过程工业工控安全技术

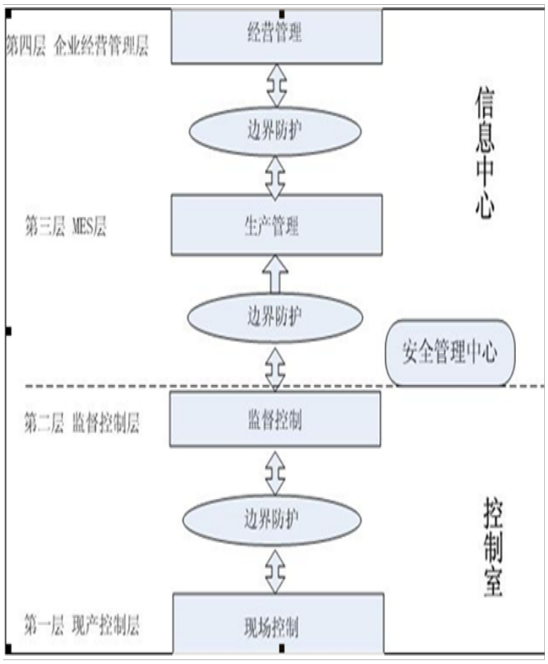
1 背景及意义

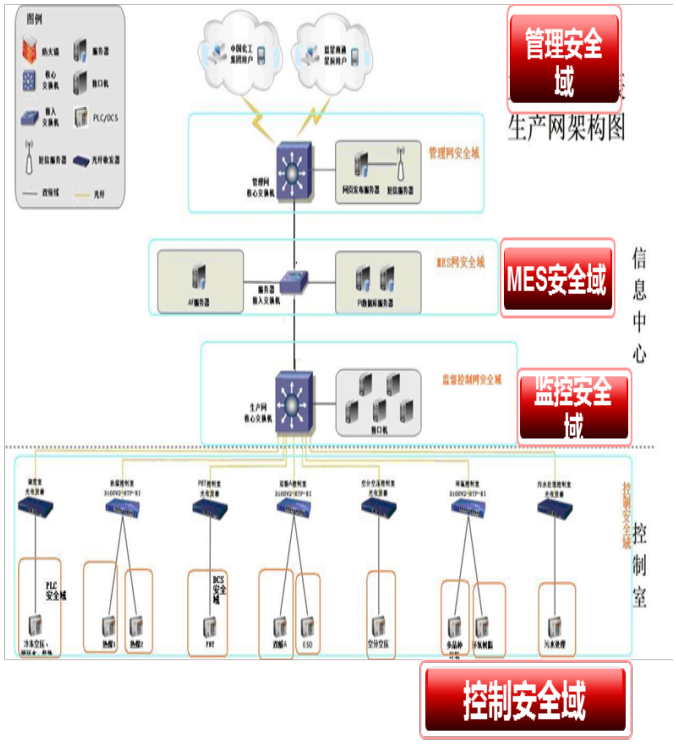
目前涉及国计民生的关键基础设施 80 以上%依靠工业控制系统来实现自动化作业，工业控制系统已经成为国家关键基础设施的重要组成部分，其安全关系到国家战略安全。一旦工业控制系统信息安全出现漏洞，将对工业生产运行和国家经济安全造成重大隐患。随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工业控制系统扩散，工业控制系统信息安全问题日益突出。从 2010 年发生的伊朗核电站“震网”病毒事件开始，到 2017 年乌克兰电网被攻击和 2019 年委内瑞拉国家电力系统大面积停电，无不充分反映出工业控制系统信息安全面临着严峻的形势。

工业控制系统一旦遭到攻击，从数据采集、数据传输到数据应用的各个环节都将带来严重后果，因此在国家将工业控制系统安全提升到国家网络空间战略高度层面后，急需开展工业控制系统安全防护研究，以保证工业大数据的数据资源可靠与工业控制系统控制策略（智能控制）的安全可信。

2 技术解决方案

以工业过程为研究对象，以工业过程控制亟待解决的网络安全问题为研究目标，突破工业过程控制网络中主机防护、APT 甄别与隔离、工控系统安全威胁预警与追溯等关键技术，解决工业控制系统信息安全问题。构建四个层次的信息安全防护体系：控制层（现场层）、监控层、MES 层、管理层（ERP）。将控制系统结构划分成不同区域，以有效建立“纵深防御”策略，通过大数据分析建模，动态感知系统安全态势，最大限度地保障工业控制系统安全稳定运行。





3 技术创新点

综合边界防护、访问控制、主机安全等技术手段，采用工业防火墙、安全网关、工控安全管理平台等软硬件构成工控系统安全防护架构；基于工业大数据的事件关联和态势分析技术，采用数据挖掘、数据融合等方法对不同来源的事件数据进行关联分析，识别当前控制系统的安全态势，保证工控系统安全。

（1）精细化过程控制系统漏洞扫描

针对漏洞扫描结果误报率较高的缺点，研制精细化漏洞扫描系统。精细化漏洞扫描技术在节点探测识别的基础上，分别在操作系统、网络服务软件、嵌入式设备三个层面进行细粒度的漏洞扫描。在每个层面上，采用不同的属性进行匹配，每个属性使用合理的匹配算法并赋予不同的权重进行相似度计算，从而使漏洞扫描结果的更加合理，并提高了准确率。

（2）自动化漏洞验证

自动化漏洞验证技术根据设备信息探测结果，启动漏洞验证协程进行并发漏洞验证，并将漏洞验证获取到的一些信息反馈到节点。在进行实际漏洞验证之前会根据用户参数配置，过滤出那些漏洞概率较低、对节点破坏较大的漏洞，有效提高了漏洞验证效率，降低了对目标节点的伤害。

（3）安全态势感知

集检测、预警、响应处置为一体的工业大数据安全分析平台，以全流量分析为核心，结合威胁情报、行为分析建模、UEBA、失陷主机检测、图关联分析、机器学习、大数据关联分析、可视化等技术，实现威胁可视化、攻击与可疑流量可视化等功能，可有效帮助工业控制系统在高级威胁入侵之后,损失发生之前及时发现威胁并提出处理对策。

4 推广应用

（1）国家工业信息安全发展研究中心--化工流程控制系统信息安全靶场建设

以典型的常减压化工生产流程为背景，以常用工业过程控制系统--DCS 系统和安全仪表系统 SIS 为对象，开展常减压化工流程仿真模型和工业控制系统信息安全仿真测试平台建设，提升现有化工流程工控信息安全系统防护水平，检验主流工业控制系统设备厂商的产品安全性能，验证工控系统信息安全产品安全防护能力，为国内工控系统和智能设备安全组网、攻防演练提供测试环境。

（2）国家发改委工控系统信息安全示范工程--南通星辰化工生产控制系统安全防护

根据南通星辰网络结构分为四个层次：生产管理层、MES 层、监控层、控制层（现场层）。参照 ANSI/ISA-99 、GB/17859、GB/T25070 等相关要求，将企业系统结构划分成不同的区域可以帮助企业有效地建立“纵深防御”策略。区域与区域之间利用安全产品进行策略控制，确保每个区域的相互独立性，实现风险的最小化和可控。

5 对接联系

联系人：赵国新（信息工程学院教授）

邮　箱：zhaoguoxin@bipt.edu.cn