《边缘计算安全白皮书》及相关技术研究(附 PPT)

物联网 工业安全产业联盟 2019-10-08

本文从编写目的、边缘计算 3.0 架构、边缘计算安全分析、边缘安全边界及需求特征、边缘安全框架、典型场景下的边缘安全案例等几个方面介绍白皮书的基本框架和思路。

2019 年 9 月 18 日，由工业控制系统信息安全产业联盟（以下简称工业安全产业联盟）、智能制造推进合作创新联盟、边缘计算产业联盟、上海市自动化学会智能自动化专业委员会、控制网（www.kongzhi.net）&《自动化博览》、中国国际工业博览会组委会、东浩兰生集团上海工业商务展览有限公司联合举办的"2019 第八届工业控制系统信息安全峰会暨 2019 第三届工业互联网系统解决方案高峰论坛"在上海举行，**边缘计算产业联盟安全工作组副主席、中国科学院沈阳自动化研究所研究员尚文利**现场分享了《<边缘计算安全白皮书>及相关技术研究》的报告。

报告中介绍了边缘计算产业联盟即将发布的《边缘计算安全白皮书》，**从白皮书编写目的、边缘计算 3.0 架构、边缘计算安全分析、边缘安全边界及需求特征、边缘安全框架、典型场景下的边缘安全案例等几个方面介绍白皮书的基本框架和思路**。最后，阐述了中国科学院沈阳自动化研究所在泛在电力物联网边缘计算方面的最新研究工作和进展。以下为 PPT 全文！

边缘计算产业联盟安全工作组副主席、中国科学院沈阳自动化研究所研究员尚文利

工业控制系统信息安全产业联盟

《边缘计算安全白皮书》及相关技术研究

汇报人：边缘计算产业联盟安全工作组副主席、
中国科学院沈阳自动化研究所研究员 尚文利

汇报日期：2019年9月18日

工业安全产业联盟

目录

Contents

工业控制系统信息安全产业联盟

工业安全产业联盟

2019年工作计划

《边缘安全白皮书1.0》编制组

编制单位：

中国科学院沈阳自动化研究所

北京奇安信科技有限公司、华为技术有限公司、北京神州绿盟信息安全科技股份有限公司、英特尔(中国)有限公司、国家工业信息安全发展研究中心、北京和利时系统工程有限公司、西安电子科技大学、盛科网络、华中科技大学、北京大学、中山大学、中国移动通信有限公司研究院、国网辽宁省电力有限公司电力科学研究院、南方电网科学研究院有限责任公司... ... ...。

边缘计算进入2.0

边缘计算是在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开放平台，就近提供边缘智能服务，满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。

——ECC边缘计算参考架构3.0

边缘计算1.0

概念定义

- **形式：**分布式开放平台
- **位置：**靠近网络边缘或数据源头
- **能力：**计算/存储/网络/应用
- **价值：**联结/实时/数据优化/智能/安全

边缘计算2.0

能力构建

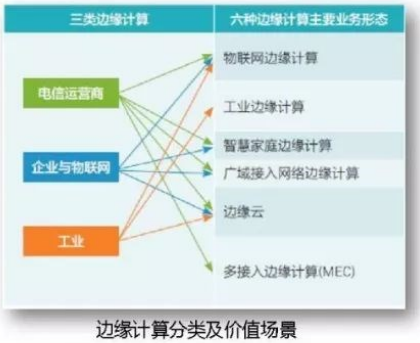
- **落地形态：**边缘云、云化网关
- **软件平台：**云原生架构与技术
- **硬件平台：**异构计算
- **核心能力：**边云协同/边缘智能

边云协同白皮书引领产业方向

边云协同的能力与内涵，涉及IaaS、PaaS、SaaS各层面的全面协同。EC-IaaS与云端IaaS应可实现对网络、虚拟化资源、安全等的资源协同；EC-PaaS与云端PaaS应可实现数据协同、智能协同、应用管理协同、业务管理协同；EC-SaaS与云端SaaS应可实现服务协同。

——2018边云协同白皮书

边云协同总体能力与内涵



边缘计算分类及价值场景

《边缘安全白皮书》编写项目背景

《边缘计算参考架构3.0》的延伸，进一步的支撑边缘计算产业的落地和发展，加速并保障边缘计算产业的发展。

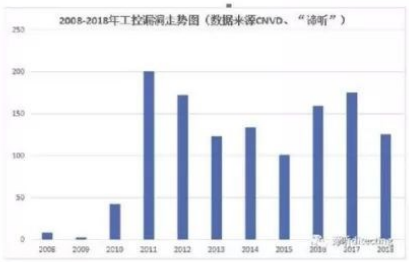
加速并保障边缘计算产业的发展

边缘计算面临的主要威胁和挑战	边缘计算网络架构下的安全内涵	指导典型价值场景下的安全措施部署
边缘安全挑战	边缘安全边界	边缘安全框架

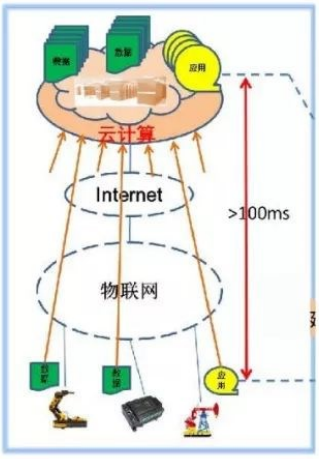
边缘安全的重要性和价值

- 国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见
- 工业和信息化部关于印发《工业控制系统信息安全行动计划（2018-2020年）》的通知
- 工业和信息化部发布了《关于加强工业互联网安全工作的指导意见》

网络安全形势日渐严峻

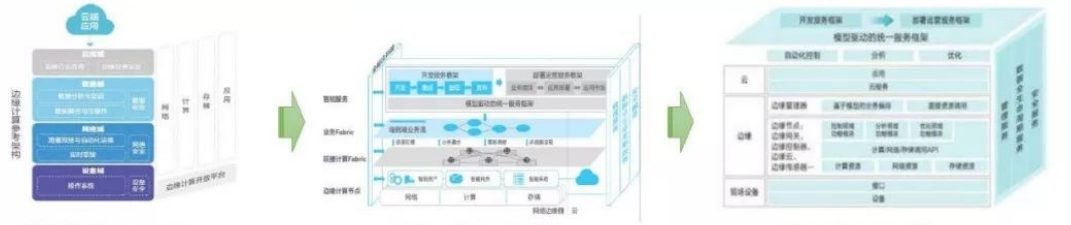


边缘安全的重要性和价值



- 端到端覆盖的安全防护
- 可信的网络及覆盖
- 设备的安全接入和协议转换
- 可靠的基础设施
- ...

边缘安全现状

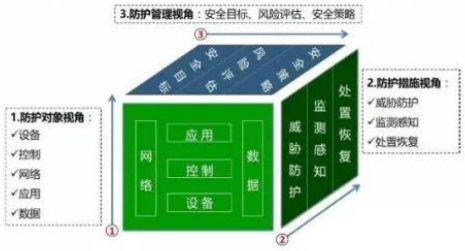


边缘计算参考架构1.0　　边缘计算参考架构2.0　　边缘计算参考架构3.0

安全服务　　安全服务　　安全服务

边缘安全现状

产业界在工业互联网边缘计算方面开展的研究



AII从防护对象、防护措施、防护管理三个视角构建工业互联网安全框架，从不同的视角指导企业开展工互联网安全防护工作。

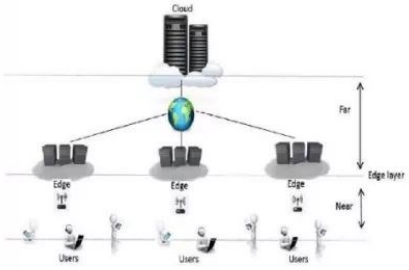
IIC安全参考架构从功能视角出发，为工业互联网端到端通信提供防护，安全模型和策略则作为整体统一的框架存在，进行统一调度。

边缘安全的现状

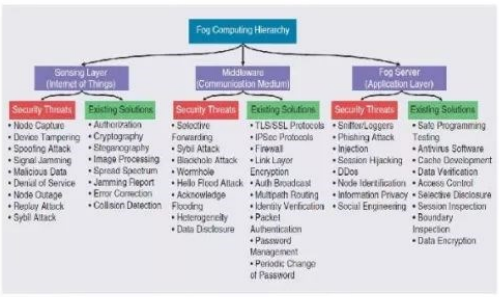
学术界在边缘安全方面开展的研究：

1）边缘计算面临的信息安全风险概述；

2）边缘计算平台与边缘设备/用户之间的互认证和通信安全性。



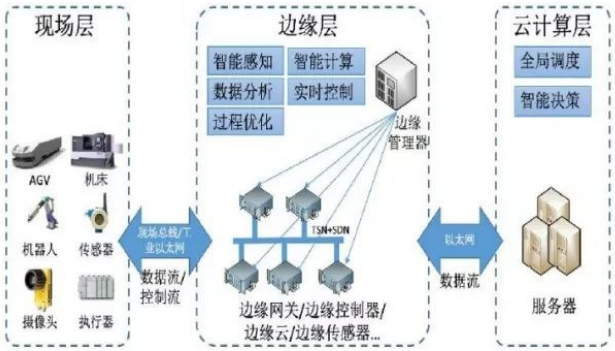
* Octopus: An Edge-Fog Mutual Authentication Scheme



缺乏典型价值场景下的完整边缘安全体系研究

边缘计算面临的风险

- 不安全的通信协议
- 边缘节点数据易被损毁
- 隐私数据保护不足
- 不安全的系统与组件
- 身份、凭证和访问管理不足
- 设备账号易被劫持
- 恶意的边缘节点
- 不安全的接口和API
- 易发起分布式拒绝服务
- 易蔓延APT攻击
- 难监管的恶意管理员
- 硬件安全支持不足



边缘计算部署视图

目录

Contents

工业控制系统信息安全产业联盟
工业安全产业联盟

边缘安全的挑战

节点海量与可扩展

边缘网络中设备数量大、物理连接条件和连接方式多样，相关安全服务需要突破可支持的最大接入规模限制，具有可扩展性

资源约束与边云协同

边缘节点本身的资源约束性，导致安全措施难以部署，脱离云中心将无法为这些设备提供全方位的安全防护

分布式与动态性

边缘计算具有多中心、分布式特点，脱离云中心的离线情况下，对边缘节点资源的需求和安全的需求也发生动态变化

实时性与弹性

边缘节点和现场设备均容易受到各种攻击，安全机制的增加必将对工业实时性造成影响

目录

Contents

工业控制系统信息安全产业联盟
工业安全产业联盟

边缘安全参考框架

5+1个层次　4个类别　3个场景　29个模块

完整性阐述的逻辑分别为：

基础设施安全：设备+硬件+虚拟化+OS

网络安全：纵深防御，从内到外

数据安全：传输-->存储-->使用

应用安全：开发-->上线-->运维

管理：安全生命周期

边云协同：事前，事中，事后

目录

Contents

边缘安全关键技术

■ **设备的可信安全防护**

针对工业边缘计算设备研究安全协处理技术，保证设备的启动和运行过程安全可信。

■ **边缘平台安全隔离**

根据边缘侧业务传输需求，结合虚拟化隔离技术，实现多业务安全隔离，支持边缘侧业务的可信敏捷接入与多级安全隔离。

■ **网络行为的深度访问控制与实时异常检测**

依据工业网络通信的内容和特性，实现工业通信的深度访问控制，通过设计最优化的边缘网络异常检测引擎，实现高精度的异常检测。

■ **轻量级的应用统一接入认证**

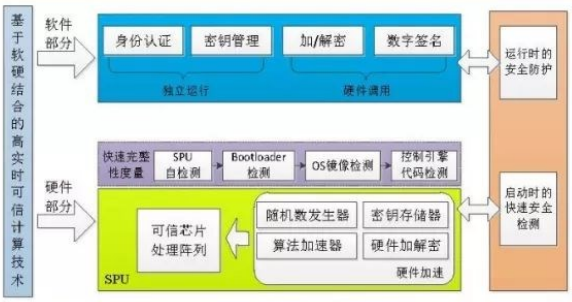
研究工控设备轻量级的接入认证算法，实现异构设备的安全接入和统一管理。

边缘安全关键技术

➢设备的可信安全防护

基于软/硬结合的高实时可信计算技术，安全协处理可以与边缘计算设备并行操作，保障节点安全

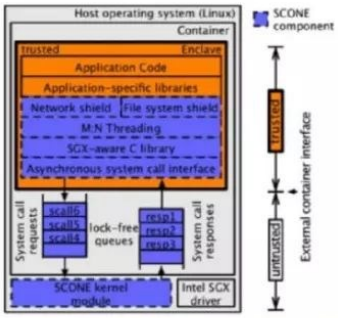
- **在设备启动阶段度量设备各阶段执行的任务，使设备最终的运行状态达到预期的预测效果。**
- **在设备运行阶段，仅检查设备的运行状态，同时对传输的数据提供机密保护。**

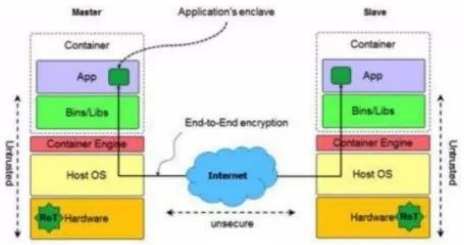


ICSISIA 工业控制系统信息安全产业联盟
工业安全产业联盟

➢边缘计算平台安全隔离

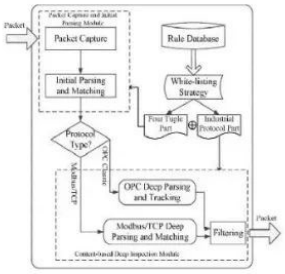
边缘节点通常采用虚拟化技术实现异构硬件上应用程序的隔离，即将应用程序运行在不同的虚拟机中来实现隔离。由于同一host上的多个容器共享host内核，因此容易导致如容器逃逸漏洞等危害。



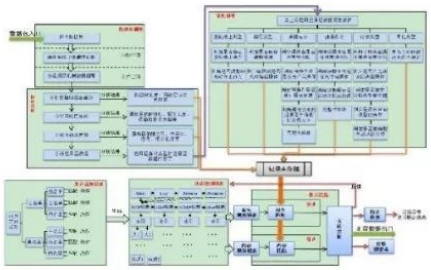


➢边缘网络访问控制与实时异常检测

采用深度包解析技术，对接入边缘网关的通信协议进行细粒度的内容分析，基于“白名单”策略进行过滤，保障网络边缘的信息安全。



白名单的纵深防御

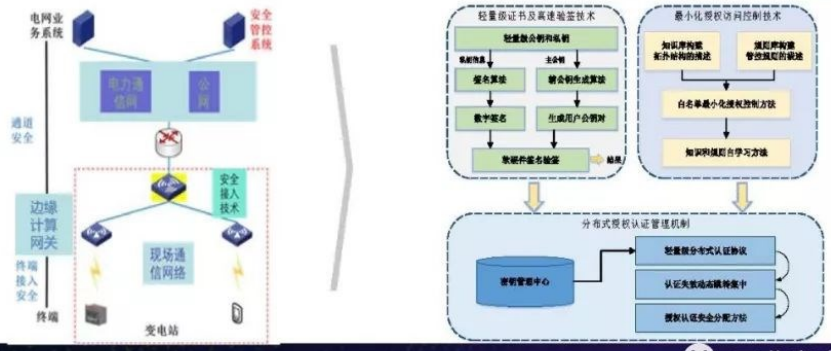


细粒度的内容解析

边缘安全关键技术

➢边缘计算轻量级身份认证及管理机制

针对泛在业务的安全接入认证需求，利用“轻量级证书+白名单”解决接入过程面临的窃听、匿名攻击、接入点伪装、中间人攻击、终端违规接入、重放攻击等网络攻击问题。



融合·协作·共赢

共同把握边缘计算的历史机遇

感谢聆听！

联盟名称：边缘计算产业联盟

联盟网址：http://www.ecconsortium.org/