ISC 2019 第七届互联网安全大会

工业企业侧安全事件溯源技术与运营框架

龚亮华

烽台科技总经理

小鹅助理

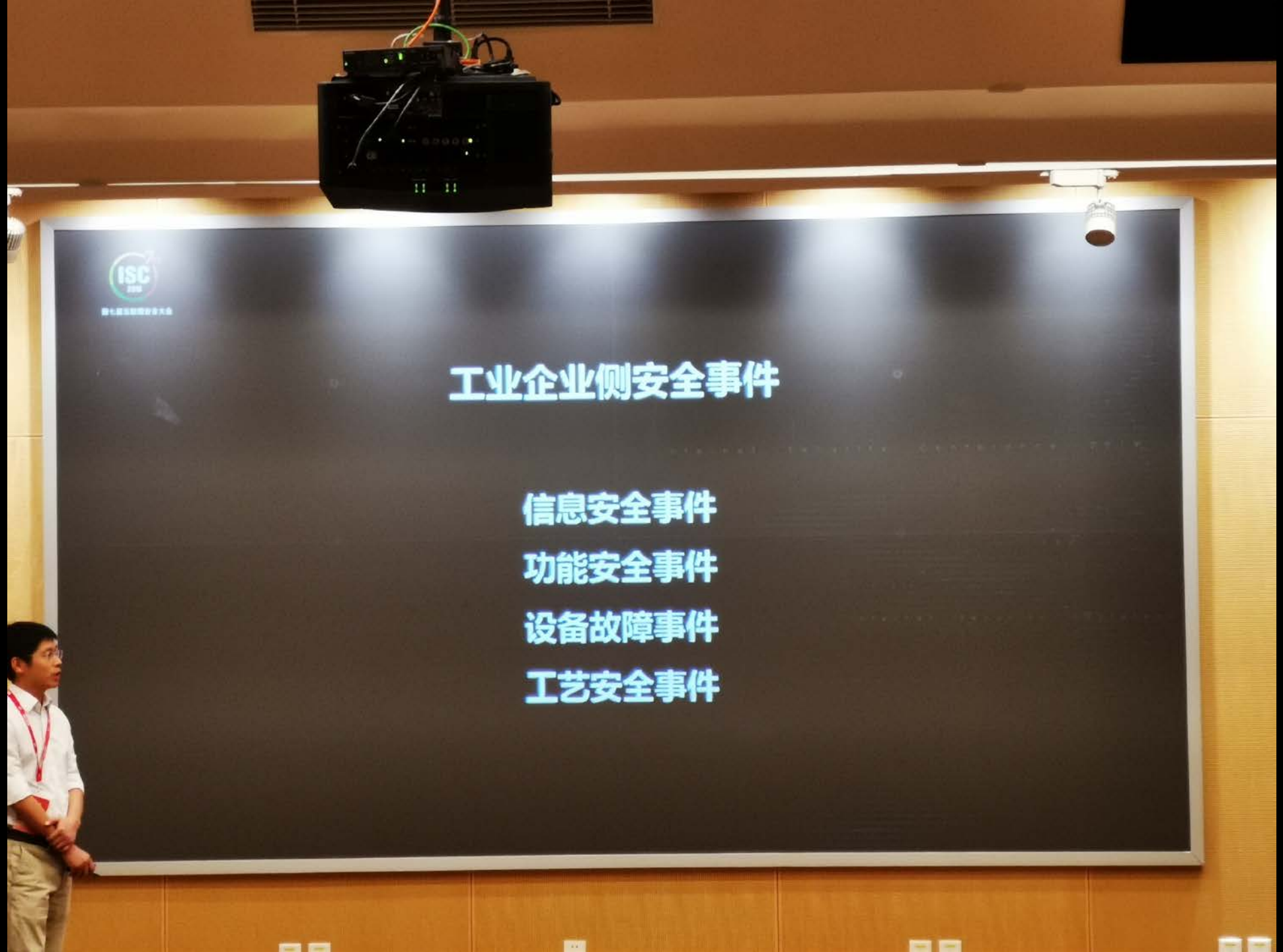
扫码添加小鹅助理，与数万科技圈人士

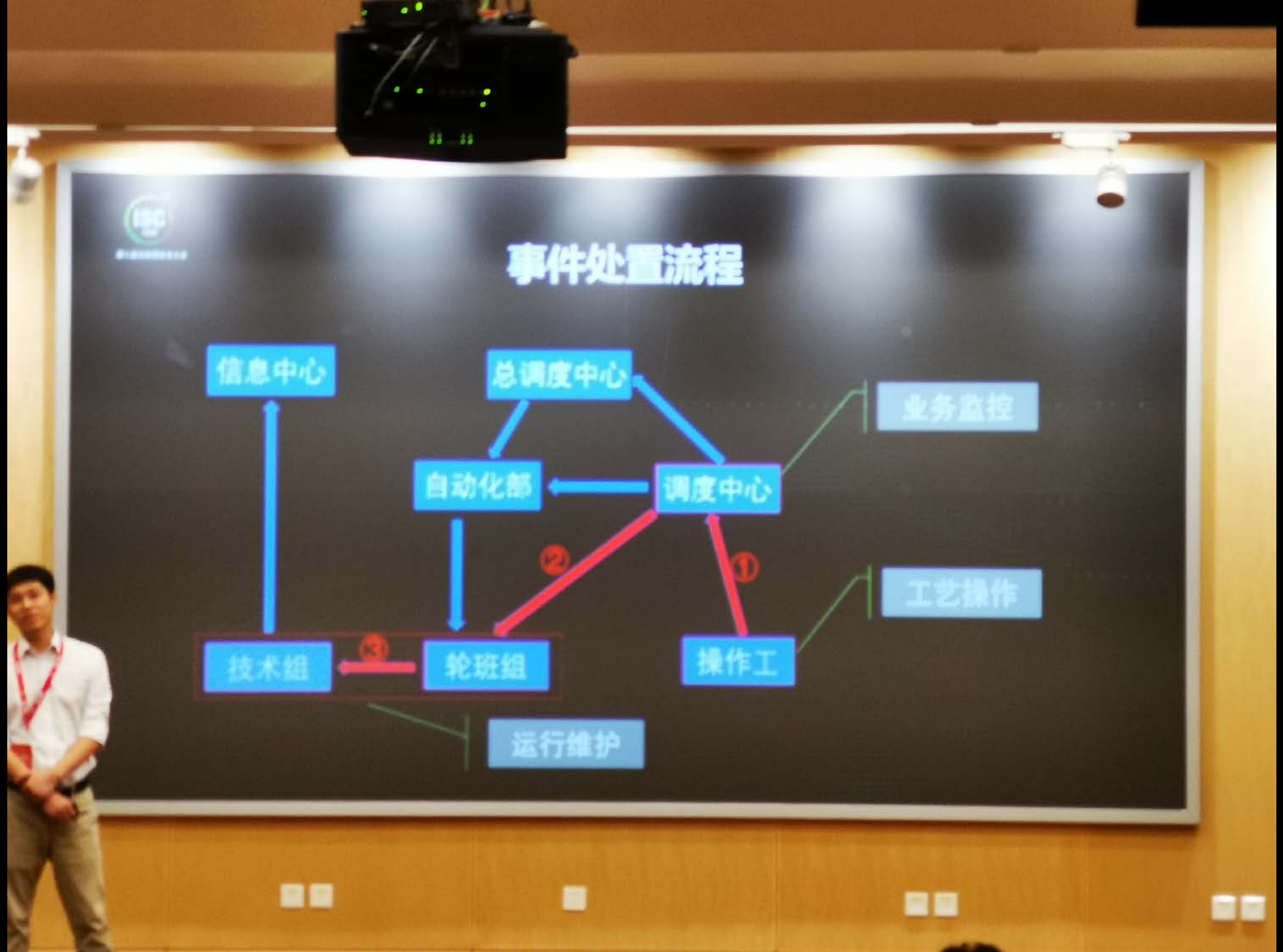
分享重量级活动PPT、干货培训课程、高端会议免费

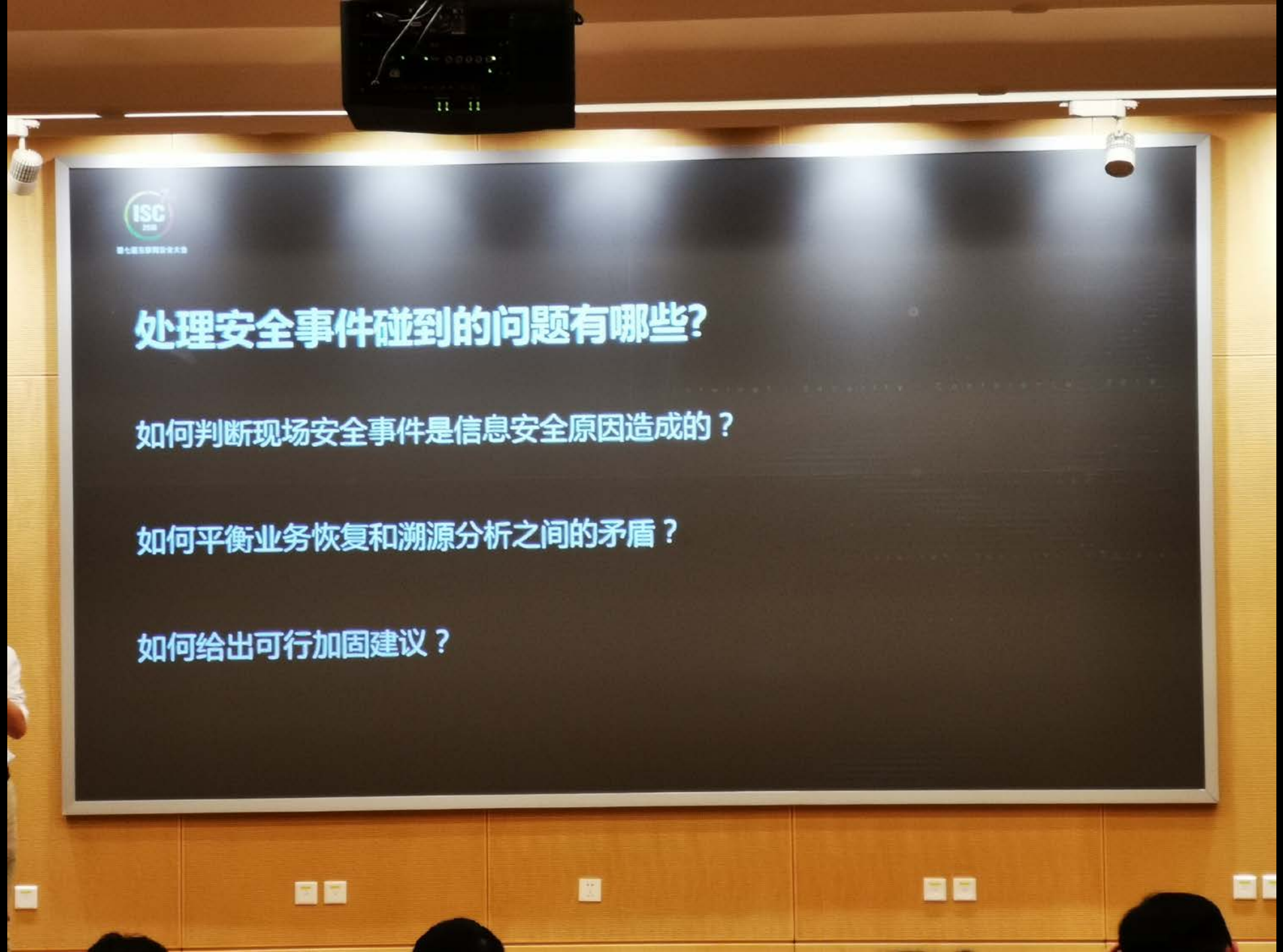
门票


ISC
龚亮华
烽台科技（北京）有限公司 总经理

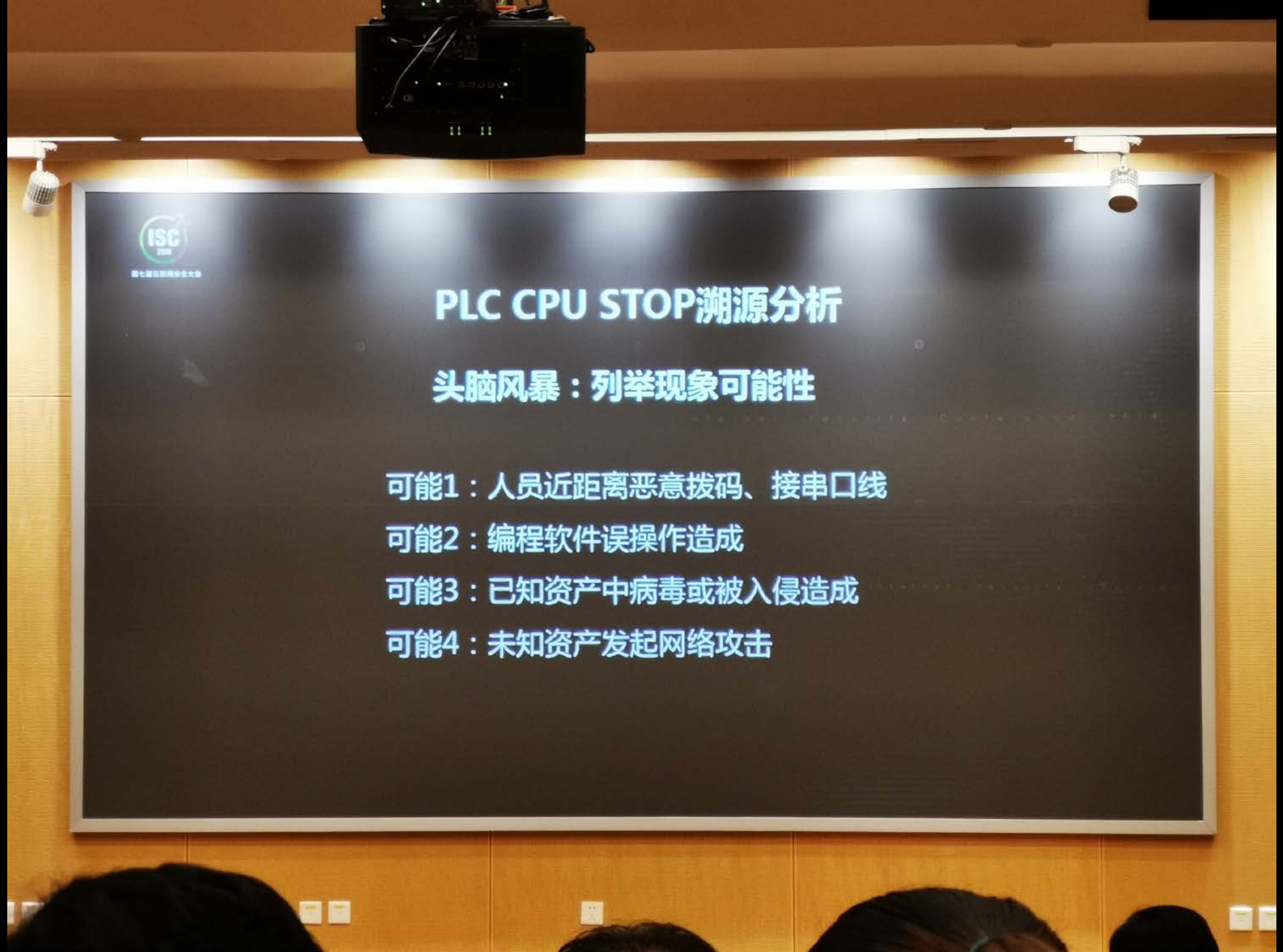

ISC
工业企业侧安全事件溯源技术与运营框架
烽台科技（北京）有限公司 / 灯塔实验室
总经理 龚亮华


工业企业侧安全事件
信息安全事件
功能安全事件
设备故障事件
工艺安全事件


事件处置流程
信息中心
总调度中心
业务监控
自动化部
调度中心
②
①
工艺操作
技术组
③
轮班组
操作工
运行维护

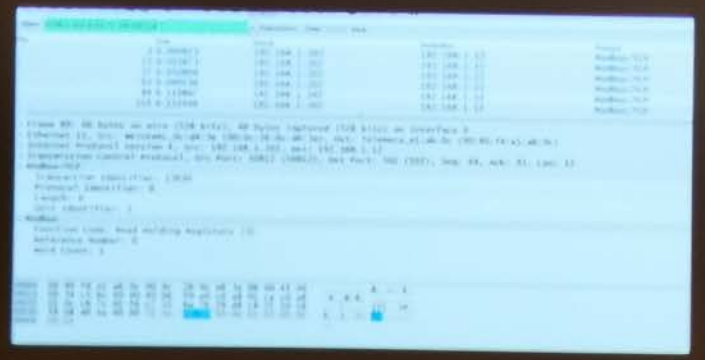

ISC
处理安全事件碰到的问题有哪些?
如何判断现场安全事件是信息安全原因造成的？
如何平衡业务恢复和溯源分析之间的矛盾？
如何给出可行加固建议？


PLC CPU STOP 溯源分析


PLC CPU STOP溯源分析
头脑风暴：列举现象可能性
可能1：人员近距离恶意拨码、接串口线
可能2：编程软件误操作造成
可能3：已知资产中病毒或被入侵造成
可能4：未知资产发起网络攻击

PLC CPU STOP溯源分析

本地 OR 远程 ？



PLC CPU STOP溯源分析

上位机 OR 未知 IP ？

IP设备管理列表

PLC CPU STOP溯源分析

未知IP攻击取证

人员进入登记及视频记录

PLC CPU STOP溯源分析

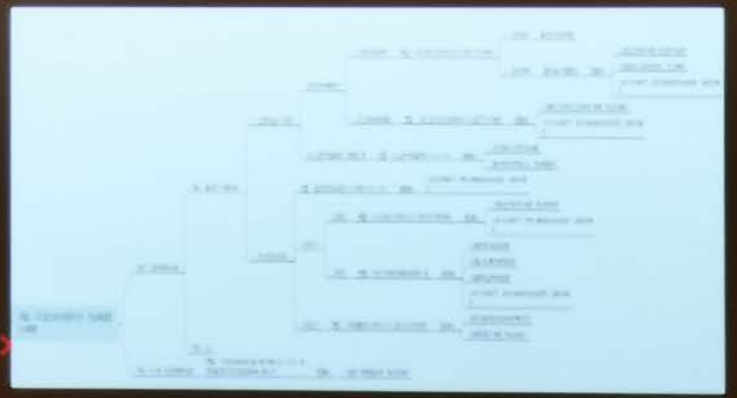
根因分析

可能1：编程软件误操作造成×

可能2：未知资产发起网络攻击√

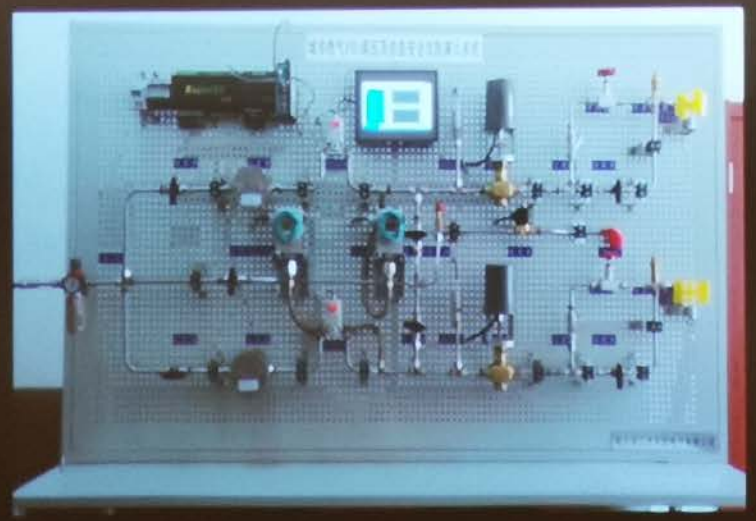
可能3：已知资产中病毒或被入侵造成×

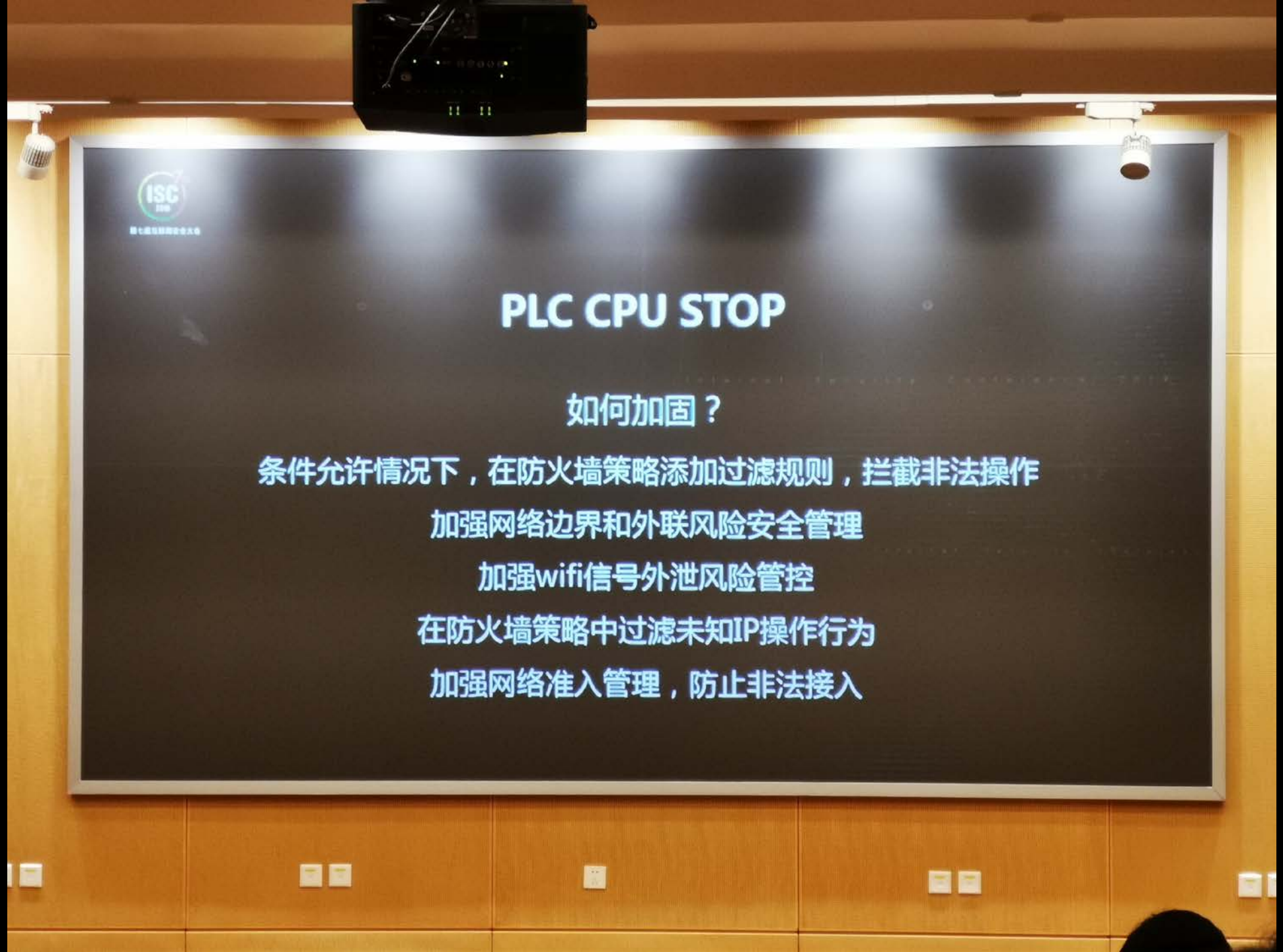
可能4：人员近距离恶意拨码、接串口线×



PLC CPU STOP溯源分析

验证分析



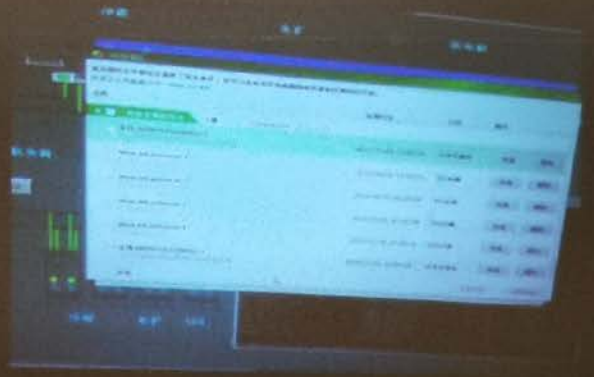

PLC CPU STOP
如何加固？
条件允许情况下，在防火墙策略添加过滤规则，拦截非法操作
加强网络边界和外联风险安全管理
加强wifi信号外泄风险管控
在防火墙策略中过滤未知IP操作行为
加强网络准入管理，防止非法接入


PLC DOS 溯源分析

PLC DOS 溯源分析

已知IP攻击取证

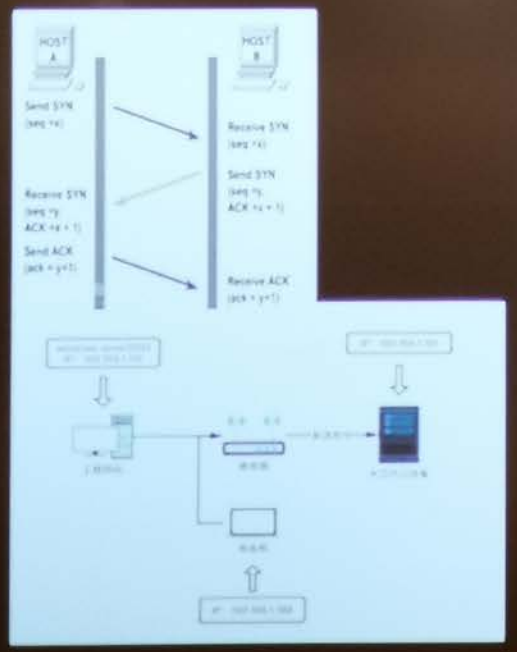
Ip列表和病毒检测记录

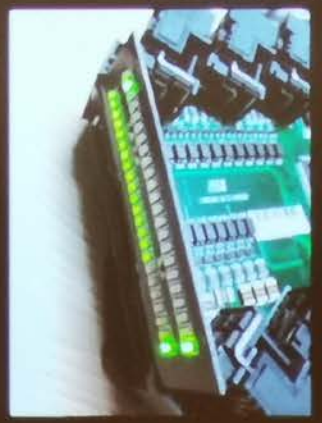


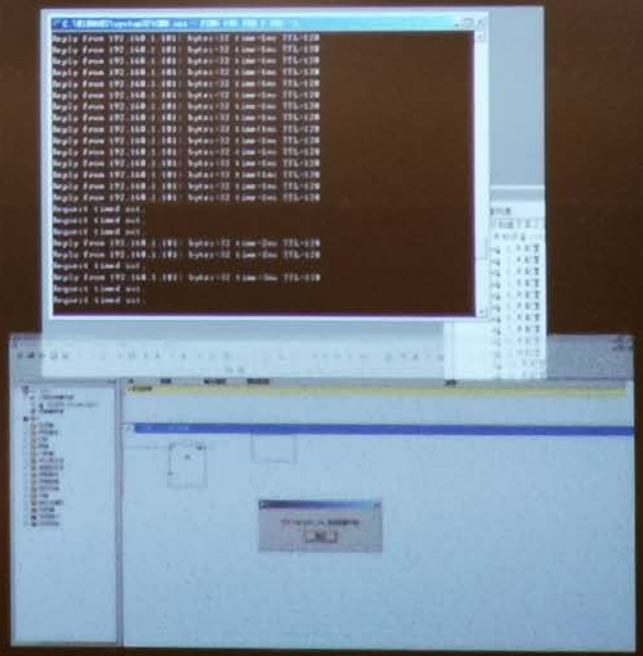

PLC DOS 溯源分析
验证分析

PLC DOS 溯源分析

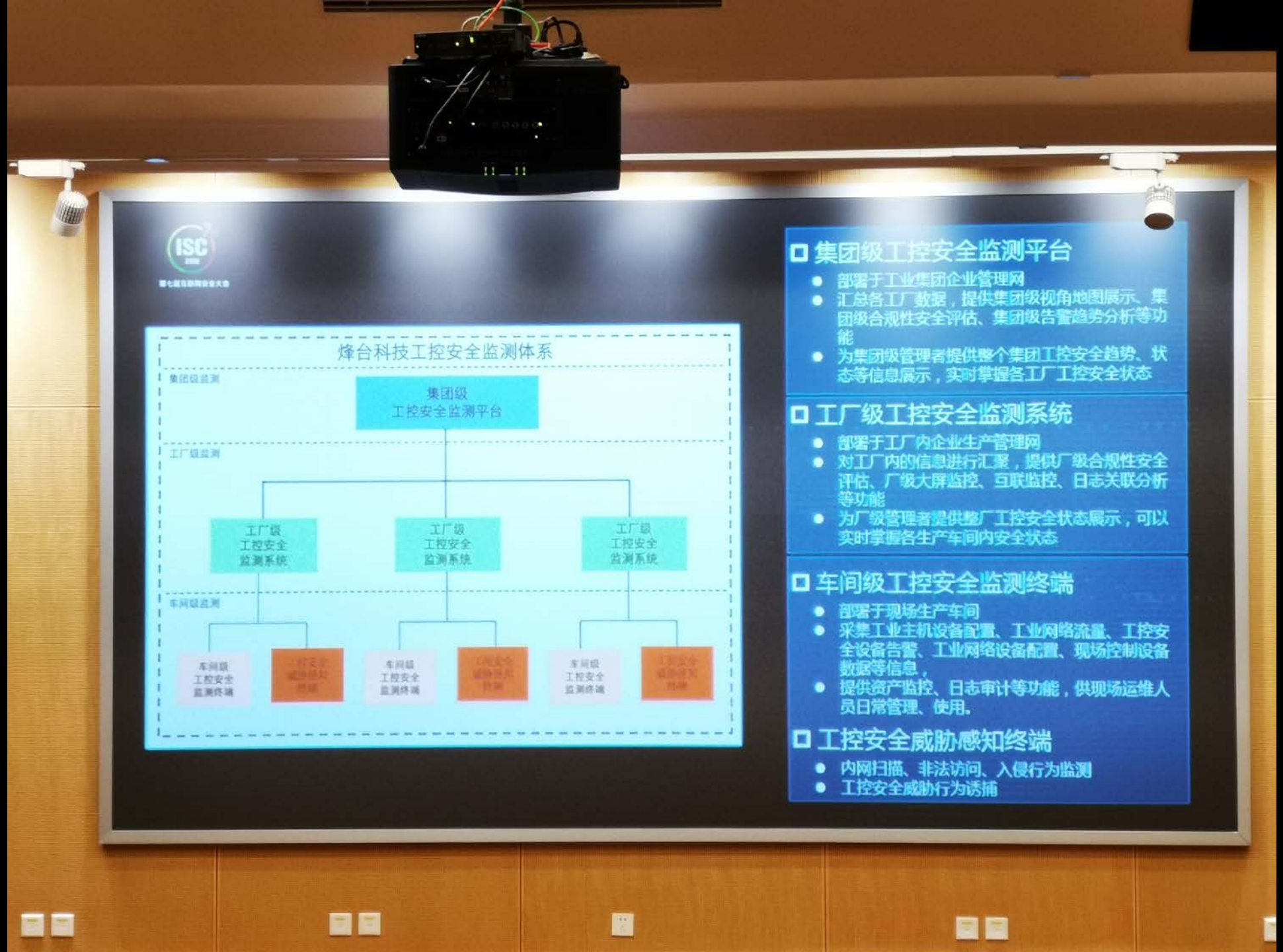
验证分析








工控设备异常告警
发现未知资产发起攻击行为


ISC
烽台科技工控安全监测体系
集团级监测
集团级
工控安全监测平台
工厂级监测
工厂级
工控安全
监测系统
工厂级
工控安全
监测系统
工厂级
工控安全
监测系统
车间级监测
车间级
工控安全
监测终端
车间级
工控安全
监测终端
车间级
工控安全
监测终端
集团级工控安全监测平台
部署于工业集团企业管理网
汇总各工厂数据，提供集团级视角地图展示、集团级合规性安全评估、集团级告警趋势分析等功能
为集团级管理者提供整个集团工控安全趋势、状态等信息展示，实时掌握各工厂工控安全状态
工厂级工控安全监测系统
部署于工厂内企业生产管理网
对工厂内的信息进行汇聚，提供厂级合规性安全评估、厂级大屏监控、互联监控、日志关联分析等功能
为厂级管理者提供整厂工控安全状态展示，可以实时掌握各生产车间内安全状态
车间级工控安全监测终端
部署于现场生产车间
采集工业主机设备配置、工业网络流量、工控安全设备告警、工业网络设备配置、现场控制设备数据等信息，
提供资产监控、日志审计等功能，供现场运维人员日常管理、使用。
工控安全威胁感知终端
内网扫描、非法访问、入侵行为监测
工控安全威胁行为诱捕

构建有效响应及处理运营框架

以保障生产业务为核心，涉及安全人员、安全技术、安全管理三个维度内容，由工业信息安全保障建设生命周期中策略制定、评估分析、方案设计、工程实施、运行管理、应急响应、安全教育各阶段建设内容构成。

ISC 2019
第七届互联网安全大会

运营架构具体内容

策略制定

评估分析

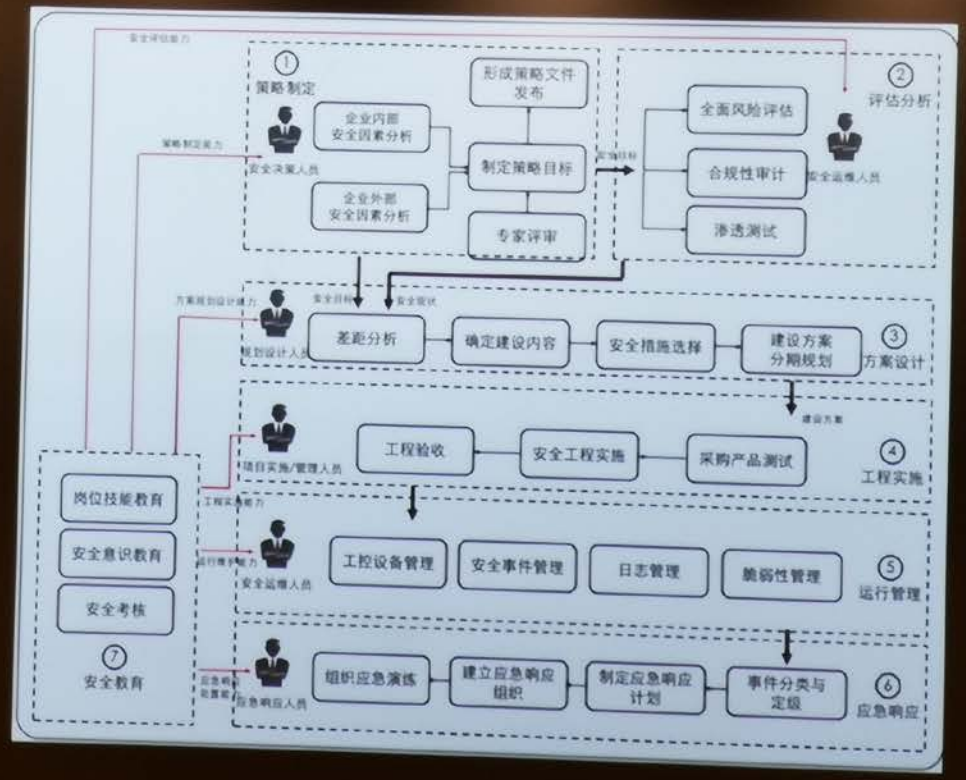
方案设计

工程实施

运行管理

应急响应

安全教育



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