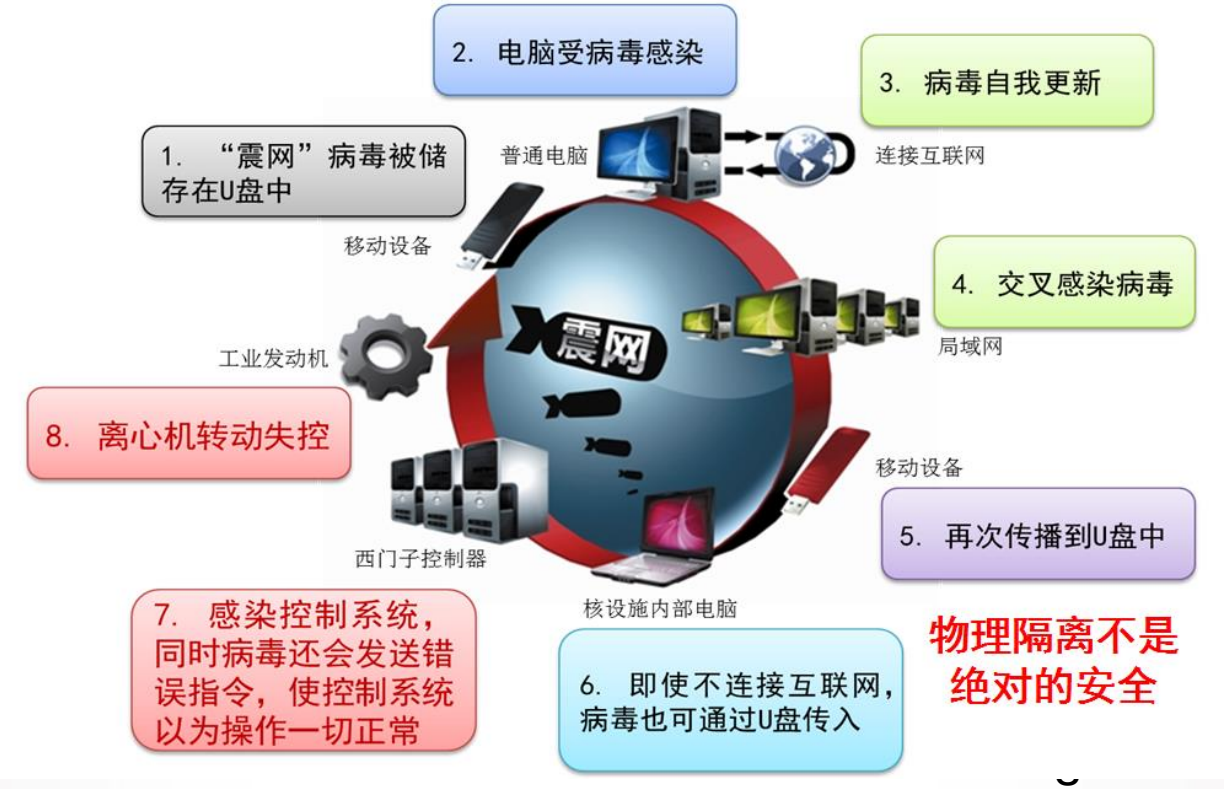
国家电网公司
STATE GRID
CORPORATION OF CHINA

目 录

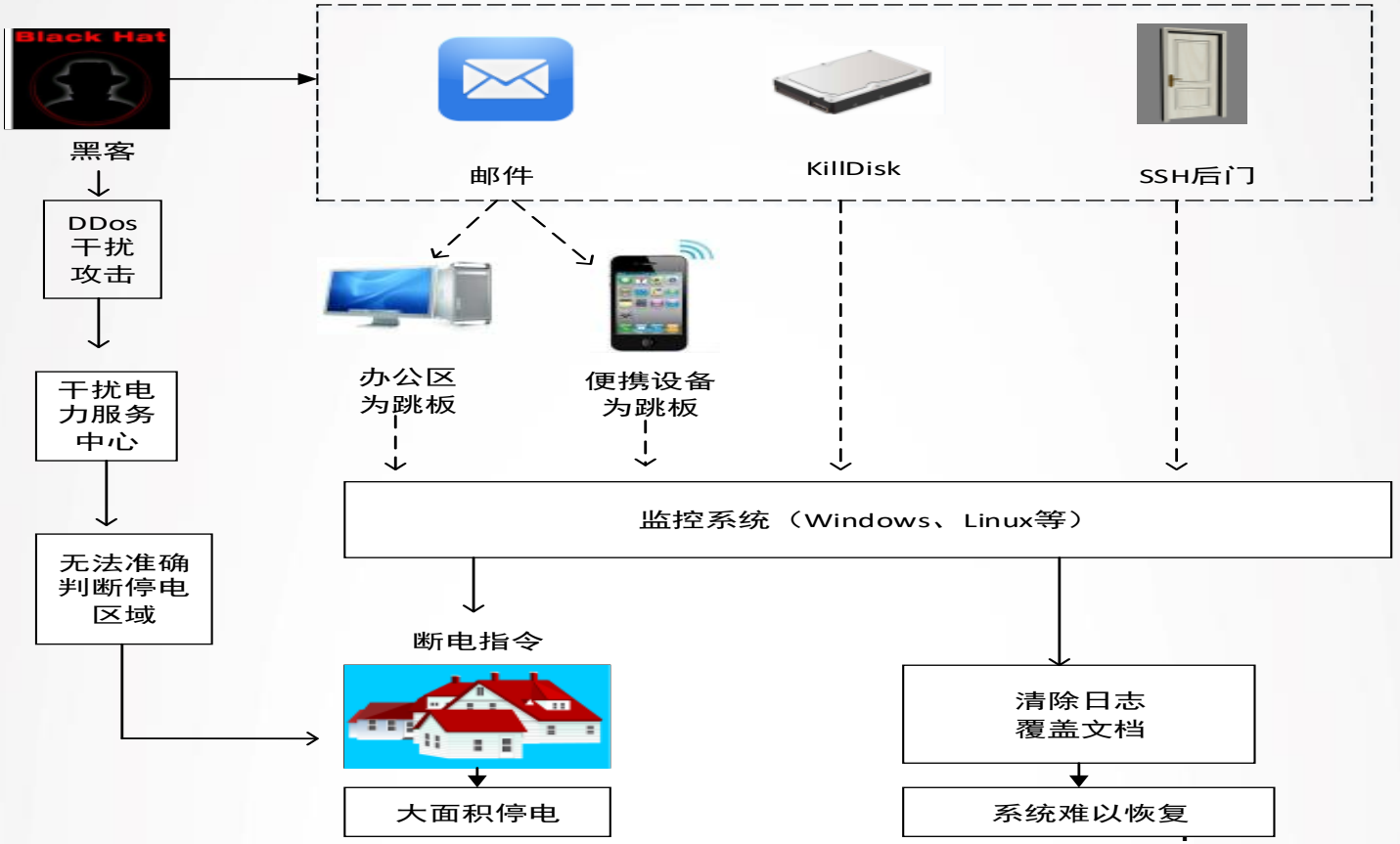
背景

2011年2月，伊朗突然宣布暂时卸载首座核电站——布什尔核电站的核燃料，因为布什尔核电站遭到“震网”病毒攻击，1/5的离心机报废。自2010年8月该核电站启用后就发生连串故障，伊朗政府表面声称是天热所致，但真正原因却是核电站遭病毒攻击。一种名为“震网”（Stuxnet）的蠕虫病毒，侵入了伊朗核电站，导致大量离心机无法正常工作。



背景

2015年12月23日，乌克兰电力部门遭到恶意病毒攻击，至少三个区域的电力系统被BlackEnery恶意软件攻击，其中部分变电站的控制系统（SCADA）遭到破坏，监控管理系统同时遭到入侵，导致发电设备产生故障，造成用户大面积停电。



概念

工业控制系统（Industrial Control Systems,ICS），是由各种自动化控制组件和实时数据采集、监测控制组件等共同构成。

其组件包括数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）、远程终端（RTU）、智能电子设备（IED），以及确保各组件通信的接口技术。

典型的ICS控制过程通常由控制回路、HMI、远程诊断与维护工具三部分组件共同完成，控制回路用以控制逻辑运算，HMI执行信息交互，远程诊断与维护工具确保ICS能够稳定持续运行。

术语

工业控制系统其他专业术语：

PCS

过程控制系统

ESD

应急停车系统

HMI

人机界面(Human Machine Interface)

MIS

管理信息系统(Management Information System)

SIS

生产过程自动化监控和管理系统（Supervisory Information System)

MES

生产执行管理系统

术语

工业控制系统其他专业术语：

DCS

被用来控制工业生产过程，如发电、炼油、水和废水处理、化工、食品、汽车生产。DCS被集成为一个控制架构，包含一个监督级别的控制，监督多个、集成的子系统，负责控制本地化过程的细.

PLC

是基于计算机的固态装置，控制工业设备和过程。虽然PLC是整个SCADA和DCS系统中使用的控制系统组件，它们通常在较小的控制系统配置中作为主要组件，用于提供离散过程的操作控制，如汽车装配生产线和电厂吹灰控制。PLC被广泛应用于几乎所有的工业生产过.

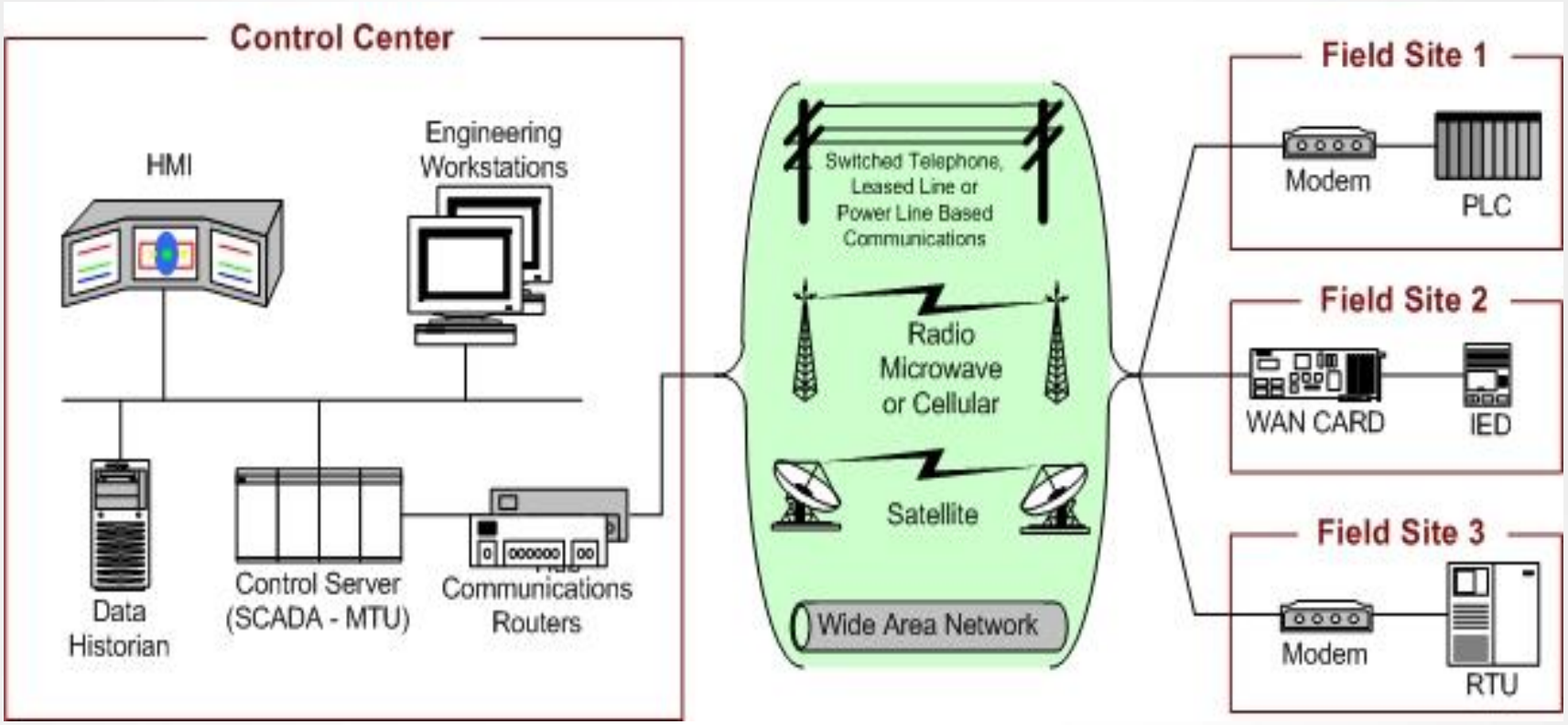
RTU

远程终端装置，也称为遥测遥控装置，是特殊用途的数据采集和控制单元，被设计为支持SCADA远程站点。RTU是现场设备，往往配备无线电接口以支持有线通信不可用的远程站点。

IED

IED是一种“智能”传感器/执行器，包含采集数据、与其他设备通信和执行本地过程和控制所需的智能。IED可以组合一个模拟输入传感器，模拟输出，低层次的控制能力，通信系统，以及一台设备中的程序存储器。在SCADA和DCS系统中使用IED，可以在本地级别实现自动化控制。.

SCADA系统的组件和总体配置典型配置图：



协议

工业控制系统主要通信协议：

1. Modbus
2. OPC
3. S7
4. DNP3
5. ICCP
6. IEC61850
7. PROFIBUS

端口

代表厂商	PLC	端口	协议
施耐德	Quntom	502	Modbus
西门子	C-300/400	102	S7
RockWell	allen-bradley	44818	Ethernet/IP
HoneyWell	HC950	502	Modbus
菲尼克斯	Inline	1962	私有
菲尼克斯	ProcConOS	20547	私有
DNP3		20000	DNP3
三菱	Mitsubishi	5006/5007	私有
欧姆龙	CP/CJ/CS/CQ/CV	9600	私有
Niagara	Fox	1911	私有
配电终端	配电终端	2404	IEC-104

对比

对比项	工业控制系统	传统IT信息系统
体系架构	ICS系统主要由PLC、RTU、DCS、SCADA等工业控制设备及系统组成	计算机系统通过互联网协议组成计算机网络
操作系统	广泛使用VxWorks、uCLinux、debian等，并是根据需要进行功能的裁剪或定制	通用操作系统(Windows Unix Linux等)，功能相对强大
数据交换协议	专用通信协议或规约(OPC、Modbus、DNP3等)直接使用或作用TCP/IP协议的应用层使用	TCP/IP协议栈(应用层协议：HTTP、FTP、SMTP等)
系统实时性	系统传输、处理信息的实时性要求高、不能停机和重启恢复	系统实时性要求不高，信息传输允许延迟，可以停机和重启恢复
系统升级难度	专有系统兼容性差； 软硬件升级较困难； 很少进行系统升级，升级需整个系统进行升级换代	采用通用系统，兼容性较好； 软硬件升级较容易； 软件系统升级较频繁
系统故障响应	不可预料的中断会造成经济损失或危机人身安全，必须紧急响应处理	不可预料的中断可能会造成损失，系统故障的处理响应级别随IT系统要求而定

对比

1.大部分工控是基于协议漏洞的安全检测，大多数终端不具备网站,通常检测手段为构造并发送特定的畸形数据包，通过返回的数据进行分析

2.操作系统基于vxworks、uclinux等

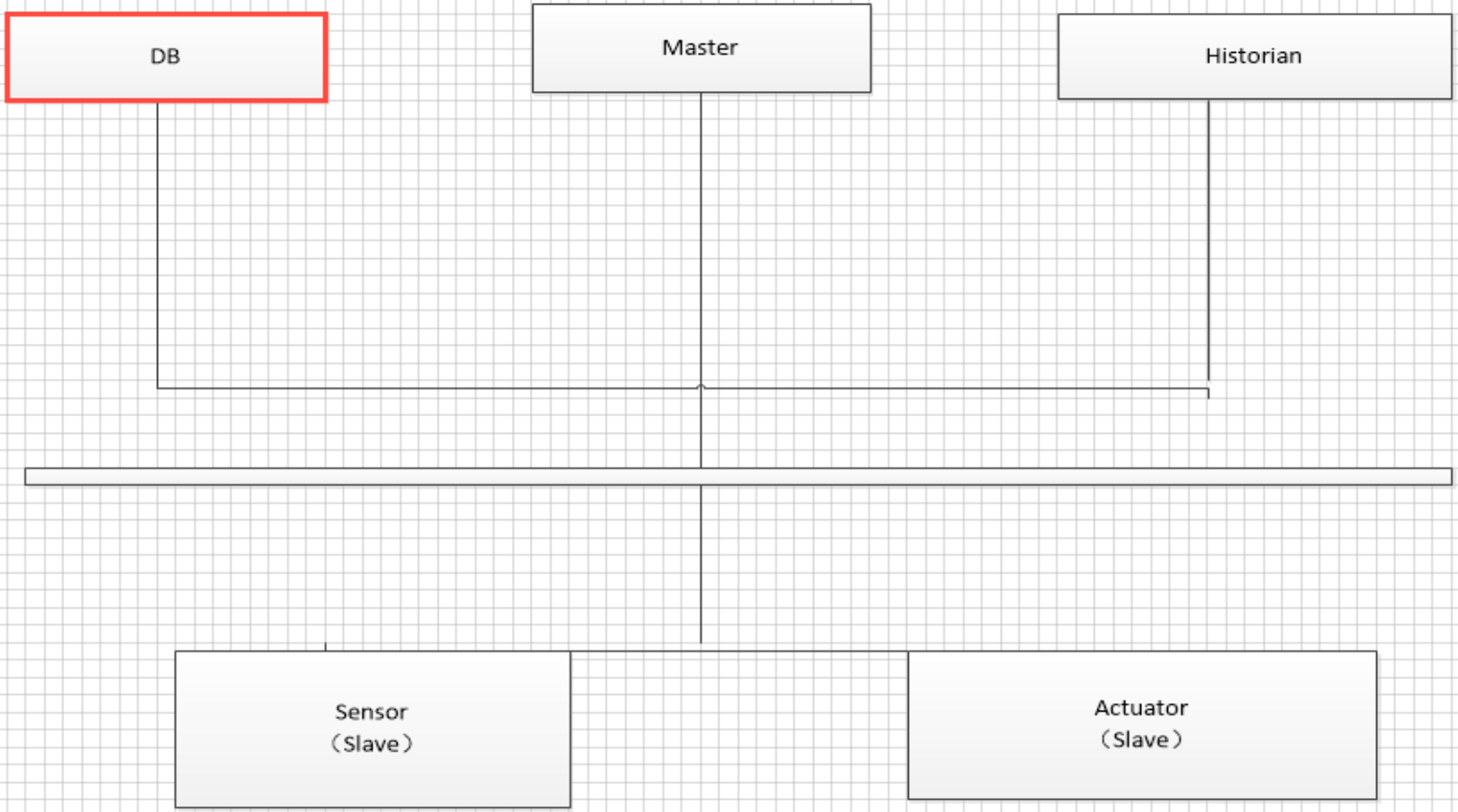
3.互联网上漏洞检测工具很少，大部分就是基于python的脚本

1.大部分基于web站点的漏洞安全检测

2. 漏洞类型有注入、跨站、上传、弱口令等等

3.公网有很多传统安全检测工具，如wvs\appscan\sqlmap\stratus等

目 录


DB
Master
Historian
Sensor
（Slave）
Actuator
（Slave）

风险

工控系统安全风险

- 1.操作系统的安全漏洞问题
- 由于考虑到工控软件与操作系统补丁兼容性的问题，系统开机后一般不会对操作系统平台打补丁，导致系统带着风险运行。如：vxworks5.5版本存在多个漏洞。
-
- 2.杀毒软件安装及升级更新问题
- 用于生产控制系统的操作系统基于工控软件与杀毒软件的兼容性考虑，通常不安装杀毒软件，给病毒与恶意代码传染与扩散留下了空间。
-
- 3.使用U盘、光盘导致的病毒传播问题
- 由于在工控系统中的管理终端一般没有技术措施对U盘和光盘使用进行有效的管理，导致外设的无序使用而引发的安全事件时有发生。

风险

4.设备维修时笔记本电脑的随便接入问题

- 工业控制系统的管理维护，没有到达一定安全基线的笔记本电脑接入工业控制系统，会对工业控制系统的安全造成很大的威胁。

5.工控系统安装漏洞补丁问题

- 通常情况下，工控系统安装漏洞补丁也存在一定风险，一是跟其他通信兼容问题，二是很多情况补丁安装完后需重启系统，这也造成很多不必要的麻烦。

控制系统与传统信息系统存在巨大差别，存在信息不对称问题

- 控制系统和传统信息系统在网络、通信等多个方面均有很大差别，对于用户对于安全的侧重点也不一样，故两者面临的威胁和风险程度也不一样。相对来讲，控制系统较为封闭，隔离措施到位，控制系统管理人员往往只把安全侧重点放在网络边界，而忽视网络内部的安全技术和管理措施。而信息安全人员对于控制系统的技术细节并不十分了解，专业管理上也存在鸿沟，往往无法及时发现控制系统安全问题，提出有效措施，存在信息不对称问题。

物理隔离并非是一劳永逸的解决方案

- 网络隔离确实能够提高攻击难度，但目前看来，针对工业控制系统的攻击大多是apt攻击，此类攻击持续时间长，针对性强，而且往往是敌对势力主导的。绕过隔离进入内网并不是不可能的事情，只要有数据交互，就有可能被渗透。通过内部人员的U盘将精心制作的木马程序“摆渡”至内网是最常见的做法。如果内部网络的设备或服务没有防护到位，如定期更新补丁等，则有可能被木马程序利用实施进一步攻击。

传统的信息安全检测和渗透测试依然可行

- 随着智能电网的不断发展，电力系统的智能化和信息化水平逐步提高，在电力系统控制系统中也会大量采用TCP/IP协议，乃至FTP（vsftp）、HTTP等应用层协议，使用SQLServer、Oracle等传统数据库进行数据存储，搭建基于Web的信息管理系统。弱口令、SQL注入、脚本漏洞等互联网信息安全隐患和漏洞在工控领域同样存在，故传统的信息安全检测、评估手段在工控系统领域仍然适用。

风险

Modbus协议简介：

Modbus 协议是应用于电子控制器上的一种通用语言。它是一种使用最为广泛的通用协议，在1979年发明的，是全球第一个真正用于工业控制的总线协议。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。它已经成为一通用工业标准。有了它，不同厂商生产的控制设备可以连成工业网络，进行集中监控。此协议定义了一个控制器能认识使用的消息结构,而不管它们是经过何种网络进行通信的。它描述了一控制器请求访问其它设备的过程，如果回应来自其它设备的请求，以及怎样侦测错误并记录。

它制定了消息域格局和内容的公共格式。当在一Modbus网络上通信时，此协议决定了每个控制器须要知道它们的设备地址，识别按地址发来的消息，决定要产生何种行动。如果需要回应，控制器将生成反馈信息并用Modbus 协议发出。在其它网络上，包含了 Modbus 协议的消息转换为在此网络上使用的帧或包结构。这种转换也扩展了根据具体的网络解决节地址、路由路径及错误检测的方法。

风险

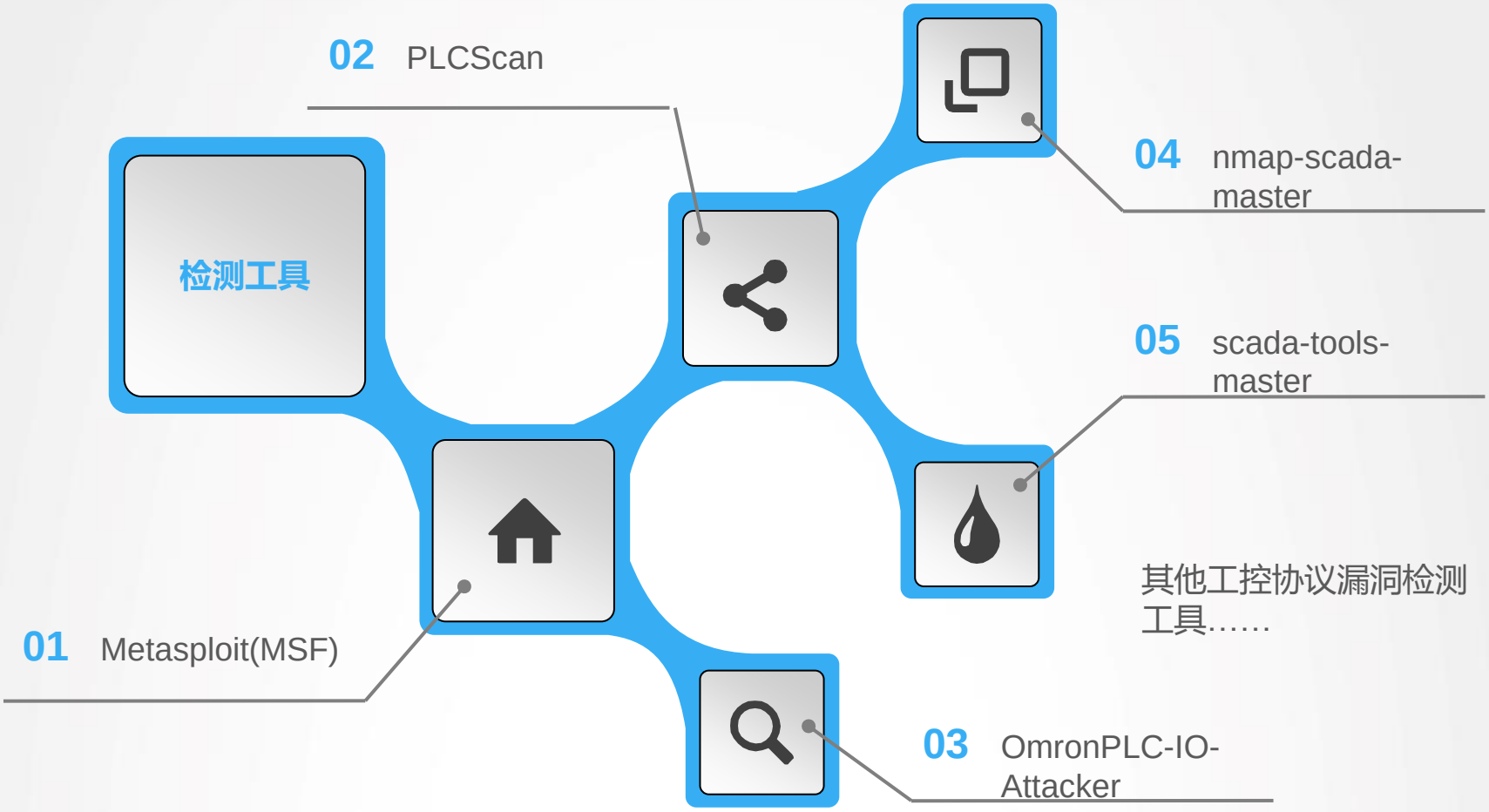
Modbus协议风险

1. 缺乏认证
2. 缺乏授权
3. 缺乏加密
4. 功能码滥用

目 录

工具

工业控制系统常用漏洞检测工具：



工具

MSF漏洞模块：

01

vxworks

auxiliary/admin/vxworks/wdbrpc_memory_dump //获取内存数据等信息
auxiliary/admin/vxworks/wdbrpc_reboot //使设备重启
auxiliary/scanner/vxworks/wdbrpc_bootline //是否开启17185端口
auxiliary/scanner/vxworks/wdbrpc_version //扫描VxWorks版本号

02

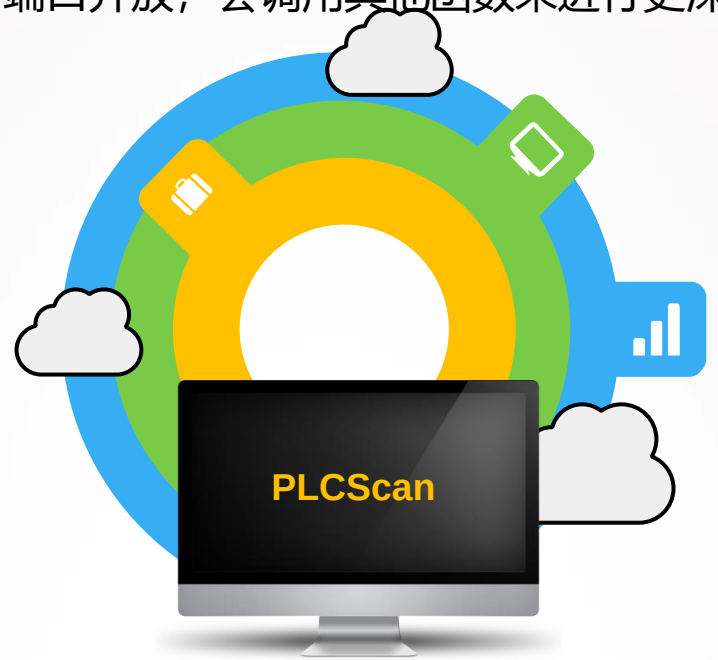
SCADA

auxiliary/admin/scada/modicon_command //施耐德的Modicon远程启动/停止命令
auxiliary/admin/scada/modicon_password_recovery //获取施耐德的Modicon密码
auxiliary/admin/scada/modicon_stux_transfer //施耐德的Modicon上传/下载利用
auxiliary/scanner/scada/digi_addp_reboot //远程重启digi_addp设备
auxiliary/scanner/scada/digi_addp_version //扫描digi_addp版本号

……

工具

PLCScan是由国外黑客组织ScadaStrangeLove开发的一款扫描工具，用于识别网上的PLC设备、S7设备和其他Modbus设备。该工具由Python编写，检测两个端口TCP/102和TCP/502，如果发现这两个端口开放，会调用其他函数来进行更深层次的检测。



扫描.

识别.

利用.

工具

scada-tools-master

get_seed_range.py
iec-60870-5-104.py
iec-61850-8-1.py
iec-identify.nse
mms-identify.nse
profinet_scanner.noscapy.py
profinet_scanner.scapy.py
profinet_set_fuzzer.py
profinet_set_network_info.py
s7-1200_brute_offline.py
s7-1500_brute_offline.py
s7-packet-structure.py
s7-show-payloads.py
s7_password_hashes_extractor.py
show_byte_sequences.py

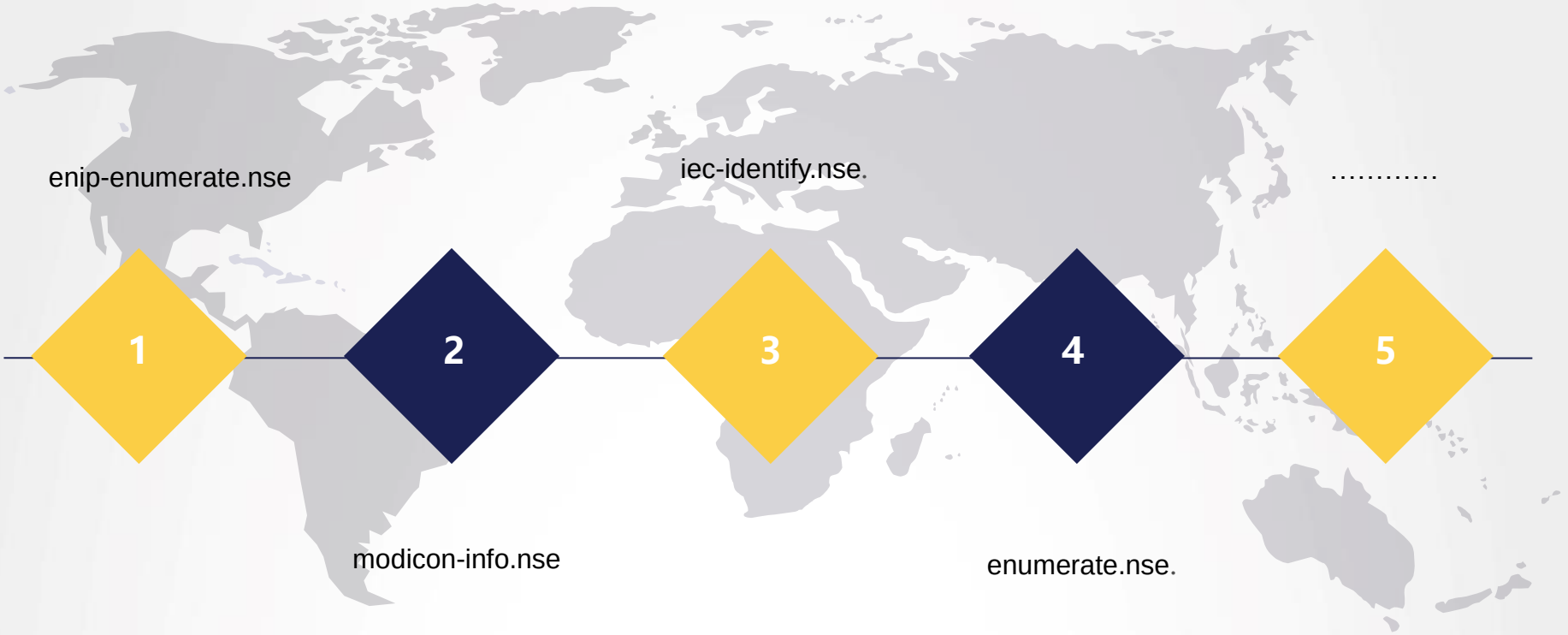
工具

欧姆龙OmronPLC-IO-Attacker-master

是一款针对欧姆龙的工控设备进行漏洞验证及利用工具，工具也是基于python语言开发

工具

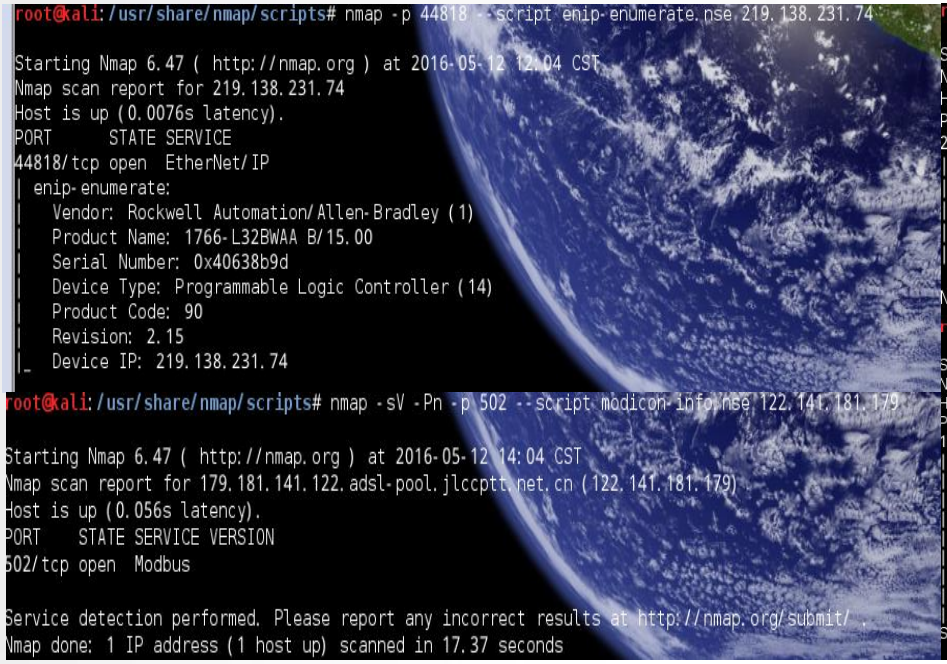
nmap-scada-master信息探测



结合nmap扫描工具进行工控相关信息探测

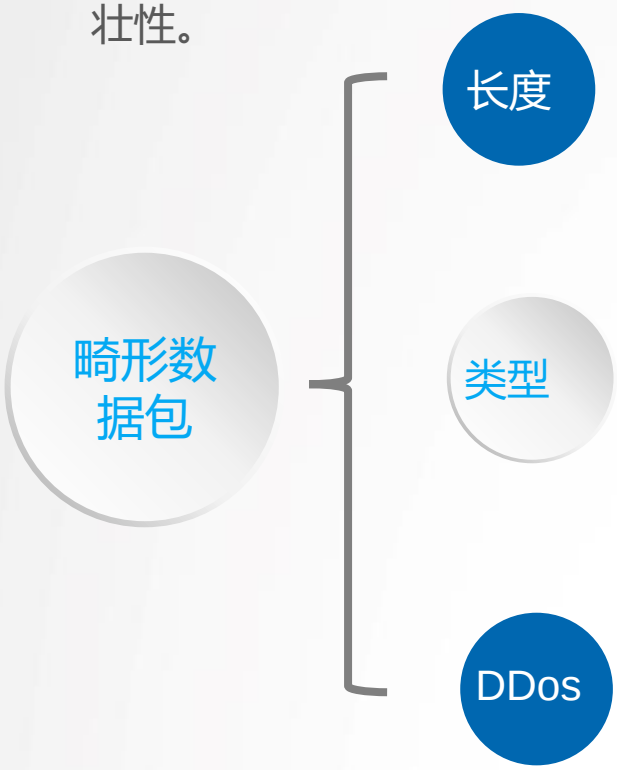
nmap-scada-master信息探测实例：

Cip协议信息探测（enip-enumerate.nse）
nmap -p 44818 --script enip-enumerate.nse 219.138.231.74



工具

畸形包攻击：通过抓包，获取工控系统通信数据包，测试工控协议的健壮性：另一种方式，即事先构造大量不同类型的畸形数据包，通过特定的客户端，对工控系统接口直接发送数据，通过查看返回的信息，判断通信是否正常，测试工控协议的健壮性。



研究基于工控安全的威胁情报分析

- 从目前国内外工控安全事件来看，工控系统受到的攻击大多是apt（高级持续性威胁）攻击，是有针对性的持续性的攻击。

- 这种攻击的特点是潜伏期长、针对性强，目前电网二次系统安全防护情况无法完全识别此类攻击。建议开展工控系统的威胁情报分析，通过旁路检测的手段，对可疑点进行提取，并分析攻击路径，追溯攻击源，还原攻击手法。

谢 谢!