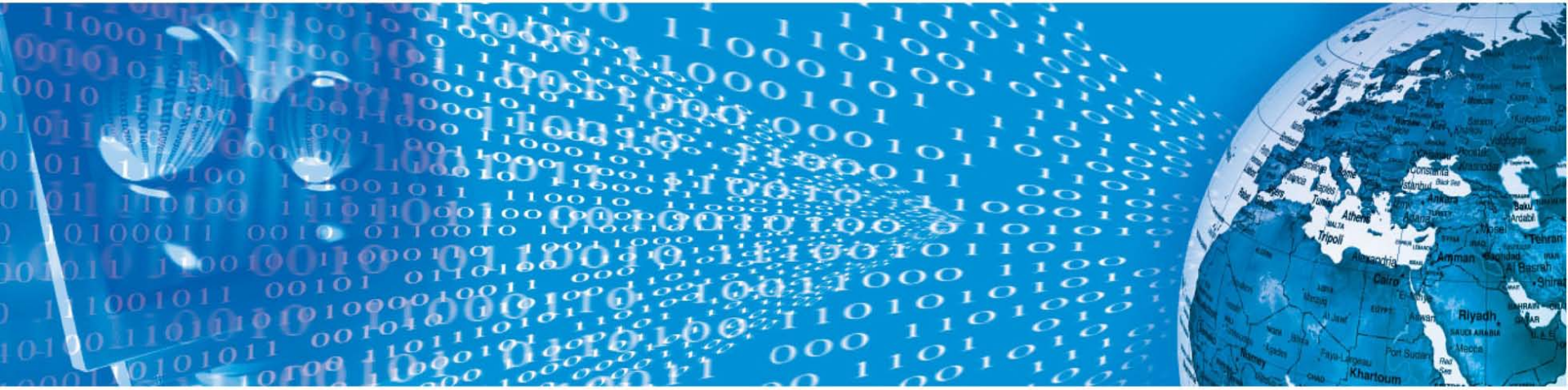
CEC
中国电子
CHINA ELECTRONICS



工控系统信息安全策略探讨

电子六所　徐新国

2013年8月

主要内容

- 形势分析
- 产业发展方面
- 理论研究方面
- 技术产品方面
- 监管与服务方面
- 行动建议

1、形势分析

越来越多的工控系统暴露于互联网上

隶属美国国土安全部的工业控制系统网络应急响应小组（ICS-CERT）报告：

在2012年4月开始的一项研究工作（**PROJECT SHINE**）中，使用简单的工具和技术（例如：SHODAN 搜索引擎等），发现大量工业设备和控制系统直接暴露在互联网上。经过ICS-CERT的鉴别和筛选，确认在美国本土，约有7200台与关键控制系统相连的系统可以在互联网上直接被访问到，美国本土之外的，涉及100多个国家和地区。这些系统的安全措施很脆弱，很容易成为对控制系统进行入侵的切入点。

—— ICS-CERT Monitor （Oct-Dec 2012），May 29, 2013, by ICS-CERT

1、形势分析

针对关键基础设施工控系统的攻击事件呈明显上升趋势

隶属美国国土安全部的工业控制系统网络应急响应小组（ICS-CERT）的关于2012财年的报告中，对近三年该组织收到的工控系统攻击事件报告进行了统计。

ICS-CERT FY Metrics	2010 Totals	2011 Totals	2012 Totals
ICS Incident Reported — tickets	39	140	197
ICS Incident Response Onsite Deployments	6	7	6
ICS Related Vulnerability Report — tickets	18	139	137
ICS CERT Information Products	110	243	347

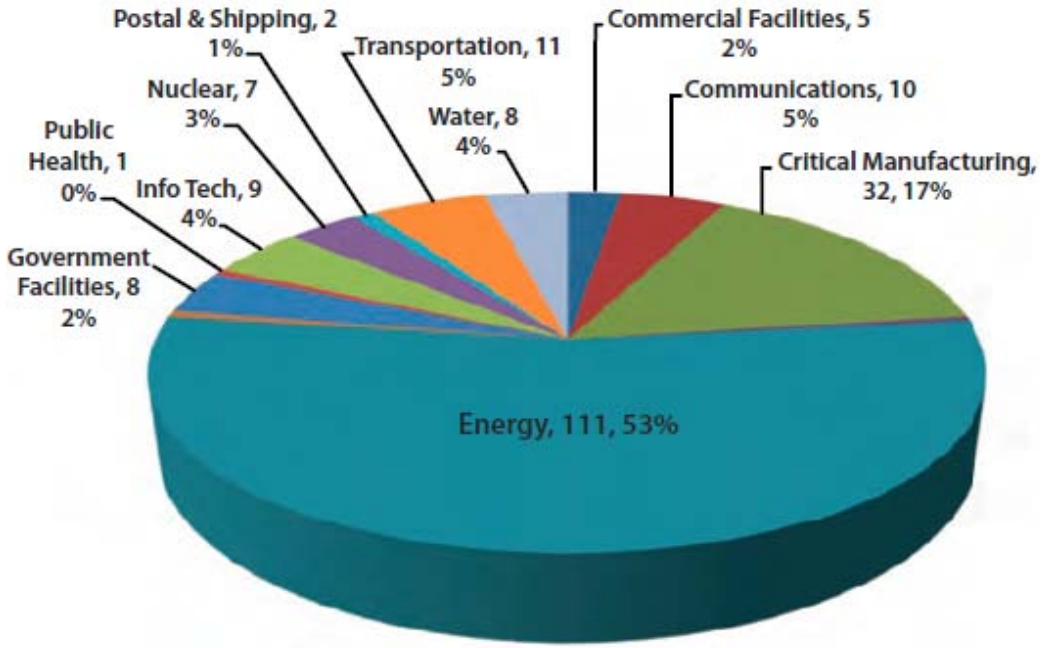
*Table 2. ICS-CERT activity trend by *Fiscal Year*

*Fiscal Year 2010 represents the time period of October 1, 2009–September 30, 2010, 2011 represents the time period of October 1, 2010–September 30, 2011, and 2012 represents the time period of October 1, 2011–September 30, 2012.

—— ICS-CERT Year-in-Review 2012, 03/07/2013, by ICS-CERT

1、形势分析

据该组织最新报告披露：从2012年10月-2013年5月，仅半年多时间，该组织响应的针对关键基础设施（critical infrastructure）的攻击报告已超过200起，比2012财年一年还多，其中能源领域111起，占53%，关键制造业32起，占17%；而2011年10月-2012年9月一年中，该数据为198起，能源82起（41%），关键制造8起（4%），呈明显的上升趋势。



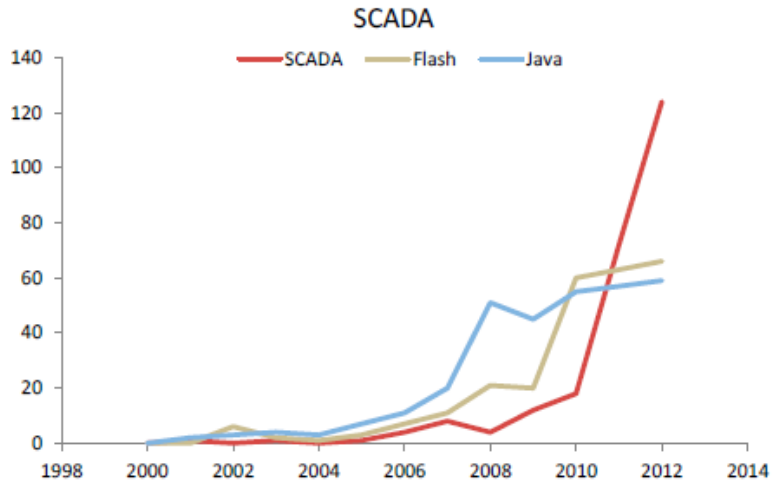
—— ICS-CERT Monitor （April-June 2013），July 12, 2013, by ICS-CERT

1、形势分析

关键基础设施工控系统的安全漏洞披露快速增长

据美国独立安全研究和评测机构 NSS Labs 报告显示：

2012年ICS/SCADA披露的安全漏洞为124个，从2010年以来增长了600%，仅2011-2012年就从74个增长到124个，增长了近1倍，涉及49个供货商。增长趋势还在进一步扩大。



——2012 Vulnerability Threat Report, February 4, 2013, by NSS Labs.

国内：国家信息安全漏洞共享平台（CNVD）已累计发布500多条工控系统安全漏洞。

1、形势分析

关键基础设施中的工控系统安全形势越来越严峻，国家经济安全和战略安全受到严重威胁。

总体而言，国内工控系统信息安全相关研究工作“相对”滞后，各方面建设刚刚起步，目前尚无专门针对工控系统攻击事件、风险漏洞的研究与处理部门，缺乏较全面的风险信息发布平台。

主要内容

- 形势分析
- 产业发展方面
- 理论研究方面
- 技术产品方面
- 监管与服务方面
- 行动建议

2、产业发展方面

现状：存量市场巨大，增量市场发展迅速，高端市场国外垄断

根据IMS Research最新的研究报告测算，2013年中国工业控制系统市场规模将会达到1311亿元人民币，年复合增长率在12%左右。

未来的增量市场正快速增长，据专家估算，到2020年，预计整体工控行业产品每年增量市场将超过2000亿元，未来10年的市场容量将超过1.4万亿元。

芯片、嵌入式操作系统、嵌入式软件、总线协议和工控软件等核心关键技术受制于人，造成中高端市场几乎全部由西门子、ABB、HONEYWELL等国外产品垄断。

工业控制系统完全自主可控在短时期内很难实现，对现有工控产品的安全监管严重缺失。

2、产业发展方面

- 存量、增量市场安全问题特点不同，需要逐步解决
- 重点保障关键基础设施工控系统的本质安全
- 服务市场需要尽快建立和规范

重点发展安全的工控产品
解决系统各层面的安全脆弱性
逐步做到自主可控、安全可靠

针对新建工控系统的安全要求

填补安全服务市场空白
安全风险评估
产品评测与认证
事件响应应急预案编制
安全管理培训等等

针对工控系统安全服务需求

优先发展安全防护产品
解决技术防护手段薄弱
保障系统本质安全

针对既有工控系统的安全问题

主要内容

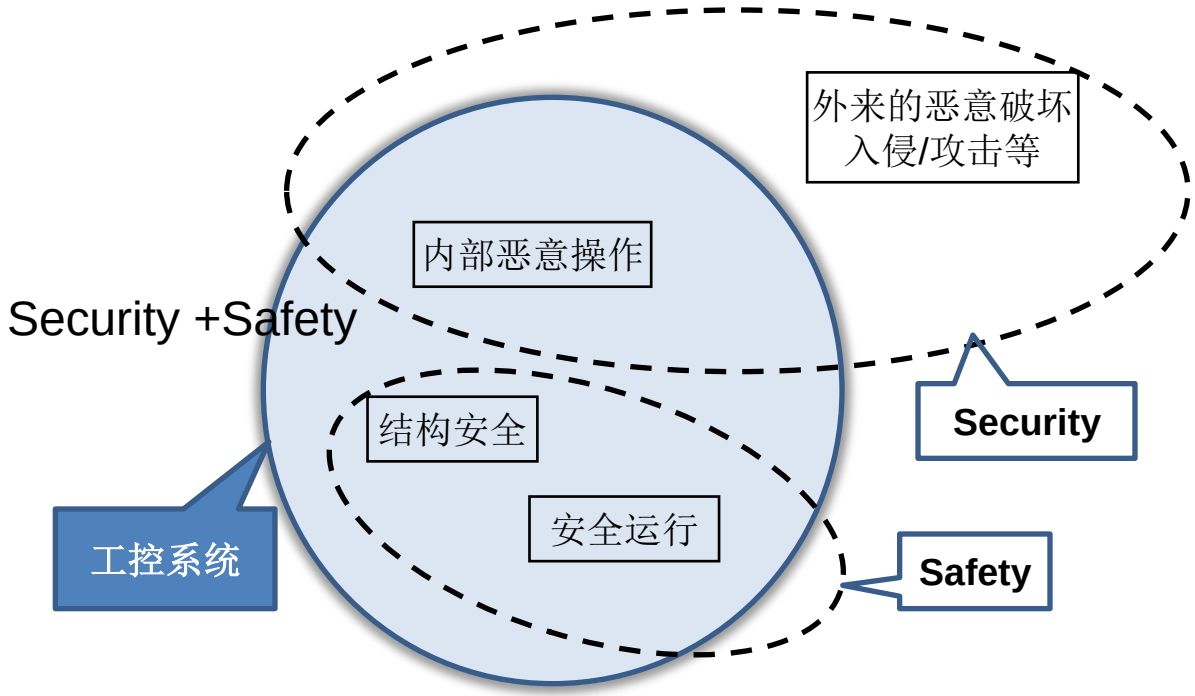
- 形势分析
- 产业发展方面
- 理论研究方面
- 技术产品方面
- 监管与服务方面
- 行动建议

3、理论研究方面

工业控制系统安全问题根源是缺乏本质安全

工控系统安全问题的根源：在设计之初，由于资源受限，非面向互联网等原因，为保证实时性和可用性，系统各层普遍缺乏安全性设计。

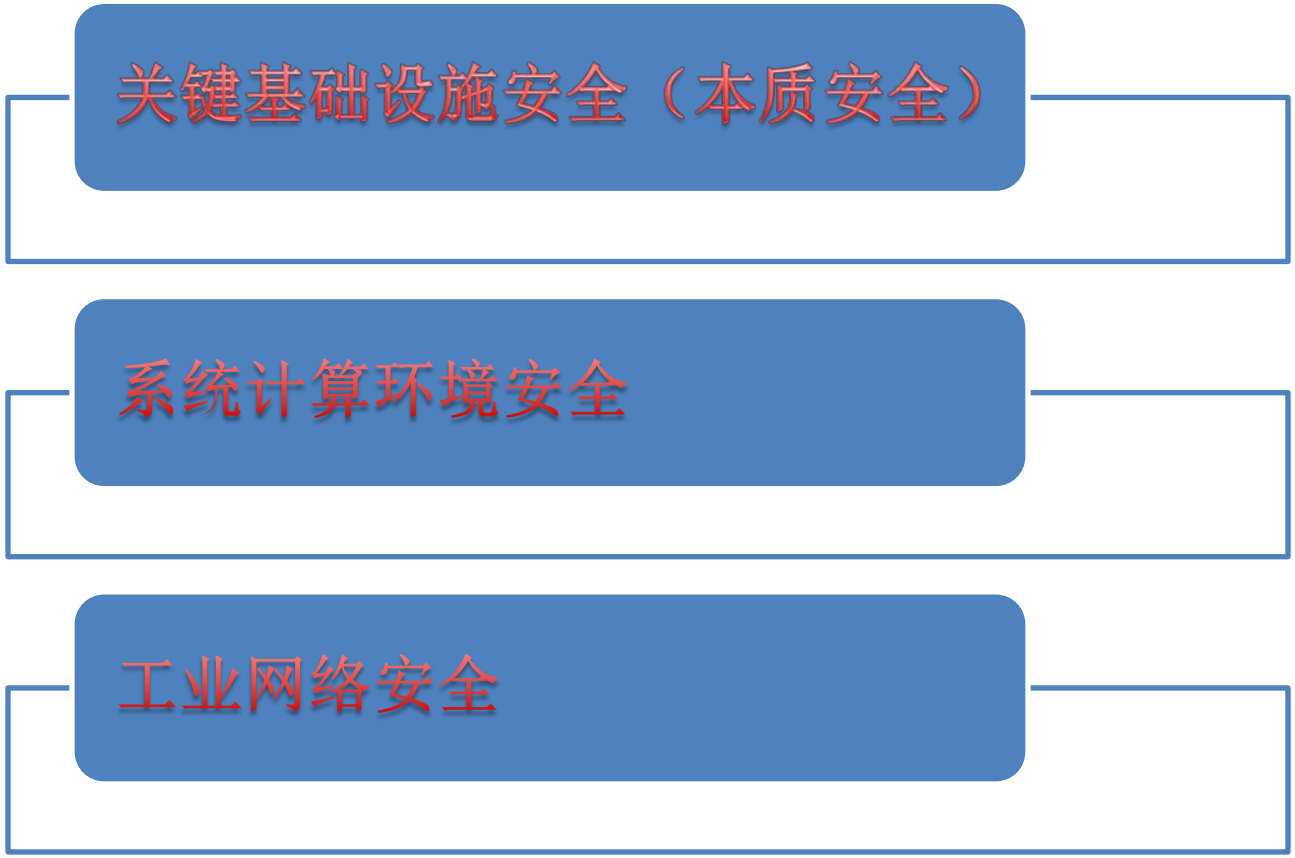
一方面，随着工控系统与信息系统的融合发展，信息系统的安全问题被带入到工控系统中，另一方面，系统规模逐渐增大、复杂性越来越高，系统错误越来越难以检测和避免。



缺乏本质安全的设计架构，系统安全隐患很难得到有效控制。

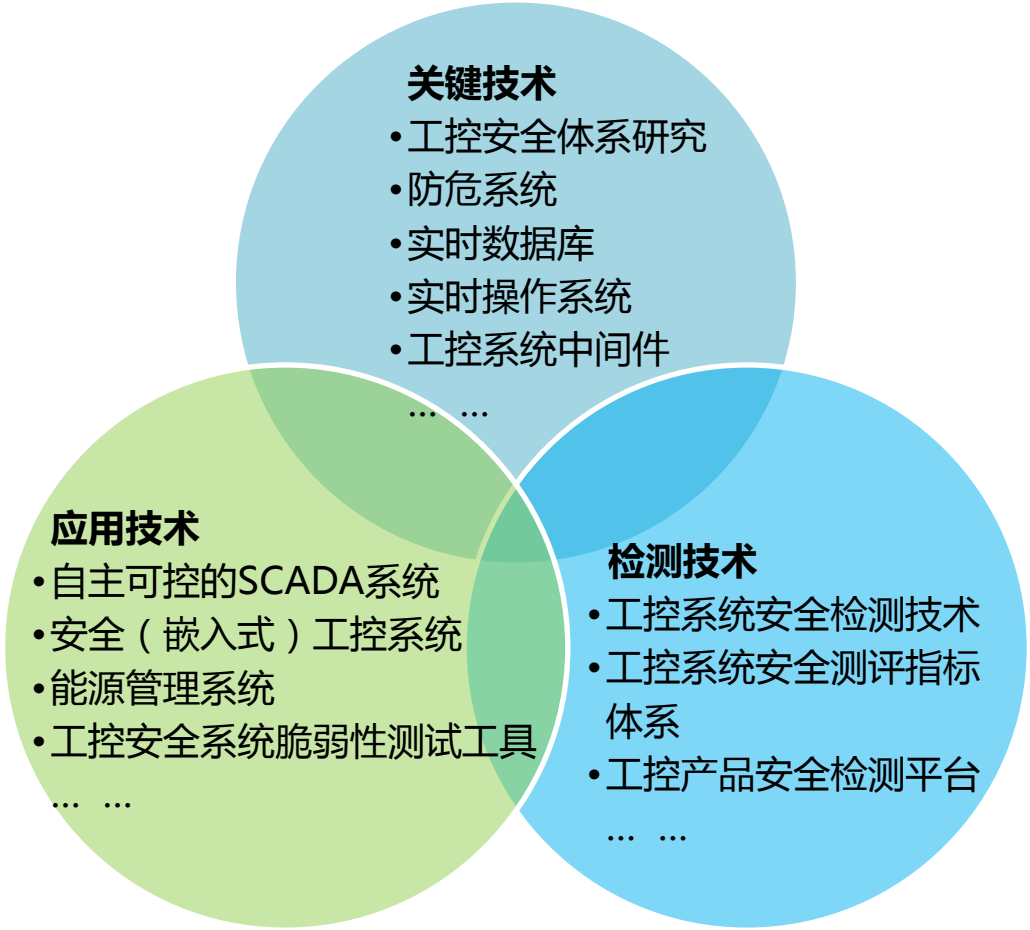
3、理论研究方面

工业控制系统安全涵盖的内容



3、理论研究方面

工业控制系统安全涉及的主要技术



3、理论研究方面

工控系统安全不仅仅是网络安全的问题，涉及自动化、通讯、信息安全、功能安全等多学科和技术。

目前：缺乏权威研究机构开展系统顶层设计，研究贯穿基础平台、通讯、应用软件等各层面的统一安全架构，解决安全性与可用性、实时性的矛盾，研究本质安全、保障工控系统在功能安全、物理安全、信息安全等方面的协调发展。

主要内容

- 形势分析
- 产业发展方面
- 理论研究方面
- 技术产品方面
- 监管与服务方面
- 行动建议

4、技术产品方面

尽管目前已有工控产品提供商开始对旧系统进行加固升级，研发新一代的安全工控产品，但是由于市场、技术、使用环境等方面的制约，工控产品生产商普遍缺乏主动进行安全加固的动力。

在缺乏安全架构顶层设计的情况下，技术研究无法形成有效的体系，产品形态目前多集中在网络安全防护的层面，工控系统自身的安全性能提升缺乏长远的规划。

4、技术产品方面

硬件平台

加强系统的安全性能，必然会占用更多的系统资源，影响系统的效率。采用硬件来完成安全功能，或许是解决工控系统实时性与安全性矛盾的有效手段。

CPU作为硬件基础平台的核心，技术掌握在国外厂商手中，“后门”漏洞的隐患始终存在，目前国内研究和生产CPU的品牌主要包括：龙芯、众志、多思等，在通用处理器、嵌入式处理器、专用处理器等方面都有了相应的产品。是否符合工控系统的性能要求和安全要求，能否在我国工控领域广泛应用，有待进一步的研究和验证。

在芯片中加入安全功能，研制安全处理器将大幅提升硬件平台的安全性。

4、技术产品方面

操作系统

系统级：普遍采用通用的商业操作系统；

设备级：实时操作系统

操作系统的安全隐患：

- 管理员一权独大
- 访问控制形同虚设
- 脆弱的登录认证方式
- 层出不穷的系统漏洞

4、技术产品方面

操作系统

现状：

- B1级以上的操作系统对中国禁运；目前主流的商业操作系统多为C2级；等级型的自主访问控制，超级管理员用户可对其他用户的客体资源直接做任意修改和访问，没有引入标记与强制访问控制。更没有相应的保障类要求。
- 现有安全产品的不足：无法改变操作系统的访问控制模型，可以直接对工控设备控制；无法应对具有针对性的恶意代码；无法保证操作系统的可信。

- 目前已有厂商在进行对操作系统进行安全加固方面的研究。
- 实时操作系统方面，国内厂商少有涉猎。

4、技术产品方面

实时数据库——工控系统核心数据源

- 需要解决实时性与安全性的矛盾；
- 系统管理员特权问题；
- 非法操作检查等。

目前主要的实时数据库产品

PI、InfoPlus、六所力数、安捷、浙大中控、紫金桥等

自主实时数据库系统提高实时性、充分利用硬件资源，解决安全性矛盾

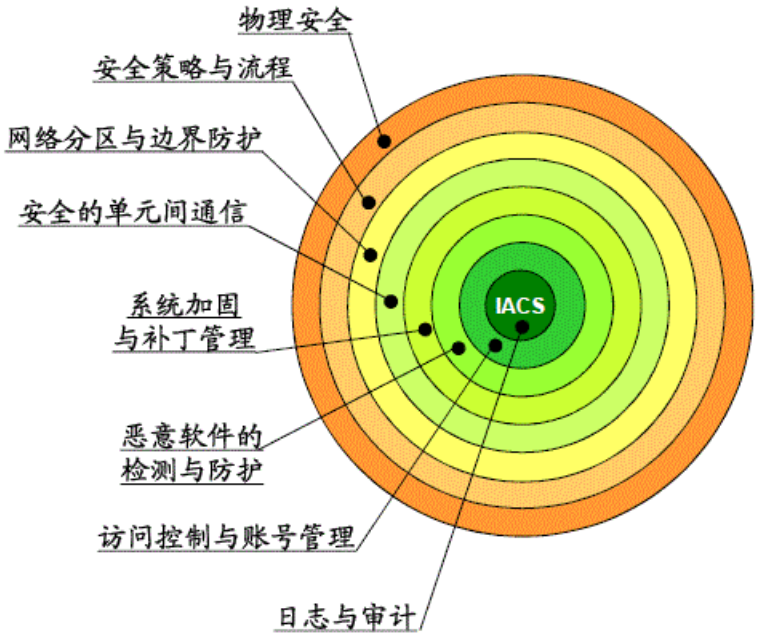
应用软件

随着系统功能越来越多，应用软件规模逐渐增大、复杂性越来越高，系统错误越来越难以检测和避免。提高软件系统安全，保证软件设计开发的正确性是亟待解决的问题。

4、技术产品方面

通讯网络

被业界广泛采纳的“纵深防御”理念



—— PROFINET Security - Risk Assessment & Security Solution,by Siemens Ltd. China

前提：系统本身目前无法达到本质安全的要求

方案：在外部世界的威胁和工控网络之间建立尽可能多层次的保护

4、技术产品方面

基于“纵深防御”理念，普遍的做法是将工业测控网络，按照功能和安全级别划分为不同的区域，加强不同区域间的边界防护。

典型应用：电力行业

电力行业是国内开展工控系统信息安全工作较早的行业：

2002年由原国家经贸委颁布了《电网和电厂计算机监控系统及调度数据网路安全防护的规定》

2004年由国家电力监管委员会颁布了《电力二次系统安全防护规定》

横向隔离+纵向认证（加密）：不同站点间单向隔离，调度指令加密认证。

4、技术产品方面

目前，多数工控系统信息安全防护产品提供商，主要集中在工业防火墙、工业网关、具有管理功能的交换机等方面开展技术和产品研究。

- 利用“白名单”机制防止非法访问；
- 细粒度的包检测防止对重要数据的非法篡改；
- 安全审计等。

其目的是：

- 尽可能阻断来自外部的攻击直达工控系统核心的通路；
- 尽可能杜绝病毒在不同区域内的传播，限制破坏的范围。

4、技术产品方面

总体来讲，安全技术和产品快速发展，在很多行业和领域得到应用和验证，但仍未形成完整的体系，工控系统的信息安全短板明显。

解决之道

必须突破利用传统信息安全手段进行外围防护的单一思路，将信息安全、工业控制、功能安全、电力电子、通讯等技术进行创新性的融合，从根本上解决系统本质安全问题。

面向在用工控系统的巨大存量市场，充分认清在短时期内国产工控系统难以完全取代进口产品的行业现状，从工控系统的关键环节入手，优先发展具有自有知识产权的安全保护技术和产品，解决在用工控系统本质安全问题。

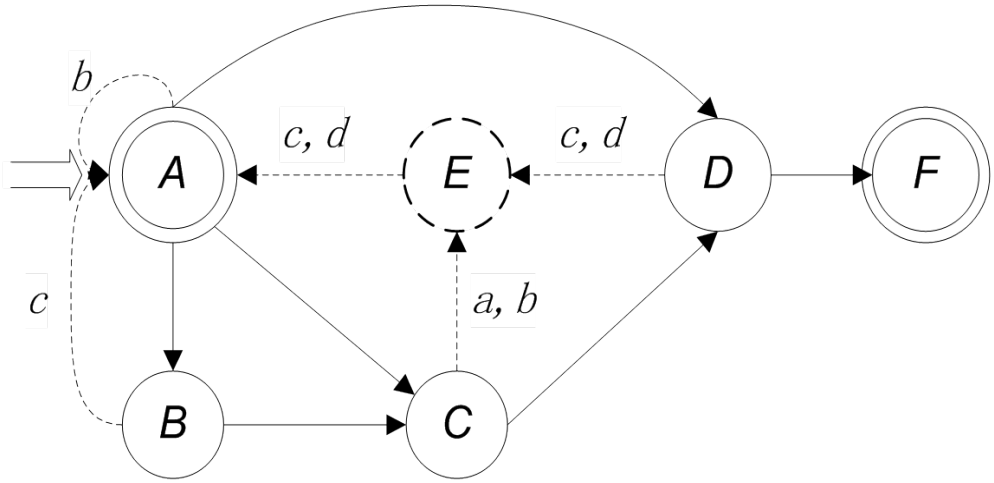
面向未来快速发展的增量市场，研究工控系统安全体系架构，解决在资源受限的条件下，工控系统缺乏安全性设计的先天缺陷，从根本上保证系统的本质安全。在完整的安全体系架构之上，研究新一代安全的工控系统，逐步实现对进口产品的替代，真正实现自主可控和安全可靠。

4、技术产品方面

防危机制与技术

无论安全威胁来自外部还是内部，保障与工控系统相连的重要装置、设备、基础设施不受破坏。

感知设备的安全状态，判断控制动作可能引起的状态变迁，防止危险状况的发生。



A：正常状态；*B*：警告状态；*C*：临界状态；
D：危险状态；*E*：防危保护态*F*：事故状态；

4、技术产品方面

防危机制与技术

- 主动防危

通过历史数据建立数据预测模型，实现对工业控制系统采集数据的预测，从而能够对工控系统的安全风险给出精确的预测，做到对危险的预警预报，防范于未然。

- 实时防危

利用预设的规则，通过高效的计算，进行实时现场异常检测，及时发现出现的异常操作和异常节点，做到对系统的实时现场异常检测。

- 全局防危

要根据现场环境、历史数据和经验，建立起系统网络模型。通过风险传递算法的运算，预测出某一个（或多个）设备出现风险后系统中所有相关设备受影响的情况。做到对系统的整体风险预测和整体防危。

- 自主防危

对系统各模块进行状态监控，在系统处于超负荷情况下，采取合理的措施，在确保系统稳定的前提下，通过优化配置，实现系统的升降级优化运行，确保系统自身的稳定安全。

主要内容

- 形势分析
- 产业发展方面
- 理论研究方面
- 技术产品方面
- 监管与服务方面
- 行动建议

5、监管与服务

尚无监测平台和监管机制

国家层面

行业层面

企业层面

出于成本的考虑和技术的考虑，工控系统产品提供商很少对自身产品的安全漏洞进行主动检测和公布。再加上缺少强有力的监管制度，厂商普遍缺乏行动的主动性。

缺乏具有必要检测技术和手段的第三方评测机构

安全标准远未完备

测试评估的理论研究、技术和工具研发有待提高

测试平台建立投入巨大

行业壁垒严重

主要内容

- 形势分析
- 产业发展方面
- 理论研究方面
- 技术产品方面
- 监管与服务方面
- 行动建议

6、行动建议

整合资源，建立联盟

工控系统信息安全隐患普遍存在于技术、设备、工程服务和运行管理当中，并不是单一学科、单一技术就能解决的问题，需要由政府主管部门主导，打破行业壁垒，开展深入合作，充分发挥大政府的优势，从顶层设计出发，带动相关行业、企业，进行思路上的深刻变革和高度的资源整合，才有可能实现工控安全研究的突破。

呼吁成立工控系统信息安全的联盟组织，包括基础硬件设计与制造、系统软件、工控系统生产商、网络安全产品提供商、相关理论与技术研究单位等。

6、行动建议

建立产品准入制度，设立第三方评测机构

呼吁国家立法，规范国外产品进入中国市场，对工控系统和产品提供商、系统集成商，推行安全性检测和认证准入制度，要求厂商进行系统安全风险评估，提供安全检测报告，主动发布安全漏洞，对软件升级和漏洞补丁要进行安全评估和验证，在供货合同中或以其他方式明确承担的信息安全责任和义务。

结合应用行业，搭建仿真测试验证平台，建立专业化安全保障队伍，提供第三方评测服务。针对相关应用工程信息及控制系统出现的安全问题，加强日常安全测评服务，帮助被测评单位准确地发现安全方面的问题、漏洞和薄弱环节，并为其提供切实可行的改进建议，对防护策略和防护措施进行有效验证，以达到整体防护的功效。

6、行动建议

开展行业试点，制定行动路线图

由政府部门主导，组织自动化行业、信息安全行业、工控系统应用领域的有关专家，成立专家指导工作小组，负责组织协调相关行业资源，指导起草相关行业标准和实施指南，指导制定行业工业控制系统安全工作行动路线图，确定目标和时间计划，切实推动和落实行动方案。

选择电网、石油石化、轨道交通等重点应用领域，尽快开展试点示范工作，确立风险评估制度、建立企业工控系统安全管理体系，细化信息安全应急预案，通过1-2年的积累经验，由点及面，分步实施，完善方案，争取在五年内，在重点应用领域初步实现关键工控系统的设计、安装、运行和维护等环节的信息安全基本可控目标。

6、行动建议

加强政策资金支持，鼓励自主技术和安全产品研发，推动产业发展

设立国家工控系统信息安全专项资金，集中有效资源，以自主可控、安全可靠为目标，支持开展工控系统核心关键技术和产品的研发；鼓励安全问题检测、安全防护技术和产品的研究；引导相关标准规范的制定及服务能力提升的研究。

在研发政策支持的基础上，国家有关部门要进一步对相关企业在财税政策、投融资政策、人才政策、知识产权以及市场政策等方面予以倾斜和支持，优化企业的发展环境，提高产业发展质量和水平，鼓励企业的快速发展。积极发挥行业协会、产业联盟的作用，建立相关企业的沟通和交流渠道，推动相关技术和产品的广泛应用。

CEC
中国电子

工业智能与仿真实验室、工业信息安全实验室

求实 进取 合作 创新

品牌 资源运营 商业模式

打造自动控制与系统工程领域国内领先
国际一流的创新型高科技集团

电子六所NCSE