两化融合的安全保障之道
实战“固、隔、监”

三零卫士

30 WISH
INFORMATION SECURITY

30Services

十八大：推动量化深度融合，坚持四化同步发展

当前我国企业转型升级和可持续发展面临的核心问题

环境问题

环境约束已经成为当前我国企业实现可持续发展的刚性约束；
环境因素成为企业生产需要考虑的重要生产要素；
国家在污染排放等方面的环境治理要求将为企业带来全新的挑战。

资源问题

资源能源的有限性与稀缺性与不断增长的生产需求之间存在供给与需求之间的不平衡；
我国资源密集型生产企业如何转型；
我国高投入、高消耗的粗放式增长方式如何转变。

以劳动生产率为核心的竞争问题

2013年国民经济和社会发展统计公报显示：我国劳动生产率为66199元/人，远低于发达国家的水平
以劳动密集性产业为主，但是劳动力成本上升导致人口红利难以为继；
产业链两端高附加值环节的企业竞争力不足。

两化融合是推动我国企业实现转型升级和可持续发展的必由之路！

机械化	电气化	自动化	信息化
机器代替手工，机械力代替自然力	解决能量的转换和远距离传输，为工业发展提供新能源	带来全新的生产控制工程，提高生产率，使工业化进入现代化	信息和知识的大规模生产，工业化步入数字化、智能化、网络化时代

中国工业是**赶超型工业**，中国工业化不可能也不必要沿袭传统的机械化、电气化、自动化、信息化发展历程。在工业化尚未完成的前提下，通过加速信息化进程，推动工业化跨越式发展，我们取得了丰硕成果，但也不可避免的存在一些不足。

- 在信息化条件（环境）下，两化融合是企业获得可持续竞争优势的必由之路。

在信息化条件（环境）下，没有两化融合，想形成有竞争优势的研究开发、生产和管理决策能力，只是水中捞月的空想而已。

自动化与信息化

深度融合

正在加速

工控信息安全

威胁

正在加剧

工业互联网

1%提效创

造1万亿美

元市场

固.隔.监

工控信息安全防护理论体系

固隔监体系

2013年，上海三零卫士信息安全有限公司承担了安标委《信息安全技术工业系统安全防护技术要求和测试评价方法》国家标准的编制工作。期间，三零卫士结合自身多年对工业控制系统信息安全的探索与实践经验，结合国内外相关标准，并与多位信息安全领域、自动化控制领域以及多个行业仪电控制系统专家多次碰撞后，产生了“固、隔、监”工控信息安全防护理念。

“固、隔、监”不同于传统信息安全的安全五性：“机密性、可控性、可靠性、完整性和不可抵赖性”，将工控领域头等重要的稳定性，作为固，放在首位；针对工控系统网络化趋势，将传统安全的安全域隔离理念引入工控，作为工作重点；面对工控系统工作连续性要求高，因此以监视作为主要手段，提高发现问题的能力，早预警，早应对。

所以，“固、隔、监”是设计理念，可以引导工控信息安全加固方案设计；“固、隔、监”是工作方法，可以引导工控信息安全集成建设和实施；“固、隔、监”是评判标准，用于衡量传统信息安全产品与工业控制领域的适应度。“固、隔、监”是一套完整的方法论，帮助工控专家理解信息安全工作方法，引导信息安全专家进入工控领域。

更具体说：“固”：是建立信息安全基线，稳守物理安全，稳固工控信息系统运行环境。“隔”：根据实际需要，建立安全分区，采用恰当的设备执行网络隔离。“监”：对于控制网内部进行全流量监视分析，建立早期攻击症状发现处置机制。以“固、隔、监”为指导思想，三零卫士经过多年坚持不懈地工作，目前已经在核工业、冶金、石油石化、轨道交通、水利、冶金等多个领域取得了丰硕的成果。已经初步形成了知识培训、安全咨询、风险分析、合规检查、方案设计、集成建设、运维保障等全系列服务体系。

在“固、隔、监”凭借中国电子科技集团和中电科第三十研究所的强大市场能力和技术实力的支撑，三零卫士当仁不让地成为工控信息安全领域的领跑者。

固

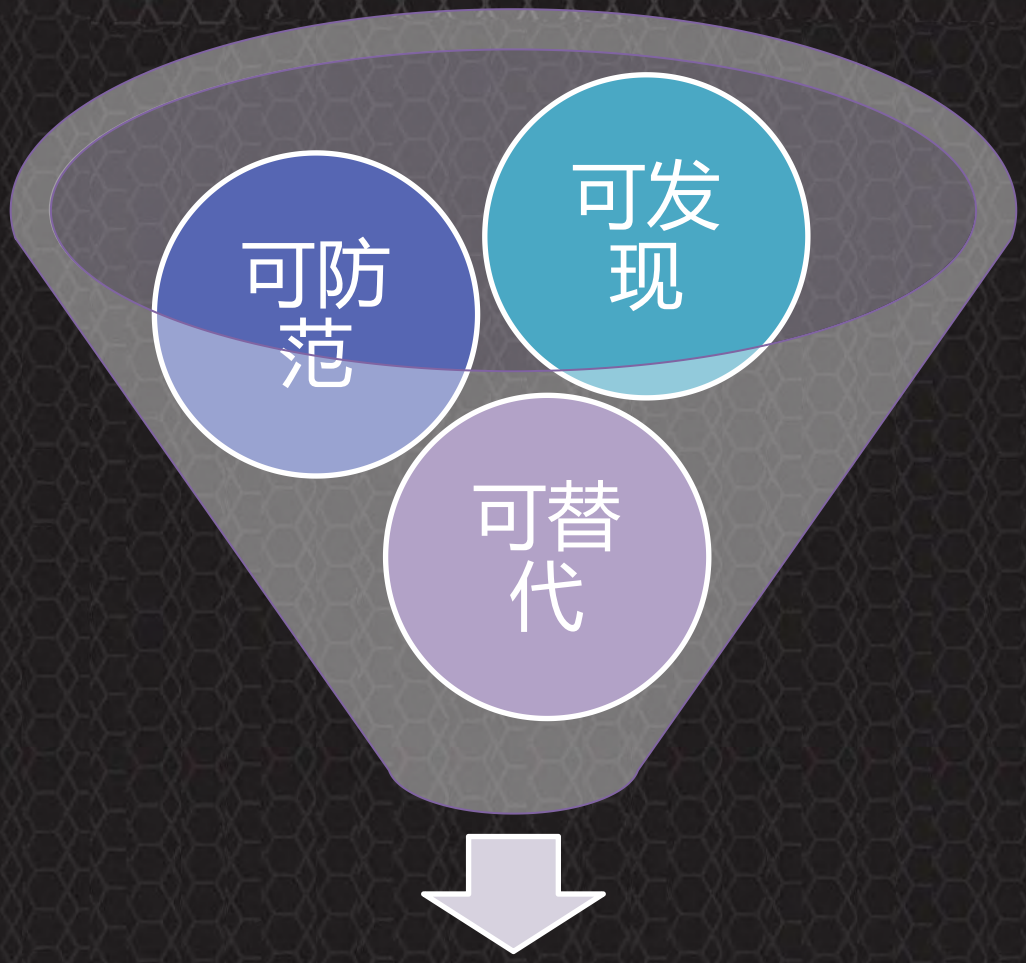
通过向工业控制产品厂商提供服务和产品模块的方式，帮助工业控制产品厂家提高产品自身的信息安全防护能力；针对控制系统设计单位、集成商、业主，以提供服务的方式，帮助其提高整个工控系统的信息安全防护能力。

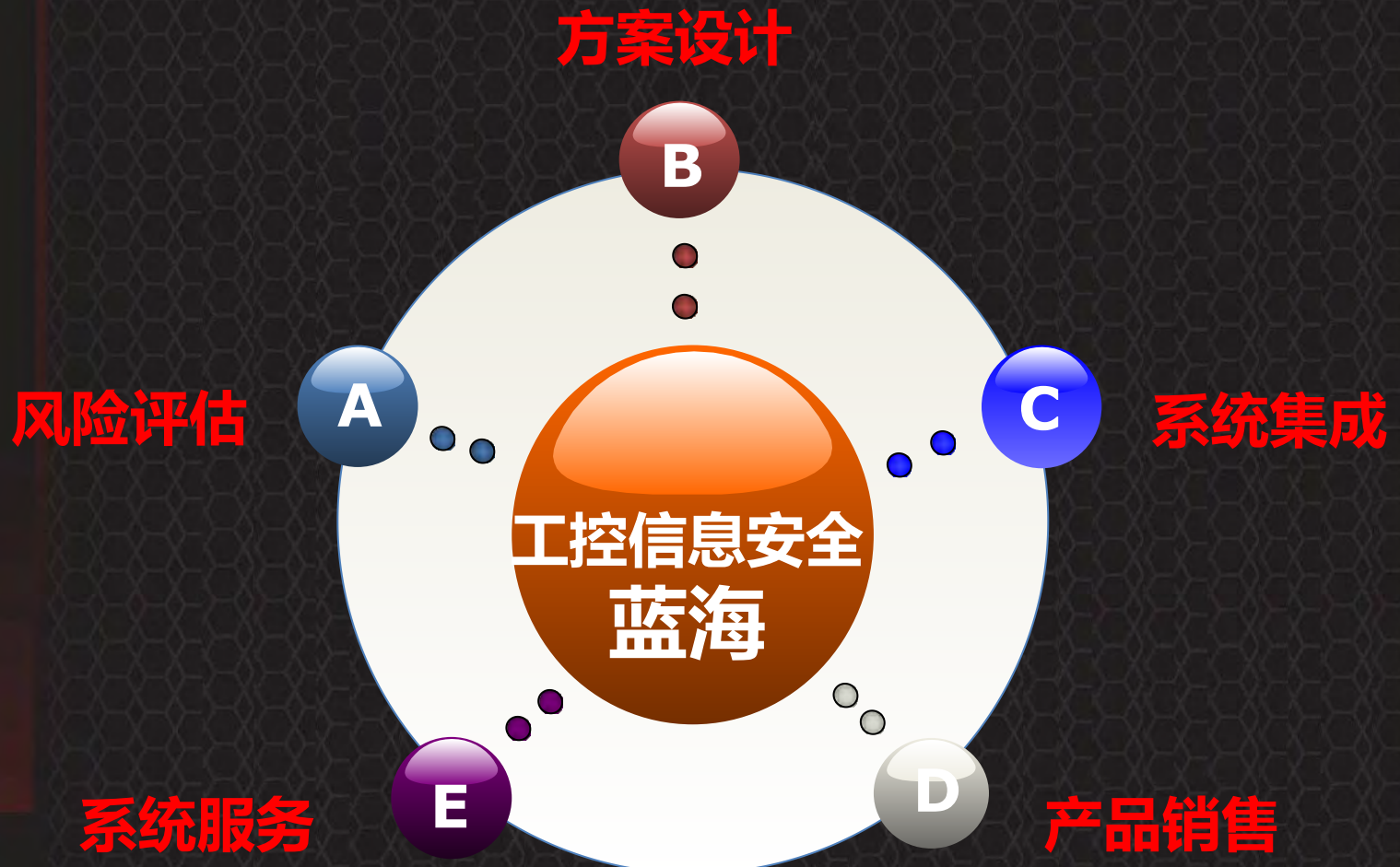
隔

推出通用型的隔离产品和技术，解决控制系统中的“安全隔离”问题，帮助控制系统实现安全前提下的信息交换。

监

研究对工控系统无影响的监控技术和产品，帮助用户实现对控制系统的安全监控，为实现工控系统的相对可控提供最基础的技术和管理支撑。


可防范
可发现
可替代
安全可控


方案设计
B
风险评估
A
C
系统集成
工控信息安全
蓝海
E
D
系统服务
产品销售

信息管理层

生产管理层

过程控制层

隔

30TrustCON FWS

工业防火墙

监

30TrustCON MCS

工控信息安全监控系统

标准：国家、地方、行业

风险评估

工业防火墙、工业网络监控

固

隔

监

掌握现状

关键工艺

漏洞隐患

评估风险

后果

PDCA

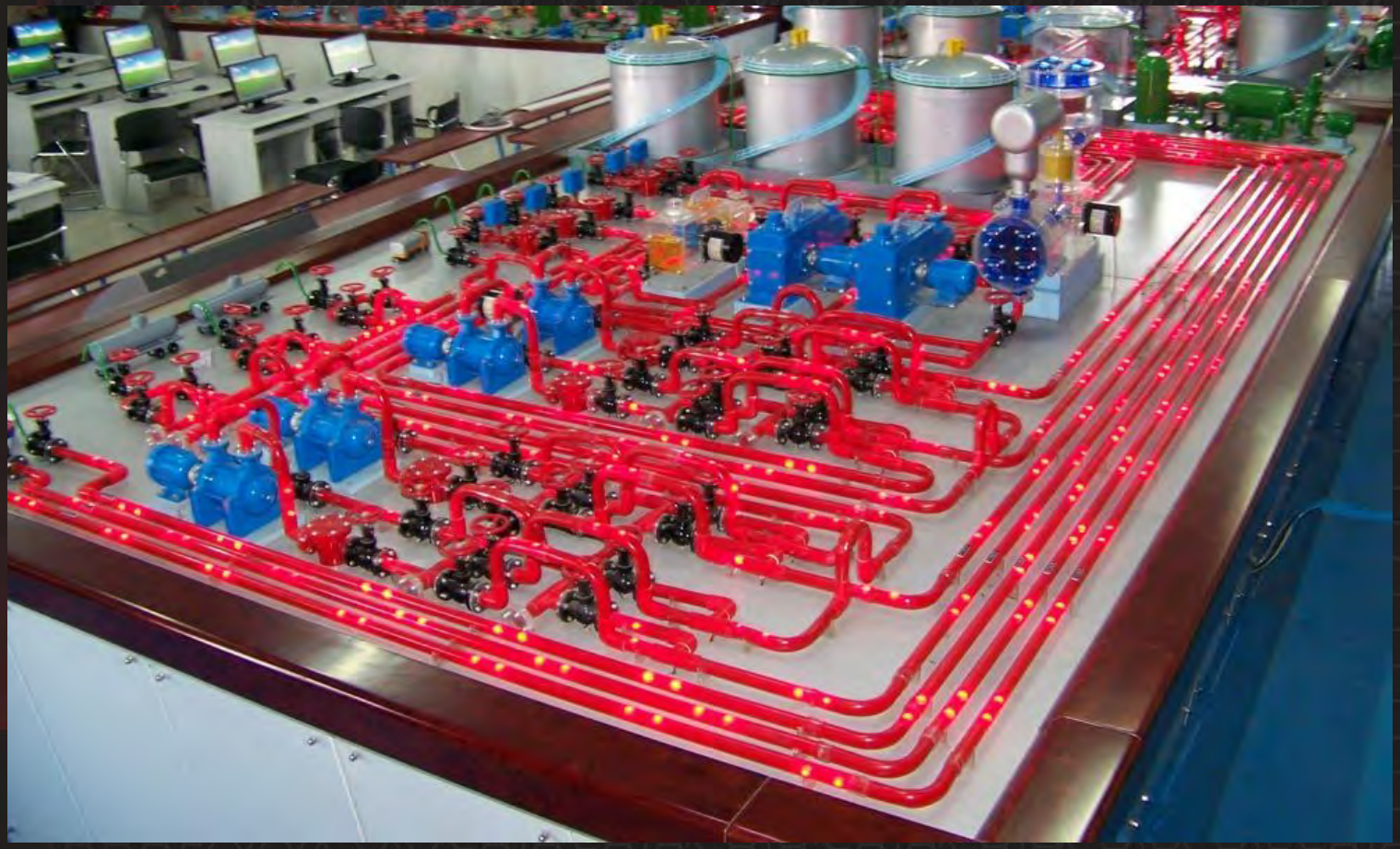
安全加固

方案集成

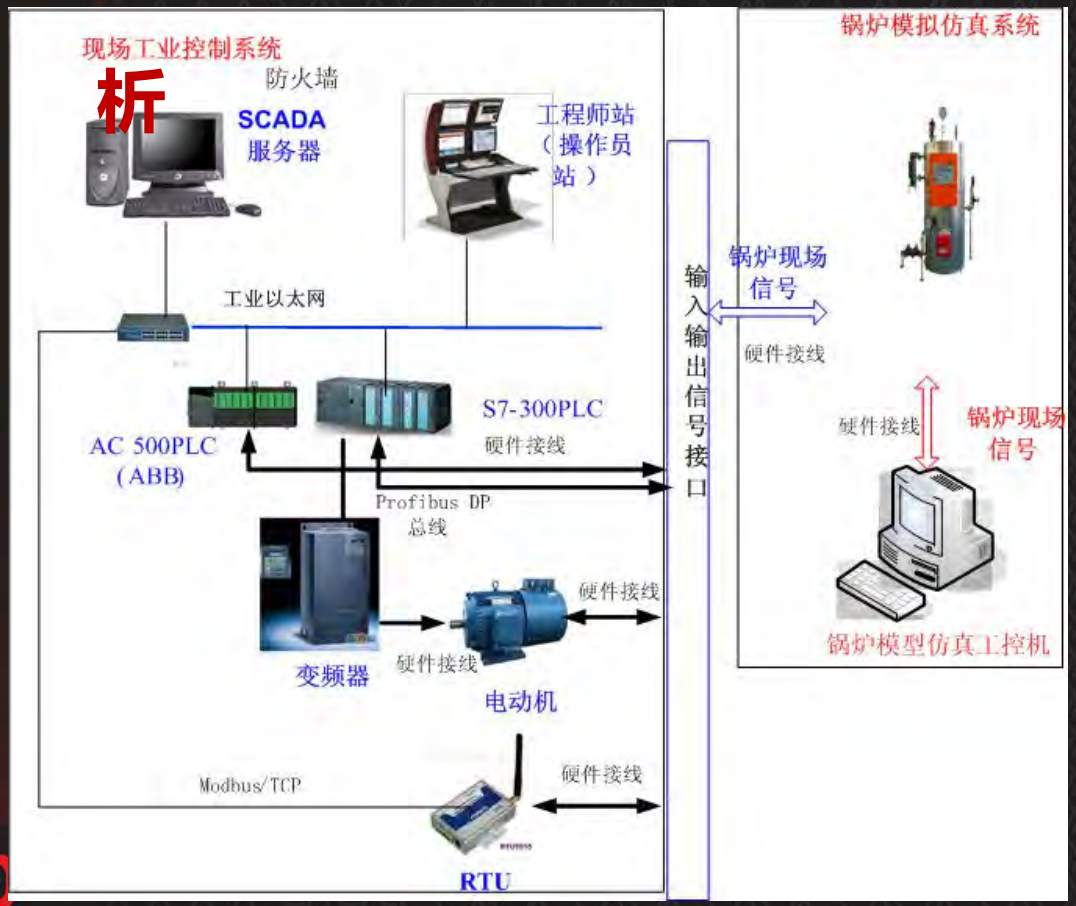
产品部署

行业：石油石化、钢铁、轨道交通、核电、电网、烟草

口仿真：整厂信息安全场景沙盘



□仿真+实物典型工业控制系统模拟仿真/PLC隐患分



口实物：完整工艺流量分析仪/信息安全攻防演练

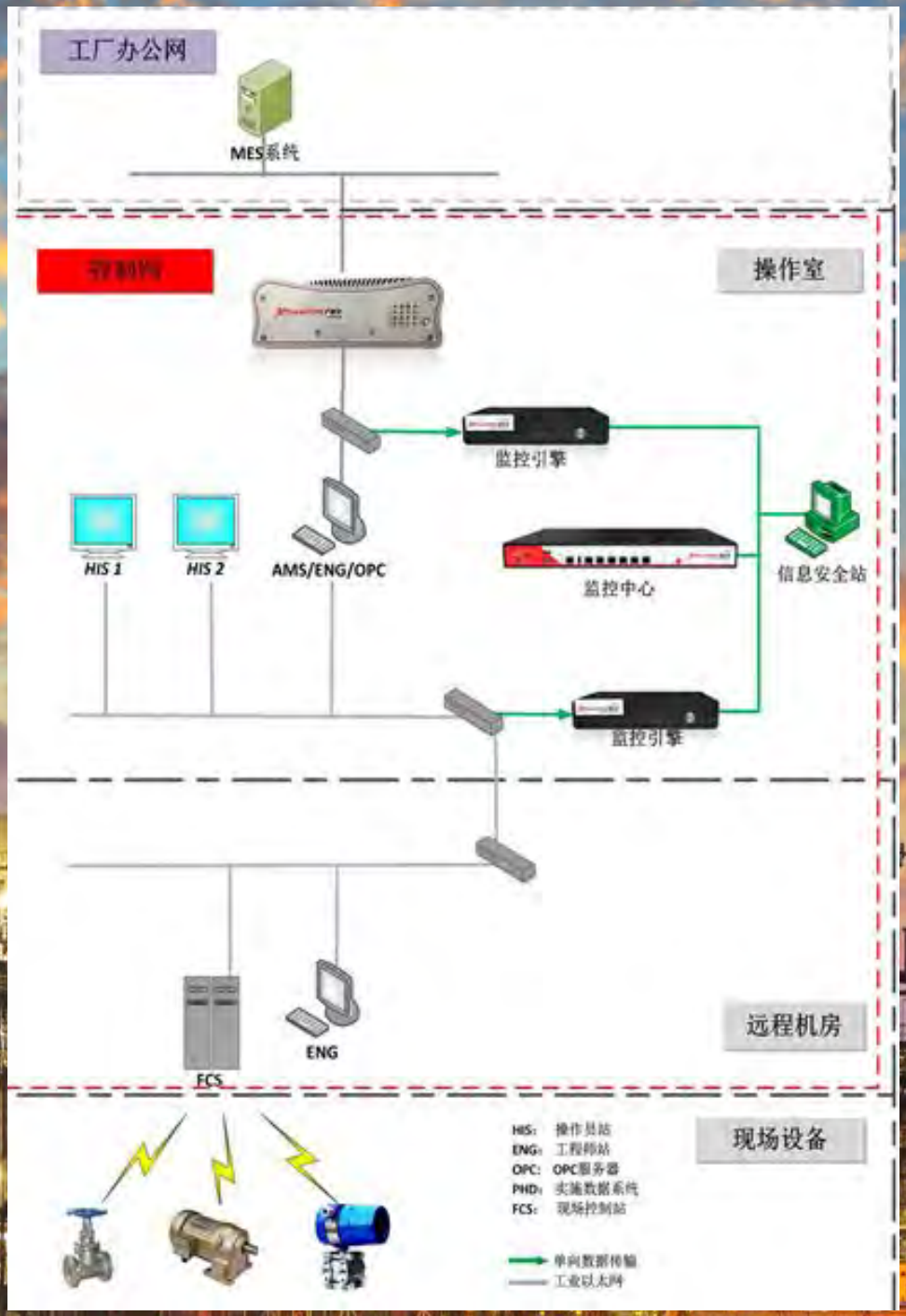
石化炼化

部署的安全产品对现有生产影响最小化

OPC服务器和上层管理网络数据通讯需要监控和隔离，确保该数据通路只能传OPC数据

对控制网内部进行监控，若有非授权设备进入网络中，能及时报警。

若发现有可疑文件或病毒传播，能及时告警和定位。


工厂办公网
MES系统
操作室
监控引擎
HIS 1
HIS 2
AMS/ENG/OPC
监控中心
信息安全站
监控引擎
远程机房
ENG
FCS
现场设备
HIS: 操作员站
ENG: 工程师站
OPC: OPC服务器
PHD: 实施数据系统
FCS: 现场控制站
单向数据传输
工业以太网

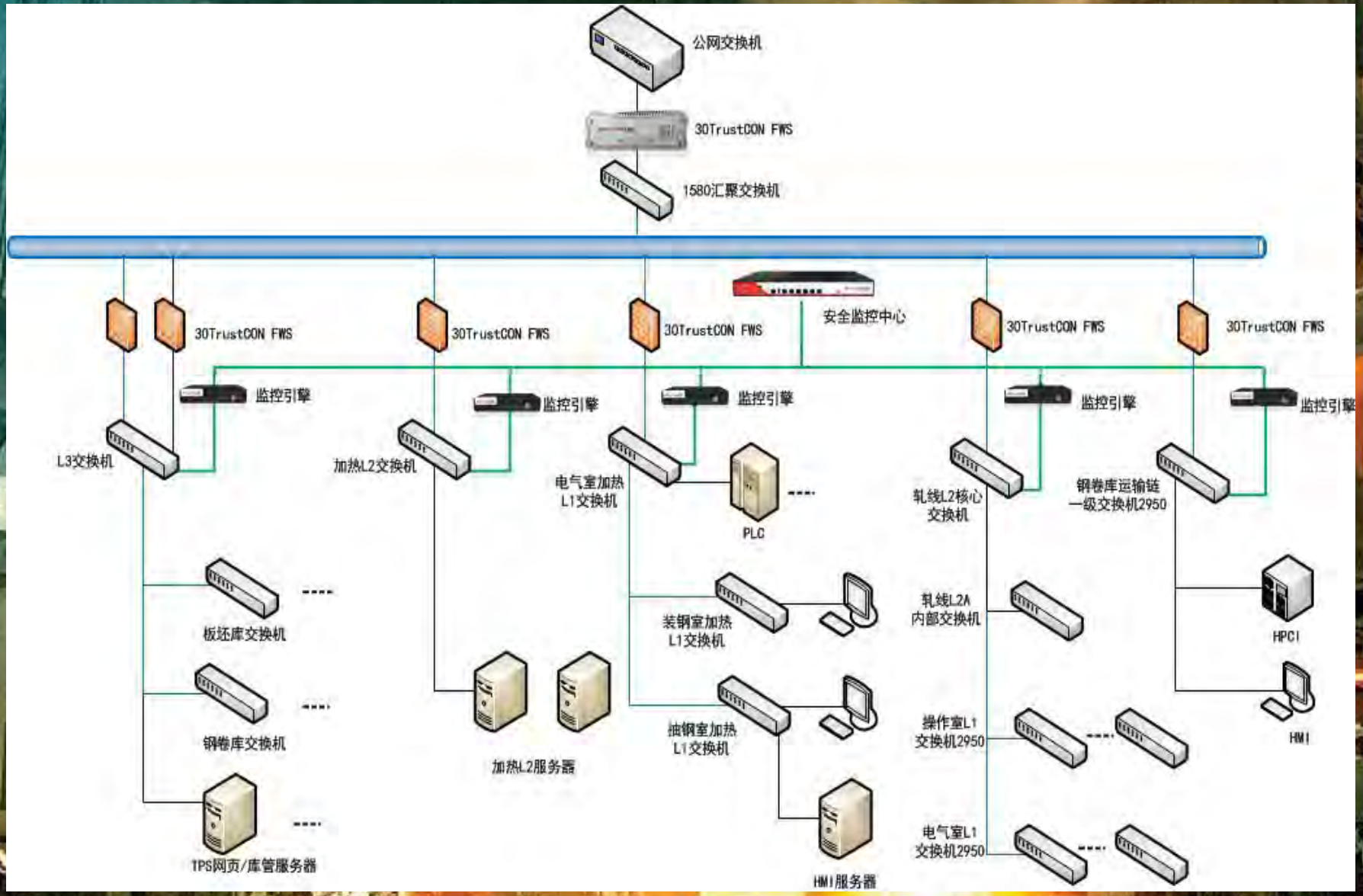
钢铁

控制网与企业公网间的通信数据需要过滤，防止病毒、恶意代码传入、防止内网敏感信息外泄。

控制网内部关键服务器间通信需要监控与过滤，保证关键服务器正常运行。

控制网内部各业务系统间通信数据需要监控，防止控制网内病毒、恶意代码的传播，并及时告警、定位。

控制网需要监控，防止非授权设备连入网络，并及时报警

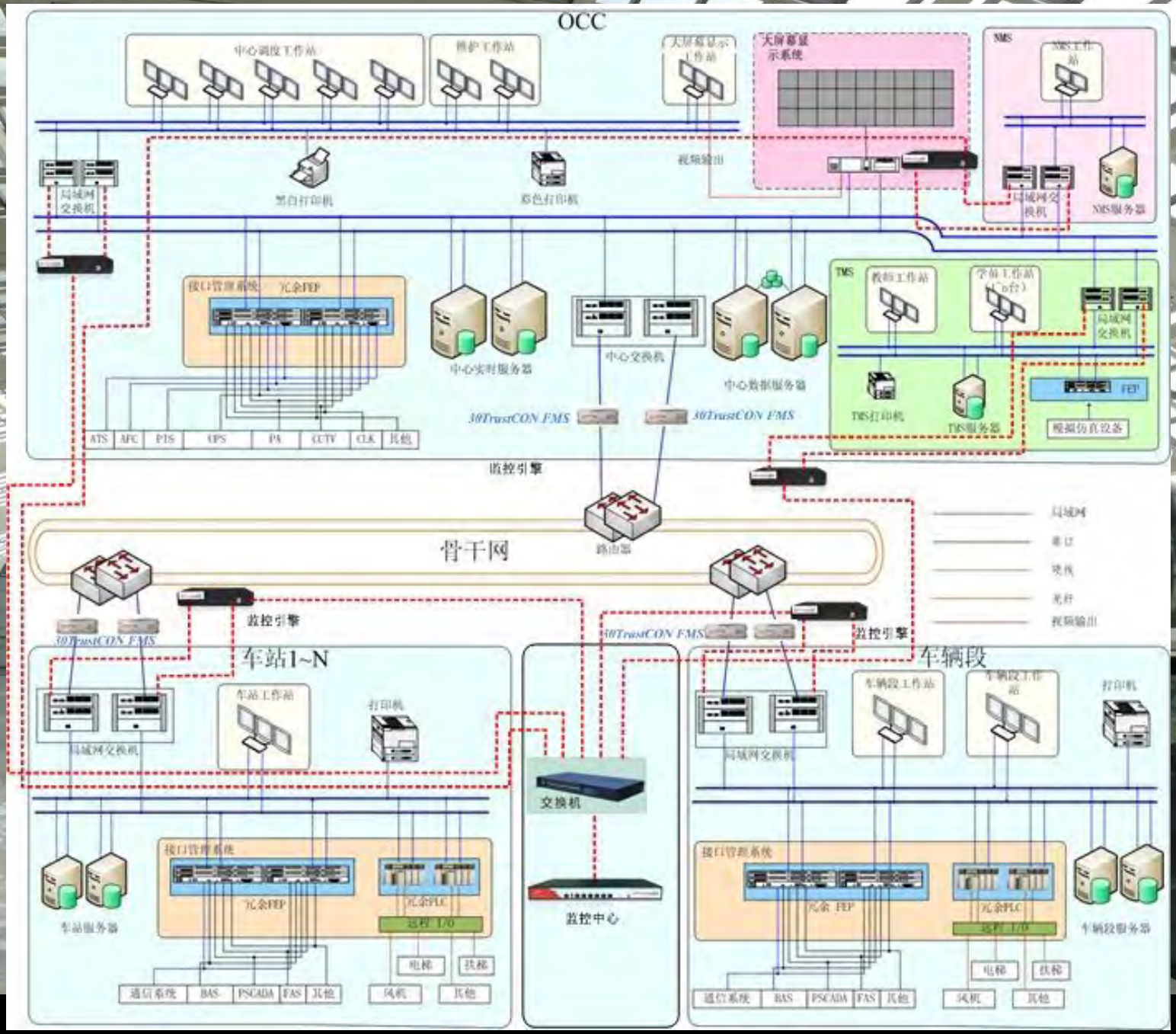

公网交换机
30TrustCON FWS
1580汇聚交换机
30TrustCON FWS
30TrustCON FWS
30TrustCON FWS
安全监控中心
30TrustCON FWS
30TrustCON FWS
监控引擎
监控引擎
监控引擎
监控引擎
监控引擎
L3交换机
加热L2交换机
电气室加热
L1交换机
PLC
轧线L2核心
交换机
钢卷库运输链
一级交换机2950
板坯库交换机
装钢室加热
L1交换机
轧线L2A
内部交换机
HPCI
钢卷库交换机
加热L2服务器
油钢室加热
L1交换机
操作室L1
交换机2950
HMI
TPS网页/库管服务器
HMI服务器
电气室L1
交换机2950

轨交

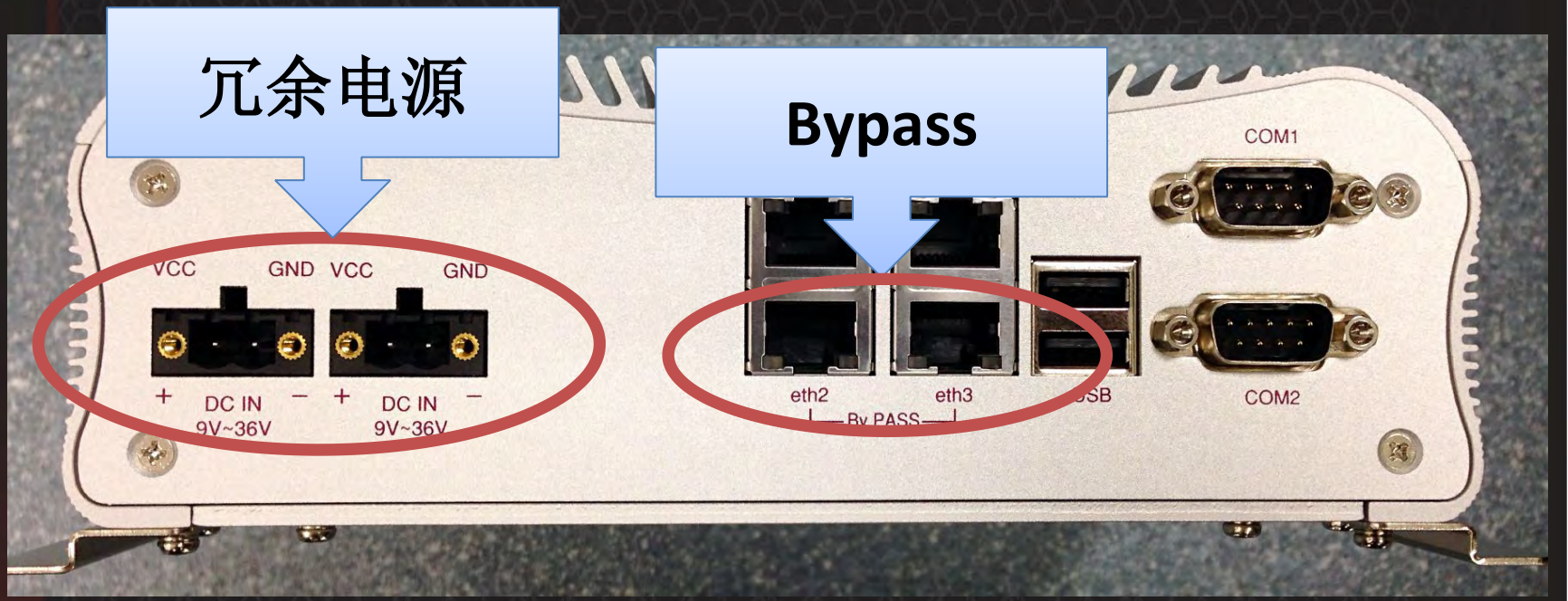
网络层次结构复杂，各子网边界划分不清，极易遭受跨网攻击入侵，使得ATC（列车自动控制）、电力SCADA系统、门禁系统等核心设备暴露于危险境地；

信息网络与控制网络集中管理，通信协议、接口等类型众多导致互联关系复杂，极易出现安全事故的连锁反应，信息系统的安全问题可能会波及其它重要子系统；

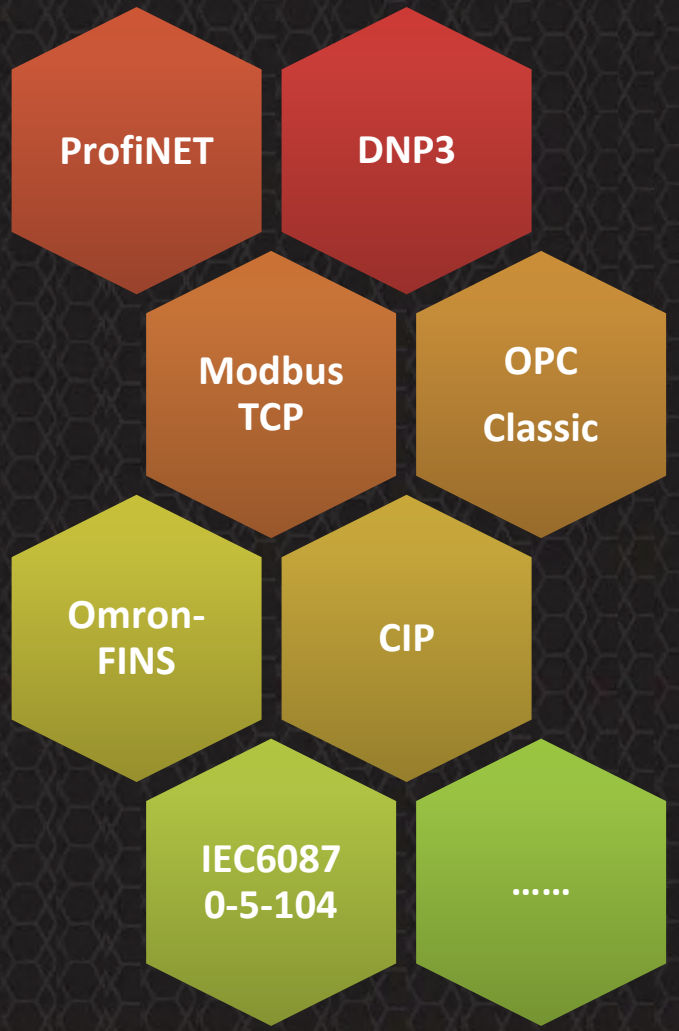
工控信息安全防护措施不到位，由于传统信息安全手段都是基于TCP/IP协议的，面对工控类病毒攻击时形同虚设


OCC
中心调度工作站
维护工作站
大屏幕显示工作站
大屏幕显示系统
NMS
NMS工作站
局域网交换机
黑白打印机
彩色打印机
视频输出
NMS服务器
接口管理系统
冗余FEP
中心实时服务器
中心交换机
中心数据服务器
TMS
教师工作站
学员工作站（n台）
FEP
TMS打印机
TMS服务器
模拟仿真设备
ATS
AFC
PIS
UPS
PA
CCTV
CLK
其他
30TrustCON FMS
监控引擎
骨干网
路由器
局域网
串口
光纤
视频输出
车站1~N
车站工作站
打印机
车站服务器
冗余PLC
远程 I/O
电梯
扶梯
通信系统
BAS
PSCADA
FAS
风机
交换机
监控中心
车辆段
车辆段工作站
车辆段服务器

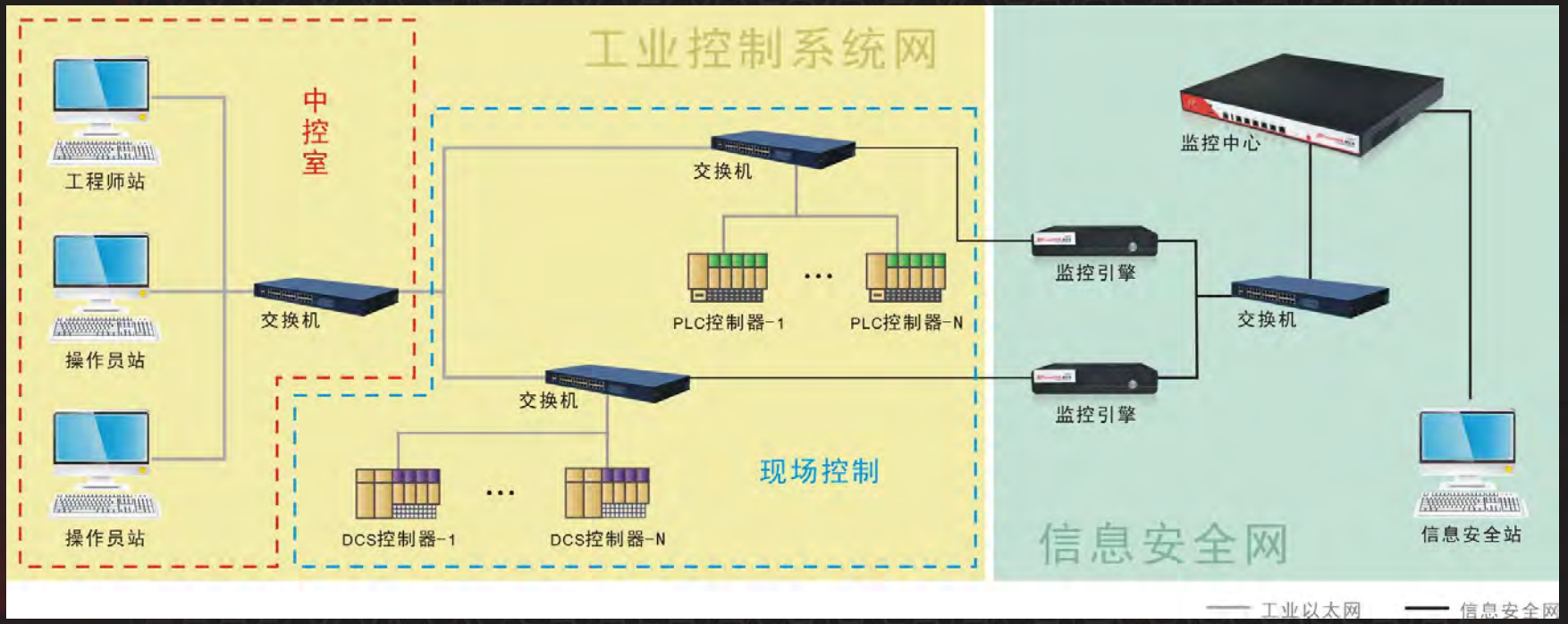
高可用


冗余电源
Bypass
VCC
GND
VCC
GND
+
DC IN
−
9V~36V
+
DC IN
−
9V~36V
eth2
eth3
By PASS
COM1
COM2

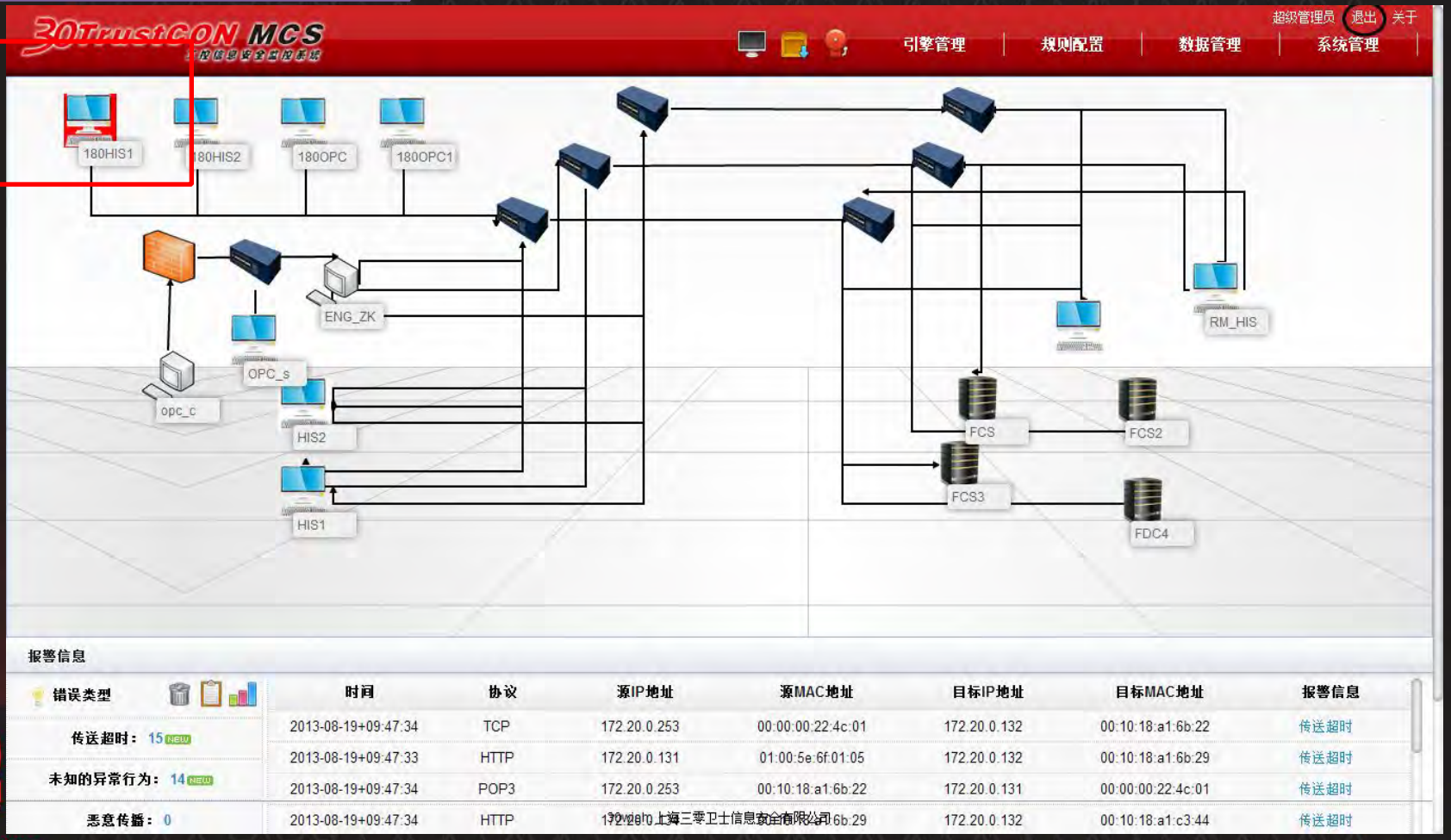
工业协议


ProfiNET
DNP3
Modbus TCP
OPC Classic
Omron-FINS
CIP
IEC6087 0-5-104
……

“零”风险部署

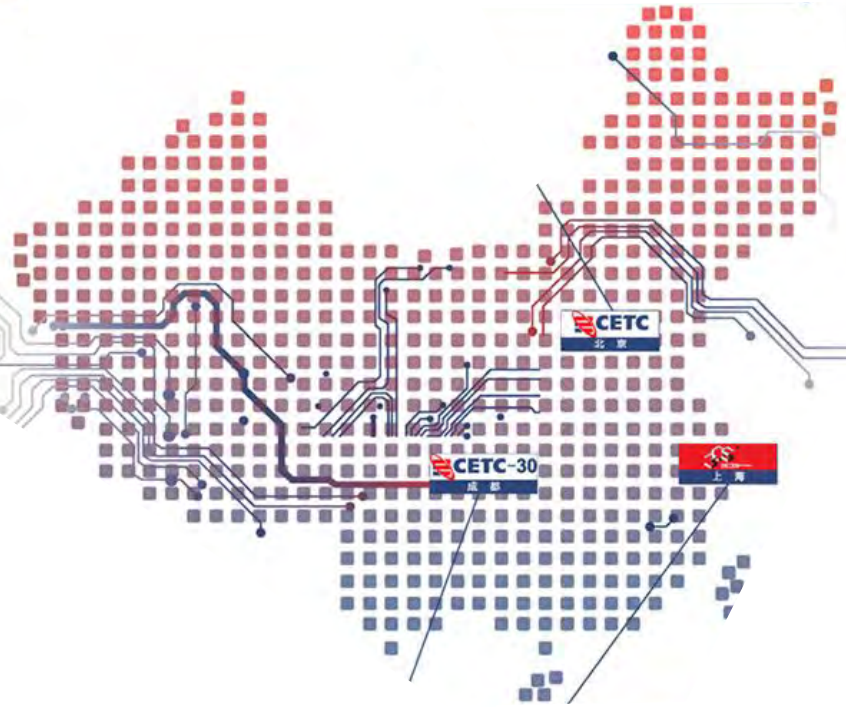

工业控制系统网
中控室
工程师站
操作员站
操作员站
交换机
交换机
PLC控制器-1
PLC控制器-N
交换机
DCS控制器-1
DCS控制器-N
现场控制
监控中心
监控引擎
交换机
监控引擎
信息安全站
信息安全网
工业以太网
信息安全网

威胁定位




生产
规范
·工艺
·生产计划
误操作
X
操作规范
·白名单
非法操作
X
操作级监测

国家利益高于一切



上海三零卫士信息安全有限公司

SHANGHAI 30WISH INFORMATION SECURITY CO.,LTD.

www.30wish.net

谢

谢