

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



ISO 9001:2015



龚亮华

烽台科技（北京）有限公司 总经理



第七届中国国际安全大会

# 工业企业侧安全事件溯源技术与 运营框架

烽火科技（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

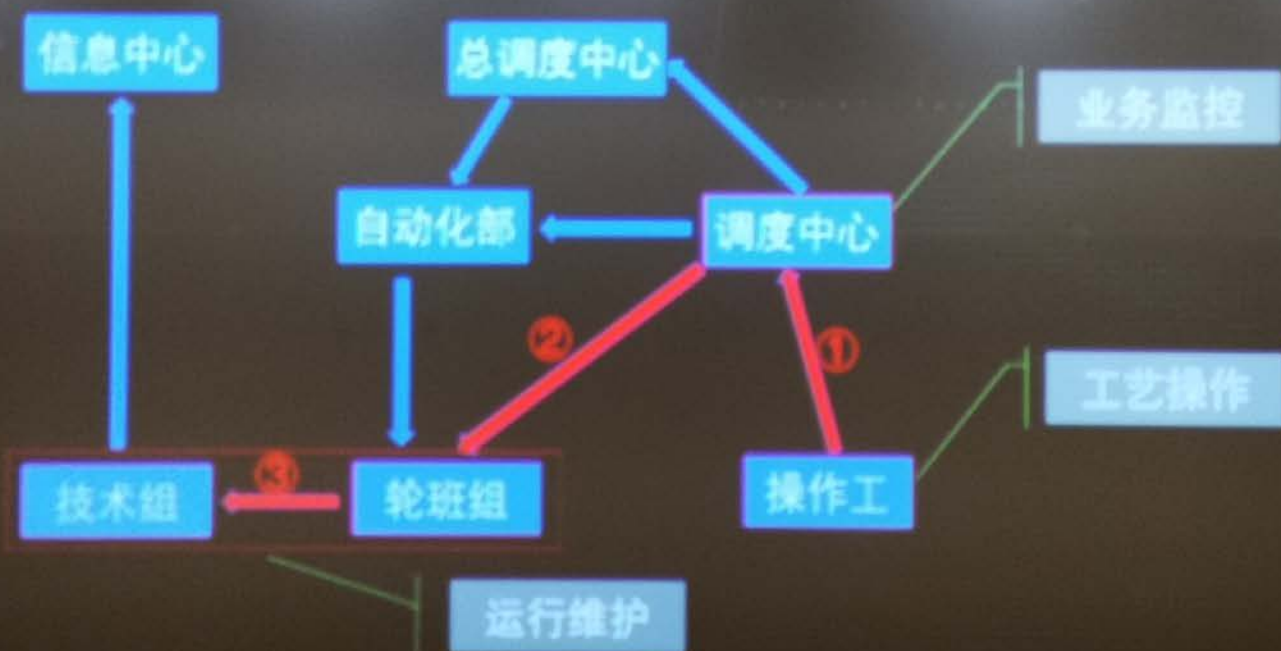
设备故障事件

工艺安全事件





## 事件处置流程





第七届中国信息安全大会

## 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







第七届中国网络安全大会

## 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



## 本地 OR 远程？

[illegible]



工业安全系统

# PLC CPU STOP溯源分析

## 上位机 OR 未知 IP ?

### IP设备管理列表

2/19		1	1	1	1	1	1	13/122/103
在线设备		1	1	1	1	1	1	1
IP	设备名称	IP地址	设备名称	IP地址	设备名称	IP地址	设备名称	IP地址
192.168.1.101	PLC	192.168.1.101	PLC	192.168.1.101	PLC	192.168.1.101	PLC	192.168.1.101
192.168.1.102	PLC	192.168.1.102	PLC	192.168.1.102	PLC	192.168.1.102	PLC	192.168.1.102
192.168.1.103	PLC	192.168.1.103	PLC	192.168.1.103	PLC	192.168.1.103	PLC	192.168.1.103
192.168.1.104	PLC	192.168.1.104	PLC	192.168.1.104	PLC	192.168.1.104	PLC	192.168.1.104
192.168.1.105	PLC	192.168.1.105	PLC	192.168.1.105	PLC	192.168.1.105	PLC	192.168.1.105
192.168.1.106	PLC	192.168.1.106	PLC	192.168.1.106	PLC	192.168.1.106	PLC	192.168.1.106
192.168.1.107	PLC	192.168.1.107	PLC	192.168.1.107	PLC	192.168.1.107	PLC	192.168.1.107
192.168.1.108	PLC	192.168.1.108	PLC	192.168.1.108	PLC	192.168.1.108	PLC	192.168.1.108
192.168.1.109	PLC	192.168.1.109	PLC	192.168.1.109	PLC	192.168.1.109	PLC	192.168.1.109
192.168.1.110	PLC	192.168.1.110	PLC	192.168.1.110	PLC	192.168.1.110	PLC	192.168.1.110
192.168.1.111	PLC	192.168.1.111	PLC	192.168.1.111	PLC	192.168.1.111	PLC	192.168.1.111
192.168.1.112	PLC	192.168.1.112	PLC	192.168.1.112	PLC	192.168.1.112	PLC	192.168.1.112
192.168.1.113	PLC	192.168.1.113	PLC	192.168.1.113	PLC	192.168.1.113	PLC	192.168.1.113
192.168.1.114	PLC	192.168.1.114	PLC	192.168.1.114	PLC	192.168.1.114	PLC	192.168.1.114
192.168.1.115	PLC	192.168.1.115	PLC	192.168.1.115	PLC	192.168.1.115	PLC	192.168.1.115
192.168.1.116	PLC	192.168.1.116	PLC	192.168.1.116	PLC	192.168.1.116	PLC	192.168.1.116
192.168.1.117	PLC	192.168.1.117	PLC	192.168.1.117	PLC	192.168.1.117	PLC	192.168.1.117
192.168.1.118	PLC	192.168.1.118	PLC	192.168.1.118	PLC	192.168.1.118	PLC	192.168.1.118
192.168.1.119	PLC	192.168.1.119	PLC	192.168.1.119	PLC	192.168.1.119	PLC	192.168.1.119
192.168.1.120	PLC	192.168.1.120	PLC	192.168.1.120	PLC	192.168.1.120	PLC	192.168.1.120





第七届中国网络安全大会

# 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

员工进出登记记录表

时间	姓名	部门	事由	进出	备注
2019-07-10 08:00	张三	IT部	上班	进	
2019-07-10 08:05	李四	IT部	上班	进	
2019-07-10 08:10	王五	IT部	上班	进	
2019-07-10 08:15	赵六	IT部	上班	进	
2019-07-10 08:20	钱七	IT部	上班	进	
2019-07-10 08:25	孙八	IT部	上班	进	
2019-07-10 08:30	周九	IT部	上班	进	
2019-07-10 08:35	吴十	IT部	上班	进	
2019-07-10 08:40	郑十一	IT部	上班	进	
2019-07-10 08:45	冯十二	IT部	上班	进	
2019-07-10 08:50	陈十三	IT部	上班	进	
2019-07-10 08:55	褚十四	IT部	上班	进	
2019-07-10 09:00	褚十五	IT部	上班	进	
2019-07-10 09:05	褚十六	IT部	上班	进	
2019-07-10 09:10	褚十七	IT部	上班	进	
2019-07-10 09:15	褚十八	IT部	上班	进	
2019-07-10 09:20	褚十九	IT部	上班	进	
2019-07-10 09:25	褚二十	IT部	上班	进	
2019-07-10 09:30	褚二十一	IT部	上班	进	
2019-07-10 09:35	褚二十二	IT部	上班	进	
2019-07-10 09:40	褚二十三	IT部	上班	进	
2019-07-10 09:45	褚二十四	IT部	上班	进	
2019-07-10 09:50	褚二十五	IT部	上班	进	
2019-07-10 09:55	褚二十六	IT部	上班	进	
2019-07-10 10:00	褚二十七	IT部	上班	进	
2019-07-10 10:05	褚二十八	IT部	上班	进	
2019-07-10 10:10	褚二十九	IT部	上班	进	
2019-07-10 10:15	褚三十	IT部	上班	进	
2019-07-10 10:20	褚三十一	IT部	上班	进	
2019-07-10 10:25	褚三十二	IT部	上班	进	
2019-07-10 10:30	褚三十三	IT部	上班	进	
2019-07-10 10:35	褚三十四	IT部	上班	进	
2019-07-10 10:40	褚三十五	IT部	上班	进	
2019-07-10 10:45	褚三十六	IT部	上班	进	
2019-07-10 10:50	褚三十七	IT部	上班	进	
2019-07-10 10:55	褚三十八	IT部	上班	进	
2019-07-10 11:00	褚三十九	IT部	上班	进	
2019-07-10 11:05	褚四十	IT部	上班	进	
2019-07-10 11:10	褚四十一	IT部	上班	进	
2019-07-10 11:15	褚四十二	IT部	上班	进	
2019-07-10 11:20	褚四十三	IT部	上班	进	
2019-07-10 11:25	褚四十四	IT部	上班	进	
2019-07-10 11:30	褚四十五	IT部	上班	进	
2019-07-10 11:35	褚四十六	IT部	上班	进	
2019-07-10 11:40	褚四十七	IT部	上班	进	
2019-07-10 11:45	褚四十八	IT部	上班	进	
2019-07-10 11:50	褚四十九	IT部	上班	进	
2019-07-10 11:55	褚五十	IT部	上班	进	
2019-07-10 12:00	褚五十一	IT部	上班	进	
2019-07-10 12:05	褚五十二	IT部	上班	进	
2019-07-10 12:10	褚五十三	IT部	上班	进	
2019-07-10 12:15	褚五十四	IT部	上班	进	
2019-07-10 12:20	褚五十五	IT部	上班	进	
2019-07-10 12:25	褚五十六	IT部	上班	进	
2019-07-10 12:30	褚五十七	IT部	上班	进	
2019-07-10 12:35	褚五十八	IT部	上班	进	
2019-07-10 12:40	褚五十九	IT部	上班	进	
2019-07-10 12:45	褚六十	IT部	上班	进	
2019-07-10 12:50	褚六十一	IT部	上班	进	
2019-07-10 12:55	褚六十二	IT部	上班	进	
2019-07-10 13:00	褚六十三	IT部	上班	进	
2019-07-10 13:05	褚六十四	IT部	上班	进	
2019-07-10 13:10	褚六十五	IT部	上班	进	
2019-07-10 13:15	褚六十六	IT部	上班	进	
2019-07-10 13:20	褚六十七	IT部	上班	进	
2019-07-10 13:25	褚六十八	IT部	上班	进	
2019-07-10 13:30	褚六十九	IT部	上班	进	
2019-07-10 13:35	褚七十	IT部	上班	进	
2019-07-10 13:40	褚七十一	IT部	上班	进	
2019-07-10 13:45	褚七十二	IT部	上班	进	
2019-07-10 13:50	褚七十三	IT部	上班	进	
2019-07-10 13:55	褚七十四	IT部	上班	进	
2019-07-10 14:00	褚七十五	IT部	上班	进	
2019-07-10 14:05	褚七十六	IT部	上班	进	
2019-07-10 14:10	褚七十七	IT部	上班	进	
2019-07-10 14:15	褚七十八	IT部	上班	进	
2019-07-10 14:20	褚七十九	IT部	上班	进	
2019-07-10 14:25	褚八十	IT部	上班	进	
2019-07-10 14:30	褚八十一	IT部	上班	进	
2019-07-10 14:35	褚八十二	IT部	上班	进	
2019-07-10 14:40	褚八十三	IT部	上班	进	
2019-07-10 14:45	褚八十四	IT部	上班	进	
2019-07-10 14:50	褚八十五	IT部	上班	进	
2019-07-10 14:55	褚八十六	IT部	上班	进	
2019-07-10 15:00	褚八十七	IT部	上班	进	
2019-07-10 15:05	褚八十八	IT部	上班	进	
2019-07-10 15:10	褚八十九	IT部	上班	进	
2019-07-10 15:15	褚九十	IT部	上班	进	
2019-07-10 15:20	褚九十一	IT部	上班	进	
2019-07-10 15:25	褚九十二	IT部	上班	进	
2019-07-10 15:30	褚九十三	IT部	上班	进	
2019-07-10 15:35	褚九十四	IT部	上班	进	
2019-07-10 15:40	褚九十五	IT部	上班	进	
2019-07-10 15:45	褚九十六	IT部	上班	进	
2019-07-10 15:50	褚九十七	IT部	上班	进	
2019-07-10 15:55	褚九十八	IT部	上班	进	
2019-07-10 16:00	褚九十九	IT部	上班	进	
2019-07-10 16:05	褚一百	IT部	上班	进	

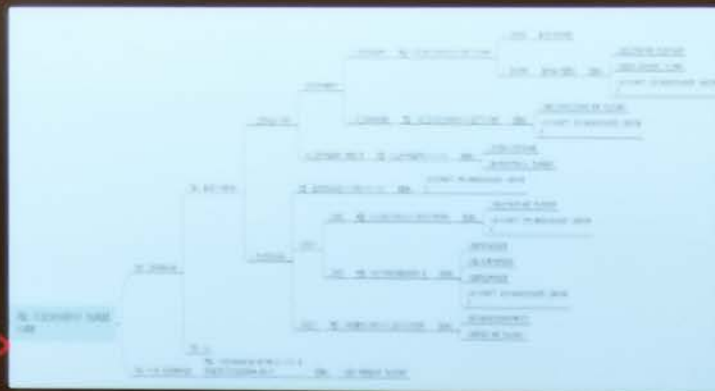


第七届中国网络安全大会

# PLC CPU STOP溯源分析

## 根因分析

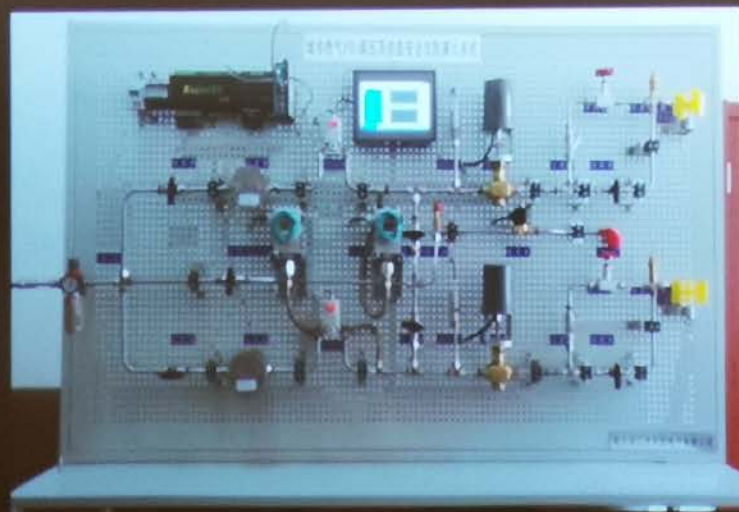
- 可能1：编程软件误操作造成✗
- 可能2：未知资产发起网络攻击✓
- 可能3：已知资产中病毒或被入侵造成✗
- 可能4：人员近距离恶意拨码、接串口线✗





# 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







第七届中国网络安全大会

# PLC DOS 溯源分析

## 已知IP攻击取证

Ip列表和病毒检测记录

IP	Port	Protocol	Source	Destination	Count	Rate	Time	Size	Status
192.168.1.1	80	TCP	192.168.1.1	192.168.1.1	100	100	100	100	OK
192.168.1.2	80	TCP	192.168.1.2	192.168.1.2	100	100	100	100	OK
192.168.1.3	80	TCP	192.168.1.3	192.168.1.3	100	100	100	100	OK
192.168.1.4	80	TCP	192.168.1.4	192.168.1.4	100	100	100	100	OK
192.168.1.5	80	TCP	192.168.1.5	192.168.1.5	100	100	100	100	OK
192.168.1.6	80	TCP	192.168.1.6	192.168.1.6	100	100	100	100	OK
192.168.1.7	80	TCP	192.168.1.7	192.168.1.7	100	100	100	100	OK
192.168.1.8	80	TCP	192.168.1.8	192.168.1.8	100	100	100	100	OK
192.168.1.9	80	TCP	192.168.1.9	192.168.1.9	100	100	100	100	OK
192.168.1.10	80	TCP	192.168.1.10	192.168.1.10	100	100	100	100	OK

IP	Port	Protocol	Source	Destination	Count	Rate	Time	Size	Status
192.168.1.1	80	TCP	192.168.1.1	192.168.1.1	100	100	100	100	OK
192.168.1.2	80	TCP	192.168.1.2	192.168.1.2	100	100	100	100	OK
192.168.1.3	80	TCP	192.168.1.3	192.168.1.3	100	100	100	100	OK
192.168.1.4	80	TCP	192.168.1.4	192.168.1.4	100	100	100	100	OK
192.168.1.5	80	TCP	192.168.1.5	192.168.1.5	100	100	100	100	OK
192.168.1.6	80	TCP	192.168.1.6	192.168.1.6	100	100	100	100	OK
192.168.1.7	80	TCP	192.168.1.7	192.168.1.7	100	100	100	100	OK
192.168.1.8	80	TCP	192.168.1.8	192.168.1.8	100	100	100	100	OK
192.168.1.9	80	TCP	192.168.1.9	192.168.1.9	100	100	100	100	OK
192.168.1.10	80	TCP	192.168.1.10	192.168.1.10	100	100	100	100	OK





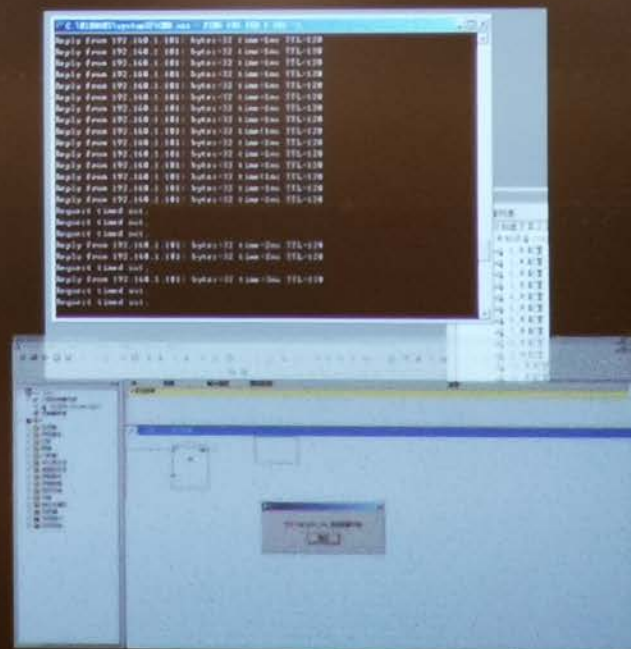
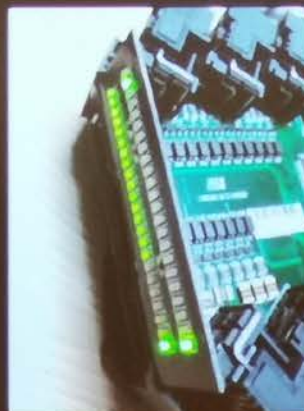
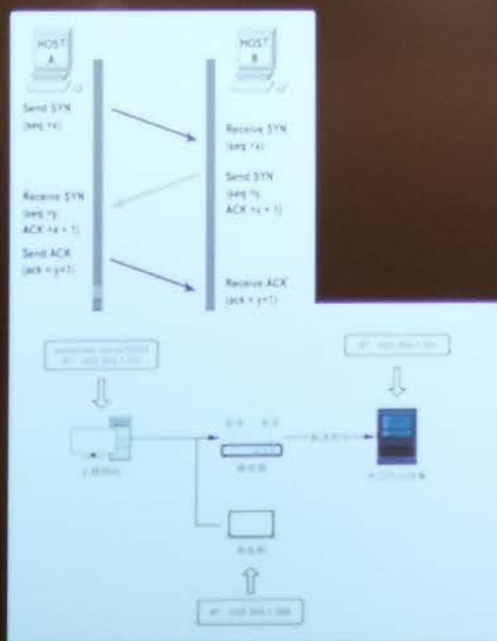
# PLC DOS 溯源分析 验证分析



第七届中国网络安全大会

# PLC DOS 溯源分析

## 验证分析





第七届中国信息安全大会

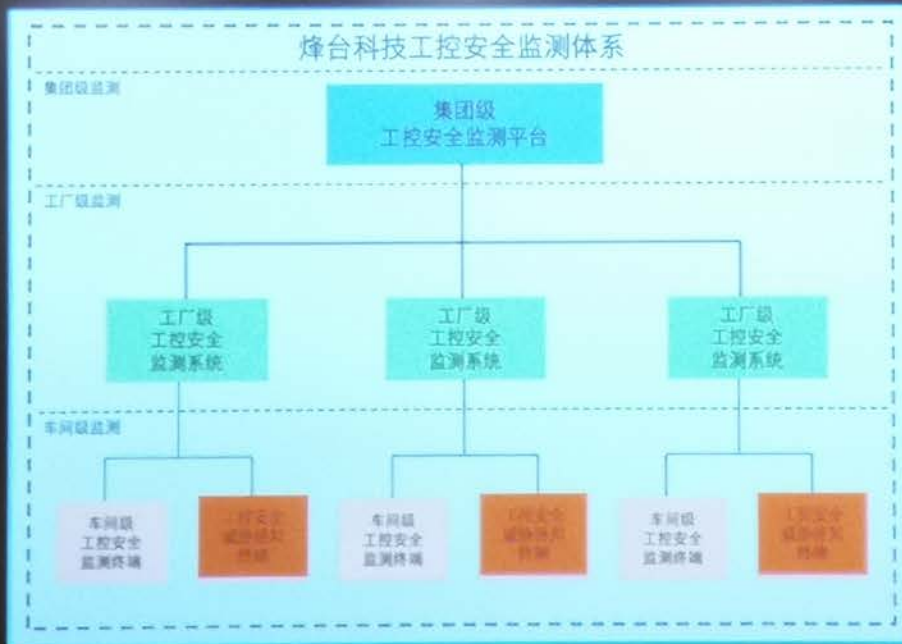
# 工控设备异常告警 发现未知资产发起攻击行为





第七届中国网络安全大会

### 烽火科技工控安全监测体系



#### □ 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



第七届中国网络安全大会

## 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。



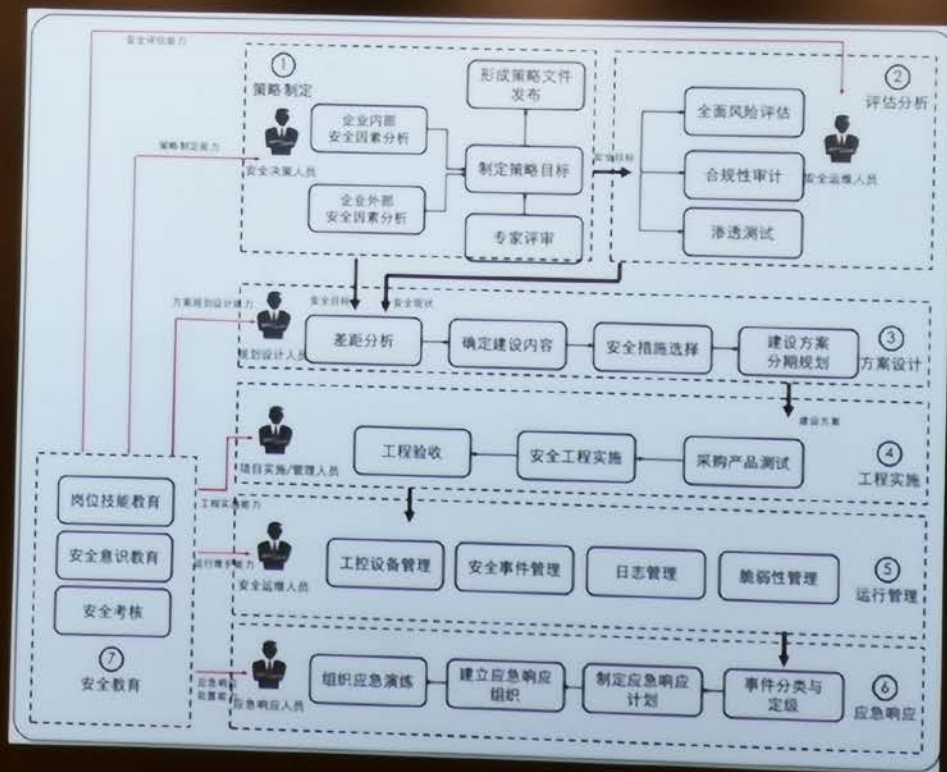




第七届中国网络安全大会

## 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