协议FUZZING在工控安全领域的应用

密级：内部使用

工业控制应用

工业化与信息化不断交叉融合

工业控制系统(ICS:Industrial Control System)

已广泛应用于电力、水力、石化、医药、食品制造、交通运输、航空航天等各大工业领域；

国家关键基础设施的组成部分

工业信息安全

以太网技术盛行，工业领域已广泛使用
传统的工业控制系统不再是自动化孤岛
逐渐的接入企业网络，乃至工业互联网

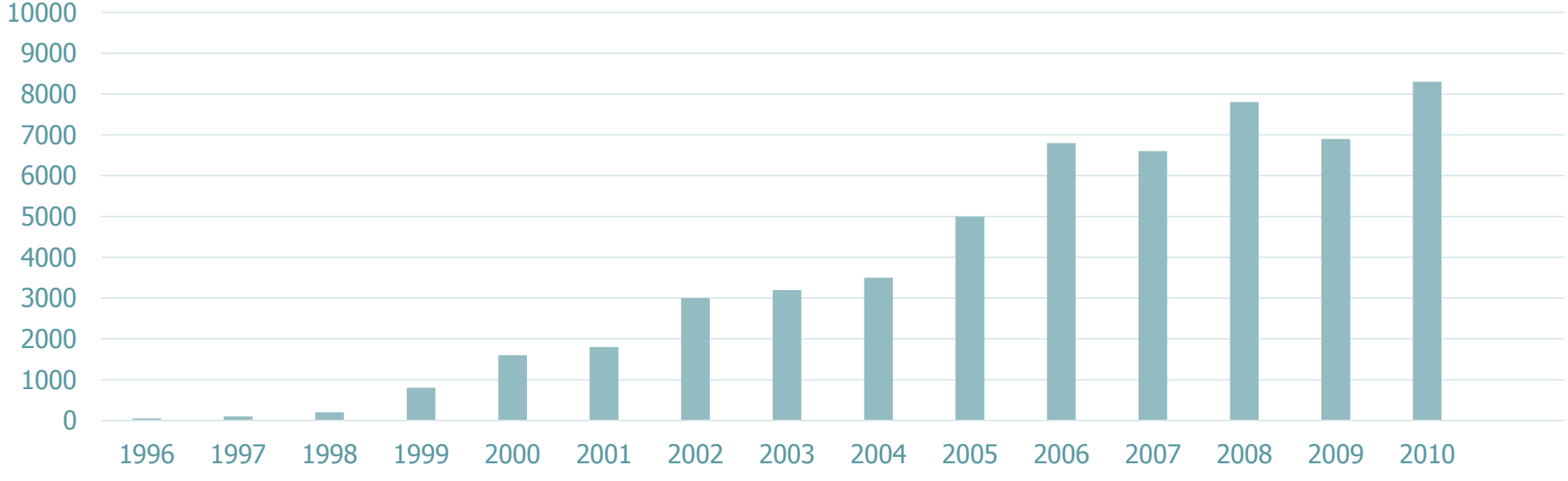
工信部协【2011】451号
一旦出现工业控制系统信息安全漏洞，将对
工业生产运行和社会经济安全造成重大隐患

工控安全事件

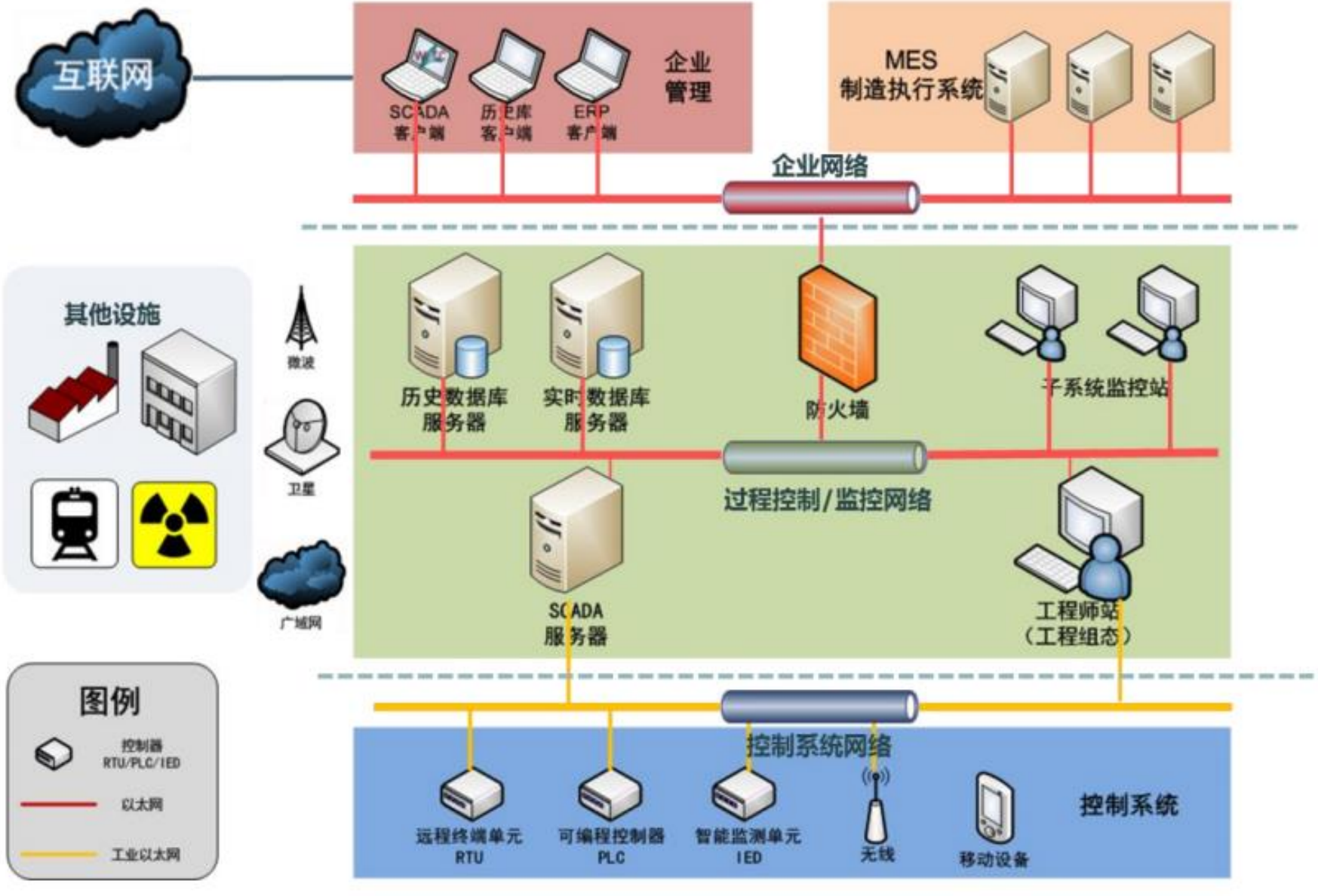
- **2010年** Stuxnet病毒，造成伊朗核电站推迟发电，感染了全球超过45000个网络
- **2011年** Duqu病毒，大多出现在工业控制系统中，收集与攻击目标的各种情报
- **2012年** Flame病毒，执行网络间谍活动，构造复杂，危害性巨大，可以通过USB存储器以及网络复制等多种方式传播
- **2014年** 全球1018座发电站感染Dragonfly恶意程序
- ……

Industrial Security Incident Database (ISID)

Vulnerability Disclosures Growth by Year

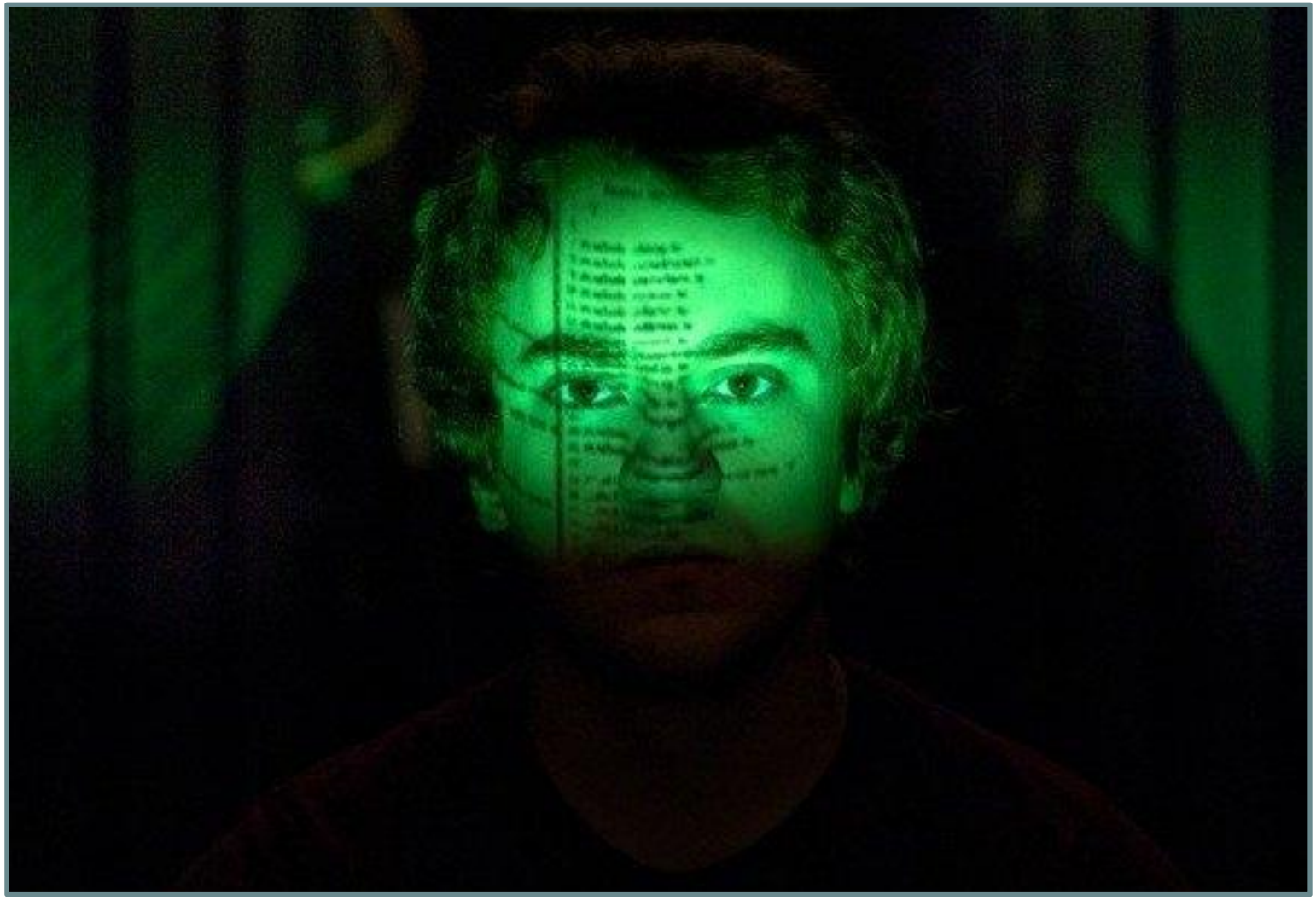


工控系统部署


互联网
企业管理
SCADA客户端
历史库客户端
ERP客户端
MES
制造执行系统
企业网络
其他设施
微波
卫星
广域网
历史数据库服务器
实时数据库服务器
防火墙
子系统监控站
过程控制/监控网络
SCADA服务器
工程师站（工程组态）
图例
控制器 RTU/PLC/IED
以太网
工业以太网
控制系统网络
远程终端单元 RTU
可编程控制器 PLC
智能监测单元 IED
无线
移动设备
控制系统

工业控制系统与传统IT系统

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



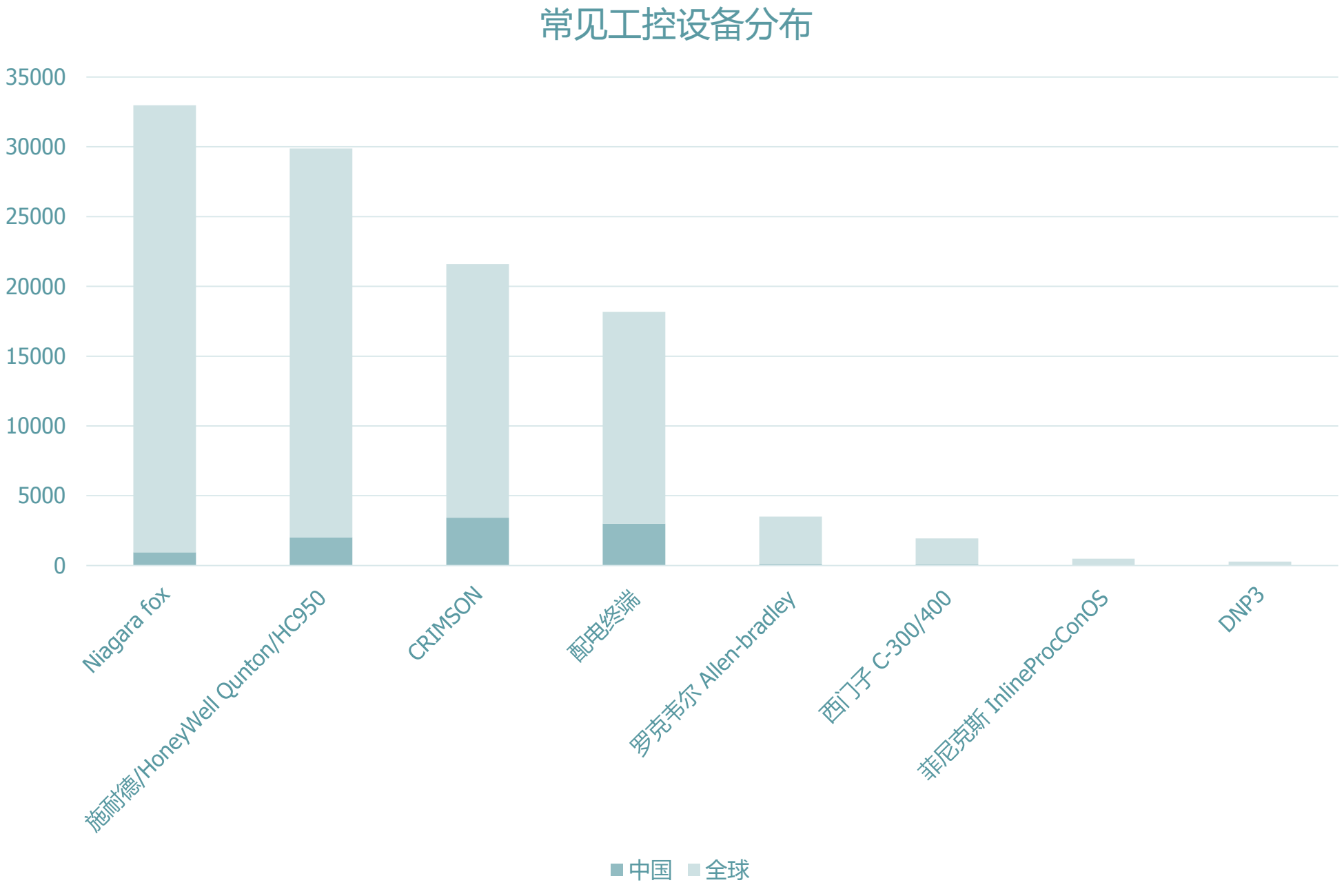
漏洞挖掘与检测

工业控制系统常见协议

协议名称	说明
Modbus **ModbusTcp** **ModbusRTU**	应用广泛的工业现场总线协议，ModbusTcp和ModbusRTU是在Tcp以太网和RTU环境下对Modbus协议的扩充
S7	西门子设备的私有协议
PROFIBUS **PROFINET**	一种国际化．开放式．不依赖于设备生产商的现场总线标准，广泛适用于制造业自动化、流程工业自动化和楼宇、交通电力等其他领域自动化
IEC101 **IEC104**	电力行业使用的设备控制协议 IEC104为IEC101协议基于以太网的实现
CANBUS	制造厂中连接现场设备（传感器、执行器、控制器等）、面向广播的串行总线系统
EtherNet/IP **EtherCAT**	程序自动化通讯协议
ZigBee	基于IEEE802.15.4标准的低功耗局域网协议

已支持探测协议

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


常见工控设备分布
35000
30000
25000
20000
15000
10000
5000
0
Niagara fox
施耐德/HoneyWell Qunton/HC950
CRIMSON
配电终端
罗克韦尔 Allen-bradley
西门子 C-300/400
菲尼克斯 InlineProcConOS
DNP3
中国
全球

白盒&&灰盒测试

- **白盒测试**

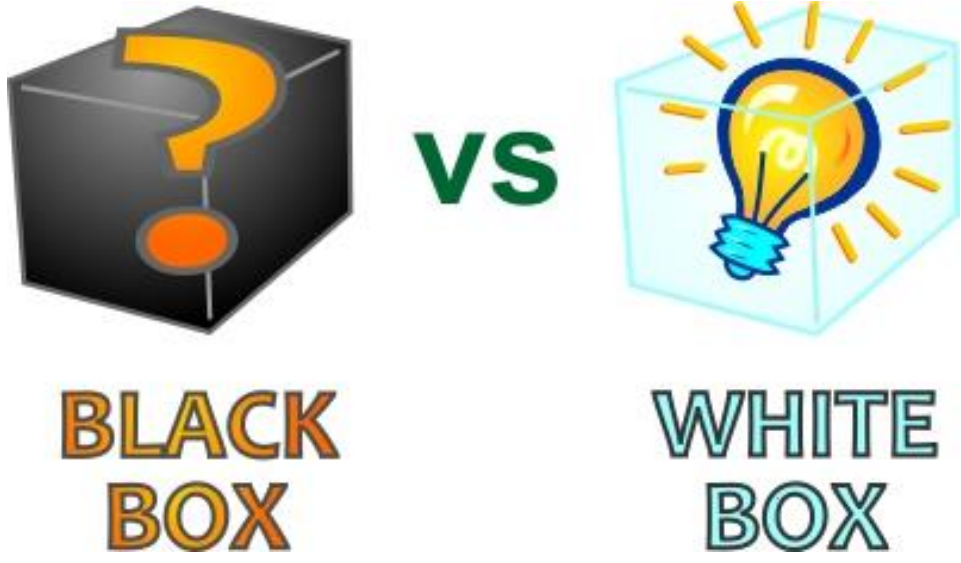
代码评审（Source Code Review）——手工或自动化工具
常用工具：ITS4，Splint，Jlint
优点：　高覆盖，理论上可以发现所有的安全漏洞。
缺点：　过于复杂，源代码不能保证，审查工具不够完美，耗时耗力

- **灰盒测试**

灰盒测试介于白盒和黑盒测试之间——黑盒测试再加上逆向工程
优点：较高的覆盖率，从灰盒分析中得到的信息能够反用于帮助和提高纯黑盒的模糊测试技术
缺点： 需要具备逆向代码工程技能的人员参与分析

◆ **工控设备来说，白盒测试与灰盒测试的条件一般无法满足**

黑盒测试



- **黑盒测试**

  方式：

  手动测试

  自动化测试——模糊测试（Fuzzing）

  优点：

  高可用性：任何情况下，黑盒测试方法总是可用且有效的

  良好的可重现性

  缺点：

  最大问题是何时测试停止和评估测试的效果。

  不够智能适合单组输入引发的漏洞，如果需要多组输入来触发漏洞条件则很难触发

网络攻击方式

攻击类型	攻击方式
源地址欺骗	构造虚假的源地址，冒充合法的设备发送报文
报文泛洪	制造网络风暴，产生拒绝服务
网络探测	ICMP 、TCP、UDP 等方式网络探测； 获取目标机服务信息
畸形报文	**构造一些特殊的异常类型的报文，让主机或者网络设备出现异常甚至崩溃**

模糊测试

- **模糊测试(Fuzzing)的定义**

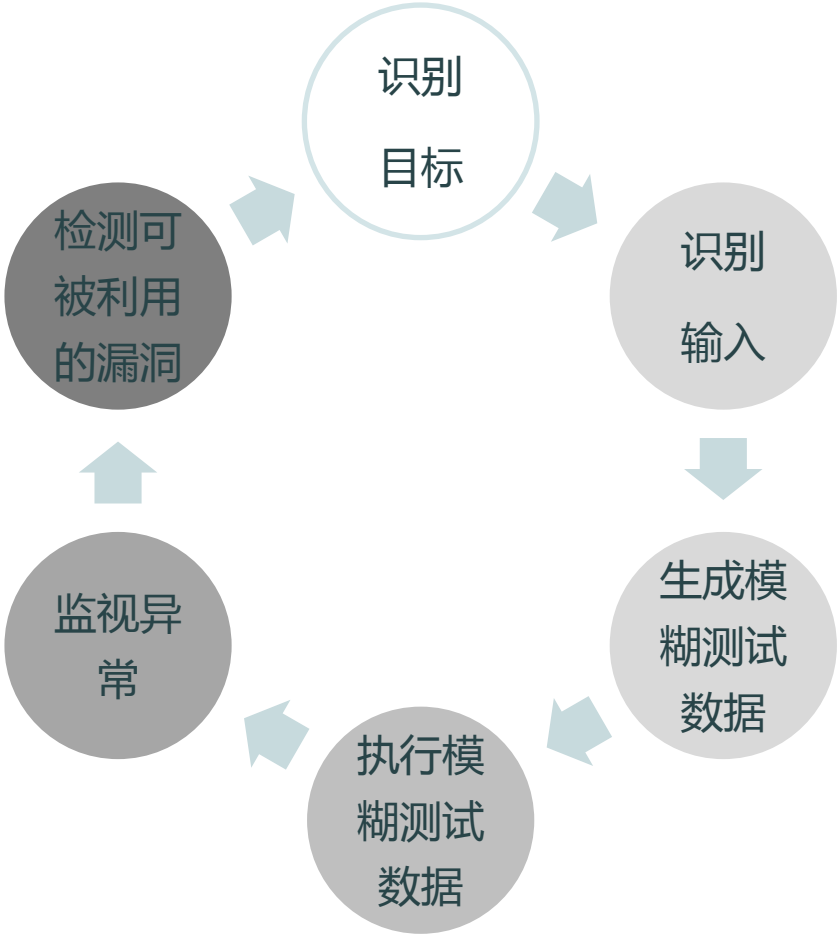
  向目标系统

  提供非预期的输入

  并监视异常结果

  来发现软件漏洞的方法

- **模糊测试的一般流程**



➢ 工控协议Fuzzing 思想

确认被测目标的工作协议，了解是否有已知的漏洞或风险

明确协议的工作原理，网络分层，接入设备的方式

研究协议格式，按逻辑块拆分字段，确认字段数据类型

逐字段、逐逻辑块进行Fuzz数据集完善补充，组装完整数据包

研究协议应用的收发包模式；

利用组装好的Fuzzing数据包集合进行原理性探测扫描

扫描前针对协议应用选择适当监控方式，扫描过程实时监控分析

发包时对数据包预分析获取预期数据，并与实际获得数据相比较，记录

扫描过程进行实时自动化程序分析记录；

完成后可对对异常数据或行为进行人工分析，对问题数据包

- **协议研究与数据拆分——协议分层**

Modbus\Tcp IEC104 DNP3 TELNET FTP SMTP……

TCP UDP

ICMP IP ARP

Modbus IEC101 PROFIBUS CANBUS

协议拆分

应用层

传输层

TCP 头

4 bits	6 bits	6 bits	8 bits	8 bits
Source Port			Destination Port	
Sequence Number				
Acknowledge Number				
Data Offset	Reserved	Code	Window	
Ckecksum			Urgent Pointer	
Options			Padding	
Data				

UDP 头

16bits	16bits
Source Port	Destination Port
Data Length	CheckSum
Data	
.....	

网间网层

ARP 头

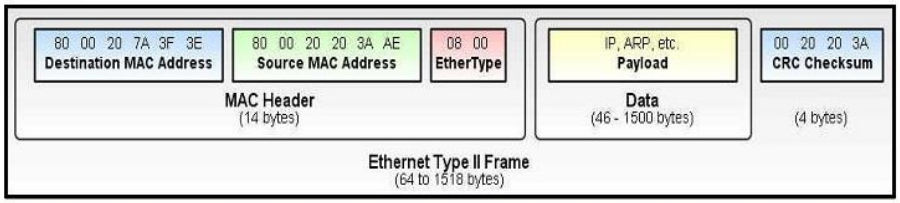
16bits		16bits
HardWare Type		Protocol Type
HardWare Size	Protocol Size	OpCode
Sender MAC Address (6 Byte)		
.....		Sender Ip Address (4Byte)
.....		.....
Target MAC Address (6 Byte)		
Target Ip Address (4Byte)		

IP 头

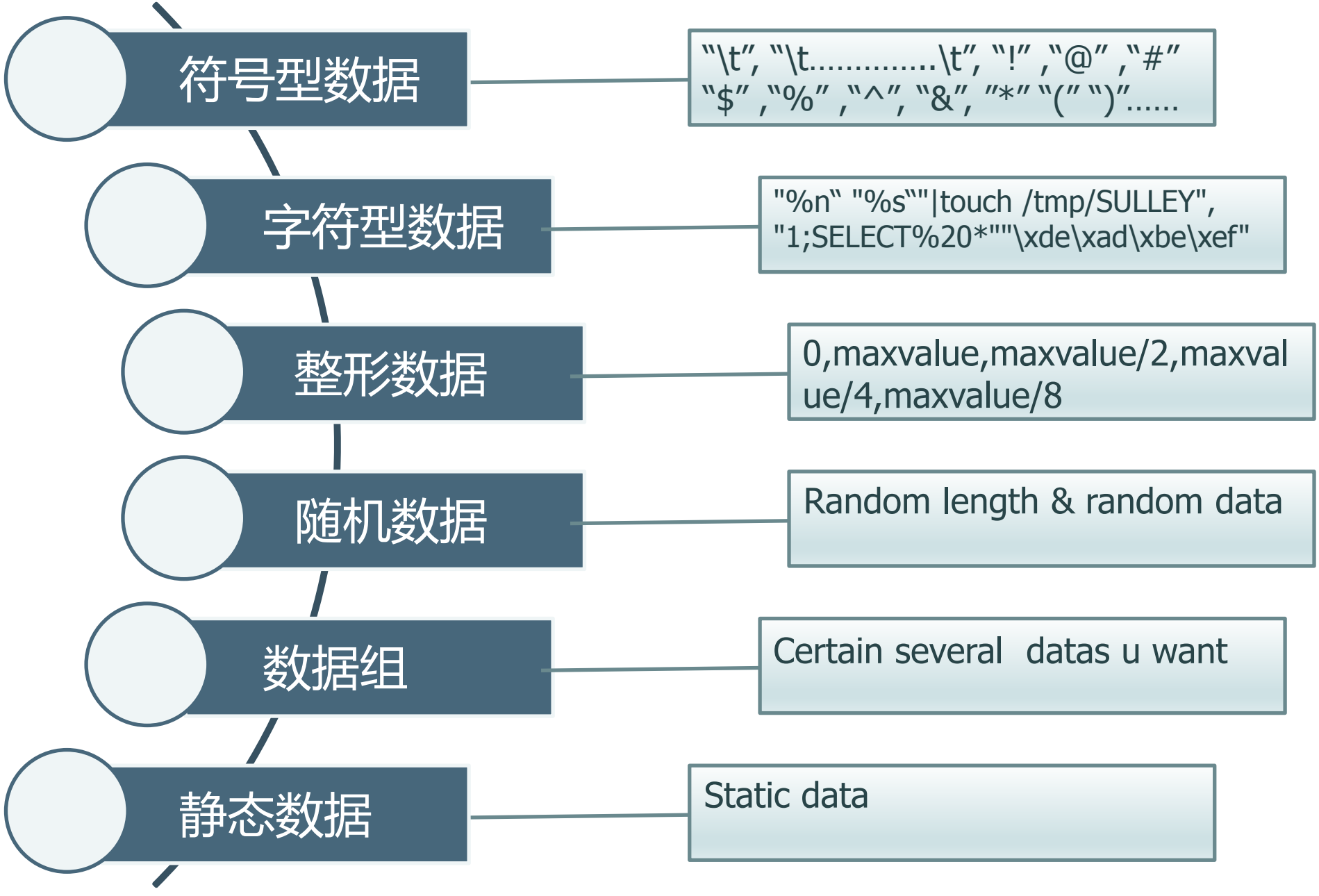
4 bits	4 bits	8 bits	3 bits	13 bits
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragmentation Offset
Time To Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				Padding
Data				

网络接口层

ETH 头



类型确认及Fuzz库组合



模糊测试方法分类

预生成测试用例

- 缺乏随机生成，测试用例有限

随机生成输入

- 所有数据随机生成，效率最低

手工协议变异测试

- 手动方式，可以依靠测试者经验，不适合新研究协议

变异或强制性测试

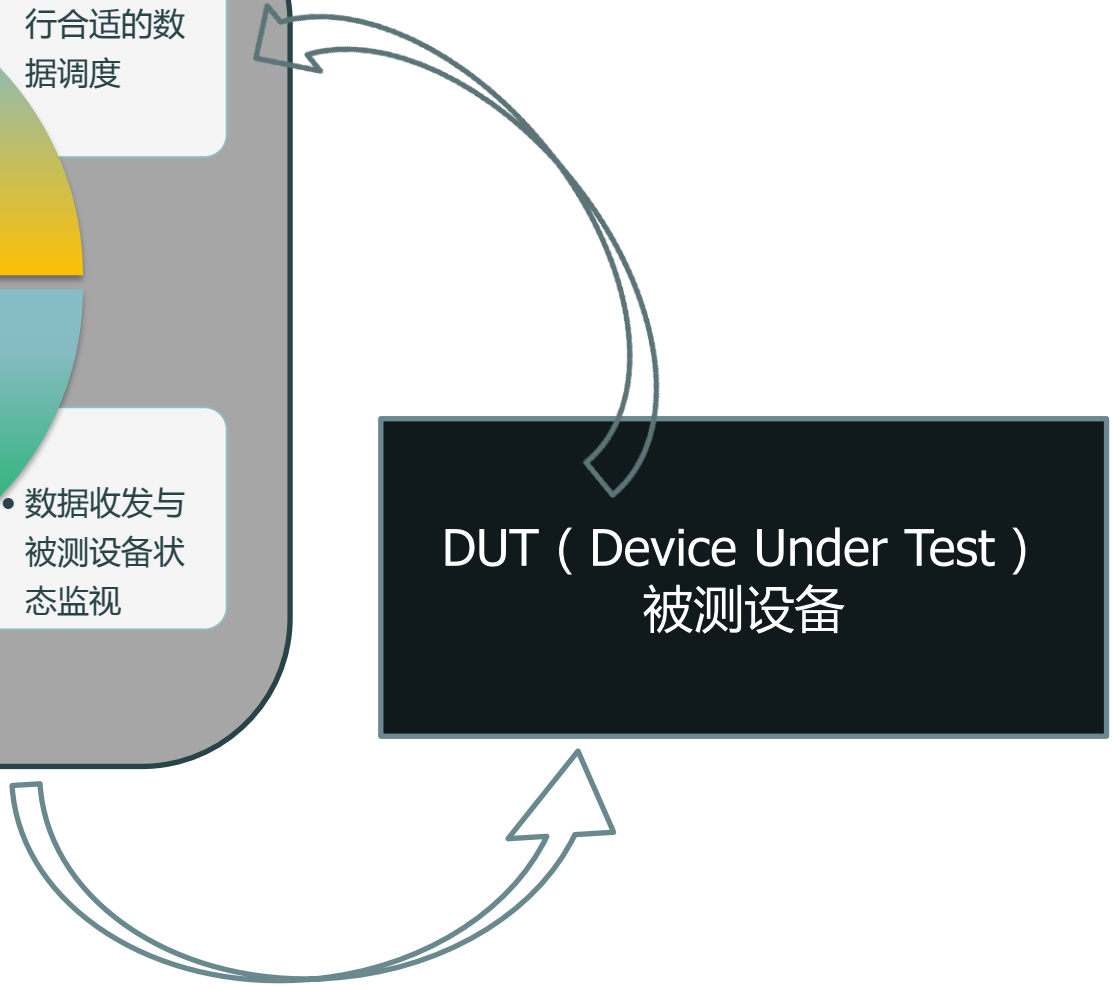
- 对每个字节进行模糊测试，相对低效

自动协议生成测试

- 生成协议工作的语法进行数据包的判断，较复杂

模糊测试框架的构建


• 模糊测试库的构建与应用
• 针对协议进行合适的数据调度
数据生成
调度框架
结果分析
通信接口
• 分析异常数据、挖掘潜在漏洞
• 数据收发与被测设备状态监视


DUT（Device Under Test）
被测设备

运行监控

网络发包探测

服务日志分析

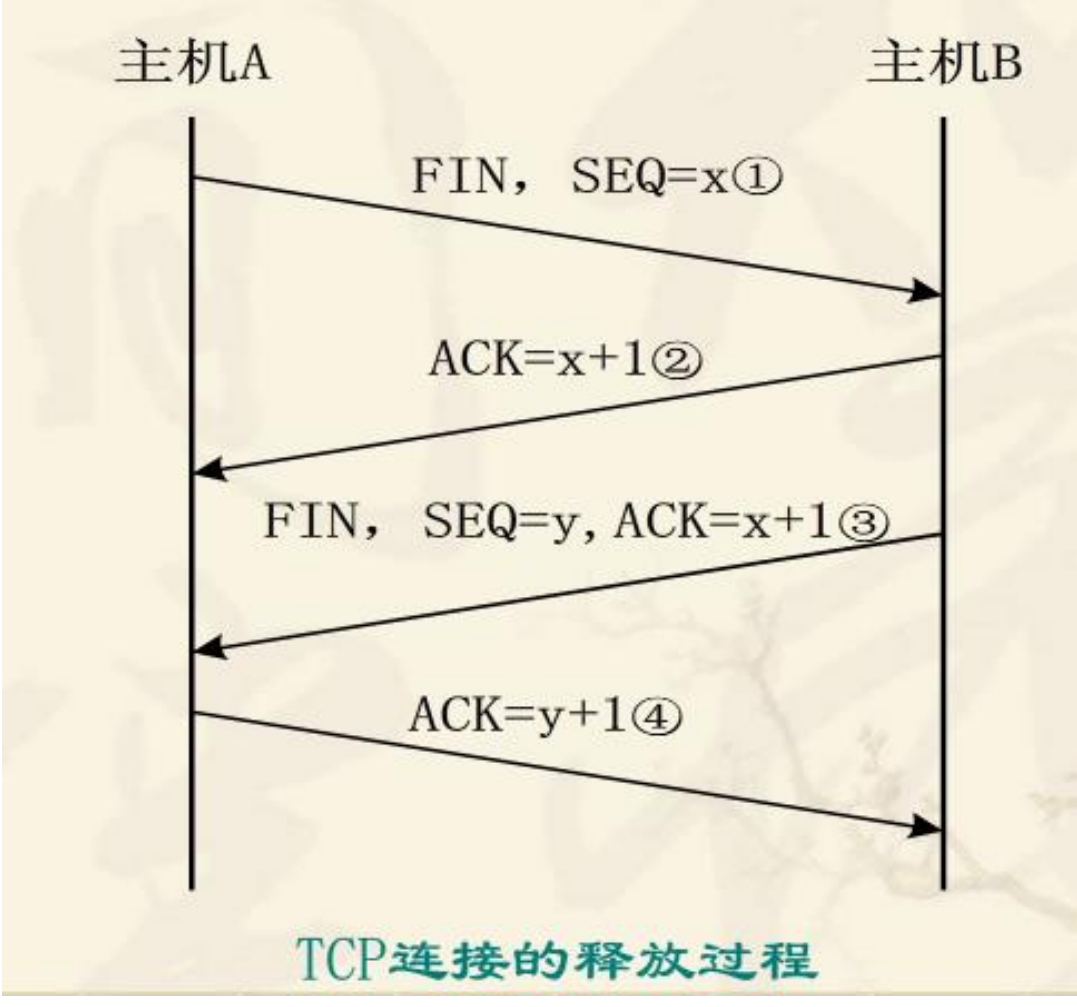
时机

正确的数据在错误的时间发送可能会导致异常

方式

平衡式收发： 自由问答

非平衡收发： 一问一答



TCP连接的释放过程

结果预判及对比

所有发送数据都应判断被测设备的响应是否与预期一致

结果分析

- 程序自动分析记录异常数据
- 手动参考协议分析异常记录
- 根据记录路径回复异常
- 远程查看目标服务日志

Modbus Tcp

Modbus TCP 协议， 使用广泛，已知漏洞较多

协议实现有国家标准，易学习，好参考

应用层协议，TCP数据部分修改即可，端口502

模仿主站操作

根据国标进行协议拆解；各字段数据类型均为整形数据

按照协议实现对各字段的Fuzz库补齐

主站对从站收发包方式为一问一答；

针对Fuzzing库包依次组合探测扫描

监控方式为Ping主机存活

完成后参考国标手动分析异常记录，及回放认证

数据生成示例

- ModbusTcp 协议

合适的Fuzzing数据需要技巧+经验+反复的试验

任意值均接受，Fuzzing意义不大

实际长度或异常长度

可用功能码或未定义功能码

该项为固定0值

描述从站的识别码

数据payload

➢ 测试环境

某款PLC，温度采集响应环境
输入：一个温度感应器
输出：三个LED灯，不同温度不同灯亮

➢ 测试步骤

字段分析、类型确认
Fuzz库选择、数据包组合
数据发送、过程监视
自动化异常记录
数据包手动分析
异常数据回放

➢写拒绝服务

●触发条件

对临界值地址为960|3c0H,和大于该地址进行数据写操作时系统均方式重启

●经典报文

功能码5：0x0 0x0 0x0 0x0 0x0 0x6 0x0 0x5 0x3 0xc0 0x0 0x0

Fuzzing 数据包					
Mbap				FunCode	Data
TransactionID	ProtocolFlag	PduLength	SlaveID	Code	data
0	0	6	0	5	0x3 0xc0 0x0 0x0

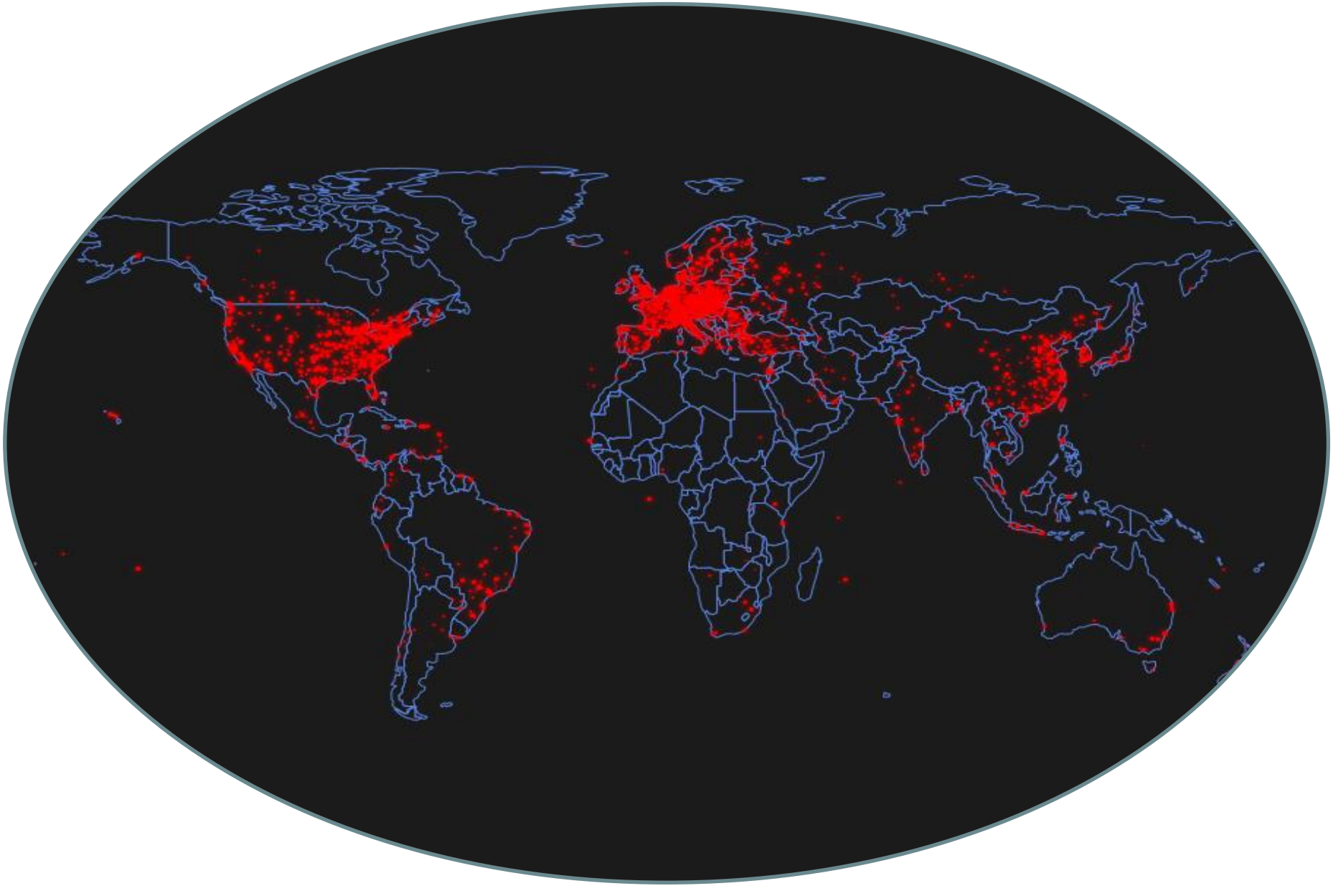
核心能力

外围能力

报表
- 详细整改建议
- 对比及趋势分析
- 直观展示

插件
- IT系统漏洞
- 工控系统漏洞
- IT系统配置核查项
- 工控系统配置核查项

广谱扫描【 PORT：502 】



漏洞挖掘检测平台

- 协议合规性检测
- 已知漏洞检测
- 未知漏洞挖掘

组包　　分析　　监视　　回放

➢参考标准

Modbus TCP协议

中华人民共和国国家标准 GB/T 19582.3-2008
《基于Modbus协议的工业自动化网络规范 第三部分 Modbus协议在TCP/IP上的实现指南》

IEC-104协议

中华人民共和国电力行业标准 DL/T 634.5014 -2009
《远动设备及系统第5-104部分:传输规约采用标准传输协议集的IEC 60870-5-101网络访问》

➢参考书籍

《模糊测试 强制发掘安全漏洞的利器》

谢谢！