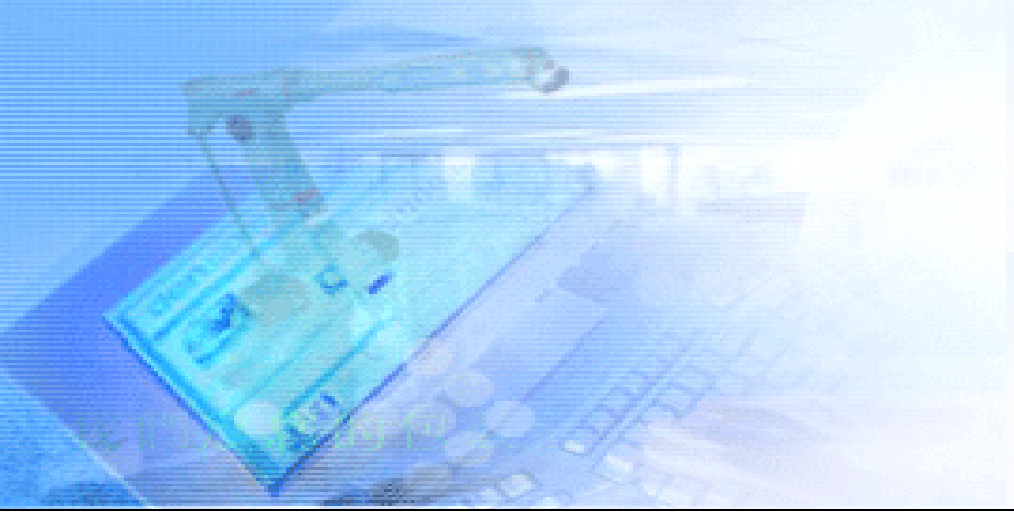


工业控制系统信息安全测试与防护技术趋势

万明

中科院网络与控制系统重点实验室

中国科学院沈阳自动化研究所

2014. 5. 22

提　纲

- 工业控制系统的脆弱性
- 工业控制系统信息安全需求
- 工业控制系统安全测试技术趋势
- 工业控制系统安全防护技术趋势
- 沈自所研究基础与开展工作

一、工业控制系统的脆弱性

正向复杂化、IT化和通用化趋势发展
基于PC+Windows的工业控制网络面临安全挑战

国外：

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；

2011年，微软警告称最新发现的“Duqu”病毒可从工业控制系统制造商收集情报数据；

2012年，两座美国电厂遭USB病毒攻击，感染了每个工厂的工控系统，可被窃取数据；

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。

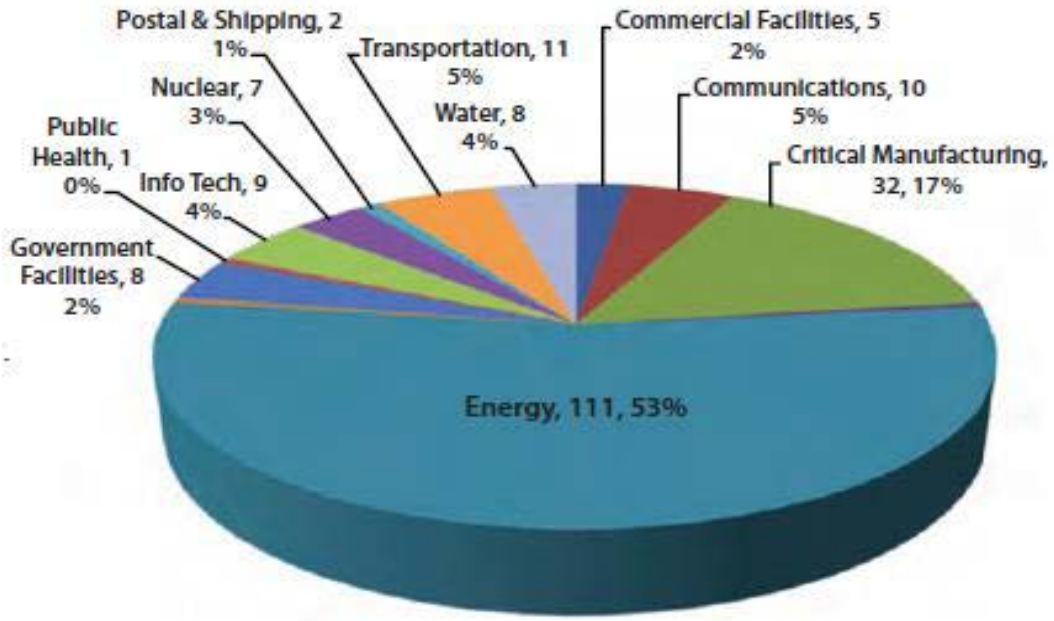
国内：

我国同样遭受着工业控制系统信息安全漏洞的困扰，比如2010年齐鲁石化、2011年大庆石化炼油厂，某装置控制系统分别感染Conficker病毒，都造成控制系统服务器与控制器通讯不同程度地中断。

一、工业控制系统的脆弱性

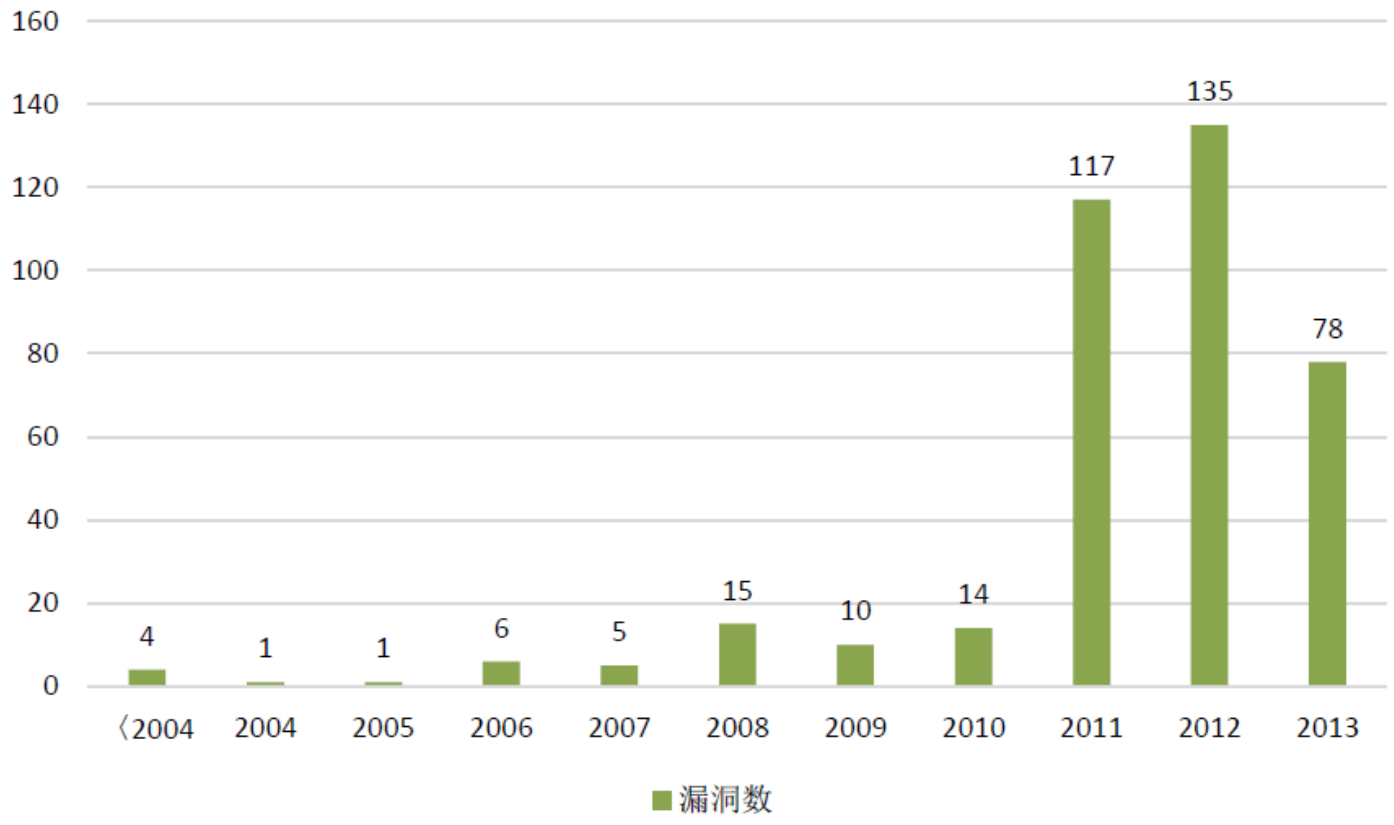
1、ICS-CERT安全报告指出“近三年针对工业控制系统的安全事件呈明显上升趋势，仅2013年度，针对关键基础设施的攻击报告已达到257起。”

2、主要集中在能源、关键制造业、交通、通信、水利、核能等领域，而能源行业的安全事故则超过了一半。



一、工业控制系统的脆弱性

归根结底就是工业控制系统的漏洞问题，截止到2013年12月底，公开的工业控制系统漏洞数总体仍呈增长趋势。



一、工业控制系统的脆弱性

2010年6月出现的Stuxnet病毒，是世界上首个专门针对工业控制系统编写的席卷全球工业界破坏性病毒，它同时利用7个最新漏洞进行攻击。这7个漏洞中，有5个是针对windows系统，2个是针对西门子SIMATIC WinCC系统。

一、工业控制系统的脆弱性

工业控制系统的漏洞主要包括：

（1）通信协议漏洞

两化融合和物联网的发展使得TCP/IP协议等通用协议越来越广泛的应用在工业控制网络中，随之而来的通信协议漏洞问题也日益突出。

（2）操作系统漏洞

目前大多数工业控制系统的工程师站/操作站/HMI都是Windows平台的，通常现场工程师在系统开启后不会对windows平台安全任何补丁，埋下了安全隐患。

（3）应用软件漏洞

由于应用软件多种多样，很难形成统一的防护规范以应对安全问题，另外当应用软件面向网络应用时，就必须开放其应用端口，是重要的攻击途径。

一、工业控制系统的脆弱性

工业控制系统的漏洞主要包括：

（4）安全策略和管理流程漏洞

追求可用性而牺牲安全性，是很多工业控制系统存在的普遍现象，缺乏完整有效的安全策略与管理流程也给工业控制系统信息安全带来一定的威胁。

（5）杀毒软件漏洞

为了保证工控应用软件的可用性，许多工控系统操作站通常不会安装杀毒软件，即使安装了杀毒软件，病毒库也不会定期的更新。

提　纲

- 工业控制系统的脆弱性
- 工业控制系统信息安全需求
- 工业控制系统安全测试技术趋势
- 工业控制系统安全防护技术趋势
- 沈自所研究基础与开展工作

二、工业控制系统的安全需求

工控系统与传统IT系统的不同

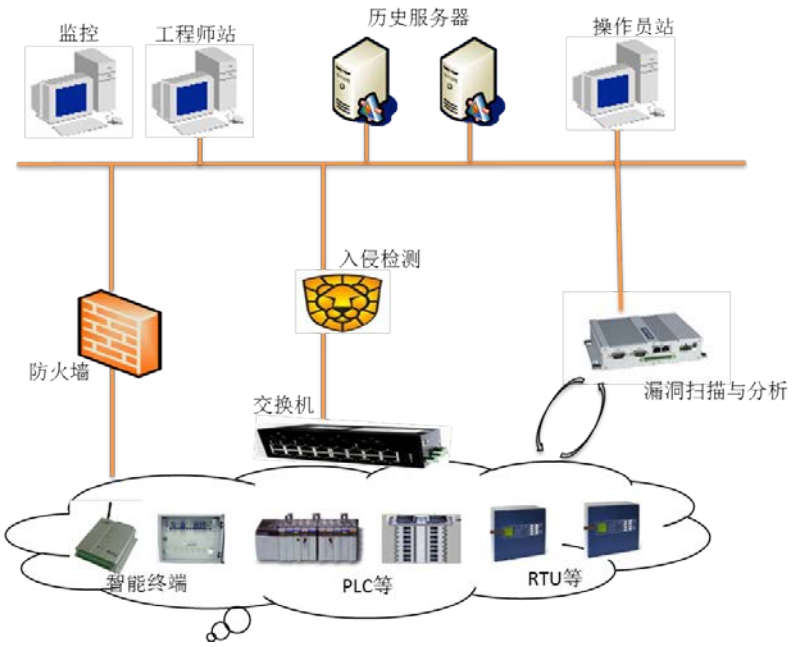
对比项	工业控制系统ICS	传统IT系统
体系结构	主要由传感器、PLC、RTU、DCS、SCADA等设备及系统组成	通过互联网协议组成的计算机网络
操作系统	广泛使用嵌入式系统VxWorks、uCLinux、winCE等，并根据功能及需求进行裁剪与定制	通用操作系统 如windows、linux、UNIX等，功能强大
数据交换协议	专用的通信协议或规约（OPC、Modbus TCP、DNP3等），一般直接使用或作为TCP/IP的应用层	TCP/IP协议栈
系统实时性	实时性要求高，不能停机或重启	实时性要求不高，允许传输延迟，可停机或重启
系统升级	兼容性差、软硬件升级困难	兼容性好、软件升级频繁

二、工业控制系统的安全需求

工控安全与传统IT安全的差异化

传统网络安全技术不适于应用到工业控制系统

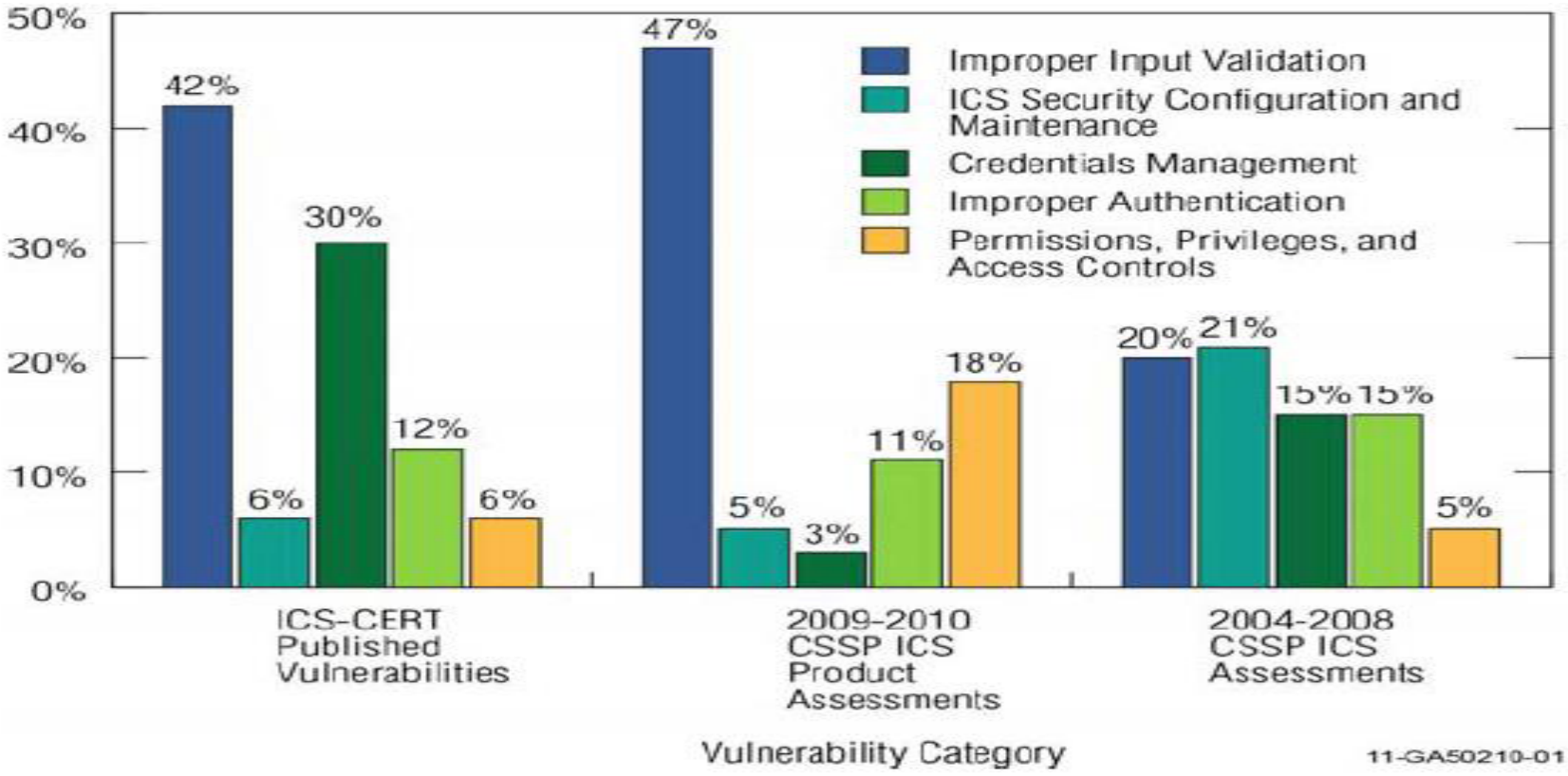
传统IT安全： 机密性 > 完整性 > 可用性
工控系统安全：可用性 > 完整性 >机密性



方式	传统IT网络	工业控制网络
防火墙	TCP/IP协议	专有协议格式
入侵检测	存在误报率	不允许存在误报
漏洞扫描	实时的补丁修复	补丁修复困难
设计初衷	传统IT系统：机密性 工业测控系统：可用性	

二、工业控制系统的安全需求

美国国土安全部下属的ICS-CERT（工业控制系统应急响应小组）及CSSP（控制系统安全项目）通过对工业控制系统软件的缺陷性分析发现，工业控制系统软件的安全脆弱性问题主要涉及错误输入验证、密码管理、越权访问、不适当的认证、系统配置等方面。



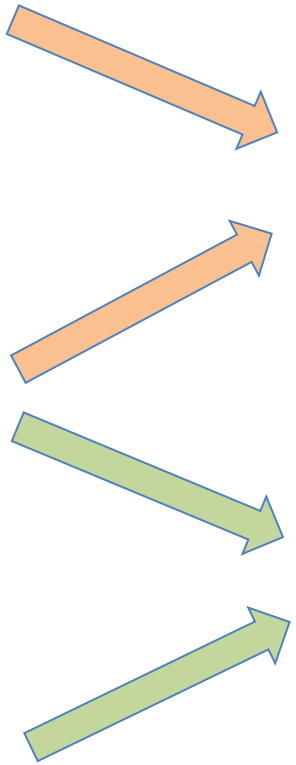
二、工业控制系统的安全需求

典型工控系统的安全问题

系统及软件的脆弱性，易被黑客利用，无法及时发现存在的系统漏洞！

控制节点无防护能力，容易被恶意接入控制；控制网络明文传输，数据易被篡改！

核心通信网络缺少认证、授权、加密，无访问控制能力，容易遭受恶意攻击！



工业控制系统的安全测试技术

工业控制系统的安全防护技术

提　纲

- 工业控制系统的脆弱性
- 工业控制系统信息安全需求
- 工业控制系统安全测试技术趋势
- 工业控制系统安全防护技术趋势
- 沈自所研究基础与开展工作

三、工业控制系统的安全测试技术趋势

工业控制系统的特点

- 封闭性：SCADA、ICS系统的设计之初安全机制不完善
- 多样性：多种数据接口（如RJ45、RS485、RS232等）,协议规约实现多样
- 复杂性：专用的通信协议或规约（如OPC、Modbus、DNP3、 Profibus等）
- 不可改变性：工控系统程序升级困难！

传统IT安全测试技术不适合工业控制系统

急需针对工业控制系统的安全测试技术：

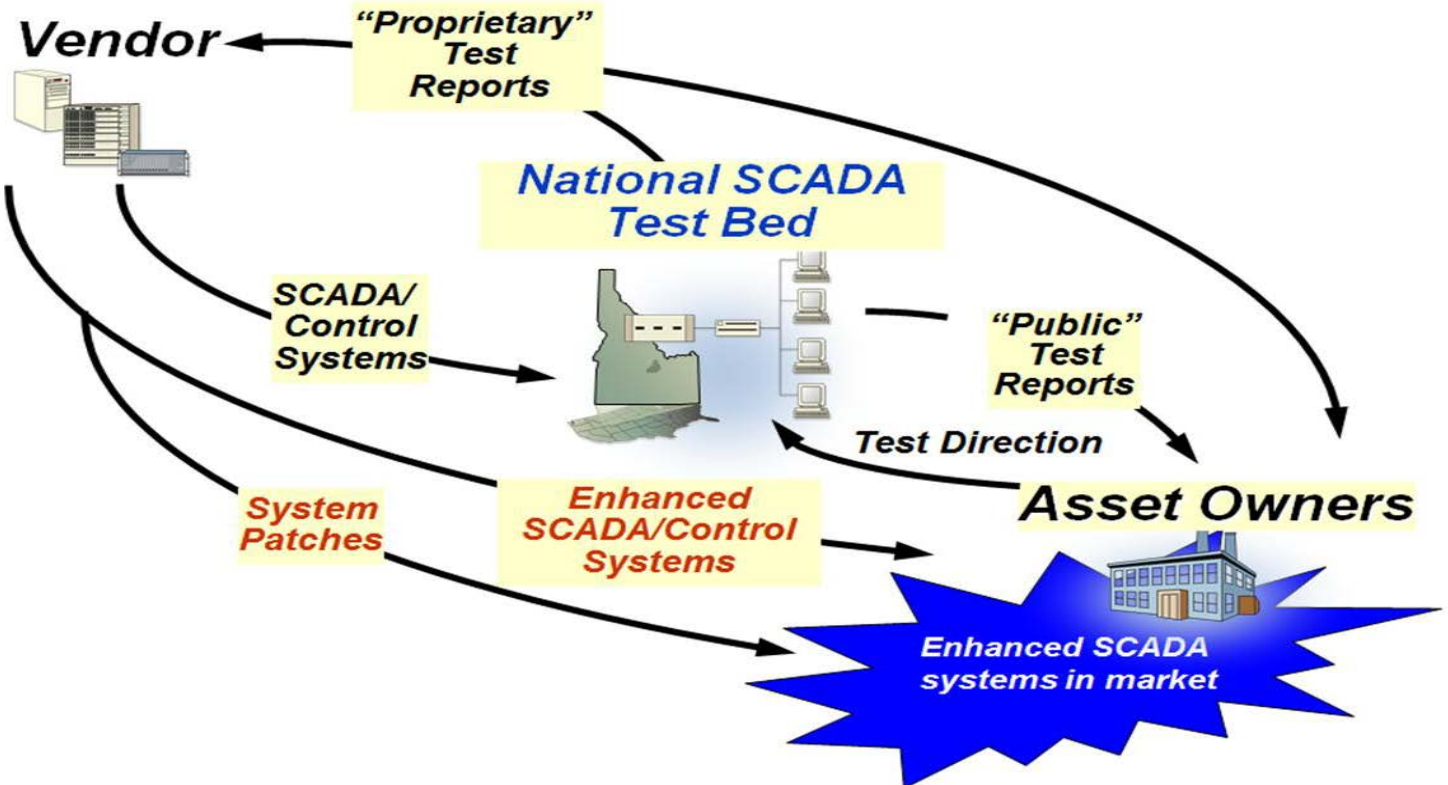
针对SCADA、ICS系统自身脆弱性（漏洞）和通信规约的安全性，研究工业控制系统的安全测试技术，分析工业控制系统中已知的与未知的安全威胁，指导其对安全威胁进行有效的防御。

三、工业控制系统的安全测试技术趋势

工控系统安全测试技术已成为重要的发展方向

- **美国能源部SCADA测试平台计划（2008-2013）**

  通过联合其下属Idaho等6个国家实验室的技术力量，提供各种工业控制系统的真实测试环境，实现对石油、电力等行业控制系统的安全测评。



三、工业控制系统的安全测试技术趋势

工控系统安全测试技术已成为重要的发展方向

美国能源部SCADA测试平台计划
——几个典型测试平台

（1）SCADA/控制系统测试平台；

（2）信息安全测试平台；

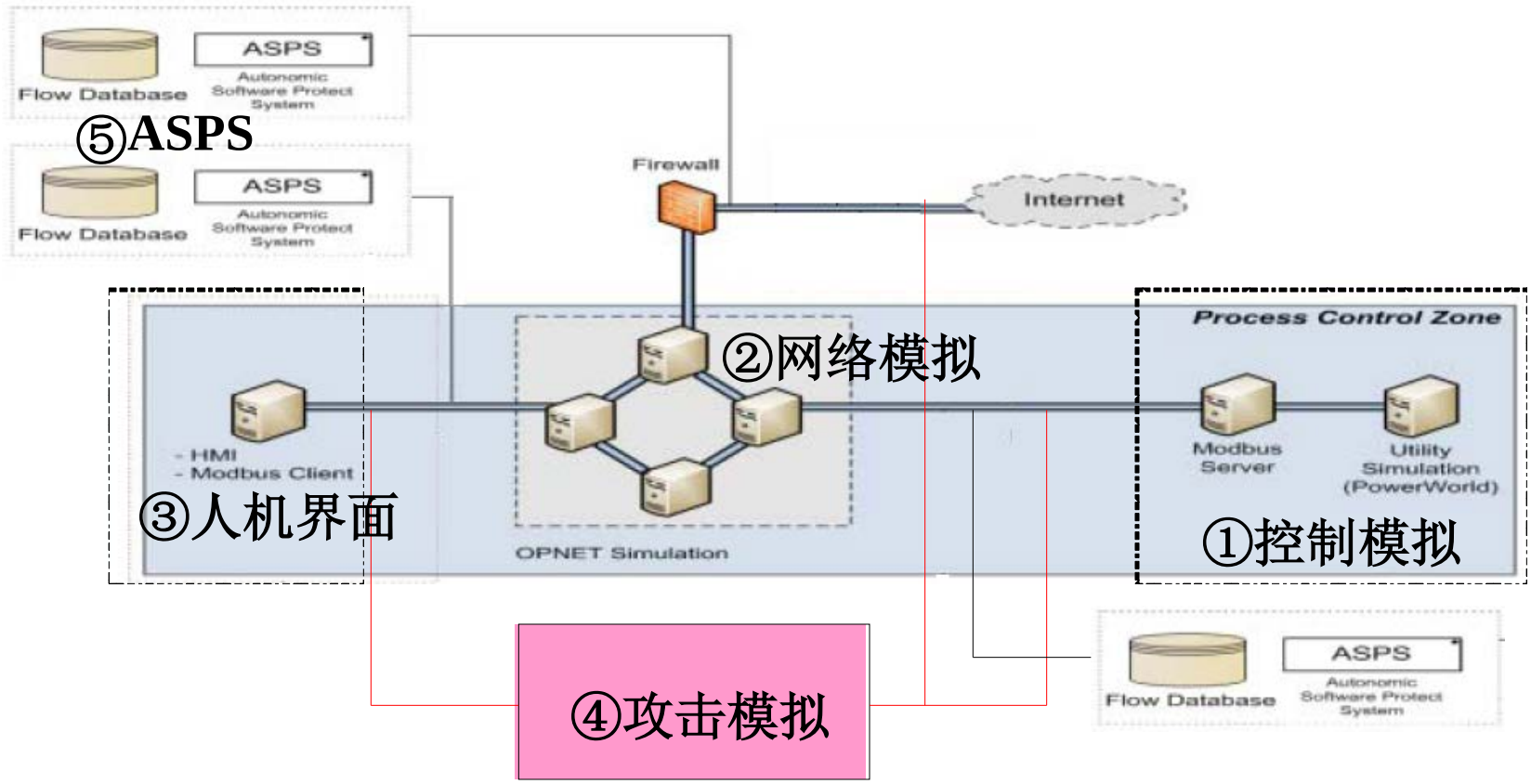
（3）电网测试平台；

（4）无线技术测试平台。

三、工业控制系统的安全测试技术趋势

工控系统安全测试技术已成为重要的发展方向

SCADA/控制系统测试平台实例



三、工业控制系统的安全测试技术趋势

工控系统安全测试技术已成为重要的发展方向

●欧洲SCADA安全测试平台

- 采用现场系统的渗透测试，建立风险分析方法，测试、评估SCADA系统的安全性。
- 对于Computer Emergency Response Team (CERT)发布的SCADA安全信息能够快速处理，以保护世界各地的运行系统。
- 具有高度重构，与其他SCADA系统安全、远距离通信连接，构建先进的分布式测试环境。

●学术界工控系统安全测试技术研究

国外学者致力于搭建SCADA系统真实测试环境，模拟攻击行为，通过仿真和建模分析SCADA系统的安全性。

三、工业控制系统的安全测试技术趋势

工控系统安全测试技术已成为重要的发展方向

国际知名工业安全测试公司相关产品和解决方案

- 加拿大 Wurldtech的Achilles 测试工具采用漏洞扫描和模糊测试的方法，测试工控系统中设备和软件的安全问题；

- 加拿大的ICS Sandbox测试平台采用渗透测试的方法，通过模拟真实的网络攻击，测试SCADA系统中关键基础设施的脆弱性。

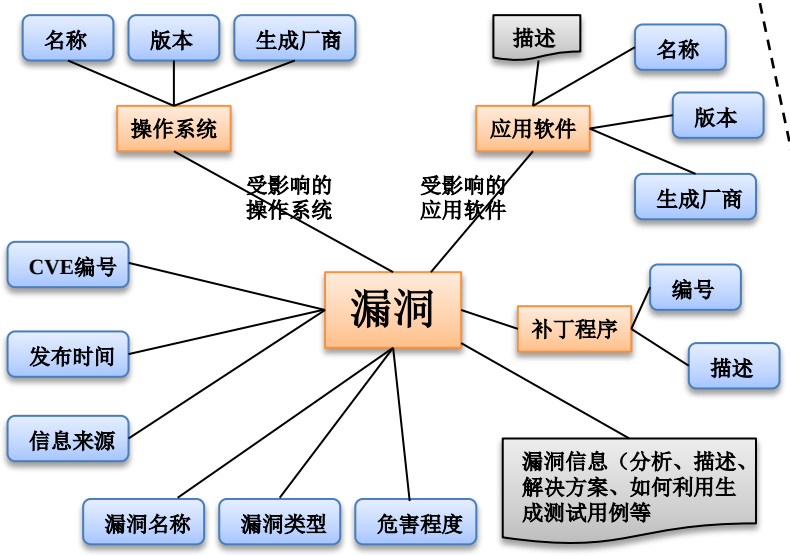
- 芬兰科诺康Codenomicon Defensics工控健壮性/安全性测试平台，采用基于主动性安全漏洞挖掘的健壮性评估与管理方案，与ISASecure合作，遵循IEC 62443标准

三、工业控制系统的安全测试技术趋势

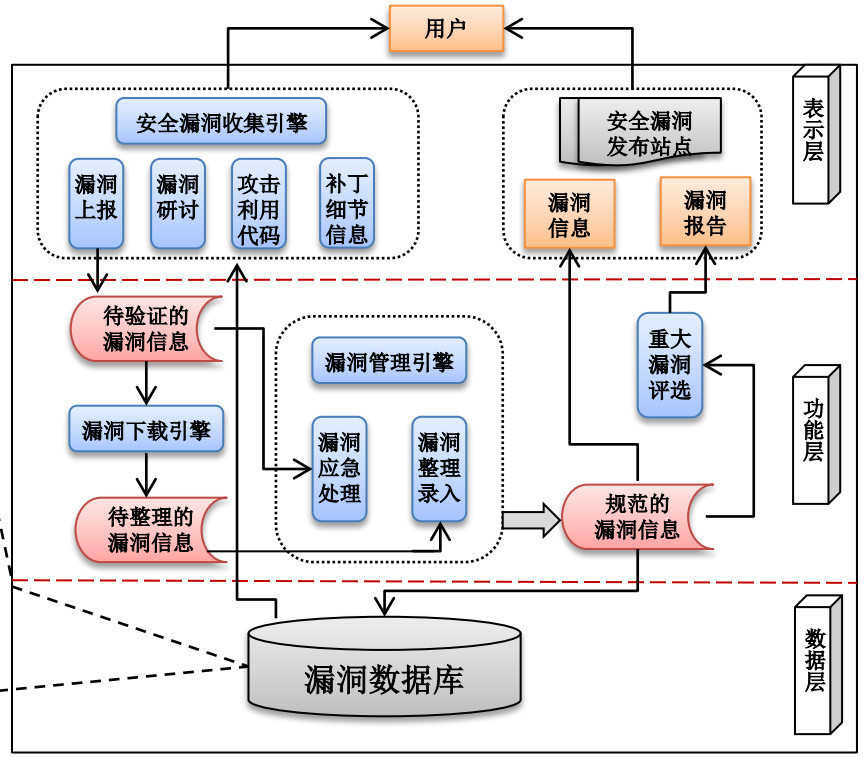
工控系统安全测试的关键技术

（1）构建工控系统漏洞库

由于通信协议的特殊性，传统漏洞库并不适应于工业控制系统安全测试领域，需要构建工控系统专有漏洞库。



漏洞描述

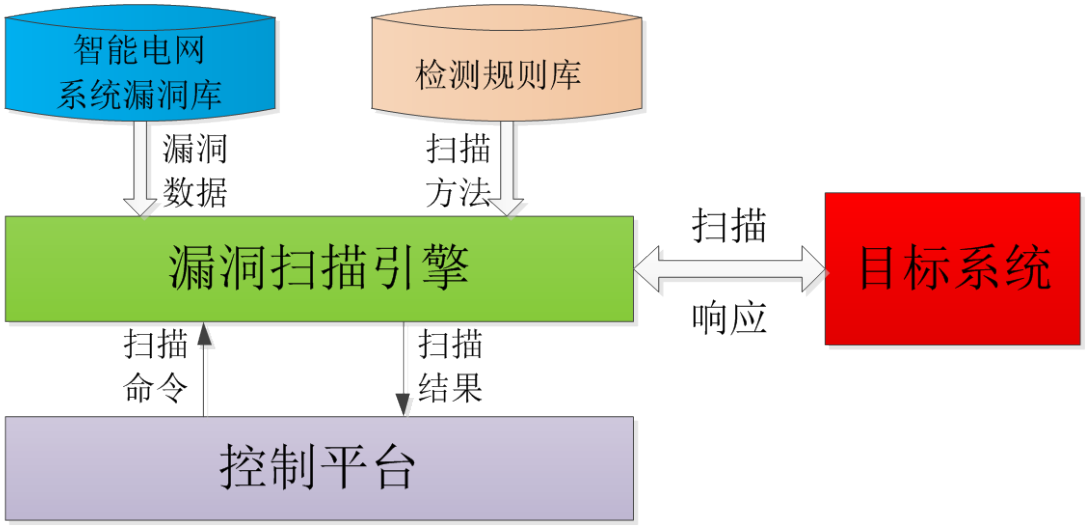


三、工业控制系统的安全测试技术趋势

工控系统安全测试的关键技术

（2）基于工业漏洞库的漏洞扫描技术

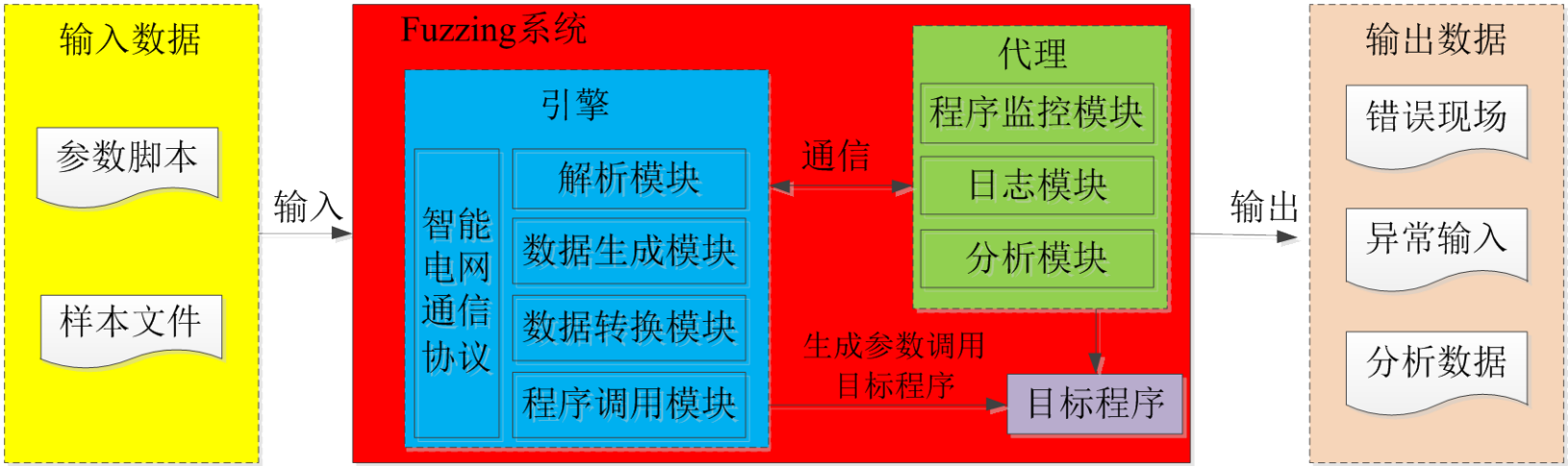
- 依靠漏洞扫描引擎、检测规则的自动匹配，通过工控系统漏洞库，扫描系统中的关键设备，检测系统的脆弱性；
- 支持Modbus、DNP3、Profinet等工业通信协议漏洞；
- 支持ICMP Ping扫描、端口扫描等传统扫描技术。



三、工业控制系统的安全测试技术趋势

工控系统安全测试的关键技术

（3）面向工业控制协议的Fuzzing测试



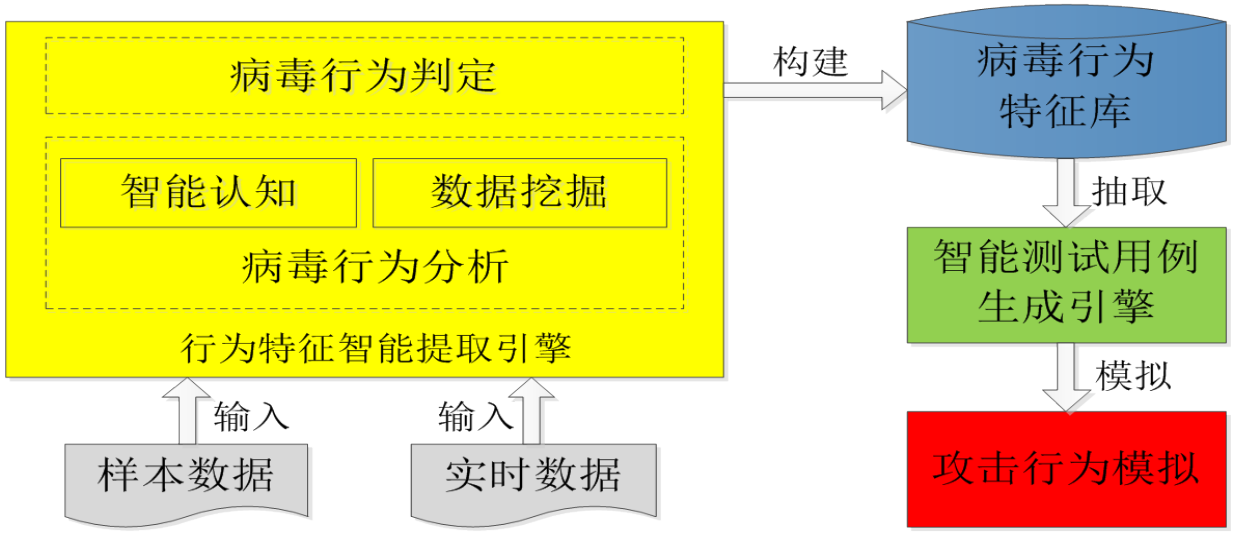
- 运用模糊测试的原理，设计变异测试用例并构造变异报文，检查工控协议实现的缺陷。
- 构建完整、可扩展的动态随机分析测试框架，监控测试目标，管理测试结果，并支持多目标（如文件、网络协议等等）、多种协议（如Modbus TCP、DNP3等不同类型的协议）、多线程（加速测试进度）

三、工业控制系统的安全测试技术趋势

工控系统安全测试的关键技术

（4）工业病毒行为特征提取与攻击模拟技术

- 数据挖掘智能认知工业病毒攻击行为，实现工业病毒行为判定，提取工业病毒行为特征；
- 根据网络流量情况、具体协议内容、交互模式以及主机或设备行为，检测工控环境特种木马等复杂攻击。



提　纲

- 工业控制系统的脆弱性
- 工业控制系统信息安全需求
- 工业控制系统安全测试技术趋势
- 工业控制系统安全防护技术趋势
- 沈自所研究基础与开展工作

四、工业控制系统的安全防护技术趋势

保证工业控制系统安全稳定运行，工业控制系统的安全防护必须达到以下三个目标：

目标	主要内容
通信可控	能够直观观察、监控、管理通信中数据。仅保证工业控制专有协议数据通过即可，其他通信一律禁止。
区域隔离	为防止局部控制网络问题扩散导致全局瘫痪，在关键数据通道上部署网络隔离。
报警追踪	及时发现网络中感染或其他问题，准确找出故障点。通过对报警事件进行记录，为故障分析提供依据。

工业控制系统防火墙技术

工业控制系统入侵检测技术

工业控制系统的安全防护技术趋势

1、工业控制系统防火墙技术

防火墙是基于访问控制技术，它可以保障不同安全区域之间进行安全通信，通过设置访问控制规则，管理和控制出入不同安全区域的信息流，保障资源在合法范围内得以有效使用和管理。

可以根据“白名单”或者“黑名单”的方式进行规则设置。对于“白名单”，可以设置允许规则，也就是说只有符合该规则的数据流才能通过，其他的任何数据流都可以被看做攻击而过滤掉，这样就保障了资源的合法使用；而对于“黑名单”，可以设置禁止规则，禁止不合法的客户端对资源的访问。

四、工业控制系统的安全防护技术趋势

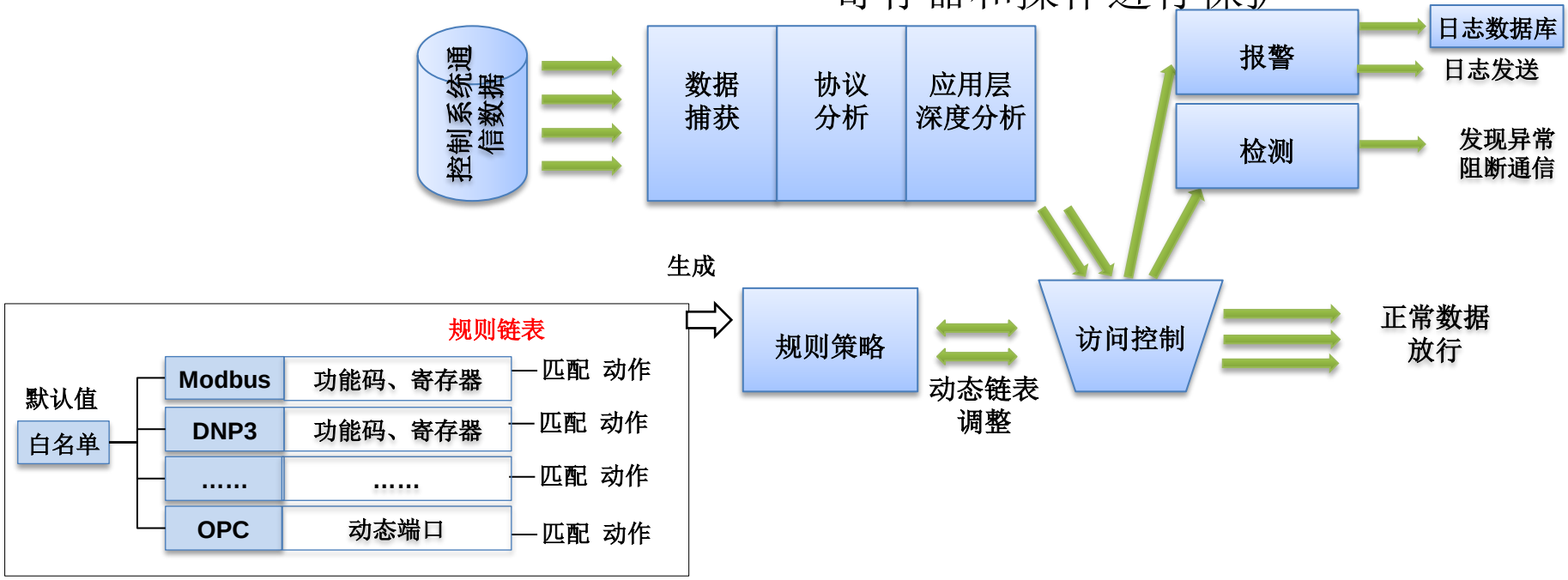
1、工业控制系统防火墙技术

区域管控

- 划分控制系统安全区域，对安全区域的隔离保护
- 保护合法用户访问网络资源

控制协议深度解析

- 解析Modbus、DNP3等应用层异常数据流量
- 对OPC端口进行动态追踪，对关键寄存器和操作进行保护

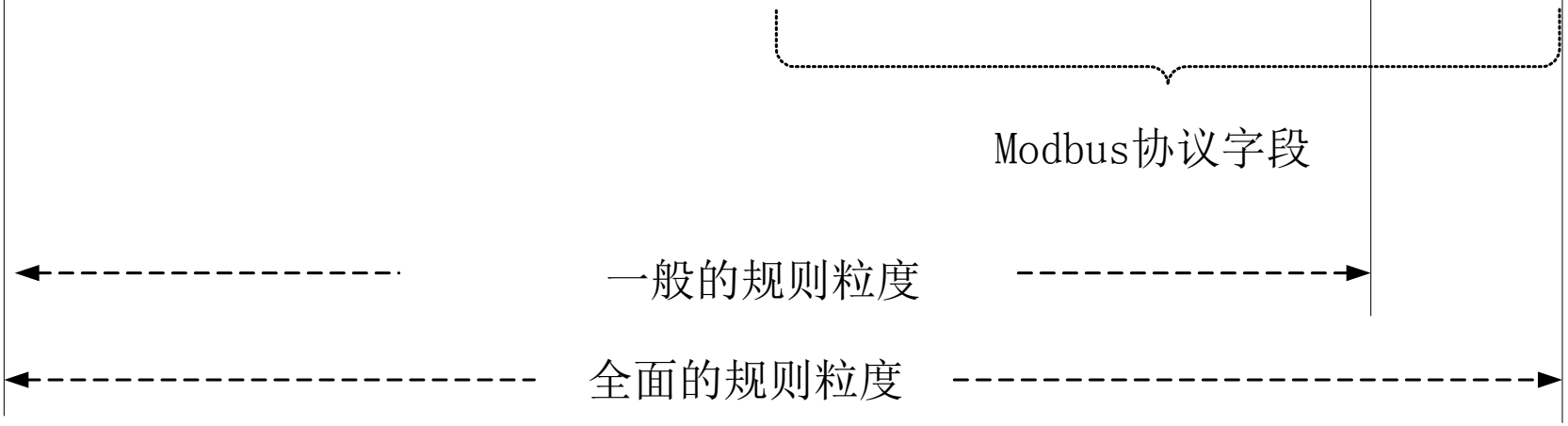


四、工业控制系统的安全防护技术趋势

1、工业控制系统防火墙技术

规则粒度问题（Modbus规则设置为例）

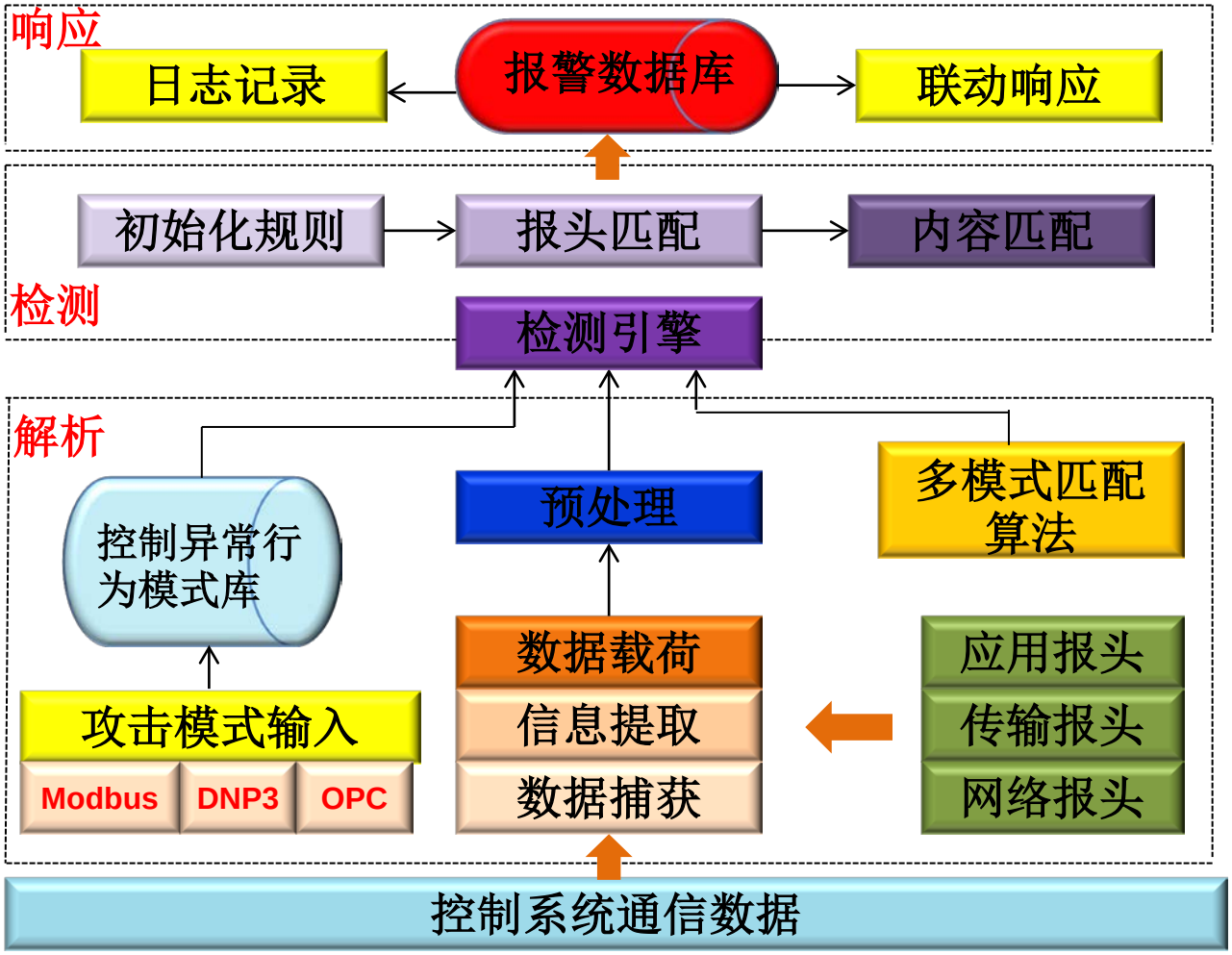
操作	协议	IP地址	端口	功能码	起始地址	数量	数据
允许	TCP	源、目的IP	源、目的端口	写线圈	100	1	200



防火墙的规则设置应该能够支持到具体数据字段的匹配，但是规则深度越深带来防火墙的效率问题。

四、工业控制系统的安全防护技术趋势

2、工业控制系统入侵检测技术

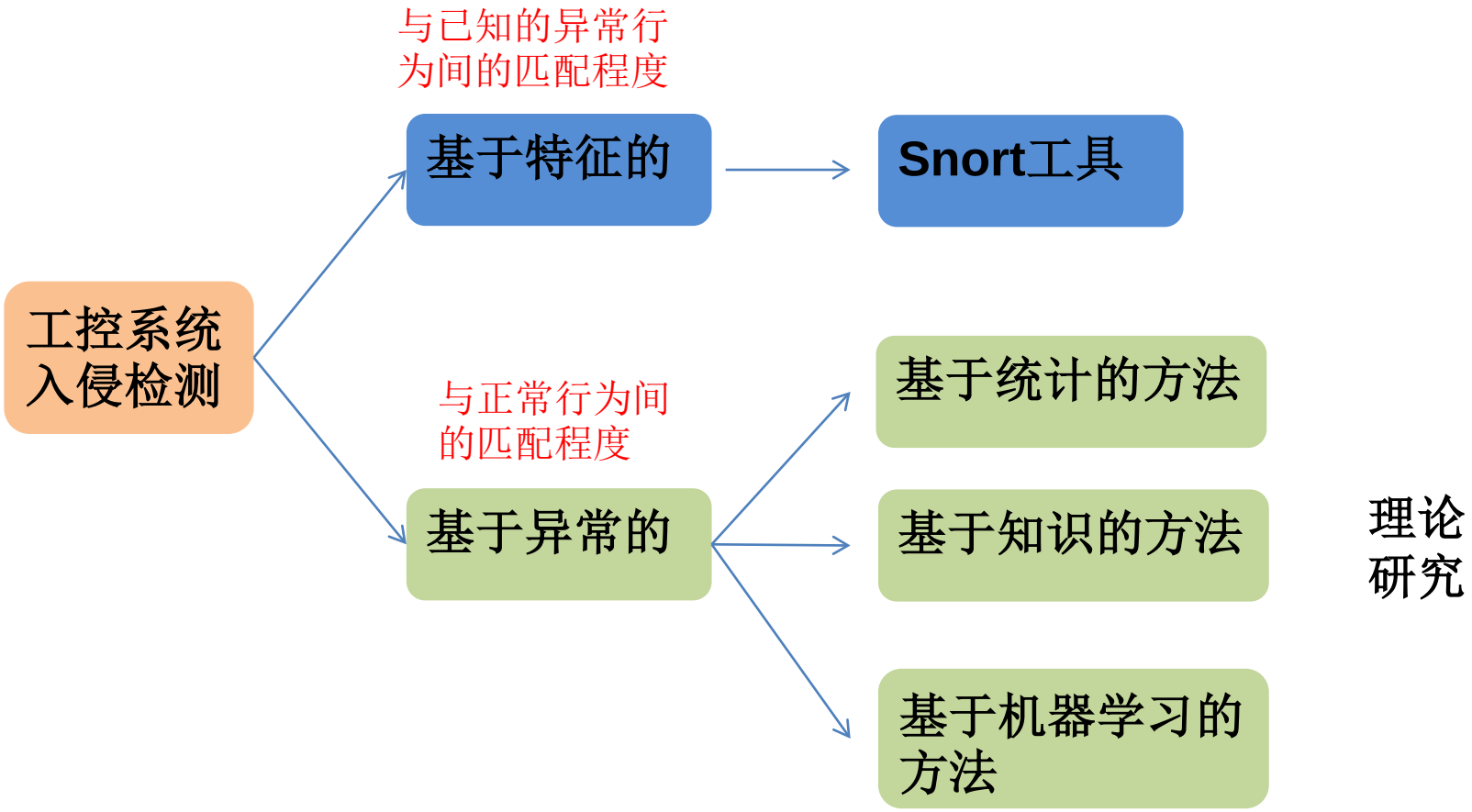


面向控制系统通信协议，根据控制异常行为模式库，对控制系统网络或主机进行异常监测：

- 监视、分析控制终端行为活动
- 审计控制系统的配置和弱点
- 识别已知进攻模式
- 异常活动的统计分析
- 实时报警和主动响应

四、工业控制系统的安全防护技术趋势

2、工业控制系统入侵检测技术



主要问题：工业控制系统以可用性为先，入侵检测技术的漏报和误报将难以商业化应用

提　纲

- 工业控制系统的脆弱性
- 工业控制系统信息安全需求
- 工业控制系统安全测试技术趋势
- 工业控制系统安全防护技术趋势
- 沈自所研究基础与开展工作

五、沈自所研究基础与开展工作

中国科学院沈阳自动化研究所

- 始建于1958年，国家机器人学重点实验室、国家机器人技术国家工程中心、中国科学院工业信息技术重点实验室、辽宁省先进制造技术工程中心、辽宁省网络化控制技术工程中心、辽宁省工业物联网重点实验室，完成各类科研项目1000余项，获得国家科技进步奖、中科院科技进步奖省、市地方科技成果奖200余项。
- 主要研究方向有机器人、工业自动化和光电信息处理，在工业自动化领域，工业无线技术和现场总线技术有深厚的积累，获得国家科技进步二等奖1项、国家技术发明二等奖1项、科学院科技进步一等奖1项。

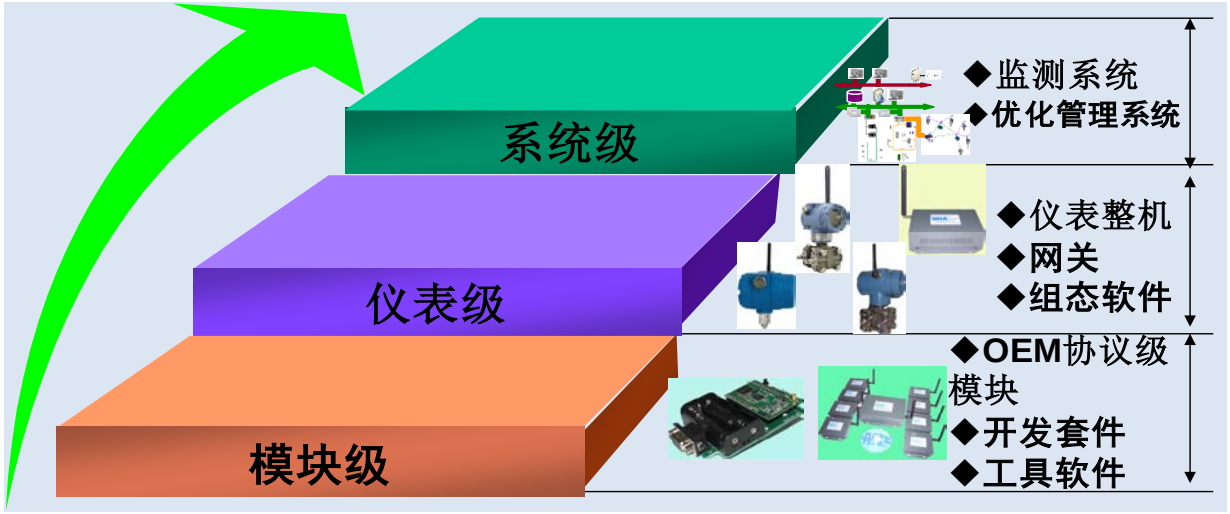
五、沈自所研究基础与开展工作

- 在现场总线方面，沈阳自动化研究所是国内第一个开展FF现场总线技术研究、国际上第三个通过一致性测试的研究机构，制定的工业以太网标准EPA已成为国家和国际标准。

量产4000片！

五、沈自所研究基础与开展工作

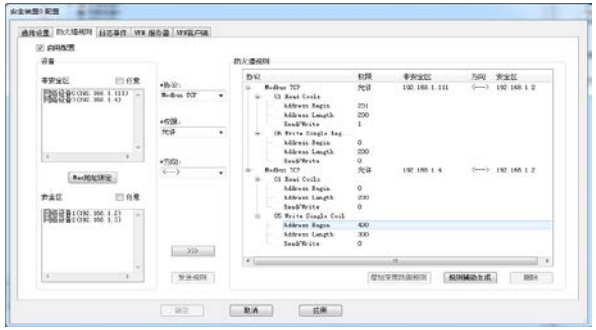
- 沈阳自动化研究所是中国工业无线联盟的发起单位，工业无线技术国家标准制定的组长单位，“十一五”863计划工业无线技术重点项目的牵头单位。
- 在工业无线技术和现场总线技术方面有深厚的积累，发表学术论文近150 余篇，出版专著1部，申请国家发明专利40余项，国际专利3项，软件著作权14 项，获得国家科技进步二等奖1项、国家技术发明二等奖1项、科学院科技进步一等奖1 项。
- 2011年7月，WIA-PA标准以中华人民共和国国家标准GB/T 26790.1-2011发布，并于2011年11月成为IEC正式国际标准。



五、沈自所研究基础与开展工作

- 在工业控制系统安全标准制定方面：开展了面向工业无线WIA-PA技术的安全标准制定工作，参与了IEC62443标准的国标转化工作。
- 面向智能无线网关、无线远程控制器（RTU）等设备，进行了基于可信加密芯片的主动安全防御技术的研究，面向石油、化工、电力、冶金、环保通等行业进行了应用。
- 完成2012年度国家863高技术计划项目子课题“工业控制系统网络安全技术研究”，研究ICS安全管控平台和安全网关技术。

技术参数
接收灵敏度：-100dBm
发射功率：19dBm
机箱尺寸：430×290×158.4mm
工作温度：-40℃～+85℃
宽幅工作电压：AC85V~265V
防护等级：IP65
防爆等级：Ex ib IIC T3
无线安全认证：AES 128bit



科技创造未来　　服务体现价值

敬请批评指正，谢谢！