ISC 2019 第七届互联网安全大会

物联网安全建设思路分享

赵明明

国网信通产业集团国网思极 副总经理

小鹅助理

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费

门票

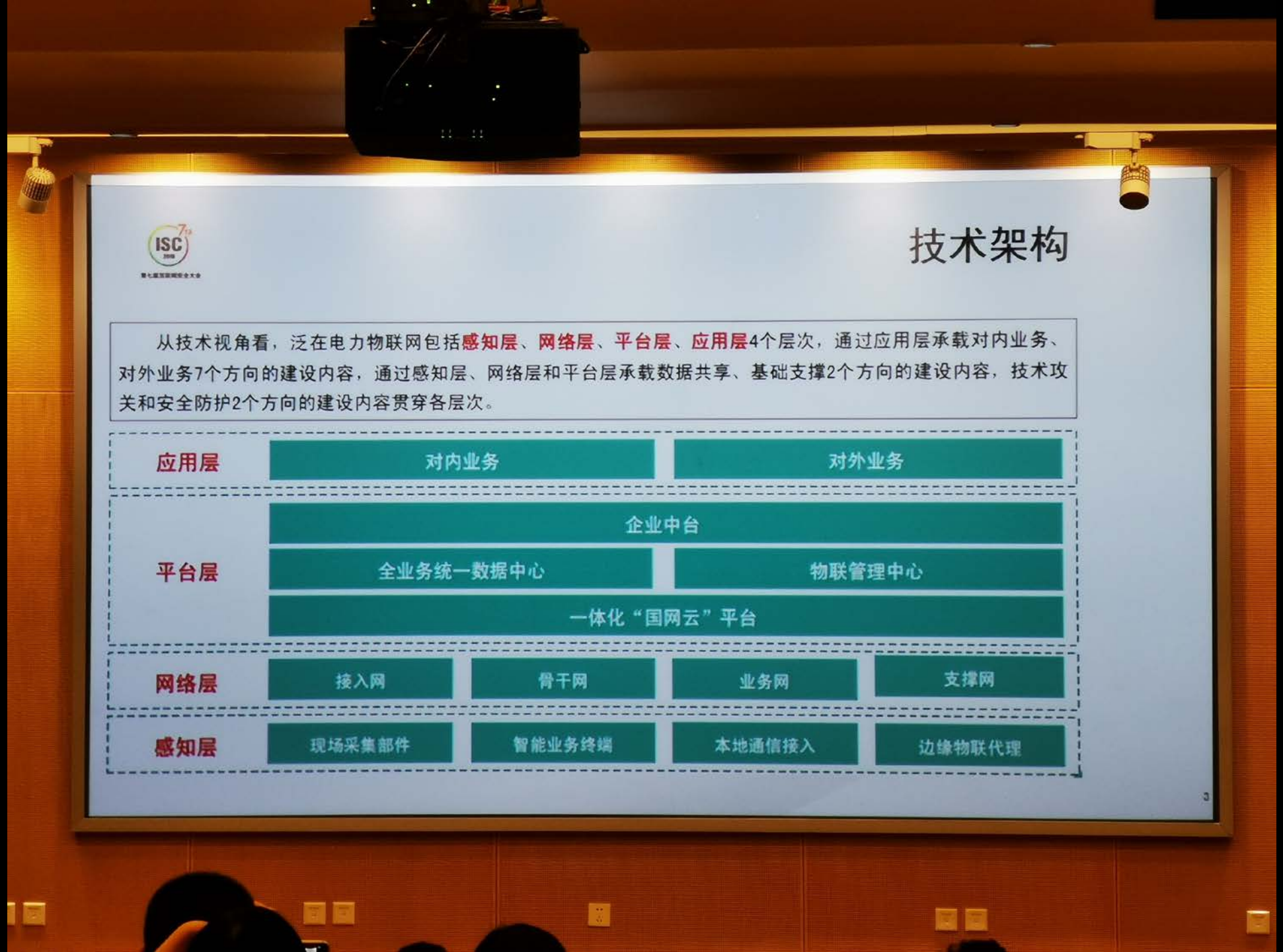

ISC
赵明明
国网信产集团国网网安公司
资深安全专家


物联网安全建设思路分享
国网网安公司—赵明明

泛在电力物联网

泛在物联是指任何时间、任何地点、任何人、任何物之间的信息连接和交互。**泛在电力物联网**是泛在物联网在电力行业的**具体表现形式和应用落地**；不仅是技术的变革，更是管理**思维**的提升和管理**理念**的创新，对内重点是**质效提升**，对外重点是**融通发展**。

泛在电力物联网将电力用户及其设备，电网企业及其设备，发电企业及其设备，供应商及其设备，以及人和物连接起来，**产生共享数据**，为用户、电网、发电、供应商和政府社会服务；以电网为枢纽，发挥平台和共享作用，为全行业和更多市场主体发展创造更大机遇，**提供价值服务**。


技术架构
从技术视角看，泛在电力物联网包括感知层、网络层、平台层、应用层4个层次，通过应用层承载对内业务、对外业务7个方向的建设内容，通过感知层、网络层和平台层承载数据共享、基础支撑2个方向的建设内容，技术攻关和安全防护2个方向的建设内容贯穿各层次。
应用层
对内业务
对外业务
平台层
企业中台
全业务统一数据中心
物联管理中心
一体化“国网云”平台
网络层
接入网
骨干网
业务网
支撑网
感知层
现场采集部件
智能业务终端
本地通信接入
边缘物联代理

基础研究

按泛在电力物联网的技术架构，主要从感知层、网络层、平台层和应用层四个方面分析物联网的新型风险。其中，感知层各类设备是风险主要来源；网络、平台和应用层面对新兴业务和外部用户的新风险也逐渐呈现。

分析维度		风险类别	典型事件	
感知	智能终端 弱资源终端	• 破解复制 • 不合规接入 • 跳板攻击 • 终端控制 • 恶意行为 • 能量攻击 • 声光电干扰 • 仿冒接入 • 固件篡改		2018年8月，美国普林斯顿大学发现通过操控大量高功耗智能家电可造成电力设施损坏。
网络	内外边界与第三方边界 网络通道	• 网络不可用 • 新技术安全 • 通道盗用 • 越权接入 • 网络边界模糊 • 云内网络风险		2016年9月13日晚，美国DNS服务商被摄像头等物联网设备组成的僵尸网络进行DDoS攻击，导致东海岸大面积断网，主要公共服务、社交平台、民众网络服务瘫痪。
平台	物联网管控平台 云平台	• 平台不可服务 • 身份仿冒 • 系统安全漏洞 • 数据篡改 • 错误注入 • 云内蔓延 • 数据泄露		2018年10月，亚马逊物联网平台底层操作系统FreeRTOS及连接模块被爆出13个安全漏洞，可被用于获得设备控制权，攻击关键基础设施。
应用	传统业务应用 新兴业务应用	• 非授权访问 • 漏洞利用 • 应用破解 • 政策适应（隐私、金融） • 数据泄露 • 应用不可用		2017年2月，智能物联网应用CloudPets的用户数据被泄露，暴露了200多万条儿童与父母的录音，以及超过 80 万个帐户的电子邮件地址和密码。。

挑战

经过十余年发展，公司已建成两级部署十大应用系统，全面覆盖企业运营、电网运行和客户服务等业务领域及各层级应用，成为日常生产、经营、管理不可或缺的重要手段。公司物联网应用已具有一定基础，接入智能电表等各类终端**5.4亿台（套）**，采集数据日增量超过**60TB**。

客户服务

覆盖全国约**4.71亿**客户的用电信息实现在线采集；通过门户网站、掌上电力、95598等渠道实现办电、购电业务线上管理；“**网上国网**”试点运行，线上缴费率超过50%。

企业运营

建成**ERP**和**人财物**、**规划计划**、**基建管理**等系统，支撑公司企业运营高效、集中、集约管理；所有省公司完成**实物ID**系统部署实施，支撑资产全寿命周期管理。

电网运行

建设**配电自动化**和**设备精益管理系统**，336家地市**供电服务指挥中心**全部建成，支撑主配网设备精益化管理；建成支撑**中长期电力交易**的技术支撑平台，开展电力直接交易。

新兴业务

车联网接入充电桩超过28万个，提供电动汽车销售、充电、支付等一站式服务；**电商平台**注册用户2.25亿，交易额超5000亿元。**综合能源服务**实现收入49亿元。

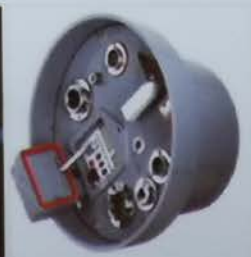
挑战

场景	人次	种类	品牌	型号	协议
16	600	24	181	256	20

某一个省公司物联网业务和终端现状调研情况








泛在电力物联网的本质安全

终端类型多样、业务场景复杂对电力物联网安全管控提出更高要求。

序号	类别	终端名称	品牌数量	操作系统	通讯协议
1	采集类终端	输电状态监测终端	7	嵌入式Linux操作系统、无	Modbus/ZIGBEE/MMS/IEC104
2		变电状态监测终端	9	Linux、无	Modbus/ZIGBEE/MMS/IEC104
3		电压监测仪	4	无	TCP
4		用电信息采集终端	48	嵌入式linux操作系统/WinXP	DL/T645、376.1、TCP/IP
5		计量周转柜	6	Windows	SOAP
6		视频终端	9	Linux、嵌入式操作系统	TCP/IP标准协、H.264、H.263、H.323
7		GIS采集终端	4	安卓、wince	Modbus
8		物联网安全出入控制终端	1	Arm- Linux	TCP/IP
9	作业类终端	生产移动作业终端	3	安卓、win10	TCP/IP、Modbus
10		物资现场作业终端	2	windows mobile/XP/10	TCP/IP
11		营销现场作业终端	15	无/安卓、winXP/7	TCP/IP、USB、串口
12		收费POS机	5	无/Linux	TCP/IP、串口
13		ATM自动缴费机	6	Linux安全操作系统、winXP/2000	TCP/IP
14		电动汽车充电桩	7	嵌入式linux、win	TCP/IP
15	办公类终端	PC终端、云桌面终端	55	WinXP/7/8/10	TCP/IP、RAP、PCoIP等
16		打印机、IP电话、考勤机、传真机、门禁等		无、Linux、嵌入式Linux	TCP/IP、串口等

嵌入式终端操作系统安全缺陷

传统操作系统及嵌入式操作系统

- ✓ 脆弱的访问控制
- ✓ 特权用户
- ✓ 对系统指令的合法性、合规性无法作出判断
- ✓ 节点欺骗
- ✓ 非授权读取终端信息
- ✓ 拒绝工作
- ✓ 恶意代码攻击
- ✓ 隐私泄露


ISC
安全免疫技术目标


ISC
对抗零日攻击
操作系统无法
被控制
无法执行
有害程序
违规指令
避免造成
大范围的故障
有效保障
电力物联网
安全
安全免疫技术目标

病毒免疫

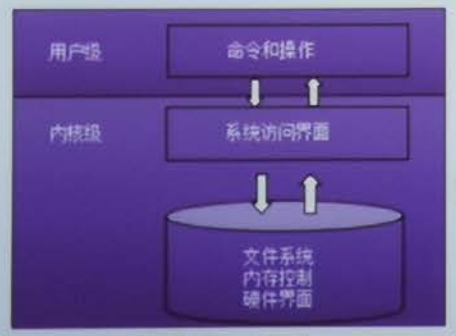
不依赖特征方式来查杀病毒，采用基于区块链的白名单ACL，使系统仅能运行经认证过的可靠应用，无法运行病毒。

对抗零日攻击

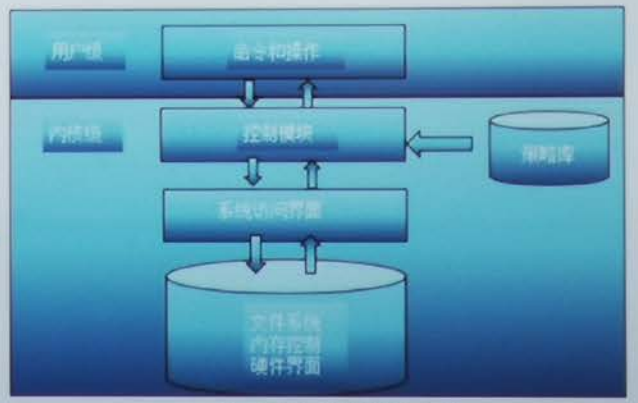
不依赖补丁，采用三权分立模式，采用强制访问控制模型，使得root权限也无法绕过验证。

创新模式：将访问控制列表，以区块链的方式进行维护。去中心化，且不能被恶意篡改。

实现思路

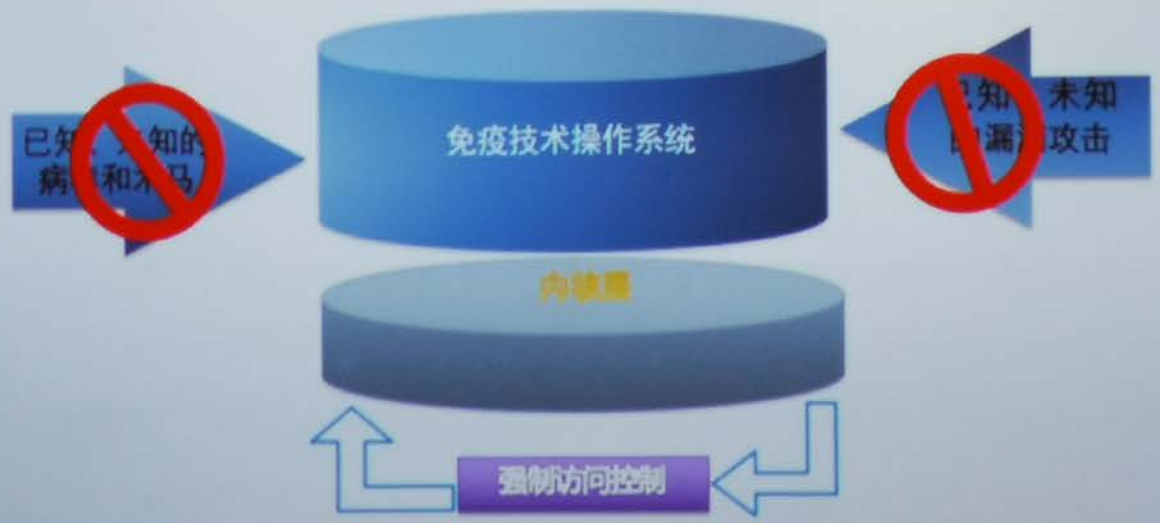


普通操作系统



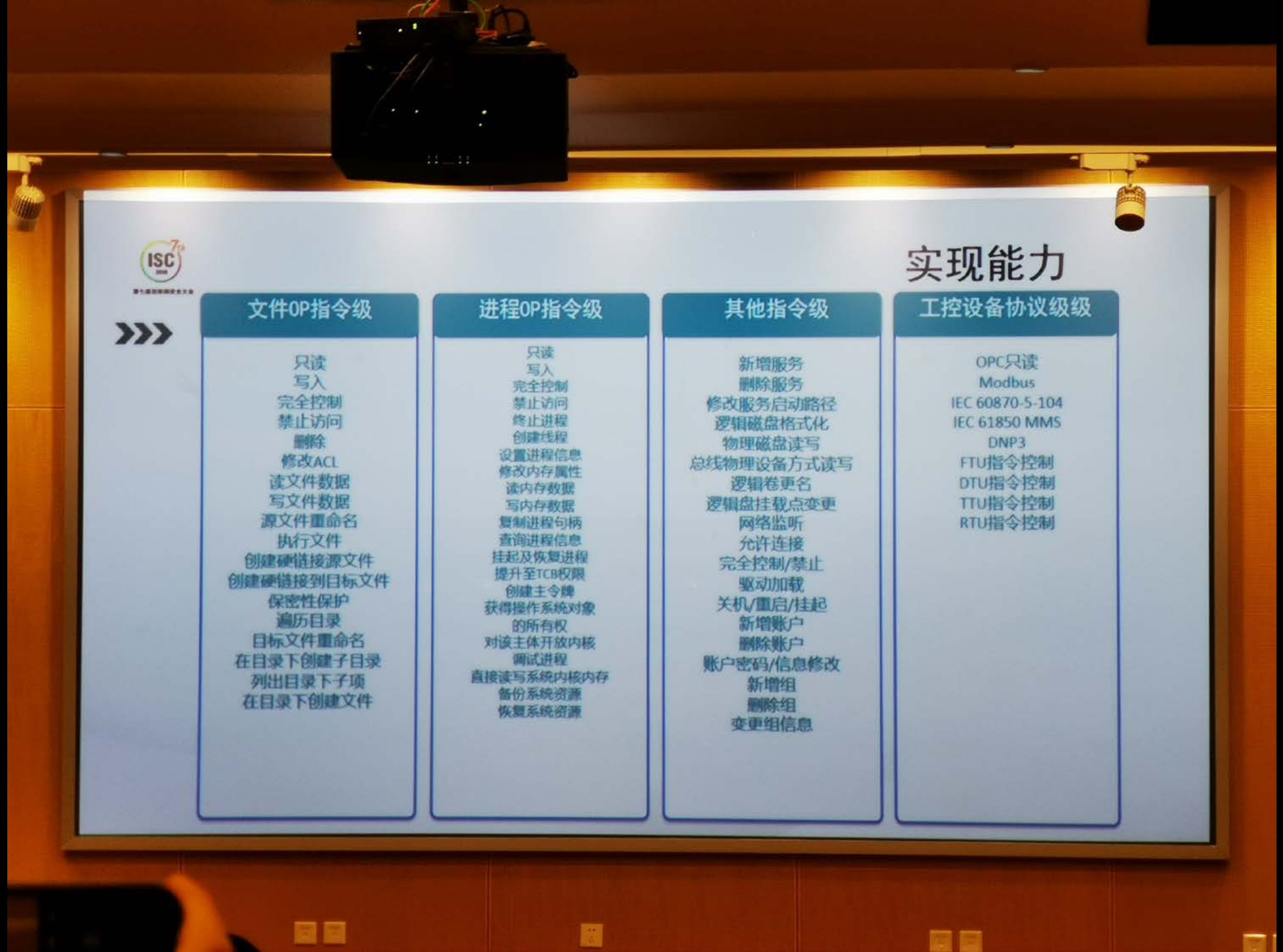
免疫技术操作系统

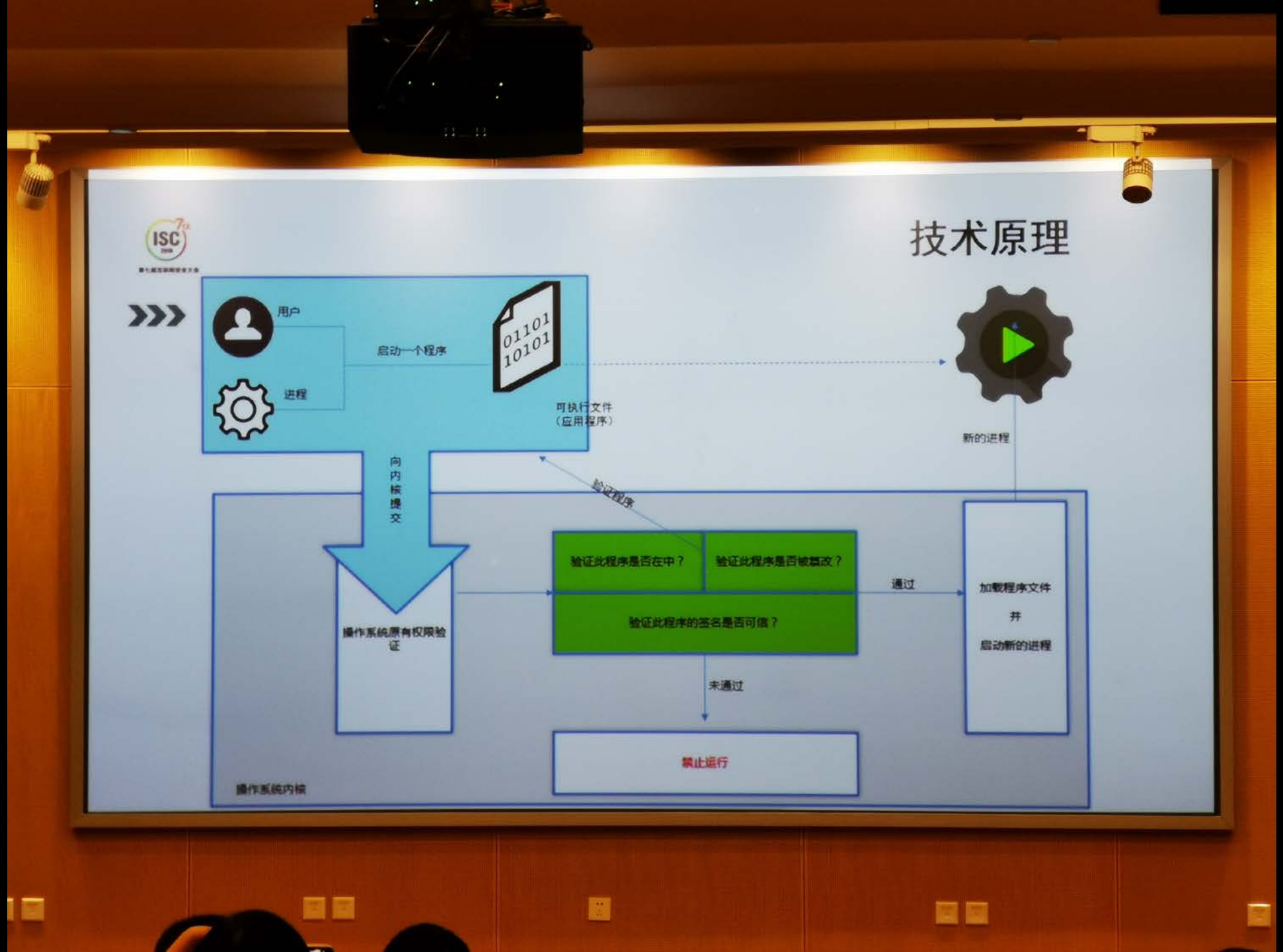
技术原理

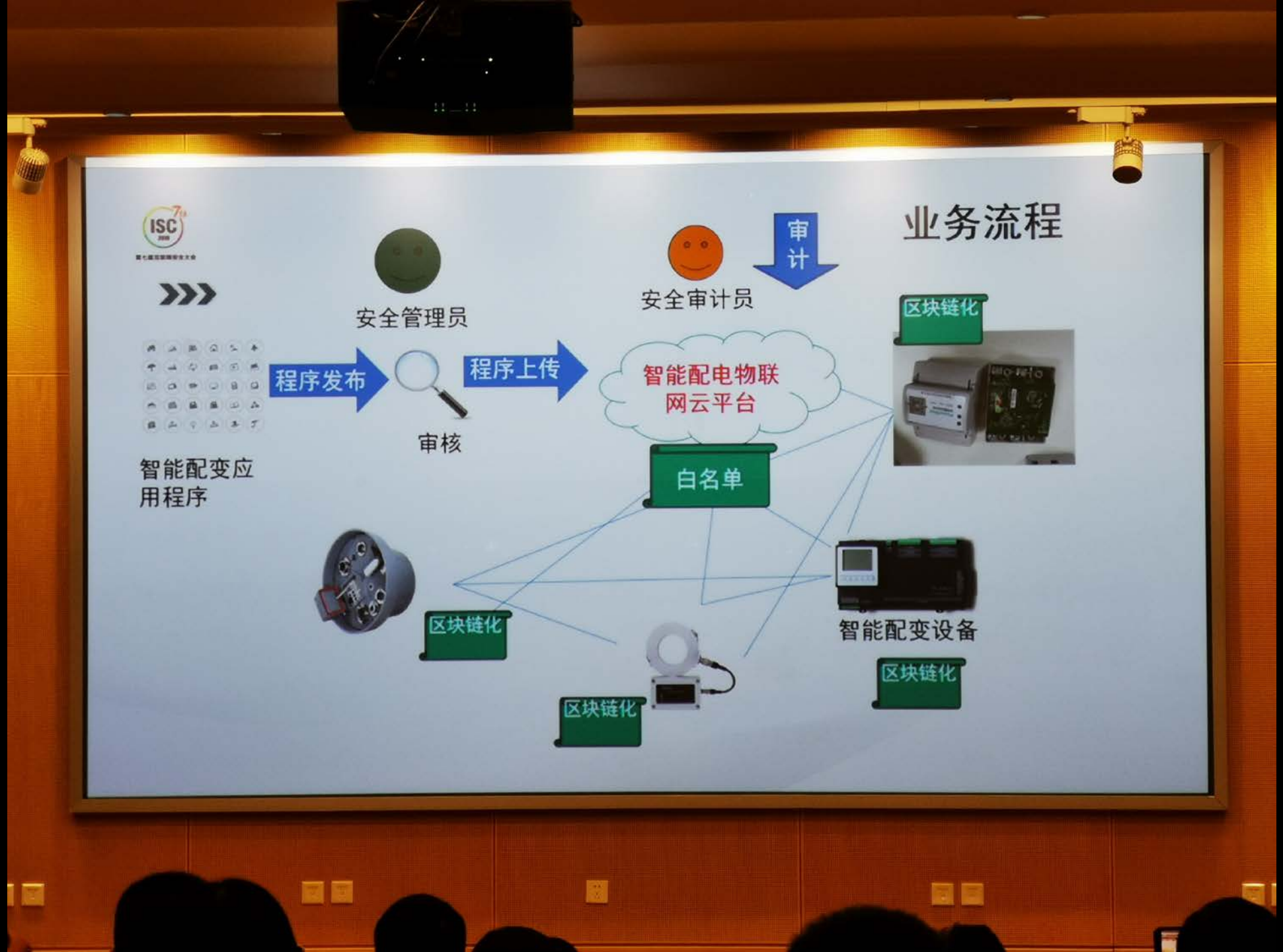


不去识别攻击的方法，细粒度的规则对任何不匹配的动作拒绝。


技术原理
主体
账户
进程
IP
免疫内核
OP指令级
应用传输指令固化
工控传感器指令固化
网络指令固化
客体
文件
进程
服务
磁盘
设备
网络


实现能力
文件OP指令级
只读
写入
完全控制
禁止访问
删除
修改ACL
读文件数据
写文件数据
源文件重命名
执行文件
创建硬链接源文件
创建硬链接到目标文件
保密性保护
遍历目录
目标文件重命名
在目录下创建子目录
列出目录下子项
在目录下创建文件
进程OP指令级
只读
写入
完全控制
禁止访问
终止进程
创建线程
设置进程信息
修改内存属性
读内存数据
写内存数据
复制进程句柄
查询进程信息
挂起及恢复进程
提升至TCB权限
创建主令牌
获得操作系统对象的所有权
对该主体开放内核调试进程
直接读写系统内核内存
备份系统资源
恢复系统资源
其他指令级
新增服务
删除服务
修改服务启动路径
逻辑磁盘格式化
物理磁盘读写
总线物理设备方式读写
逻辑卷更名
逻辑盘挂载点变更
网络监听
允许连接
完全控制/禁止
驱动加载
关机/重启/挂起
新增账户
删除账户
账户密码/信息修改
新增组
删除组
变更组信息
工控设备协议级级
OPC只读
Modbus
IEC 60870-5-104
IEC 61850 MMS
DNP3
FTU指令控制
DTU指令控制
TTU指令控制
RTU指令控制


ISC
技术原理
用户
进程
启动一个程序
01101
10101
可执行文件
（应用程序）
新的进程
向内核提交
验证程序
操作系统原有权限验证
验证此程序是否在中？
验证此程序是否被篡改？
验证此程序的签名是否可信？
通过
加载程序文件
并
启动新的进程
未通过
禁止运行
操作系统内核


业务流程
安全管理员
安全审计员
审计
智能配变应用程序
程序发布
审核
程序上传
智能配电物联网云平台
区块链化
白名单
区块链化
区块链化
智能配变设备
区块链化


ISC
国网网安·国泰民安

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票