEC设备DoS攻击的DoS攻击模块。其中，DLL Payload模块包含实现IEC104工控协议的104.dll模块。104.dll模块，主要实现了IEC104通信协议，通过配置文件的配置信息实现与目标RTUs之间的通信。



恶意软件大致工作流程

一. 从病毒开始

Launch模块分析

国家电网 STATE GRID
国网河南省电力公司 STATE GRID HANAN ELECTRIC POWER CORPORATION

通过逆向分析发现Launcher.exe会首先调用磁盘擦除模块“haslo.dat”（实为动态连接库）,然后再根据参数调加指定的payload模块，并调用其Crash函数。

```
1  DWORD __stdcall StartAddress()
2  {
3    HMODULE v0; // eax@1
4    FARPROC v1; // eax@2
5
6    SetUnhandledExceptionFilter(TopLevelExceptionFilter);
7    Sleep(0x36EE80u);
8    v0 = LoadLibraryW(L"haslo.dat");
9    if ( v0 )
10   {
11     v1 = GetProcAddress(v0, "Crash");
12     if ( v1 )
13       ((void (__cdecl *)(_DWORD))v1)(0);
14   }
15   return 0;
16 }
```

调用磁盘擦除模块

```
30 if ( v1 && pNumArgs == 4 )
31 {
32   SetCurrentDirectoryW(v1[1]);
33   v3 = LoadLibraryW(v2[2]);
34   hLibModule = v3;
35   if ( v3 )
36   {
37     v9 = GetProcAddress(v3, "Crash");
38     if ( v9 )
39     {
40       v4 = CreateWaitableTimerA(0, 1, 0);
41       if ( v4 )
42       {
43         if ( SetWaitableTimer(v4, &DueTime, 0, 0, 0, 1) )
44         {
45           WaitForSingleObject(v4, 0xFFFFFFFF);
46           v5 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartAddress, 0, 0, 0);
47           SetThreadPriority(v5, 2);
48           v6 = GetCurrentProcess();
49           SetPriorityClass(v6, 0x80u);
50           v7 = GetCurrentThread();
51           SetThreadPriority(v7, 2);
52           ((void (__cdecl *)(LPWSTR))v9)(v2[3]);
53         }
54       }
55     }
```

调用Payload

一. 从病毒开始

编写104模块调用程序

由于104.dll为动态连接库文件，不能直接运行，而Launcher.exe有较大的破坏性，为了继续下一步的分析工作，因此按照Lancher.exe调用模式，编写程序，加载104.dll，调用Crash 函数，并传入配置文件名称。

test.py | test.txt | main.cpp | 104client.py | test104.cpp

```
1  // test104.cpp : 定义控制台应用程序的入口点。
2  //
3  #include "stdafx.h"
4  #include <windows.h>
5
6  int main()
7  {
8      HMODULE hDllLib = NULL;
9      hDllLib = LoadLibrary(_T("104.dll"));
10     if (hDllLib)
11     {
12         typedef int(__cdecl *LPCRASH)(LPTSTR);
13         LPCRASH lpCrash = (LPCRASH)GetProcAddress(hDllLib, "Crash");
14         if (lpCrash)
15         {
16             TCHAR configName[] = _T("config.ini");
17             (lpCrash)(configName);
18         }
19         FreeLibrary(hDllLib);
20     }
21     system("pause");
22     return 0;
23 }
```

一. 从病毒开始

104简介

IEC-104规约是厂站与调度主站间通讯的规约，以以太网为载体，采用平衡传输，TCP/IP网络通信端口号为2404。IEC-104规约以0x68为启动字符，紧接APDU长度和4个8位控制域，之后是用户数据。

起始字 0X68	APCI	APDU
APDU 长度		
控制域 1		
控制域 2		
控制域 3		
控制域 4		
IEC 60870-5-101 和 IEC 60870-5-104 定义的 ASDU	ASDU	

IEC-104规约帧分为三种类型：

a) 可计数的信息传输功能的帧，简称I帧或者I格式帧。

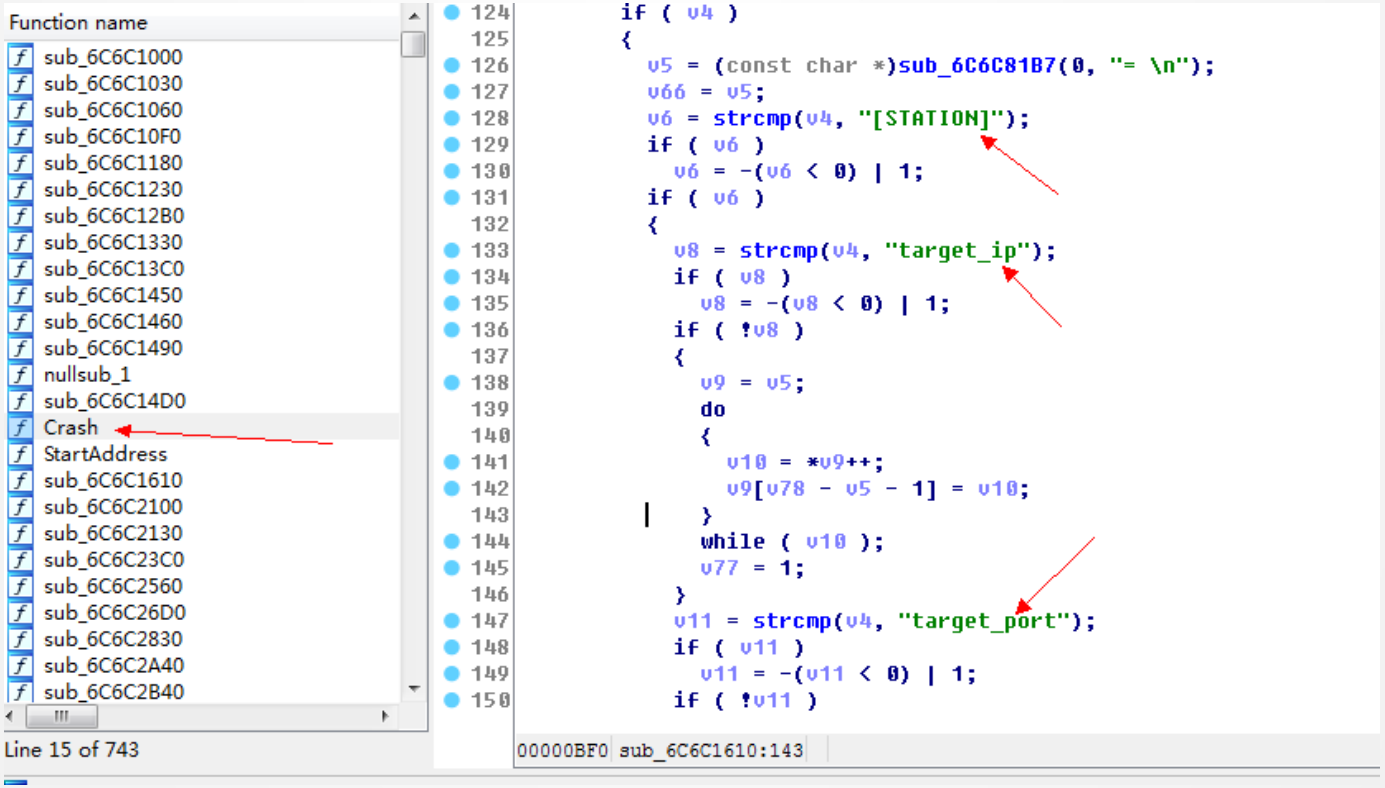
b) 可计数的确认功能的帧，简称S帧或者S格式帧。

c) 启动、停止、测试功能的帧，简称U帧或者U格式帧。

一. 从病毒开始

104模块分析

逆向分析104.dll攻击模块得知，crash函数为攻击发起的主函数，该函数可加载一个配置文件，配置文件字段有[STATION]、target_ip、target_port、logfile、asdu、stop_comm_service、change、range、first_action、operation等，如下图所示：



一. 从病毒开始

104模块配置文件

属性	说明
[station]	表示一个变电站的配置段
target_ip	目标ip地址
target_port	目标端口地址
use_log	是否记录日志 1/0
stop_comm_service	是否停止服务 1/0
stop_comm_service_name	服务名称
Silence	是否静默，1/0 为0时控制台有输出
Asdu	目标RTU公共地址编号
first_action	初次操作 On/Off
Change	是否进行反转操作
Timeout	发送命令后接收命令的间隔时间，单位毫秒
socket_timeout	接收命令的等待时间，单位毫秒
command_type	def 、short、long、persist 发送命令长指令、短指令等
Operation	操作模式 range、sequence、shift 决定使用地址范围方式、序列方式等
Range	信息体地址，指定范围
Sequence	信息体地址，指定具体地址
Shift	信息体体偏移量

一. 从病毒开始

104模块行为分析

读取配置文件之后，104 payload模块会根据配置文件中定义的每个“[STATION]”创建一个线程。在每个线程中，104payload会尝试使4标准协议与指定的IP地址行连接。在连接建立之前，104 payload模块根据配置文件中stop_comm_service属性配置去尝试终止与设备建立连接的合法进程（其默认值为D2MultiCommService.exe，也可通过stop_comm_ervice_name属性配置）。

然后根据operation属性来指定如何使用攻击地址。

第一种操作模式是range模式。是指尝试攻击range属性中指定的目标信息体地址范围。

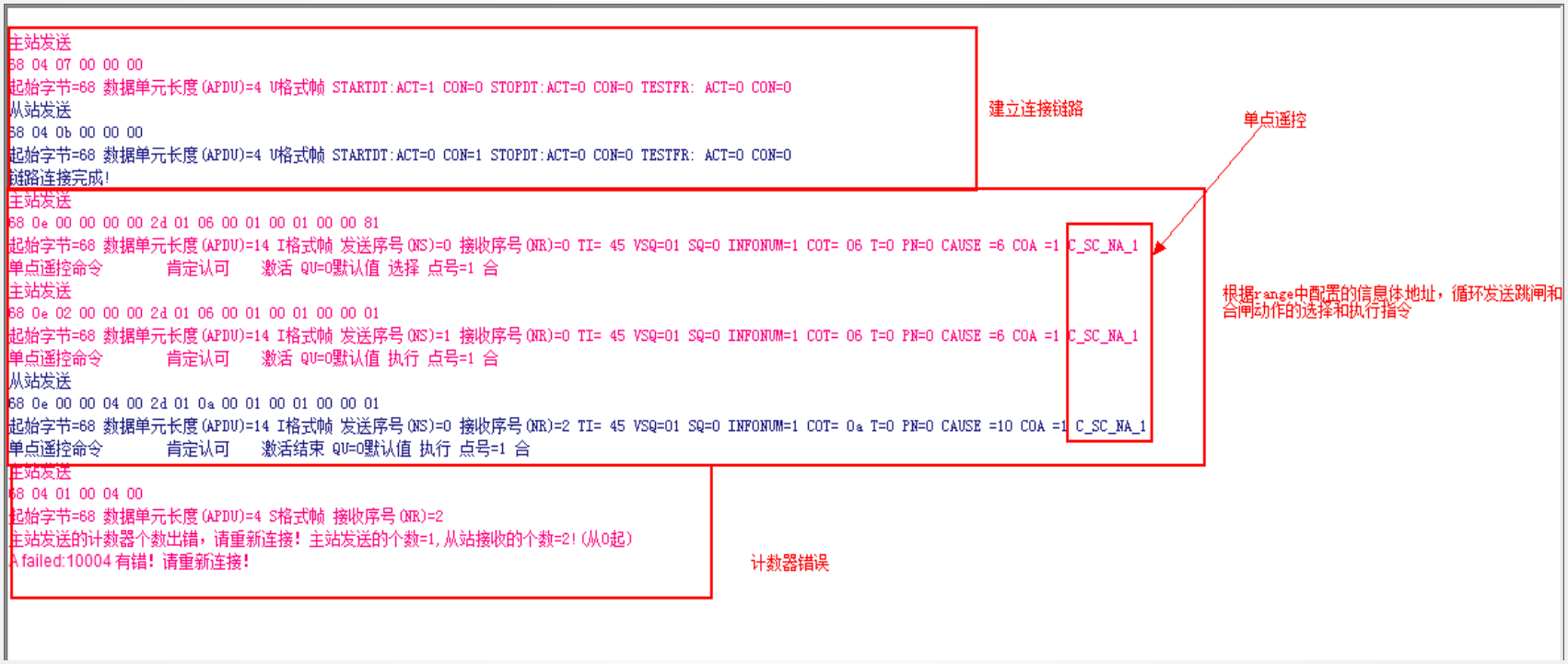
第二种操作模式是shift模式，这种模式跟range的模式非常的相似，首先是对range属性指定的目标信息体地址范围进行攻击，然后再在range属性中指定的信息体地址范围加上shift属性指定的偏移量再次进行攻击。猜测是为了适应变电站遥控地址间隔相对固定的情况。

第三种操作模式是sequence模式，指定明确的信息体地址。

一. 从病毒开始

模拟通讯测试

运行104规约模拟器模拟104从站，然后运行104 payload模块，观测通讯报文。



一. 从病毒开始

报文解析

通过对报文的分析，104 payload模块与子站的通讯过程如下：

1）104 payload模块首先按照配置文件中的从站IP地址和端口建立socket连接，发送U帧握手报文。

2）然后根据配置文件中的信息体地址和FirstAction选项配置，发送I帧单点打开或者闭合操作选择和执行命令。

3）然后会根据配置文件中的Change选项，进行反转操作，如第一次操作为打开，第二次操作就为闭合。

4）不断重复上述2、3步骤。

二. 一些思考

黑客画像

病毒涵盖了101、104、61850、OPC这些普遍应用的控制系统通讯规约，病毒作者对工业控制系统有着深入的了解。

入侵能否成功，要依赖配置文件的准确性，在配置文件中需要包含入侵目标的IP、公共地址、信息体地址等信息，甚至清楚知道合法程序的进程。因此入侵者对目标电网控制系统的情况十分了解。

病毒可以不断开合断路器设备，除了要造成停电影响外，更是企图破坏一次设备，造成电网故障难以恢复。

还有，一点点的马虎……

二. 一些思考

电力监控系统规定

电力监控系统安全防护工作应当落实**国家信息安全等级保护制度**，按照国家信息安全等级保护的有关要求，坚持**“安全分区、网络专用、横向隔离、纵向认证”**的原则，保障电力监控系统的安全。

二. 一些思考

认知问题

系统存在漏洞！

我是隔离的

协议不安全！

我是隔离的

终端未加固！

我是隔离的

。 。 。 。

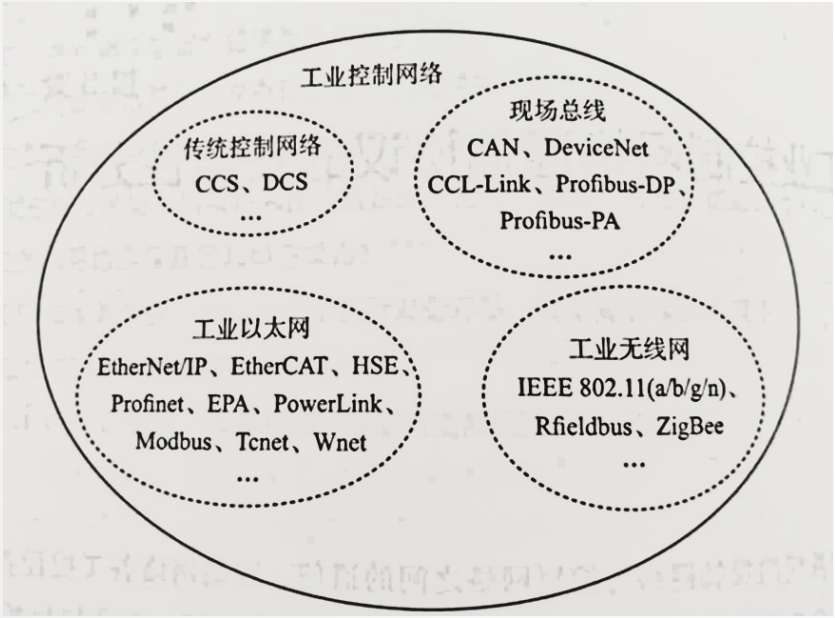
二. 一些思考

协议的原罪

概括来说协议安全性问题分为：

1. 涉及方面引入的安全问题，即协议自身的设计对安全性考虑的先天不足；

2. 协议的不正确实现引起的安全问题，黑客入侵时将对这些不安全的设计或者实现进行相关的渗透和利用。



工业控制网络的协议分类

IEC为例分析存在的安全问题：

1. IEC协议的固有问题

1）缺少认证机制

2）缺少授权机制

3）缺少加密机制

2. IEC60870-5-104协议实现产生的问题

1）TCP/IP层安全问题

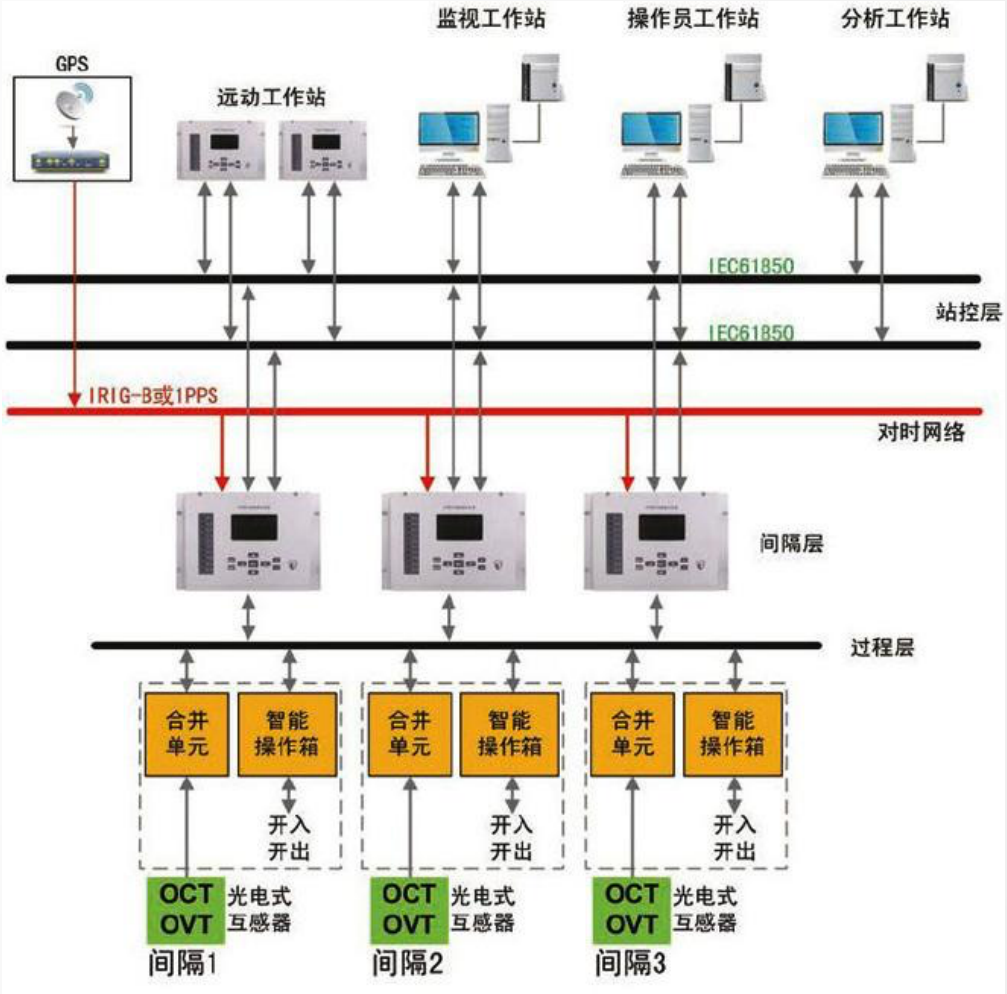
2）功能码滥用

二. 一些思考

工控系统IT化

1、IT服务器
2、通用操作系统
3、以太网络、TCP / IP协议
4、通用开发组件

接触了解相关设备漏洞
更加容易



二. 一些思考

管理措施方面不具体

关闭或拆除主机上不必要的软盘驱动、光盘驱动、USB接口、串型口、无线蓝牙等。确要保留的必须通过安全管理及技术措施实施严格监控。

生产控制大区的安全区之间应当采用具有访问控制功能的网络设备、防火墙或者相当功能的设施，实现逻辑隔离。

二. 智能电网监控系统安全防护现状

国家电网
STATE GRID
国网河南省电力公司
STATE GRID HANAN ELECTRIC POWER CORPORATION

- 系统、策略更新不及时
- 内部信息泄漏
- 主站系统内部缺乏安全机制
- 终端认证不严格

三、几点建议

防护目标

抵御黑客、病毒、恶意代码等通过各种形式对系统发起的恶意破坏和攻击，特别是能够抵御集团式攻击，防止由此导致一次系统事故或大面积停电事故及二次系统的崩溃或瘫痪。

- 使用安全的通信协议
- 采用加固操作系统
- 细化安全管理细则
- 针对性的安全配置
- 采用可信计算技术
- 终端严格认证

谢 谢！