工业控制系统网络安全专题沙龙

(ISC)2北京分会第7次沙龙　匡恩学院　司志凡

没有网络安全就没有国家安全；

没有信息化就没有现代化。

——习近平

工控网络安全危及国家安全

黑客远程入侵智能汽车，汽车也可能随时”遭遇“恐怖袭击”

智能移动

冶金

德国钢厂熔炉控制系统受攻击，导致熔炉无法正常关闭

电厂遭USB病毒攻击，大量机密数据泄漏

智能电网

智能制造

数控机床关键数据被窃取，损失难以估量

污水处理厂遭非法入侵，污水直接排入自然水系

水处理

卫生事业

黑客入侵药泵，输出致命剂量，危害人身安全

军事

代码即武器，美国政府控制漏洞市场

目录

CONTENTS

01 工控系统网络安全威胁及攻击路径介绍

02 工控网络安全风险评估技术

03 工控系统网络漏洞检测技术

工业控制系统网络的威胁来源

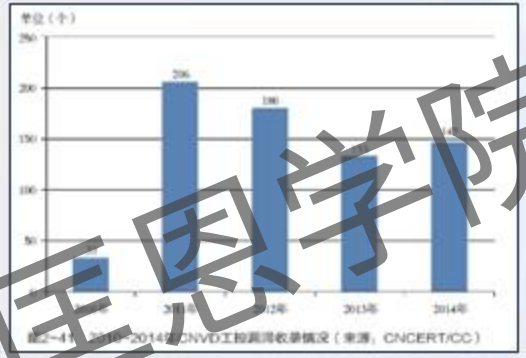
五大威胁——设备高危漏洞

工控漏洞特点

长久存在	**巨大威胁**
不易发现	**必然发现**
可交易性	恶意竞争性

工业漏洞变化趋势

工业控制网络漏洞始终处在高位，涉及多个工控厂商



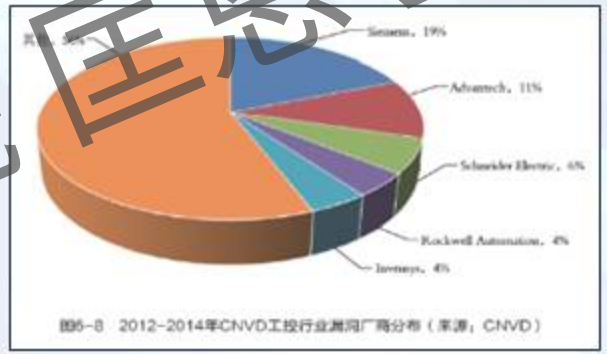


图6-8 2012-2014年CNVD工控行业漏洞厂商分布（来源：CNVD）

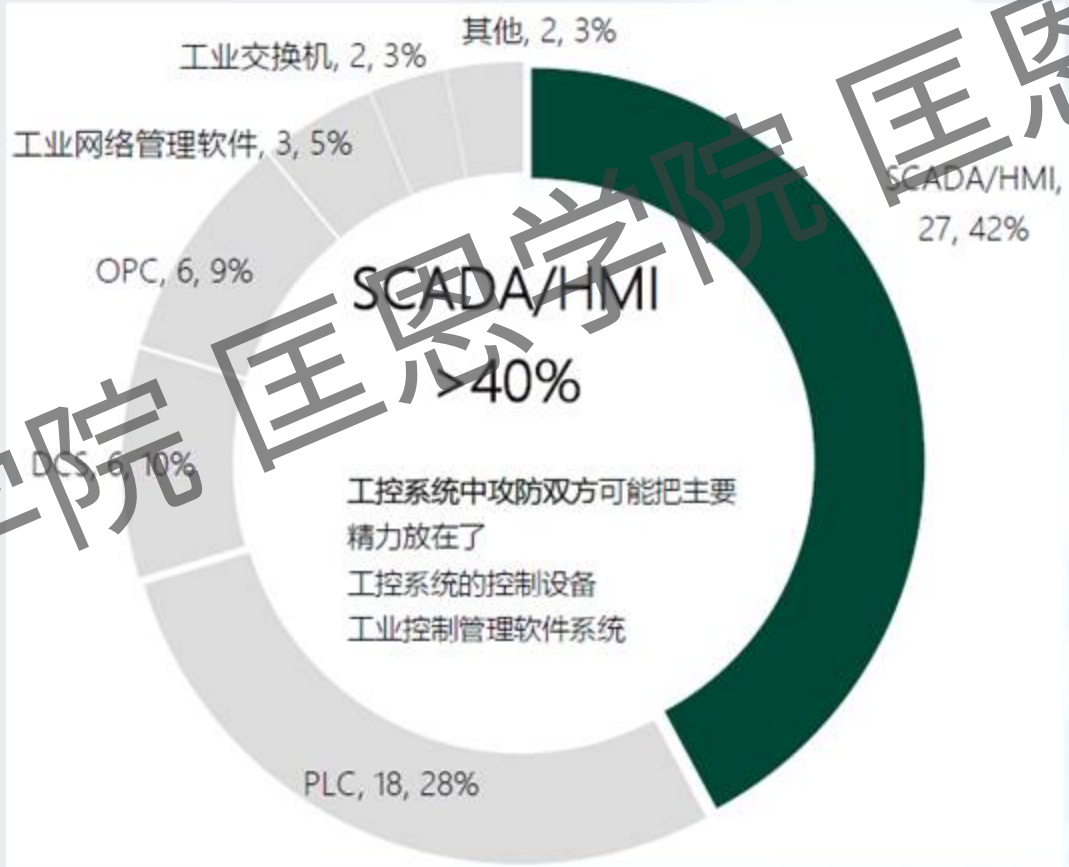
自2010年伊朗“震网”事件后，CNVD每年收录的工控漏洞数量始终处于高位，2014年共收录工控漏洞147个（包含自主挖掘零日漏洞12个），其中高危漏洞有74个，占比在50%以上

2013年7月，CNVD建立起基于重点行业的子漏洞库，目前包括：政府部门、基础电信运营商、工控行业客户等。工控系统安全漏洞不断受到关注。

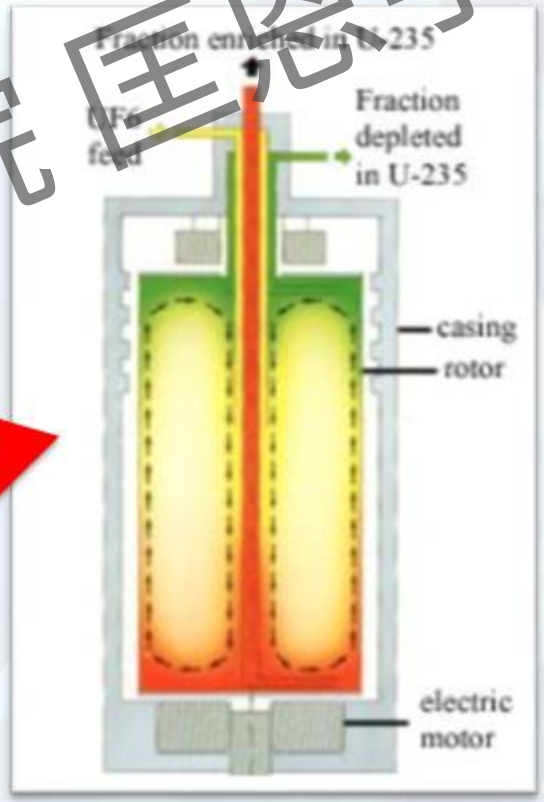
电力企业工控行业漏洞最为相关的厂商包括：Siemens、Advantech、Schneider Electric、Rockwell、Invensys、Hollis's

2014年收录的工控漏洞涉及的国内厂商则主要涉及亚控科技（WellinTech）和世纪长秋（CenturyStar）

2014年新增漏洞所涉及的工控产品分类分析



“震网事件”之漏洞利用



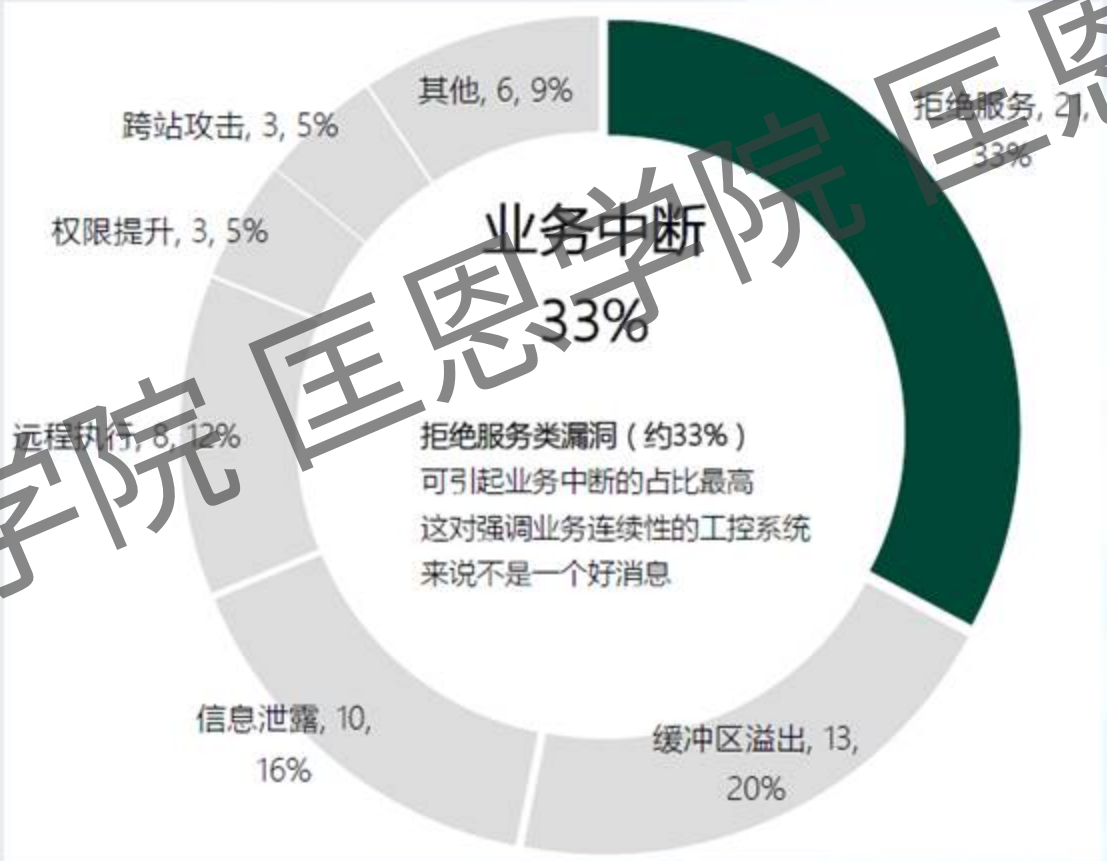
“震网事件”之漏洞利用

漏洞利用

利用包括MS10-046、MS10-061、MS08-067等7个最新漏洞进行攻击。其中，有5个是针对windows系统，2个是针对西门子SIMATIC WinCE系统。 前三个是“0day 漏洞”

违反授权、非法使用、
旁路控制、拒绝服务……

2014年新增漏洞的威胁分类及占比分析



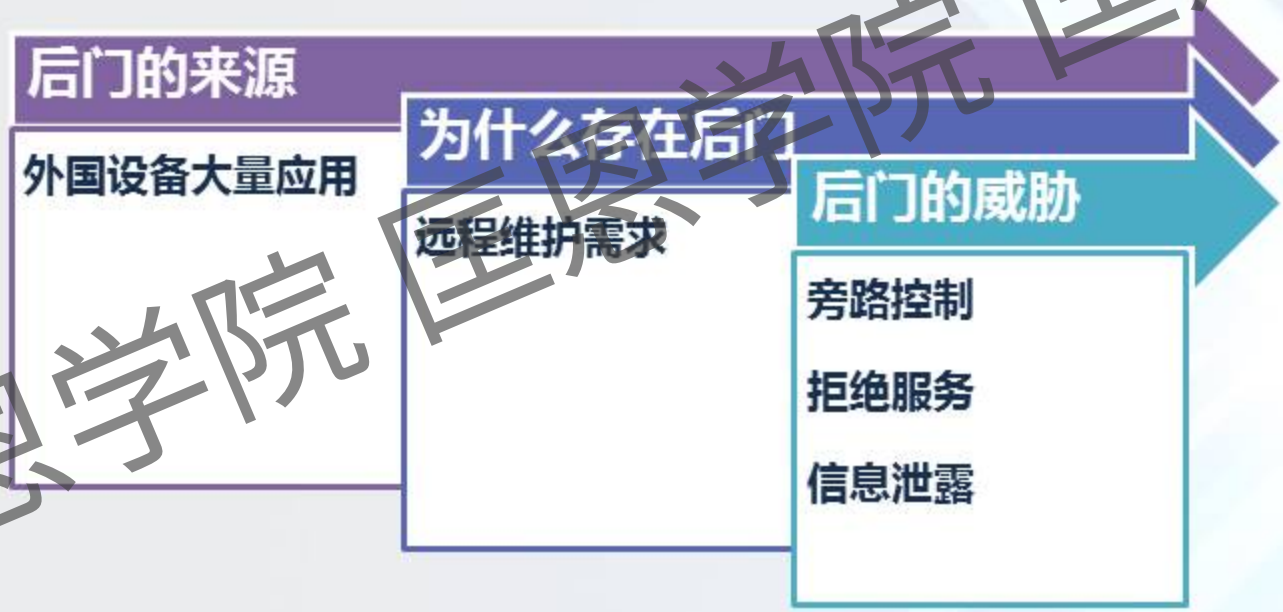
五大威胁——外国设备后门

供应商	销售额（百万元）	所占市场份额
ABB	330	20.1%
Siemens	220	13.4%
Hollis's	17[illegible]	10.6%
Shisha	[illegible]	9.1%
GE Xinhua	[illegible]	8.5%
Invensys	[illegible]0	5.5%
Emerson	70	4.3%
其它	470	28.6%
合计	1465	100

国外设备在各行业工控系统市场占有率非常高！

火电行业系统供应商市场份额统计

外国设备后门带入的威胁



五大威胁——工控网络病毒

随着两化融合的推进，互联网技术以其卓越的便捷性快速融入各行业，为病毒的快速传播也建立了更多的通道。

病毒传播途径

在被入侵厂商的主站上，向用户提供包含恶意代码的升级软件包

包含恶意代码的钓鱼邮件

利用系统漏洞，直接将恶意代码植入

现在已经有三个厂商的主站被这种方式被攻入，在网站上提供的软件安装包中包含了Havex。我们怀疑还会有更多类似的情况，但是尚未确定。

这三家公司都是开发面向工业的设备和软件，这些公司的总部分别位于德国、瑞士和比利时。其中两个供应商为ICS系统提供远程管理软件。

工控网络病毒发展趋势

黑客组织介绍

蜻蜓组织 (Dragonfly Group)　活力熊 (Energetic Bear)

主要攻击目标以能源行业为主

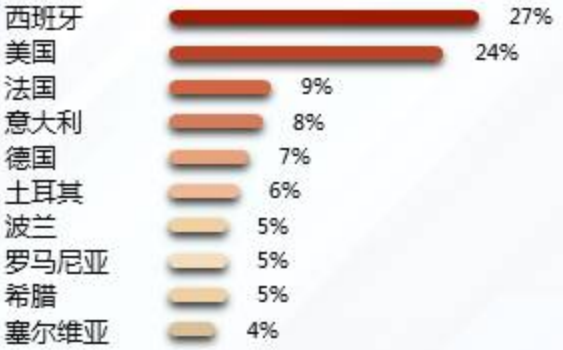
目标：窃取知识产权

方式：工业协议扫描仪

路径：TCP端口44848（欧姆龙和罗克韦尔）

102（西门子）、502（施耐德）上的设备。

已经发现的前10大主要攻击对象



方程式组织

Anonymous

Phrack

顶尖的黑客技术

来自最富有国家的支持

攻击国家明确

方程式组织

Security focus

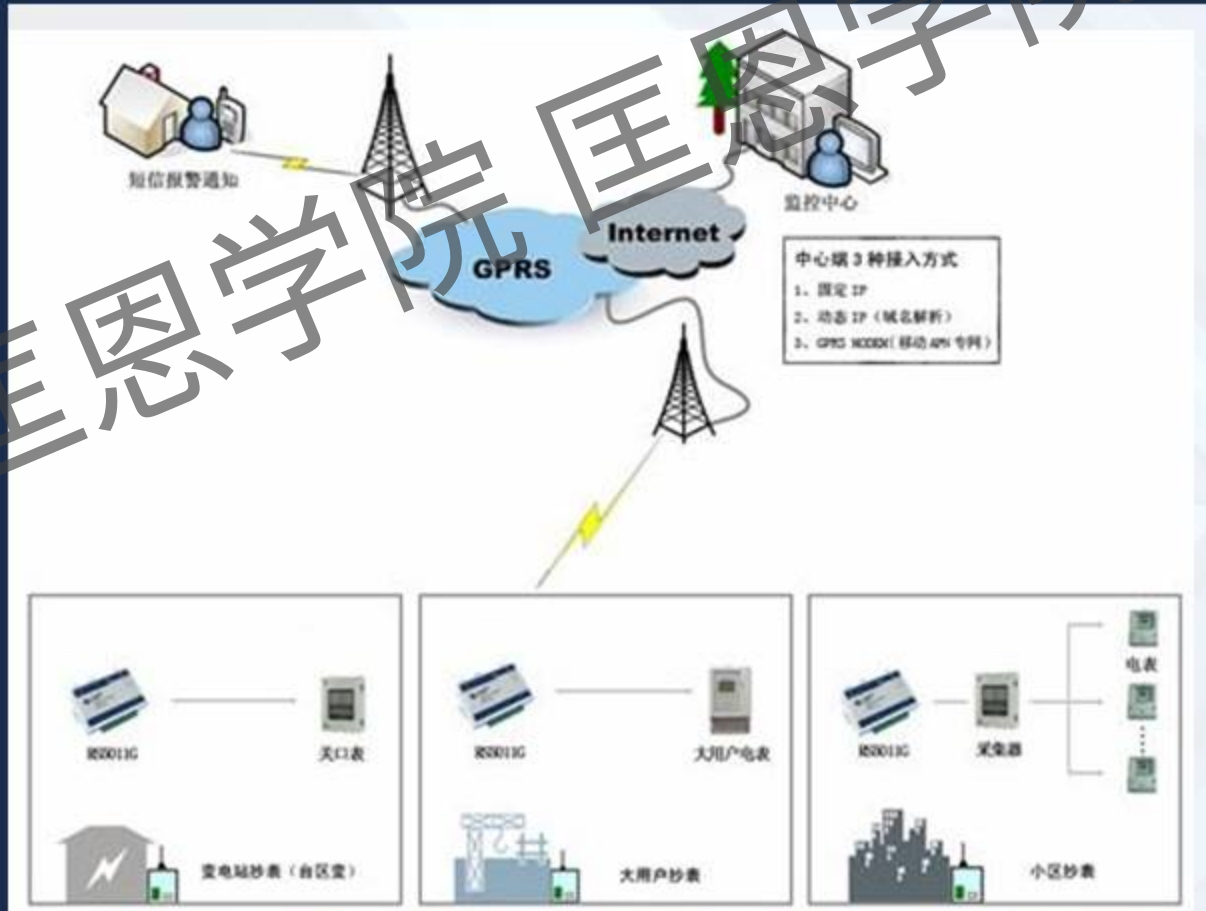
HackWire

方程式组织受害者分部

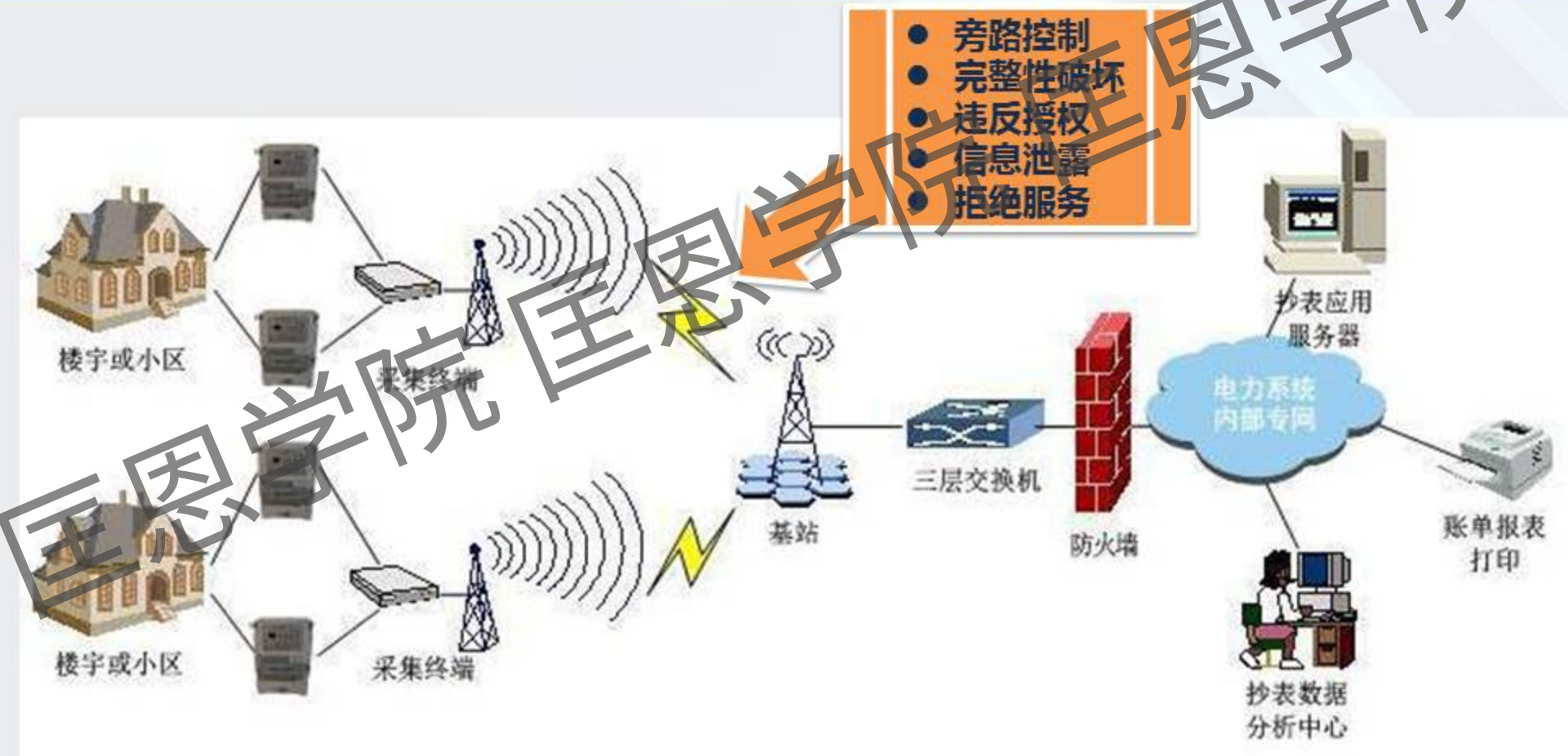
五大威胁——无线应用

- 随着无线技术的发展，无线技术以其卓越的便捷性快速融入各行业。

- 无线抄表、无线报警、无线视频监控系统应用层出不穷，在无线技术广泛应用的同时，也为工控系统带来被入侵以及资料窃取的风险。



无线应用引入的威胁



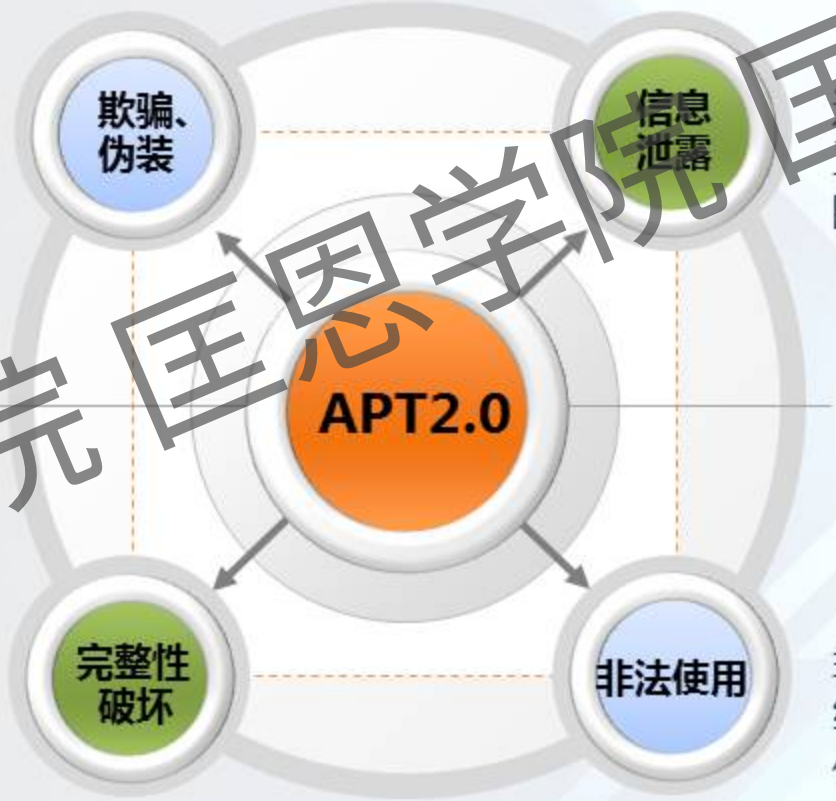
五大威胁——APT

以Havex为代表的新一代APT攻击将工业控制网络安全的对抗带入了一个新的时代

APT2.0特点

APT2.0的威胁

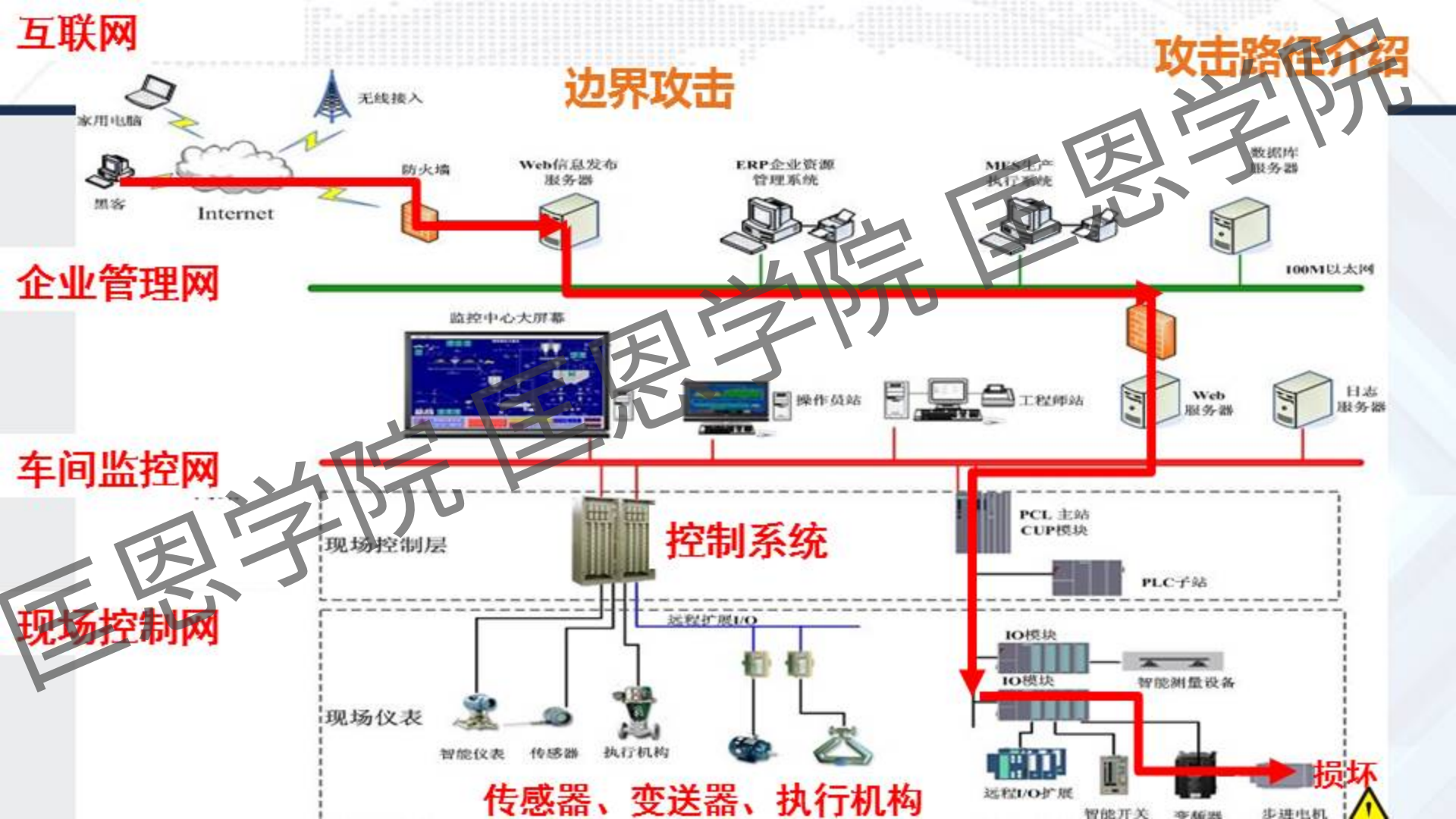
入侵者伪装合法身份，进入工业控制系统。利用合法的指令进行非法操作。

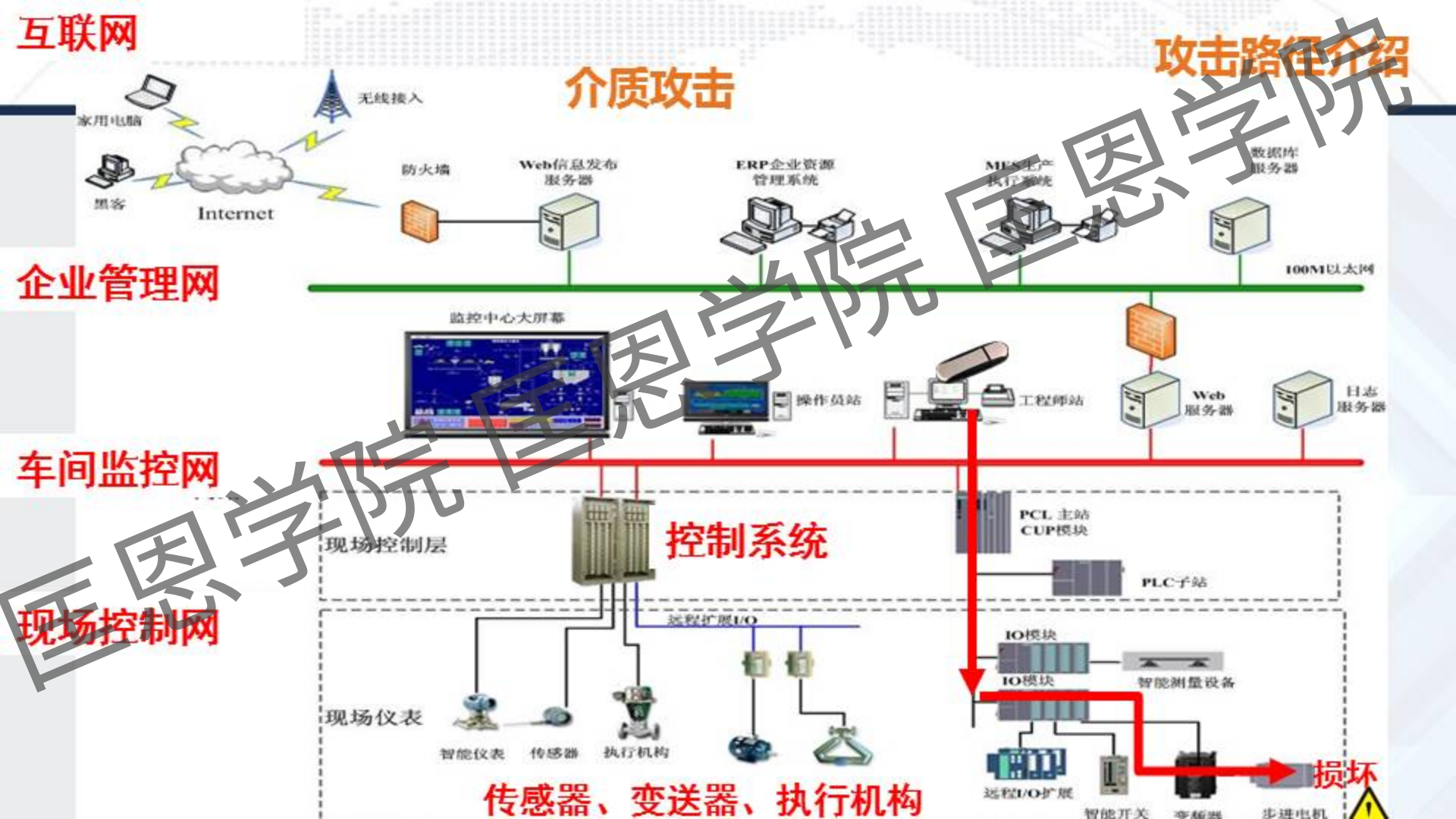


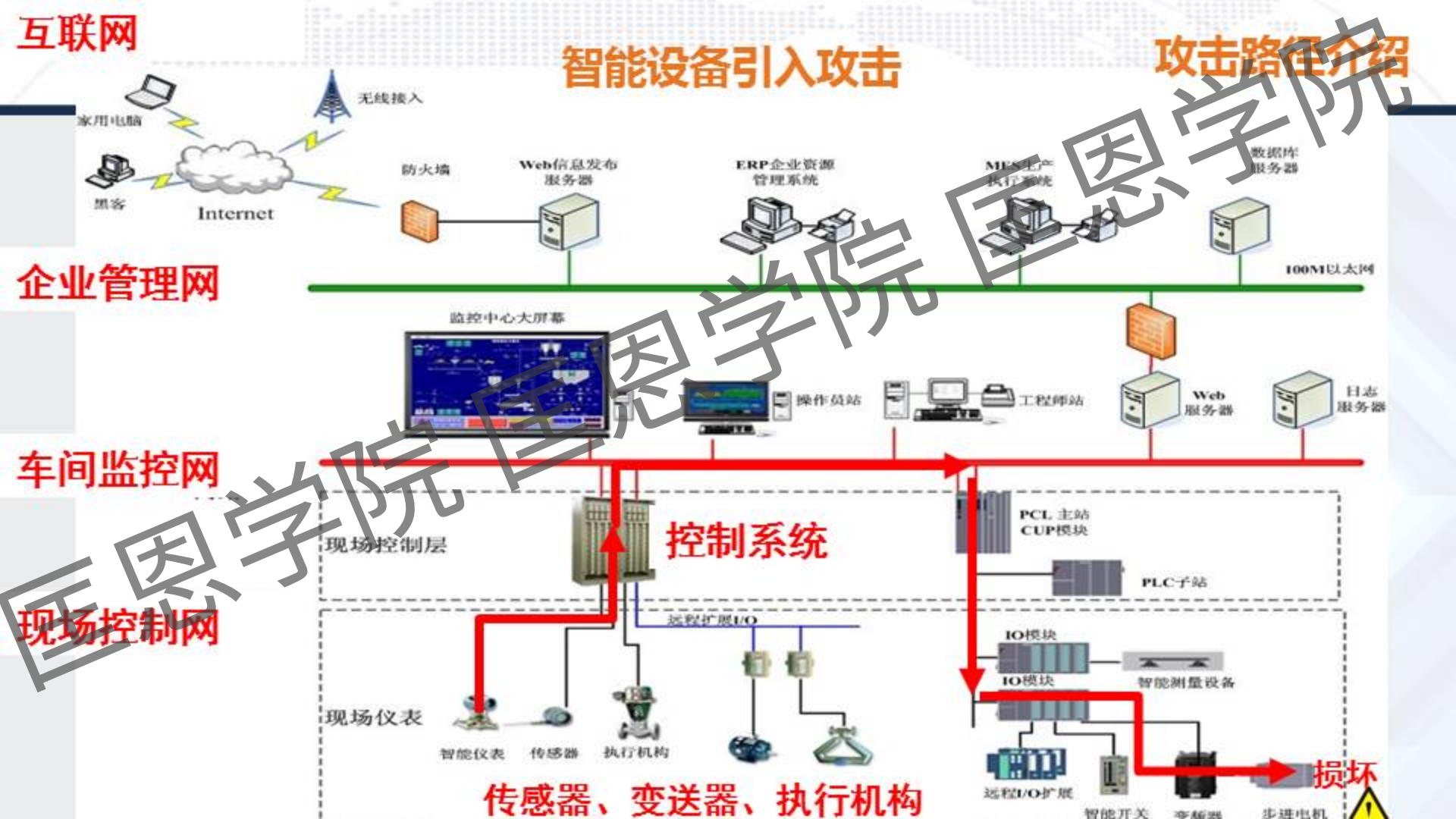
进行生产数据、工艺流程等数据的非法上传。

修改控制系统配置或程序；
修改数据库的敏感数据。

非法使用工控网络传输数据、传播病毒。


互联网
攻击路径介绍
边界攻击
家用电脑
无线接入
黑客
Internet
防火墙
Web信息发布
服务器
ERP企业资源
管理系统
MES生产
执行系统
数据库
服务器
企业管理网
100M以太网
监控中心大屏幕
操作员站
工程师站
Web
服务器
日志
服务器
车间监控网
现场控制层
控制系统
PCL 主站
CUP模块
PLC子站
现场控制网
远程扩展I/O
IO模块
IO模块
智能测量设备
现场仪表
智能仪表
传感器
执行机构
远程I/O扩展
智能开关
步进电机
损坏
传感器、变送器、执行机构





目录

CONTENTS

01 工控系统网络安全威胁攻击路径介绍

02 工控网络安全风险评估技术

03 工控系统网络漏洞检测技术

工控网络系统与传统的IT风险评估的区别

传统IT的风险评估不适用于工控网络系统

网络通讯协议不同

大量的工控系统采用私有协议

对系统稳定性要求高

不能借鉴传统IT的漏洞扫描方式

资源限制不同

系统支持固定的工业生产过程可能没有足够资源支持信息安全能力

评估目标对象不同

不同于互联网和办公网单一的系统或服务

技术支持不同

只接受供应商的技术支持

工业控制系统安全标准与传统网络安全对比

传统信息安全近100余个标准
工控系统网络安全3个

传统信息安全标准有体系
工控系统网络安全没有体系

传统信息安全自2003年开始
工控系统网络安全2011年开始

传统信息安全应用场景固定
工控系统网络安全应用场景多样

国内外工控系统安全标准介绍

国外

- NIST：NIST SP 800-82、
- NIST SP 800-53
- IEC：IEC 62443系列
- 美国国土安全局：CSSP（美国控制系统安全计划）

国内

- GB/T 26333-2010 工业控制网络安全风险评估规范
- GB/T 30976-2014 工业控制系统信息安全 第1部分：评估规范
- 第2部分：验收规范

关键基础设施工控安全评价体系

行业背景分析

网络结构安全性评估

网络结构安全性设计是工控网络安全的重要基础

大量工控网络在设计时根本没有考虑结构安全性

缺少结构安全性设计的在装系统规模远远超过新装系统

评估工控网络安全防护能力首先从结构安全性入手，
并且针对在装系统的局限性，提供创造性的有效解决方案

设备本体安全性评估

- 需要厂商离线安全评估
- 需要运营企业做入网测试和在线安全评估
- 在两化融合前提下，工业控制网络安全已经成为生产安全重要组成部分
- 对设备安全检测应该标准化、工具化，建立认证体系势在必行
- 设备检测评估的结果，应该在国家层面进行积累和共享

网络行为安全性评估

- 对于运行系统中网络行为安全性评估是整体安全性评估不可缺少的一部分
- 目前针对工控系统，尤其是基础设施的攻击具有很高的隐蔽性，只有通过深层的、持续的网络行为分析，才能够捕捉到攻击行为
- 实现有效的网络行为安全性评估，需要创新性的手段和技术
- 网络行为安全性评估必须有效避免对工业控制系统的干扰

工控网络安全可持续性评估

网络的安全性是相对的

建立工控信息安全中的组织结构

- 没有组织结构就没有可持续性
- 现实情况没有相应的组织结构
- 建立有体系的管理组织结构，必须考虑培训、认证
- 在建立企业级组织结构的基础上还需要建立国家级的组织结构

安全体系建立的深度和主动性

- 被动的防御攻击还是主动的管理威胁
- 仅仅具有应急响应的能力还不够，还需要考察威胁管理的能力和水平。
- 需要提高整体的威胁管理水平，让业主单位和安全组织在实施工控项目时负担起整个生命周期的威胁管理的责任。

安全体系中防御手段评估

防御手段不能孤立来看

考察评估阶段性解决计划

建议全生命周期来防御和评估

如何评估工控系统所受到的安全威胁

评估什么？

- 网络结构安全性
- 设备元素
- 网络行为
- 防御手段
- 人员、流程

谁来评估？

- 专业人员
- 综合素质人员

评估频率？

- 持续性而非年度性
- 回访、复查

目录

CONTENTS

01 工控系统网络安全威胁及攻击路径介绍

02 工控网络安全风险评估技术

03 工控系统网络漏洞检测技术

什么是工控系统漏洞

工控系统漏洞（Vulnerability）是指工业控制系统中存在的一些功能性或安全性的逻辑缺陷，包括一切导致威胁、损坏智能控制系统安全性的所有因素。在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

工控系统漏洞来源

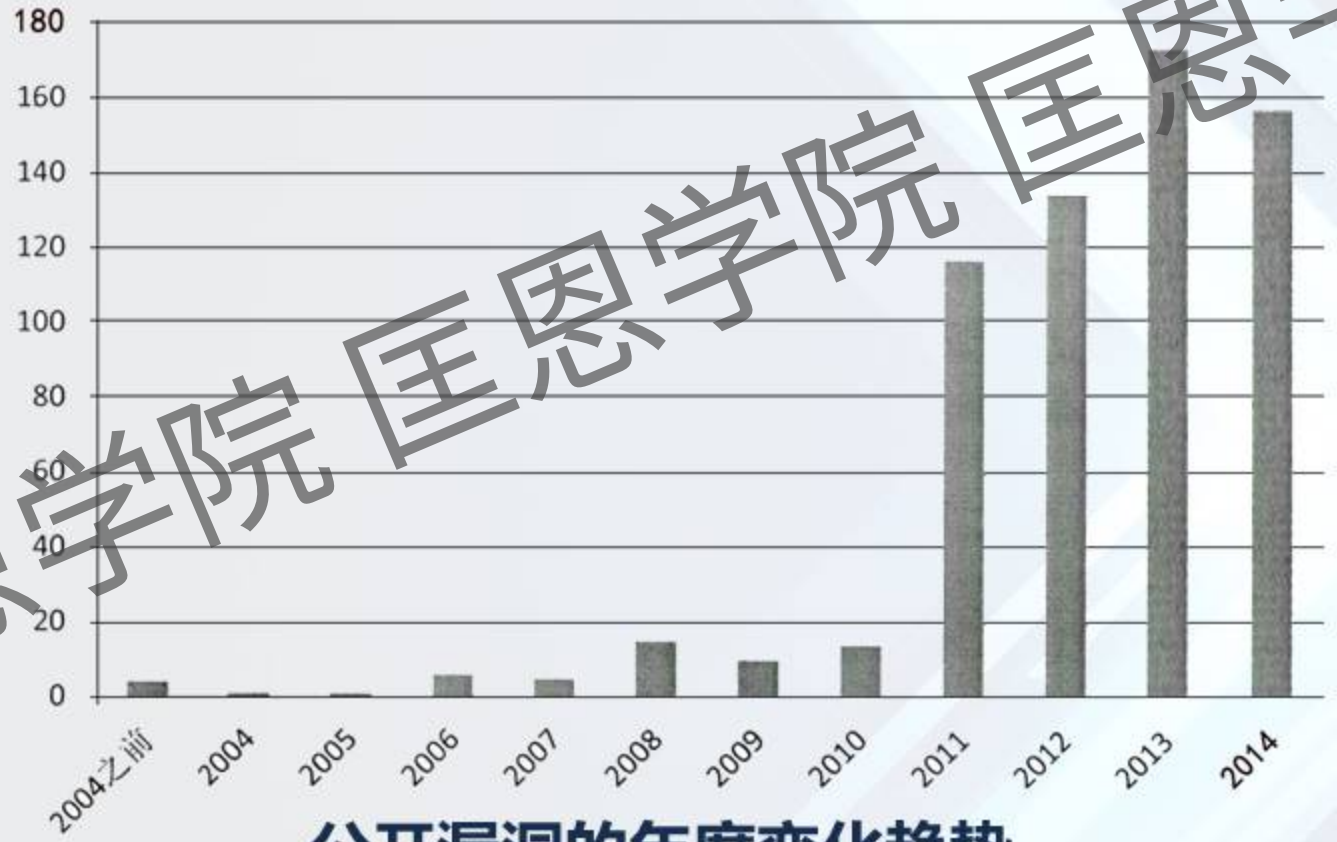
工控设备
工控系统

01 固件系统

02 软硬件设计/实现

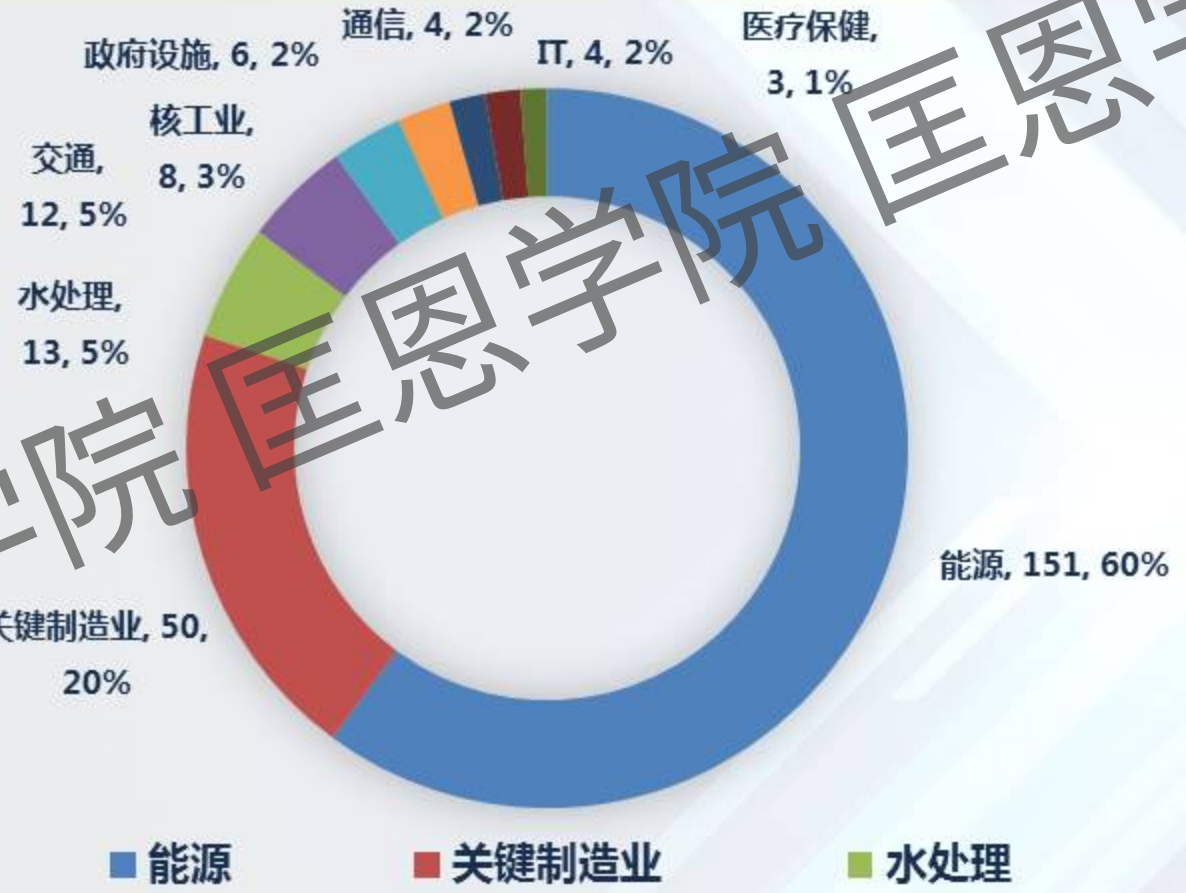
03 工控协议

工控系统漏洞现状

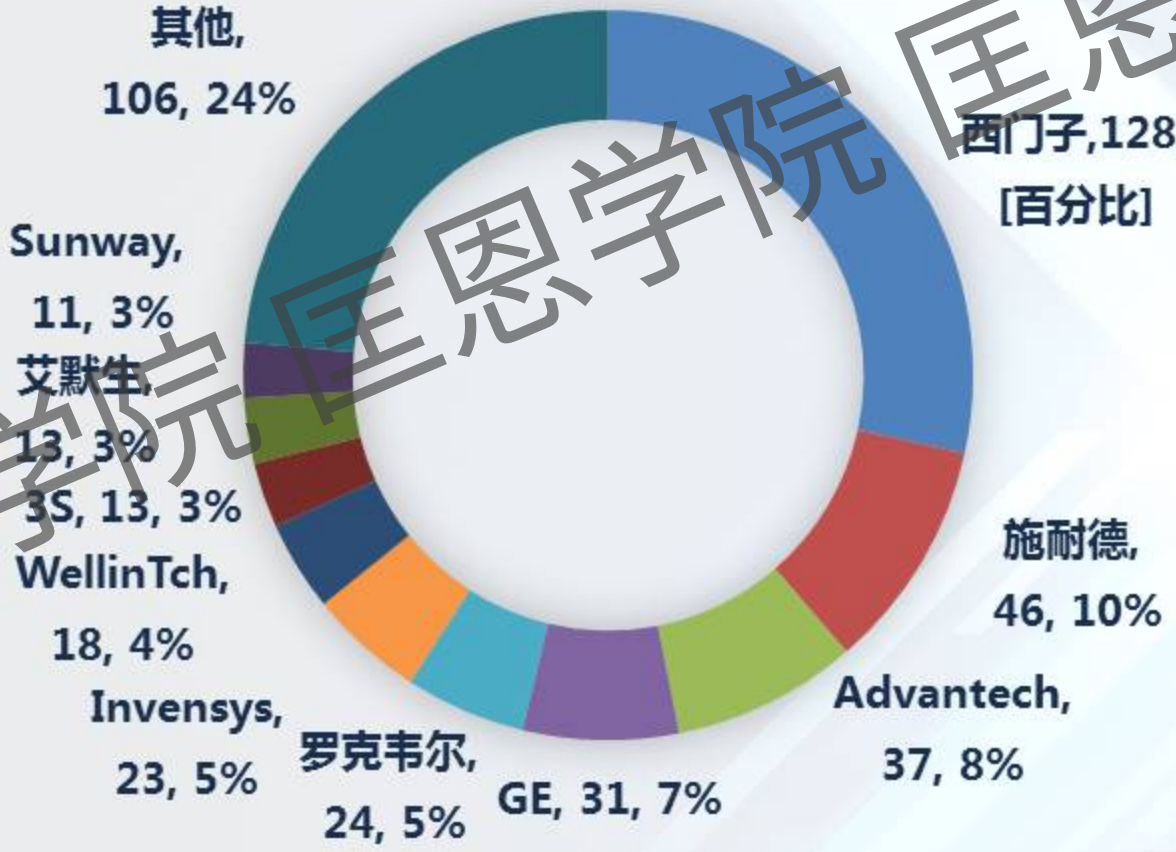


公开漏洞的年度变化趋势

工控系统漏洞涉及行业



公开工控系统漏洞的工控设备厂商



什么是漏洞扫描

通过跟已知漏洞库进行比对来确定目标系统存在漏洞的方式叫做**漏洞扫描**。

漏洞扫描分类及特点

基于主机的漏洞扫描

- 被动的、非破坏性的
- 系统的内核、文件的属性、操作系统的补丁

基于网络的漏洞扫描

- 主动的、破坏性的
- 特定脚本进行模拟攻击

漏洞扫描的优点与局限性

漏扫优点

检查速度快

非破坏性对系统影响小

漏扫缺点

局限于漏洞库中漏洞的数量

无法发现高危的未知漏洞

无法验证漏洞是否
真实存在在被测系统上

什么是漏洞检测技术

漏洞检测是多种漏洞挖掘分析技术相互结合，通过对目标系统的攻击，尽可能地找出目标中的潜在漏洞的技术。

工控网络安全亟需有效检测手段

目前检测手段局限性

01 现有检测手段仅针对外围服务器，无法触及亟待保护的核心工控设备

02 端口服务扫描、漏洞特征扫描等技术无法进行深入、全面的检测

03 基于公开漏洞库的扫描机制在时间上永远滞后于攻击者

工控系统检测对象分类

工业网络控制类设备

工业网络控制系统

工业网络安全类设备

工控系统检测手段

已知脆弱性检测功能

- 持续更新的公开漏洞库
- 持续更新的自主挖掘工控零日漏洞库
- 海量工控设备信息库
- 自主研发的产品硬件可支持工控设备脆弱性检测的全面性

未知脆弱性挖掘功能

- 基于大量实际案例积累的高效测试用例
- 先进的模糊测试算法集
- 自学习型漏洞定位能力
- 方便的测试用例自定义功能

检测内容：兼容性测试、稳定性测试、功能性测试、漏洞扫描、攻击测试等

工控系统基本检测方法

稳定性测试

漏洞扫描及验证

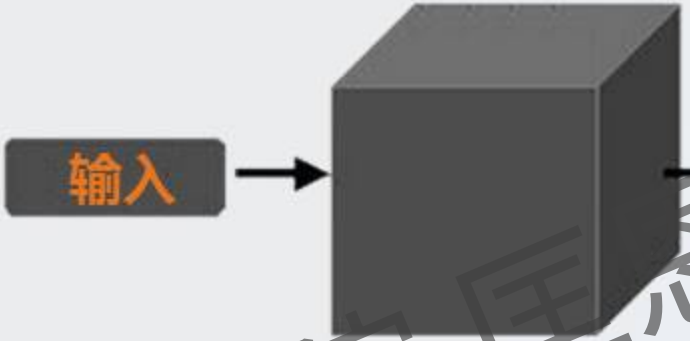
攻击测试

兼容性测试

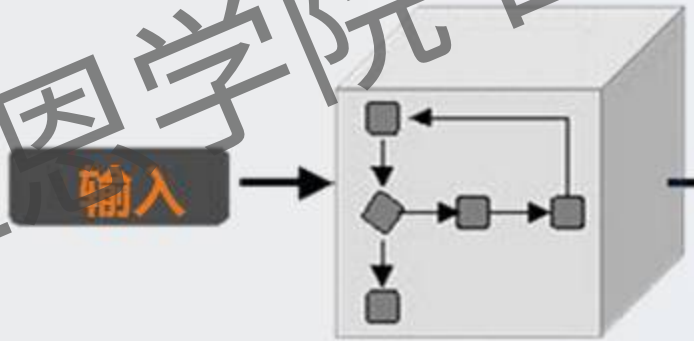
风暴测试

端口/服务扫描

工控系统检测方法-黑白盒测试



模糊测试



固件分析

工控系统漏洞检测的功能需求

漏洞发现　根源分析　衍生开发　漏洞验证　功能拓展　测试报告生成

工控系统漏洞检测的功能需求-漏洞发现

设备配置

调整设备间的拓扑连接方式，对被测设备端口进行自动扫描和配置

测试脚本

编辑进行漏洞测试或漏洞挖掘的运行脚本，提供多种快速灵活的方式

测试运行

测试时能够监视测试用例执行情况和结果，并能根据需要实时增加或减少未运行测试用例

测试结果

显示测试结果的具体细节，并可快读对结果进行漏洞标识，关联所有相关内容

漏洞编辑

对漏洞特征、触发因素等进行检查和再次编辑，并能够保存至本机漏洞库

工控系统漏洞检测的功能需求-根源分析

工控系统漏洞检测的功能需求-漏洞验证

漏洞详情

查看漏洞记录的详细信息

验证测试

重现漏洞发生环境进行验证

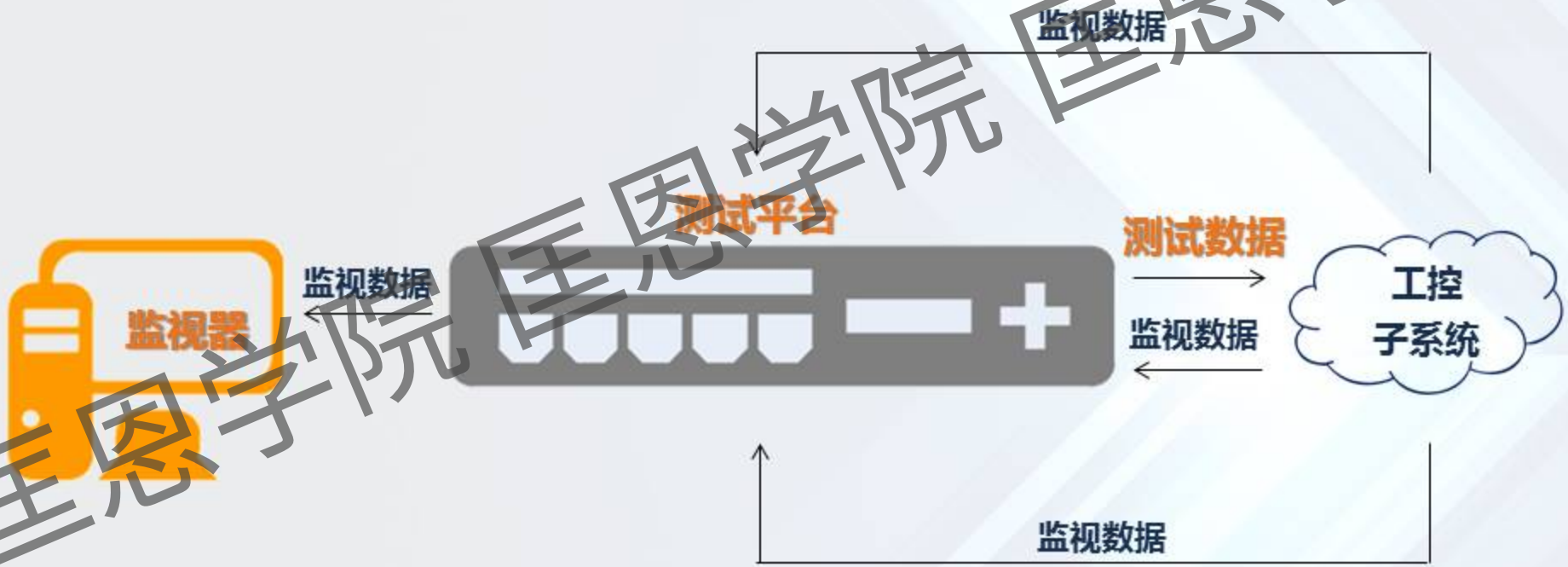
漏洞发布

审阅无误后将漏洞发布到本机漏洞库

工控系统检测环境-点对点测试

工控系统检测环境-桥接测试

工控系统检测环境-子系统测试



THANK YOU