



三零卫士

30
WISH
INFORMATION SECURITY

30Eservices



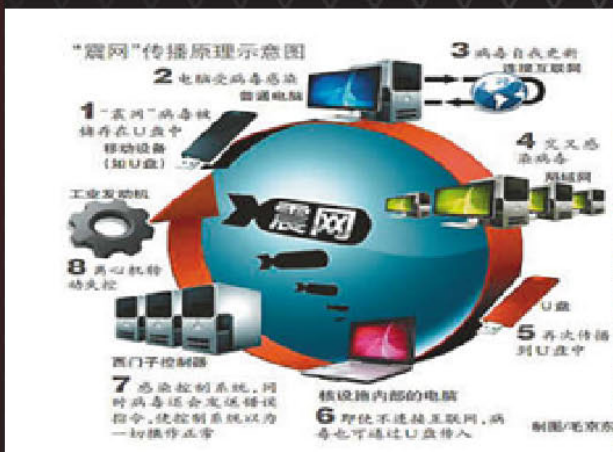
实战“固·隔·监”

工控系统信息安全定量分析方法
应用案例讲解



30
WISH
WISDOM SOFTWARE

30E-services





国务院关于大力推进信息化发展和 切实保障信息安全的若干意见 国发[2012]23号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

大力推进信息化发展和切实保障信息安全，对调整经济结构、转变发展方式、保障和改善民生、维护国家安全具有重大意义。近年来，各地区、各部门认真贯彻落实党中央、国务院决策部署，加快推进信息化建设，建立健全信息安全保障体系，有力地促进了经济社会发展。当前，世界各国信息化快速发展，信息技术的应用促进了全球资源的优化配置和发展模式创新，互联网对政治、经济、社会和文化的影响更加深刻，围绕信息获取、利用和控制的国际竞争日趋激烈，保障信息安全成为各国重要议题。但是，我国信息化建设和信息安全保障仍存在一些亟待解决的问题，宽带信息基础设施发展水平与发达国家的差距有所拉大，政务信息共享和业务协同水平不高。核心技术受制于人；信息安全工作的战略统筹和综合协调不够，重要信息系统和基础信息网络防护能力不强，移动互联网等技术应用给信息安全带来了严峻挑战。必须进一步增强紧迫感，采取更强有力的政策措施，大力推进信息化发展，切实保障信息安全。为此，提出以下意见。

工业和信息化部文件

工信部协（2011）451号

关于加强工业控制系统 信息安全管理的通知

各省、自治区、直辖市人民政府，国务院有关部门，有关国有大型企业：工业控制系统信息安全事关工业生产运行、国家经济安全和人民生命财产安全，切实加强工业控制系统信息安全管理，经国务院同意，现就有关事项通知如下：采取更强有力的政策措施，大力推进信息化发展，切实保障信息安全。为此，提出以下意见。



信息安全 对工控系统的影响

~~收入降低~~

~~违法事件~~

~~产生额外成本~~

~~违规事件~~

~~建筑和物料损失~~

~~客户不满~~

~~人身安全~~

~~负面新闻~~

~~业务停滞~~

~~引发诉讼~~





SAFTY

SECURITY

**30
WISH**

30E services



工控系统 信息安全定量分析

..... 分析范畴 ➡ 分区分域 ◀ 设备组织

等级评定和加权统计

得出切实可行的信息安全强化建议



分析范畴



网络



主机/模块



应用软件



数据和文件

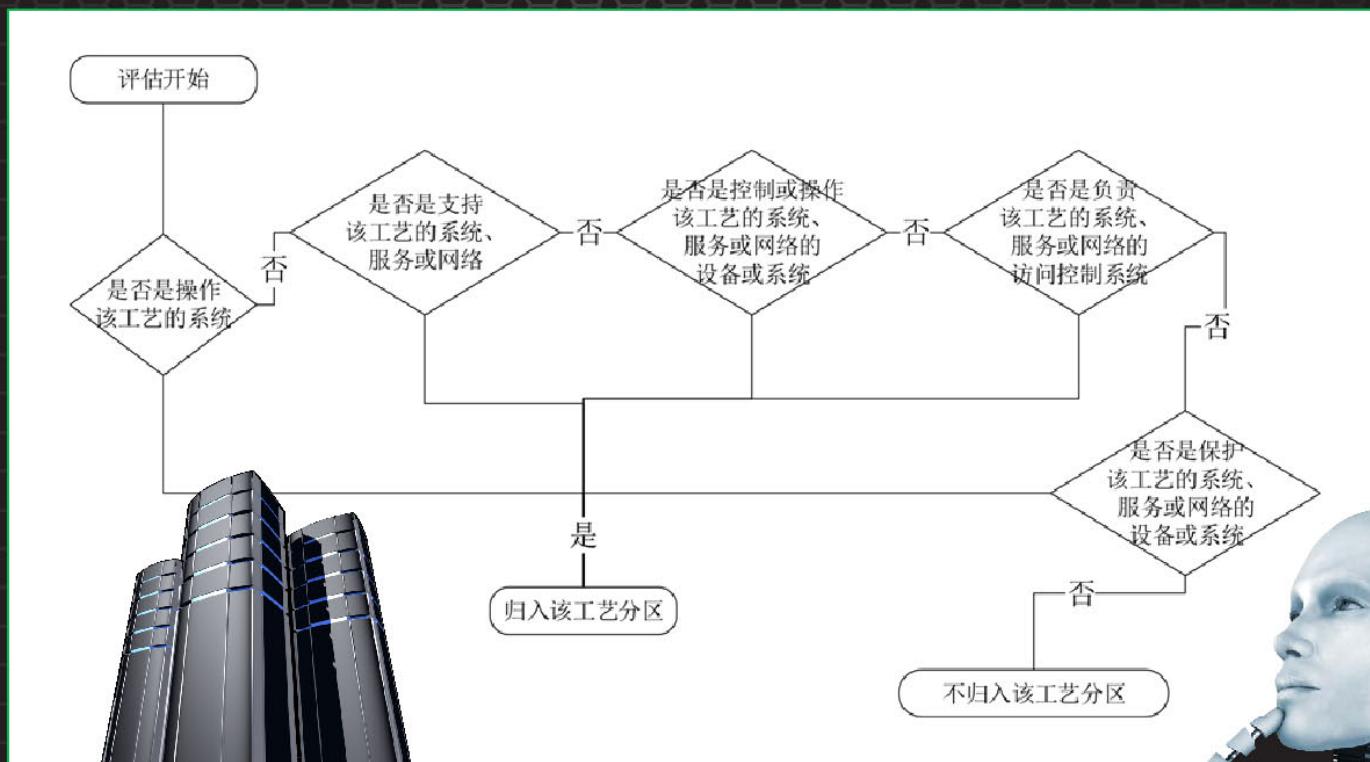


其他



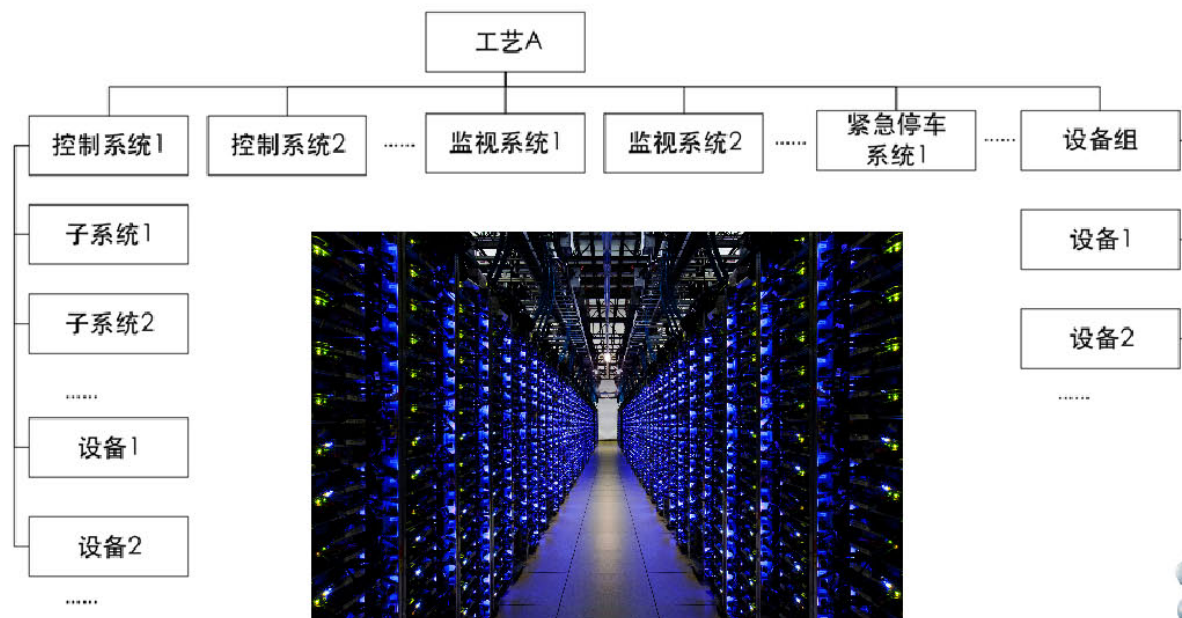


分区分域





设备组织



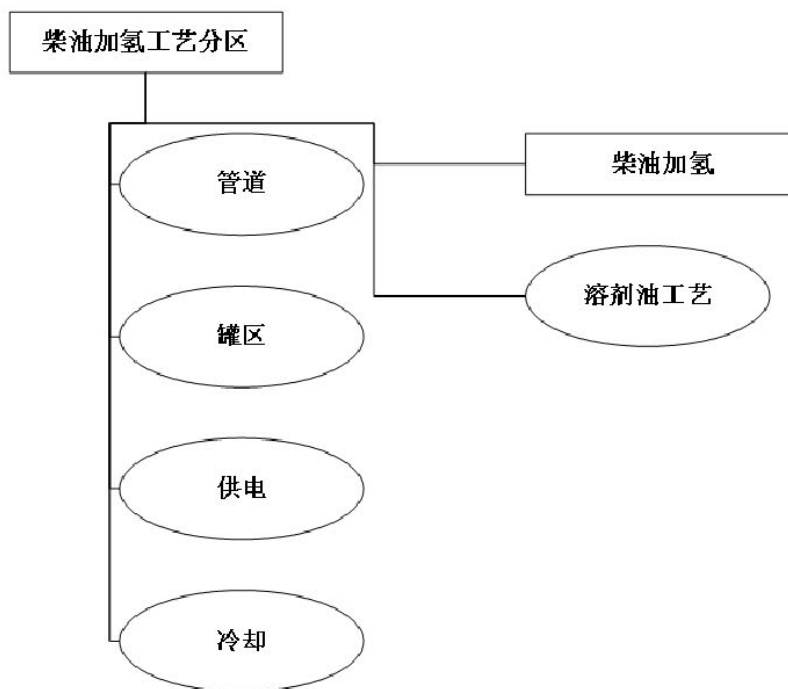


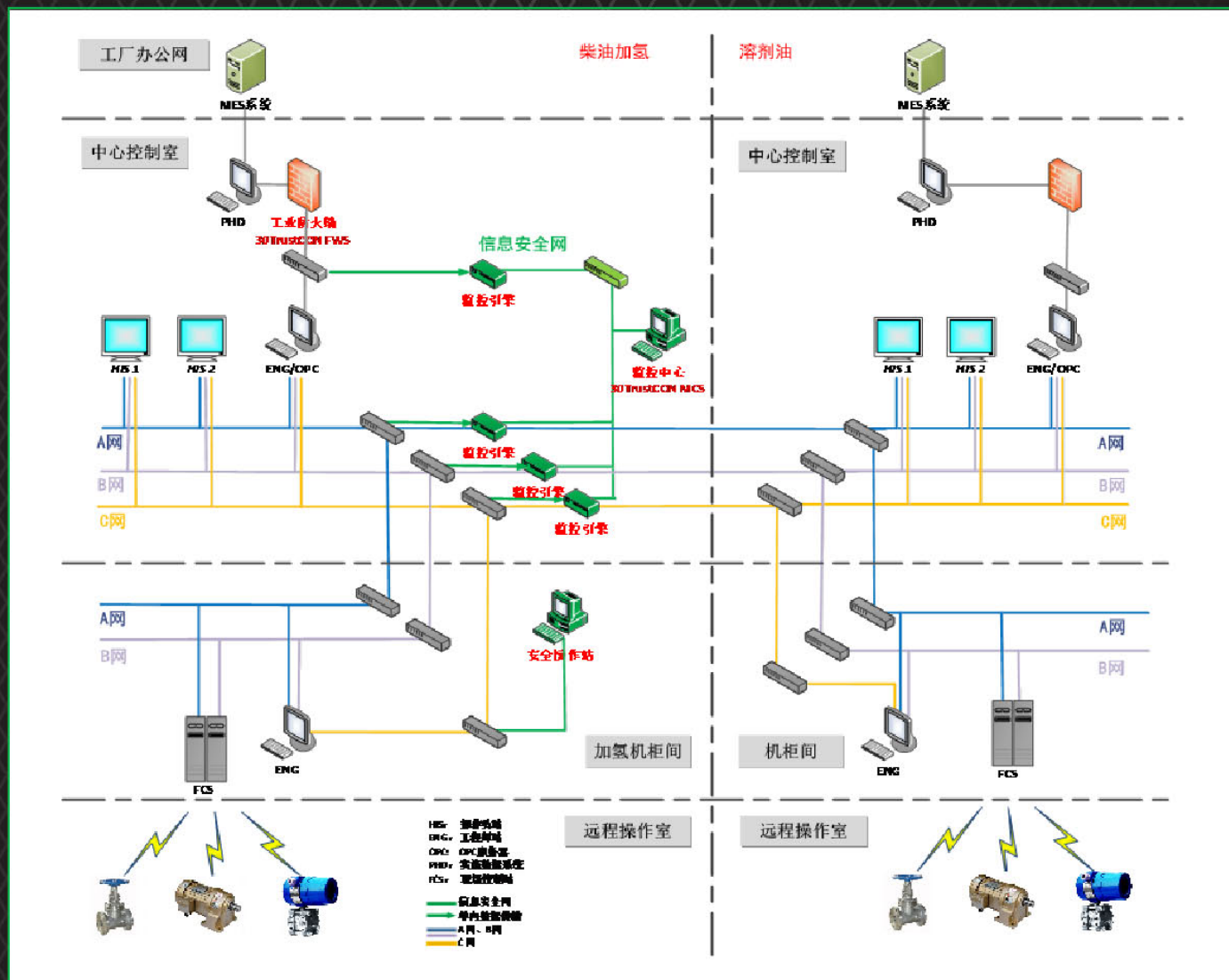
等级评定和加权统计

- 考察点：物理、网络、主机、应用、数据
- 等 级：行政、初级、中等、系统、持续改进
- 加 权：
 - ①设 备：重要性
 - ②工 艺：危险等级、工艺风险系数



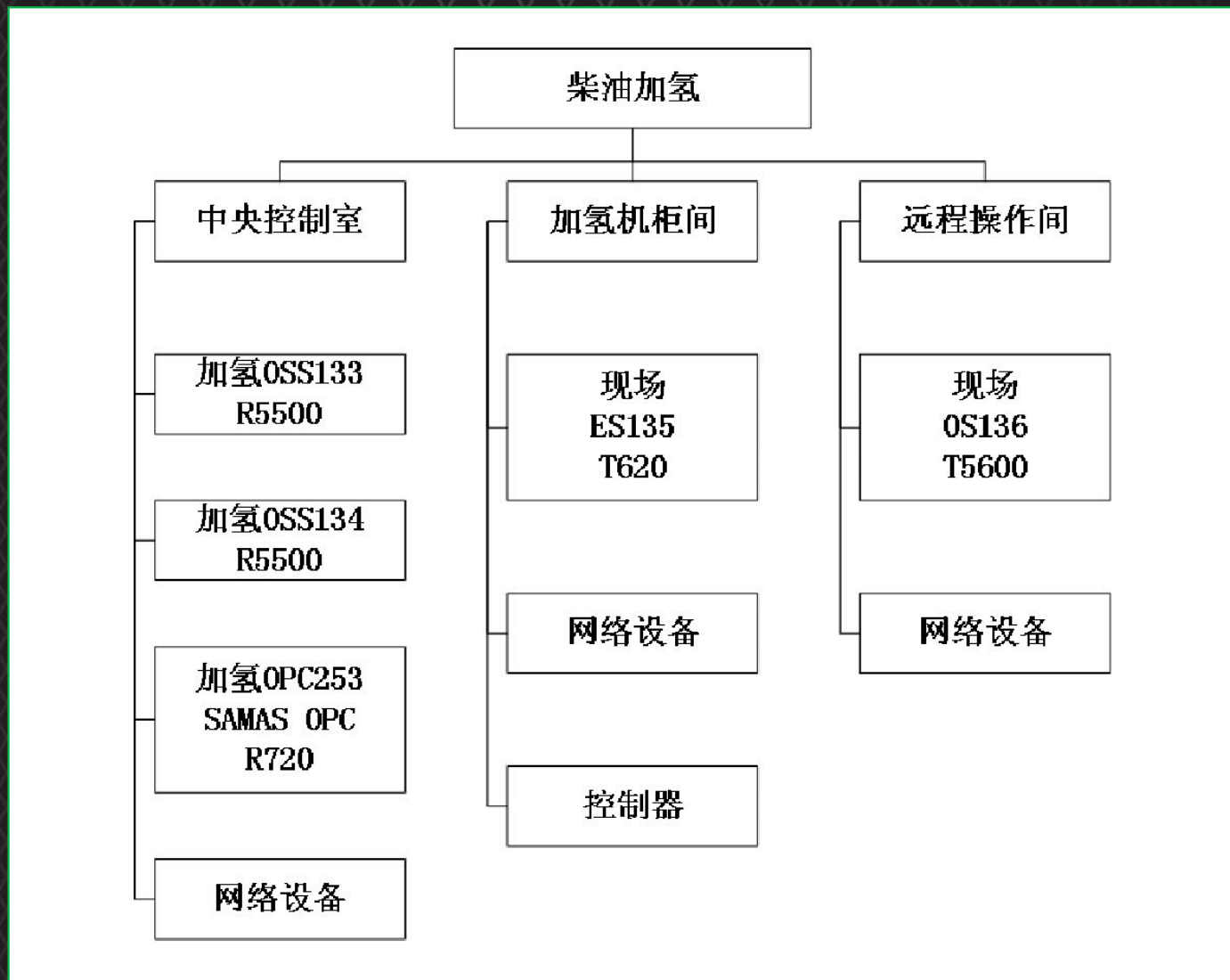
柴油加氢工艺分区

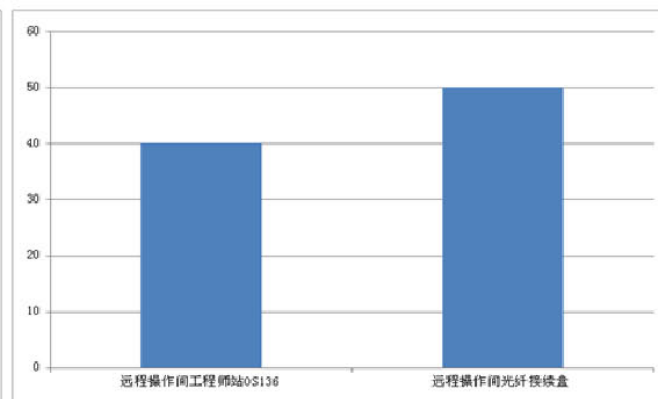
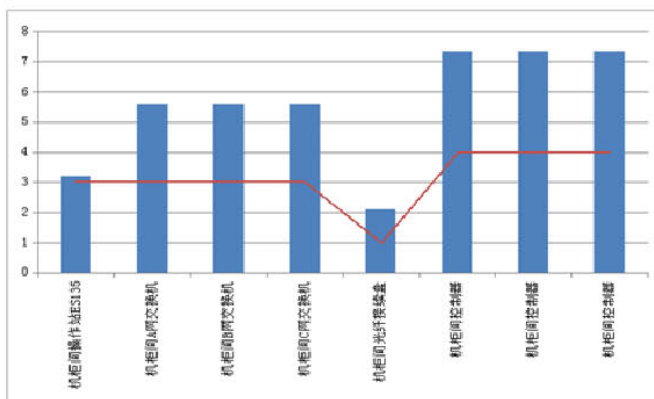
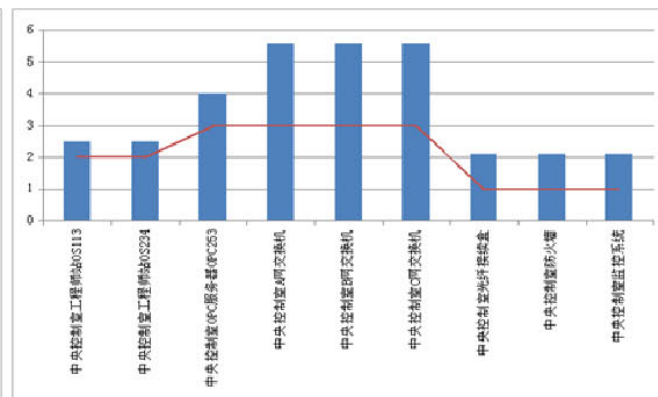
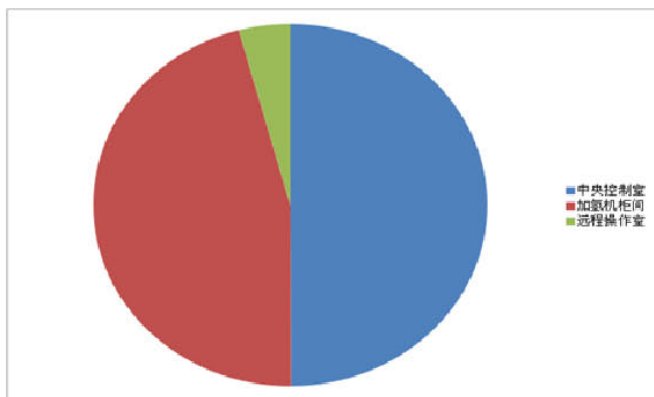




30
WISH
HYDROGENATION PLANT

30E-service





30
WISH
WISDOM COMET

30E services

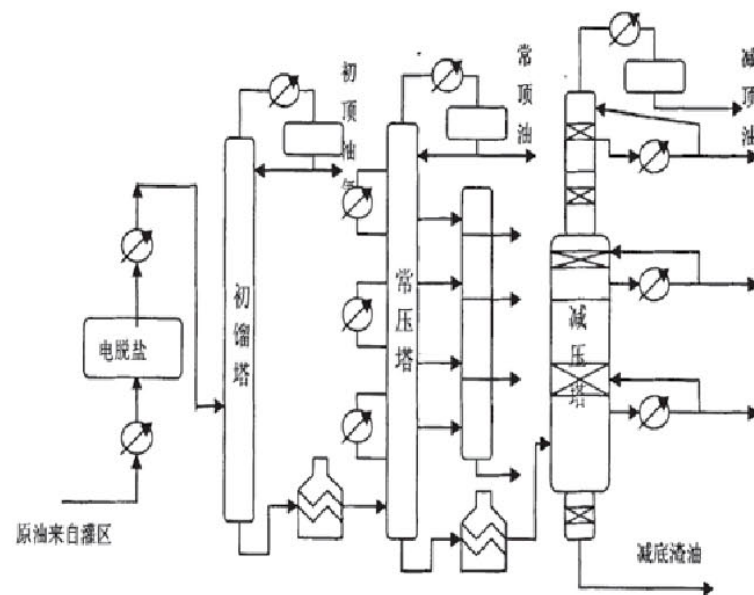


设备	物理	网络	主机	软件	数据	重要性	总分
中央控制室工程师站OS113	70	70	30	30		2	2.50
中央控制室工程师站OS234	70	70	30	30		2	2.50
中央控制室 OPC 服务器 OPC253	70	70	30	30		3	4.00
中央控制室A网交换机	70	70				3	5.60
中央控制室B网交换机	70	70				3	5.60
中央控制室防火墙	70	70				1	2.10
中央控制室监控系统	70	70				1	2.10
机柜间操作站ES135	30	70	30	30		3	3.20
机柜间A网交换机	70	70				3	5.60
机柜间B网交换机	70	70				3	5.60
机柜间控制器	70	70	30			4	7.37
机柜间控制器	70	70	30			4	7.37
机柜间控制器	70	70	30			4	7.37
远程操作间工程师站OS136	30	70	30	30		1	1.20
远程操作间光纤接续盒	30	70				1	1.50
中央控制室							32.10
加氢机柜间							29.47
远程操作室							2.70



分析结论

- 要有整体防御思想
- 做好物理安全是根本
- 网络安全是关键
- PC问题最严重





行业差异

化工：网状结构



冶金：运动控制



轨交：基于信号



核电：纵深防御



工控信息 *30TrustCON* SAS 安全评估套件

适用客户：

石化、电力、轨交、钢铁等行业客户；
主管单位及部门。

部署环境：

风险评估、安全检查及其他对标类检查。

产品作用：

无纸化办公；
规范工作流程；
提高工作效率。



30
WISH
WORKING IN THE SHIELD

30S-services



工控信息 *30TrustCON* SAS 安全评估套件

编号	名称	用 途
1	现场工作站	现场检查任务安排，数据分发
2	PAD检查工具	检查任务执行
3	设备箱	安放检查相关设备
4	USB HUB	检查设备连接
5	USB线	检查设备连接
6	便携式投影仪（可选）	会议支撑



30
WISH

30E-services



上海三零卫士 信息安全有限公司



30
WISH
INFORMATION SECURITY

30Ervision





二零卫士的工控信息安全

人大代表熊群力：将推新一代国产工业防火墙

2014年03月06日06:41 来源：人民日报  手机看新闻

打印

网摘

纠错

商城

分享

推荐

 人民微博



 关注

字号  

本报北京3月5日电 全国人大代表、中国电子科技集团公司总经理熊群力向记者透露，我国自主开发的全新一代国产工业防火墙即将推出，将为国内工业用户提供工业控制信息安全“固、隔、监”的防护体系。

据熊群力介绍，作为功能全面、安全性高的网络安全系统，这套名为二零卫士工业防火墙的新一代国产工业防火墙，采用国际上最先进的网络安全技术，是针对工控网络安全的具体应用环境完全自主开发的安全产品。工控网络安全涉及国家关键基础设施信息系统如电力、轨道交通、石油、水务等的基础网络所面临的安全问题，此前在2013年，中国电科已率先研制了两款国内首创、拥有完全自主知识产权、基于专用硬件的工业控制系统信息安全产品。

(来源:人民日报)

30
WISH

30E services



首家通过公安部 工业防火墙 测试标准符合性测试

公安部第三研究所

The Third Research Institute of Ministry of Public Security



30
WISH

30Service



工控网络的 “固” • “隔” • “监”

固：固守物理安全，稳定工控环境。

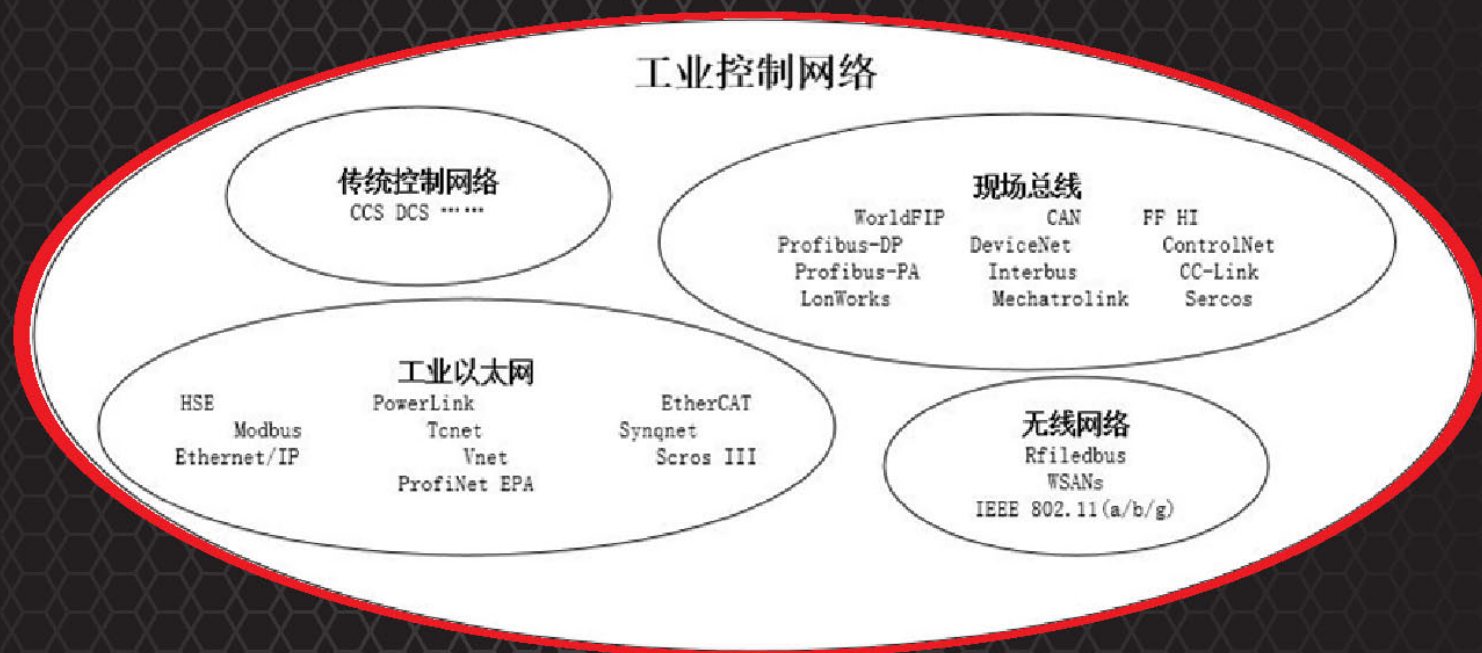
隔：网络分区之间采用防火墙产品，
净化控制流量。

监：工控网内部采用白名单审计产品，
对非法内网流量进行报警。





工控网络协议研究





“固隔监” 解决方案

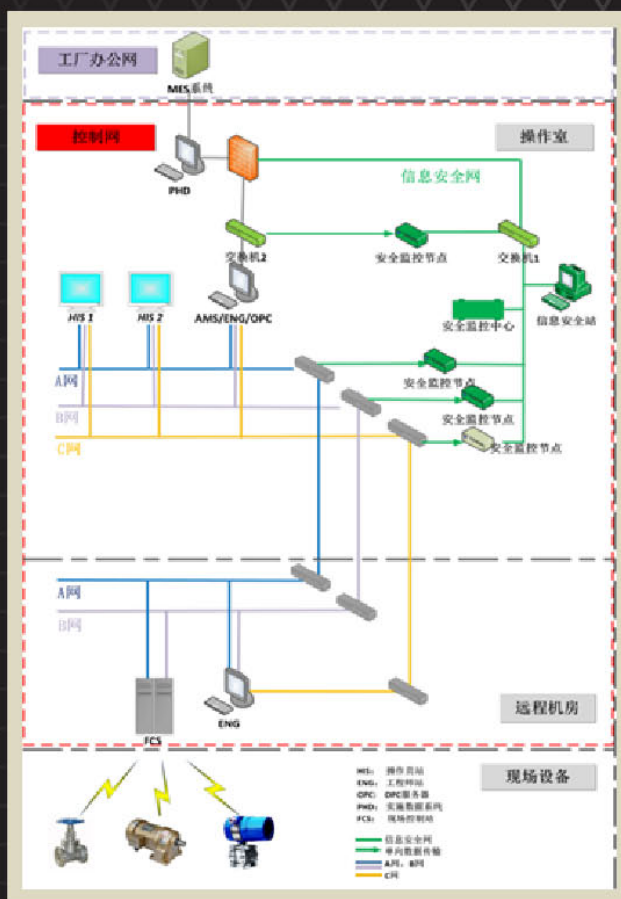
30TrustCONMO

工业控制防火墙

- 区域隔离
- 通信管控
- 传输加密
- 多种工业协议的检测与控制
- 实时报警
- 设备安全可靠

工业控制网络监控系统

- 不改变原有网络结构，对现有系统“零”影响
- 通过操作监控，设备监控，流量监控等措施，全方位掌握控制网信息安全状态。
- 及时发现并定位威胁源



30
WISH

30Service



工控信息安全系列产品

工控防火墙

30TrustCON FWS

适用行业：

核电、石化、电力、轨交、钢铁等；

部署环境：

管理网和SCADA网隔离

SCADA网络与SCADA网络之间隔离

产品功能：

阻挡针对工控系统的病毒和恶意攻击

阻挡协议探测和攻击

针对异常情况有多种应对手段

自身系统安全防护水平高



30TrustCON FWS 工控防火墙

30
WISH
WISDOMSOCIETY

30E-service



30TrustCON FWS

工控防火墙

配置页 帮助

修改密码

提交配置

网络配置

保存配置

帮助帮助

安全退出

系统导航

系统配置

基本配置

管理配置

系统维护

系统时间

工具箱

网络配置

资源配置

证书管理

用户认证

防火墙

流量控制

虚拟专用网

高可用性

日志与监控

工业协议

入侵防御

基本信息

设备名称

设置设备名称，用于识别设备。

请填入设备名称：

工控网

设置设备名称：

确定

设备基本信息

显示设备基本信息，包括CPU占用率、磁盘占用率、内存占用率、序列号和固件版本等信息。

信息类别	设备状态
CPU占用率	0%
磁盘占用率	38.17%(1503MB / 5020MB)
内存占用率	6.79%(132MB / 1940MB)
设备时间	2014-03-18 09:29:15
运行时长	0天19时11分29秒
序列号	2009270041
固件版本	102-0.1
设备健康度	29

刷新

操作模式



工控信息安全监控系统

30TrustCON MCS

适用行业:

石化、电力、轨交、钢铁等;

部署环境:

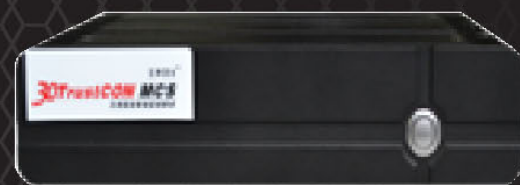
过程控制系统、SCADA控制系统等的控制室;

产品功能:

违规设备监控;

违规网络行为监控 (如震网、蠕虫);

违规操作行为监控。



30TrustCON MCS监控引擎



30TrustCON MCS监控中心

30
WISH

30WISH



工控信息安全监控系统

30TrustCON MCS

三零安全监控装置

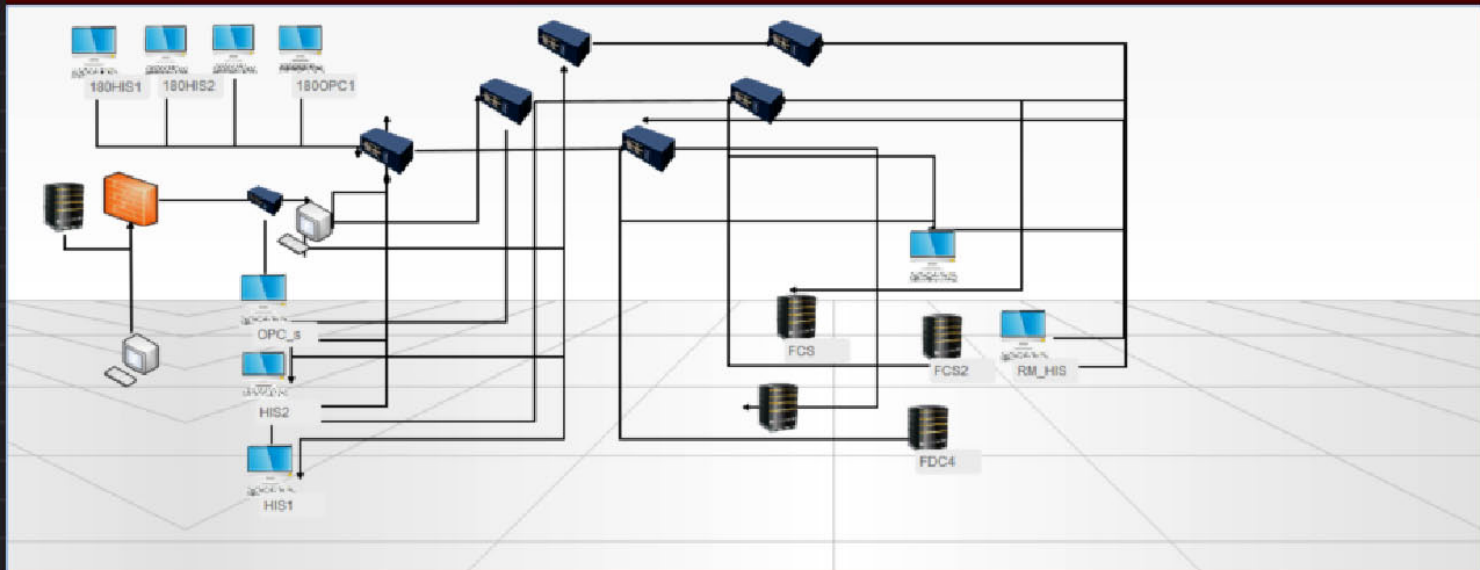
引擎管理

规则配置

数据管理

系统管理

超级管理员 修改密码 退出 关于



报警信息

错误类型	时间	协议	源IP地址	源MAC地址	目标IP地址	目标MAC地址	报警信息
未知设备: 51	2014-02-14+09:30:25	SMTP	10.10.1.4	00:e0:1c:3c:17:c2	74.53.140.153	00:1f:33:d9:81:60	未知设备
恶意传播: 0	2014-02-14+09:30:25	SMTP	10.10.1.4	00:e0:1c:3c:17:c2	74.53.140.153	00:1f:33:d9:81:60	未知设备
未授权协议: 0	2014-02-14+09:30:25	SMTP	10.10.1.4	00:e0:1c:3c:17:c2	74.53.140.153	00:1f:33:d9:81:60	未知设备

30
WISH

30S-privacy



工控信息安全的重要意义

包拯说

工控信息安全绝不是杞人忧天，
当今网络世界，威胁无处不在。
防范势在必行啊！
工控信息安全乃是未雨绸缪亦，
智者慧眼识先机！
工控信息安全最好不要亡羊补牢。
切莫千里之堤毁于蚁穴亦！





谢谢观阅

30
WISH
INFORMATION SECURITY

30services