CEC 中国电子 第六研究所

CEC 中国电子

工业控制系统等级保护测评实践

中国电子信息产业集团有限公司第六研究所

工业控制系统信息安全技术国家工程实验室

王绍杰 15811031546

邮箱：hellosys@126.com

思考

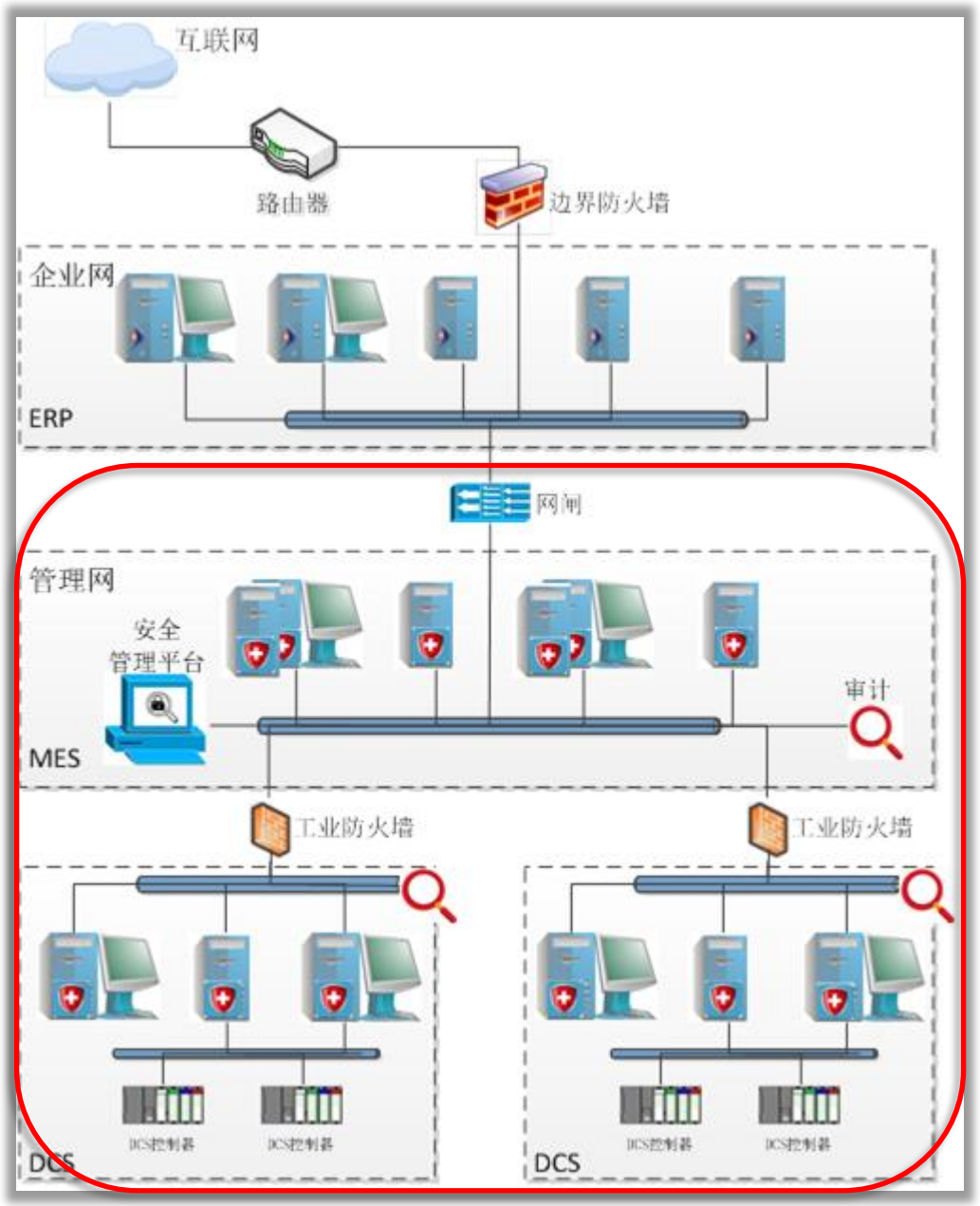
工控系统和IT系统有哪些不同?

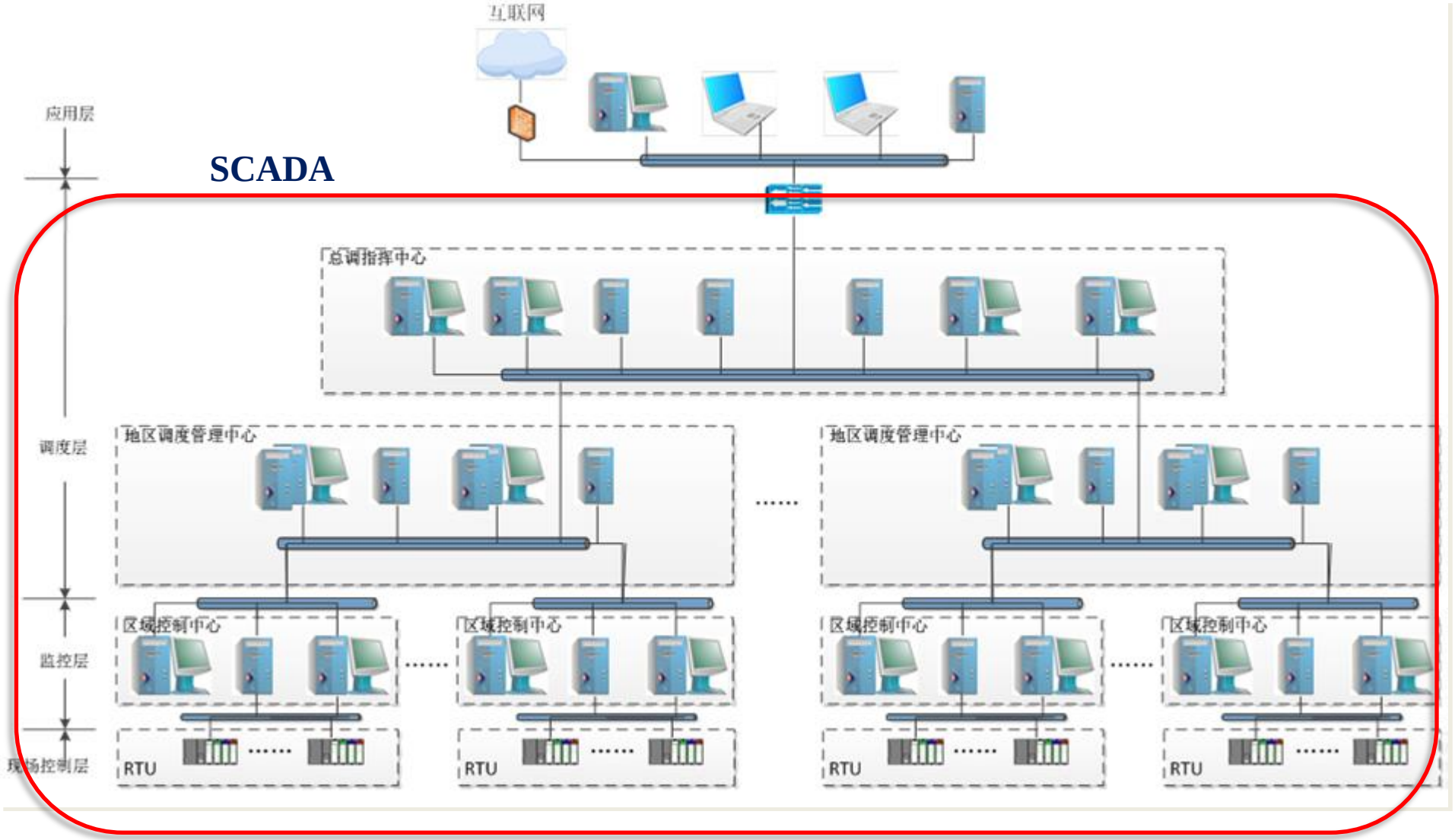
对比维度	IT系统	工控系统
体系结构	扁平化，节点间对等关系	纵向高度集成，节点间主从关系
网络边缘	边缘是智能终端	边缘是功能单一的采集和控制节点
可用性	关注保密性、完整性、可用性	更关注可用性
性能需求	允许短时业务中断和重启，高延时和抖动可接受	不允许业务中断，高延时和抖动不能接受
人机交互	紧急的交互不太重要，可实施严格限制的访问控制	紧急的交互很重要，应严格控制对ICS的访问，但不妨碍人机交互
用户认识	普遍容易接受	与外网物理隔离，不存在受到攻击等错误认识

工控系统分层怎么划分?

典型的工控系统包括现场设备层、现场控制层、过程监控层、制造执行系统（MES）层、企业管理层和外部网络。

可以看出工控系统纵向高度集成。



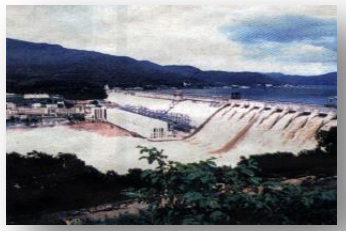

互联网
应用层
SCADA
总调指挥中心
地区调度管理中心
地区调度管理中心
调度层
区域控制中心
区域控制中心
区域控制中心
区域控制中心
监控层
RTU
RTU
RTU
RTU
现场控制层

物理位置分散


工控系统网络安全现状
测评实践
问题与建议

工控系统的重要性

- 能源的产生　水、煤、气、油、风、太阳能、核
- 能源的输送　电、气、油
- 能源的分配　电、水
- 过程工业　食品、药品、冶金、玻璃、水泥、石油和天然气、精炼、化工
- 制造业　机械加工、汽车生产线、电子柔性生产线、…
- 交通　地铁、城铁、高铁、公交、汽车、轮船、飞机、…
- 国防军工　武器装备、舰船、火箭、卫星、…
- 仓储　仓库、港口、物流、邮包包装、识别





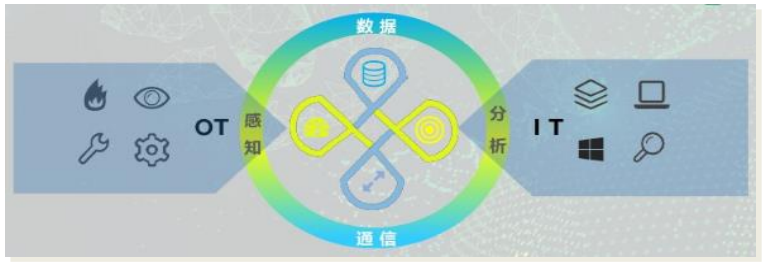

工控安全的驱动因素

合规-避免违规

外部因素

数字化转型-提升工控安全

技术融合：OT+IT+智能化



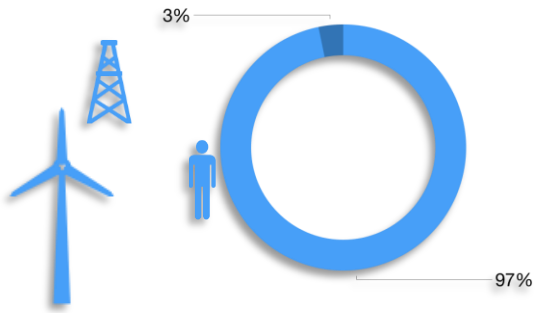
责任与义务-各司其职

- 设计单位
- 设备厂商
- 施工单位
- 运营单位

内部因素

缺少专业人才-安全运维

培训
安全解决方案

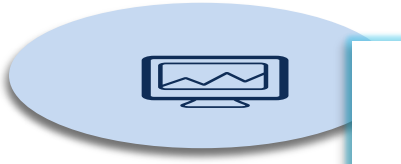


工控系统面临的威胁

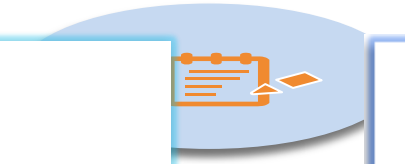
病毒木马

不恰当的操作

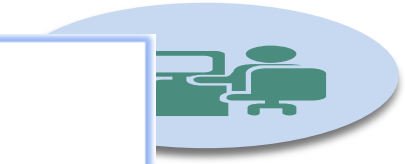
不安全的通信接入



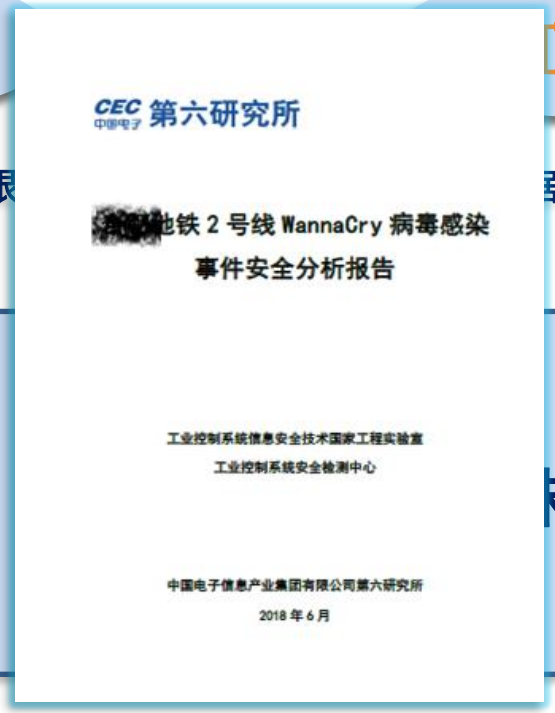
截获控制权限



据监听及篡改



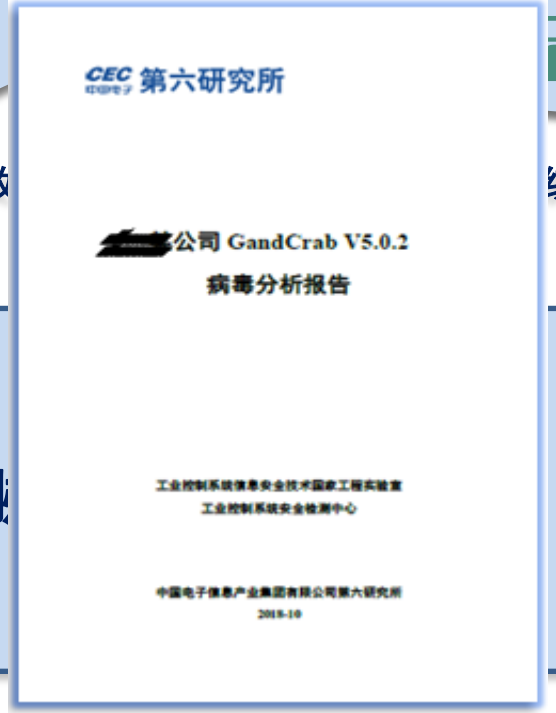
统漏洞被利用


CEC 第六研究所

[redacted]地铁 2 号线 WannaCry 病毒感染事件安全分析报告

工业控制系统信息安全技术国家工程实验室
工业控制系统安全检测中心

中国电子信息产业集团有限公司第六研究所
2018 年 6 月


CEC 第六研究所

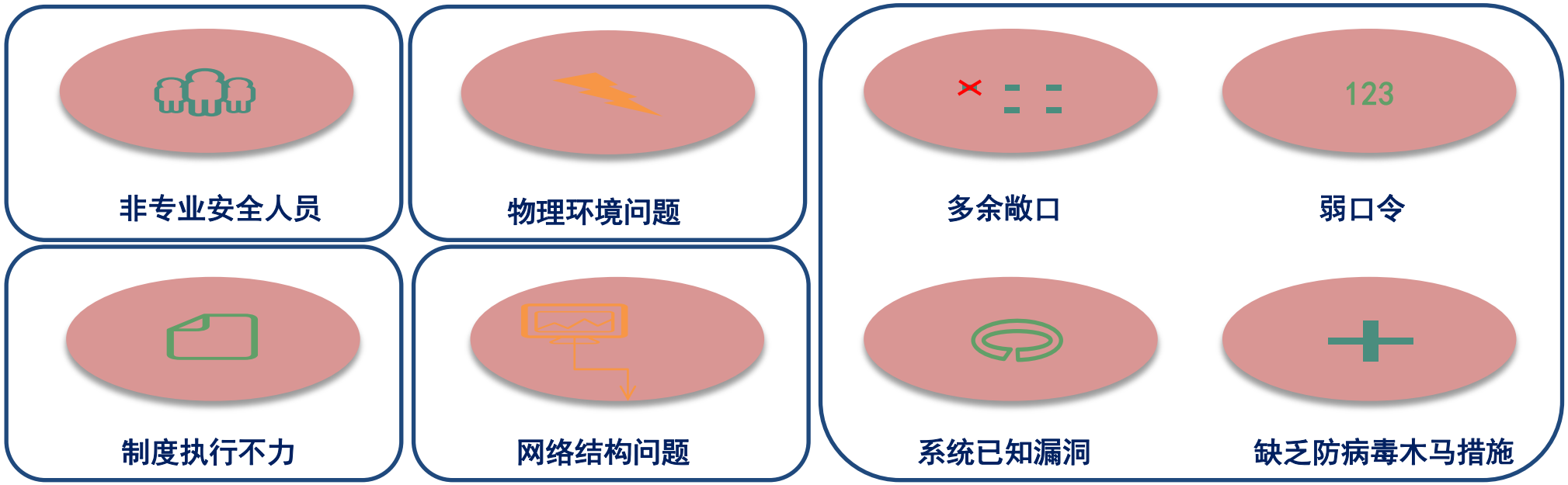
[redacted]公司 GandCrab V5.0.2 病毒分析报告

工业控制系统信息安全技术国家工程实验室
工业控制系统安全检测中心

中国电子信息产业集团有限公司第六研究所
2018-10

卡知威胁

工控系统存在的脆弱性



“未知”漏洞

工控系统故障后的危害

工控安全事件导致的危害

01 **危及国家安全及人民生活**
国防军工、航空航天、能源、交通、水利等

02 **环境灾难**
污染物排放

03 **人员伤亡**
人身严重伤害甚至死亡

04 **破坏国家基础设施**
造成国防军工、能源、交通、水利等基础设施的破坏

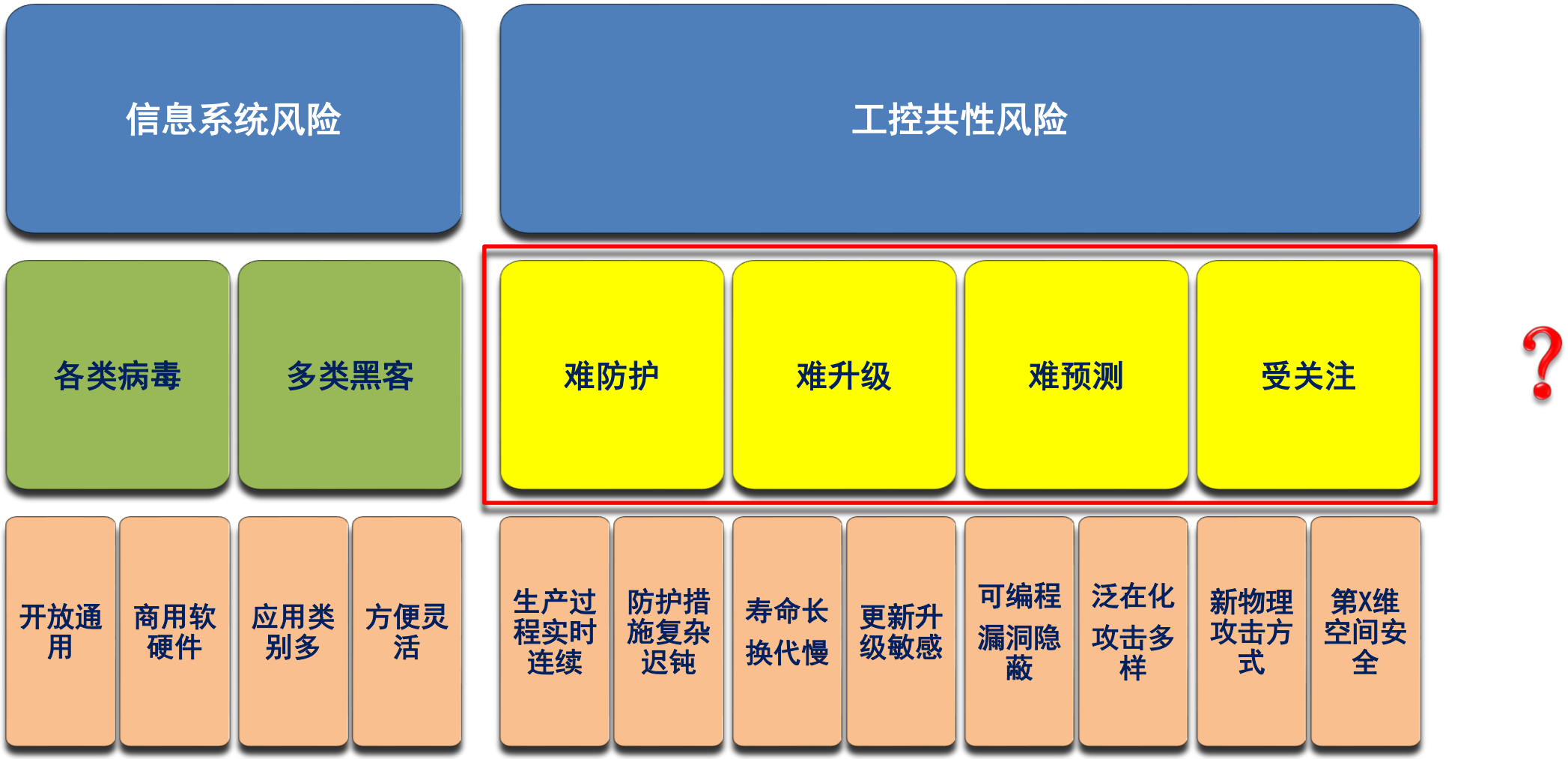
05 **严重的经济损失**
生产停止、财产损失

06 **设备失控或受损**
生产设备失控或受损

07 **关键数据被窃取、篡改或丧失**
关键数据、配方及控制程序遭窃取或清除，关键参数及程序遭篡改

08 **系统性能下降，影响系统可用性**
系统响应变慢，甚至造成“死机”、“瘫痪”

工控系统的安全需求


信息系统风险
工控共性风险
各类病毒
多类黑客
难防护
难升级
难预测
受关注
开放通用
商用软硬件
应用类别多
方便灵活
生产过程实时连续
防护措施复杂迟钝
寿命长换代慢
更新升级敏感
可编程漏洞隐蔽
泛在化攻击多样
新物理攻击方式
第X维空间安全


工控系统网络安全现状
测评实践
问题与建议

系统定级

保护对象是什么?

“突出重点、保护重点”

等级如何确定?

- **国标**
- **行业定级指南**
- **企业定级指导意见**

（不遗漏、不过度）

电力

石化&
化工

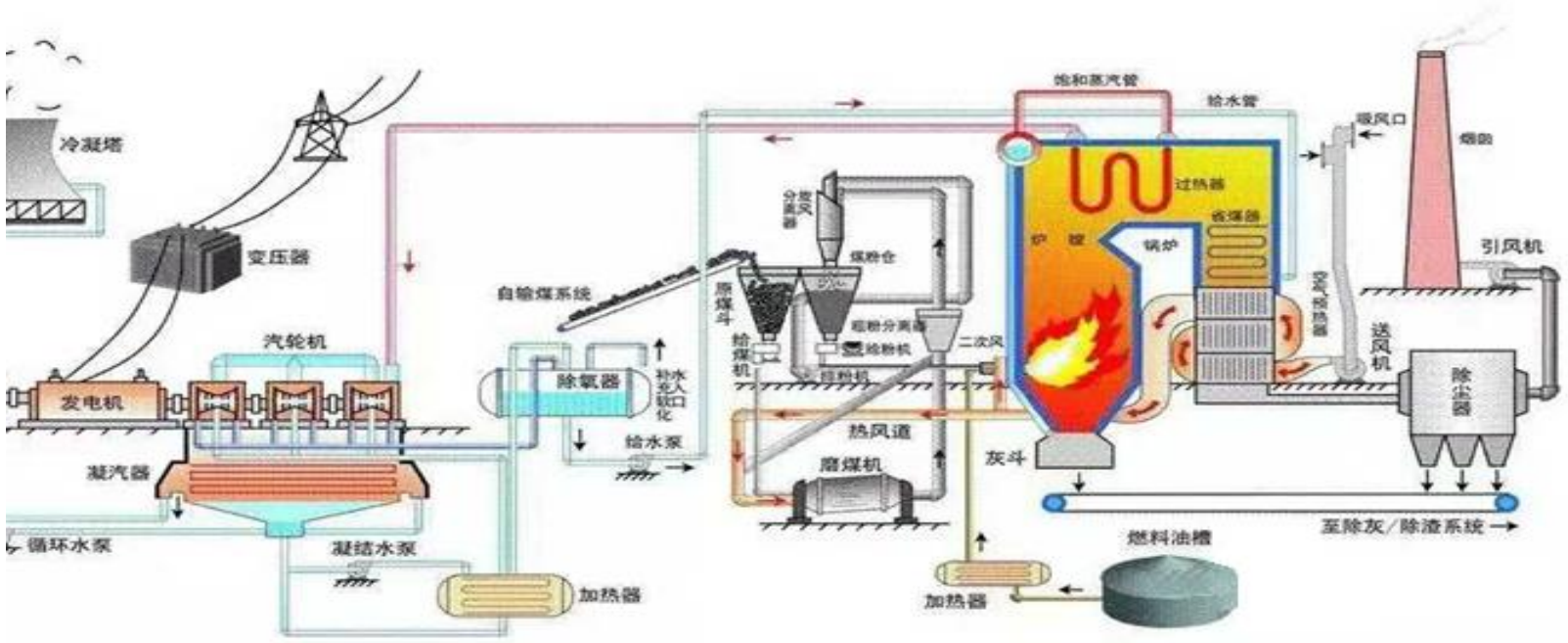
国防科技
工业

煤炭

轨道
交通

市政

关注
可用性



■ 经验分享

以某电厂DCS系统（含辅控）等保测评为例，分享电子六所等保测评经验。

测评实践-信息收集

■ 信息收集

《系统调研表》重点关注的几个方面：

（1）安全组织结构

✓ 摸清负责网络安全工作的领导，组织分工、人员职责

（2）网络结构

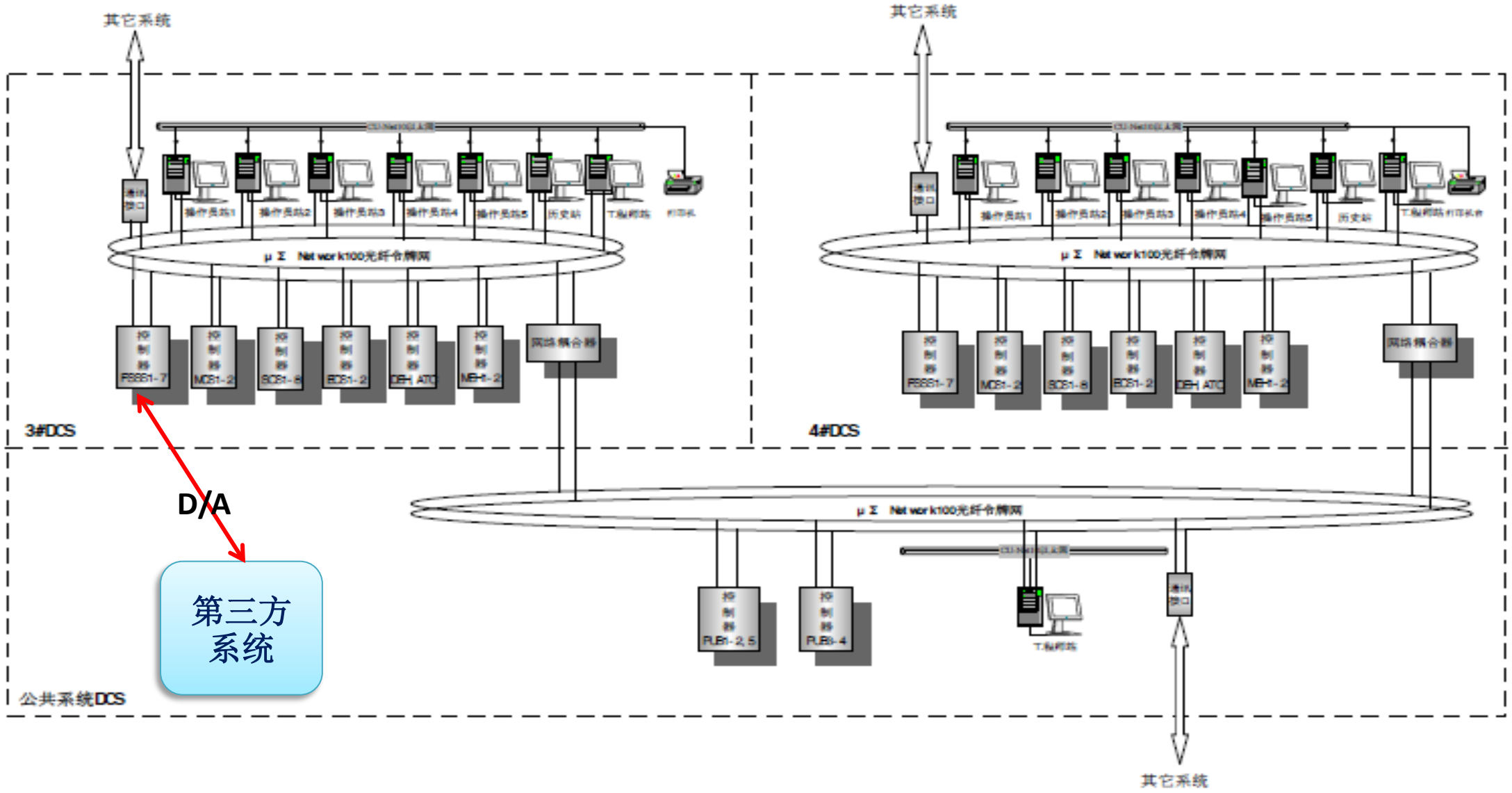
✓ 摸清系统边界（包括第三方边界）

✓ 摸清边界通信方式

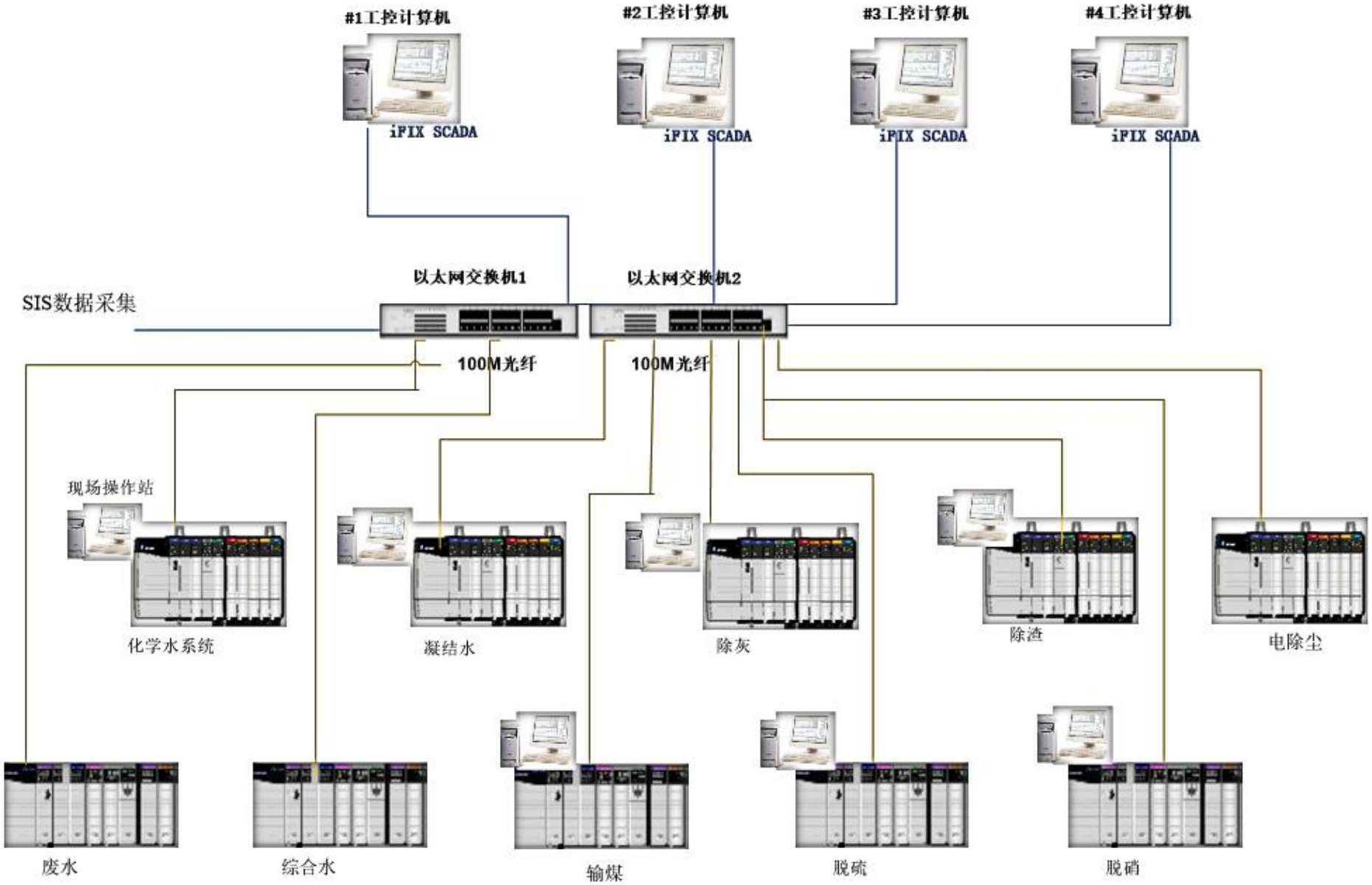
（3）资产清单

✓ 控制系统软件版本、控制器型号

测评实践-网络结构分析


其它系统
其它系统
μΣ Network100光纤合牌网
μΣ Network100光纤合牌网
3#DCS
4#DCS
D/A
第三方
系统
μΣ Network100光纤合牌网
公共系统DCS
其它系统

测评实践-网络结构分析


#1工控计算机
#2工控计算机
#3工控计算机
#4工控计算机
iFIX SCADA
iFIX SCADA
iFIX SCADA
iFIX SCADA
以太网交换机1
以太网交换机2
SIS数据采集
100M光纤
100M光纤
现场操作站
化学水系统
凝结水
除灰
除渣
电除尘
废水
综合水
输煤
脱硫
脱硝

测评实践-信息收集

✓ 工控系统资产类型：

资产类别	资产类型
应用软件	组态软件（EWS）
	DCS运行软件（OWS）
操作系统及数据库	操作系统（OS）
	数据库（DB）

资产类别	资产类型
工业控制设备	可编程逻辑控制器（PLC）
	集散控制系统（DCS）

资产类别	资产类型
网络通讯设备	交换机（Switch）
	通讯协议转换器（CPC）
安全防护设备	防火墙（FW）
	加密认证设备（EAE）

资产类别	资产类型
工作站	操作员站（OPS）
	工程师站（EWS）
	接口机（IPC）
服务器	OPC服务器（OPC）

……

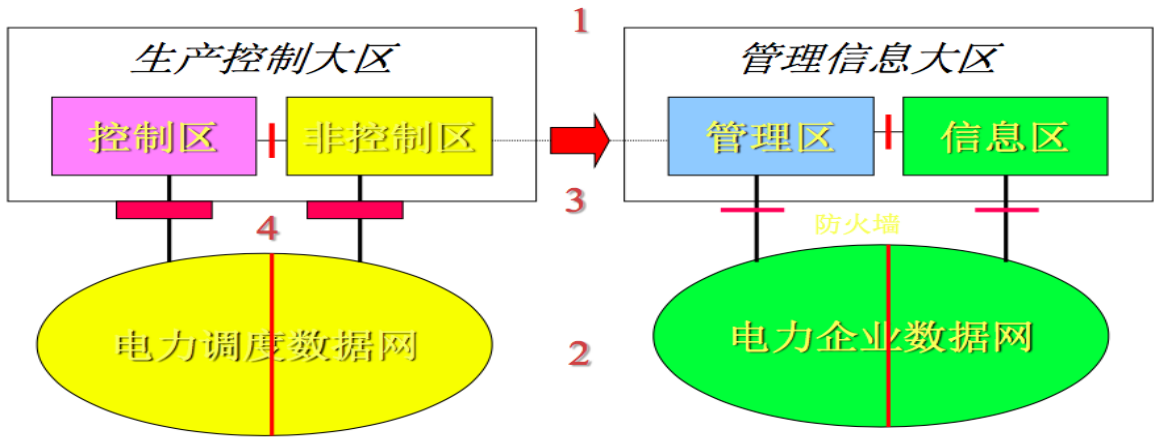
测评实践-方案编制

方案编制

总体指标 —— 行业规范

特殊指标 —— L1层及以下

应急预案 —— 风险处置



现场控制层与现场设备层设备

01 **工具测试风险**

规避措施：选择停机检修时进行

02 **验证测试风险**

规避措施：选择备机或测试环境下测试，备份、应急预案、用户监督

03 **泄露敏感信息**

规避措施：机构保密管理、保密协议

测评实践-现场实施

- 项目启动会（很重要）
- 现场实施

渗透测评	内网渗透（实验室半仿真环境、现场停机检修）
模糊测评	CRT测试平台（实验室半仿真环境、现场停机检修时）
协议健壮性测试	CRT测试平台（实验室半仿真环境、现场停机检修时）

- 项目结束会（很重要）

测评实践-标准应用

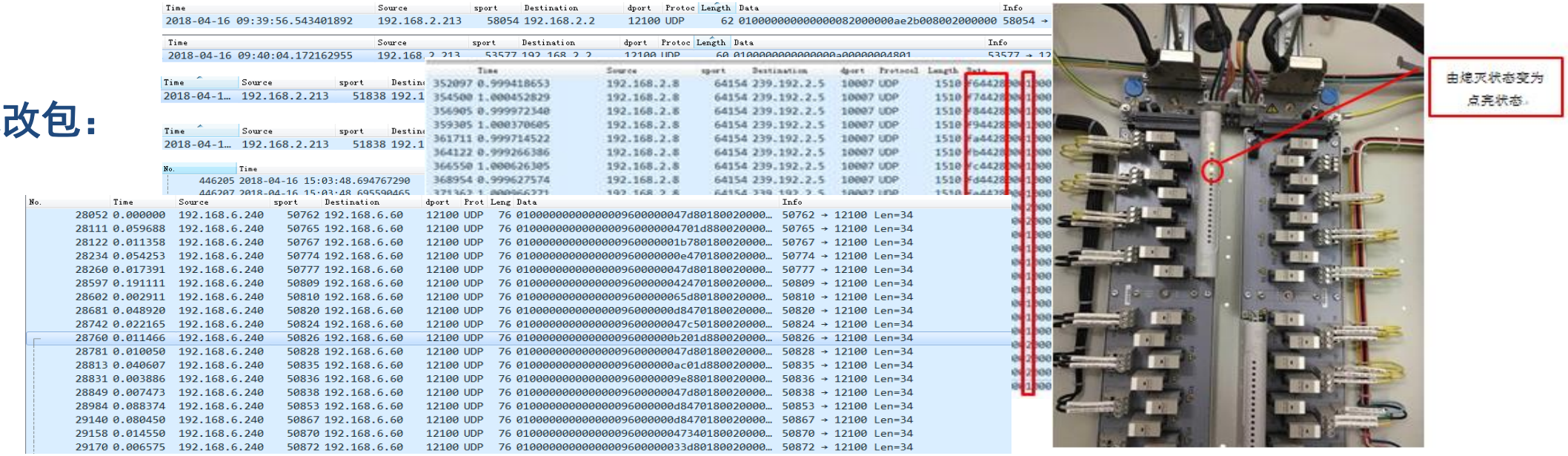
工控系统中几个关键指标如何测评?

1、通信传输

a）应采用校验码技术或密码技术保证通信过程中数据的完整性；

测评方法：抓包分析；若现场不具备工具接入条件，需要联系并调阅设备供应商的佐证材料，或者征求设备供应商的正式回复。注：私有协议≠加密

抓包改包：



测评实践-标准应用

工控系统中几个关键指标如何测评?

2、入侵防范

a）应采用技术措施**对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的分析**；

测评方法：

检测类工具（采用网络行为分析工具、应用载荷深度检测工具、溯源取证工具等）；

试验环境下利用载荷生成工具进行验证。

工控系统中几个关键指标如何测评?

3、边界防护

d) 应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。

测评方法：检查无线网络使用情况（kismet等）。检查系统的网络边界，尤其是DCS与烟气采集机的网络边界。

工控系统中几个关键指标如何测评?

4、身份鉴别

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有**复杂度**要求并**定期更换**；

需要注意的是：*部分DCS监控软件身份鉴别模块包含在windows系统中，定期更换口令难度大。运行人员为了保证紧急情况下的快速操作，监控软件**口令复杂度**和**定期更换**普遍不符合信息安全要求，但整体测评时可从物理访问控制等方面进行弥补。*


工控系统网络安全现状
测评实践
问题与建议

问题与建议

1、测评过程中遇到的几个典型问题

（1）测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换。	**目前状况：**部分DCS监控软件身份鉴别模块包含在windows系统中，定期更换口令难度大。
（2）测评指标：应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。	**目前状况：**大部分DCS系统均未采用双因子鉴别。

问题与建议

（3）测评指标：应对登录的用户分配账户和权限。

目前状况：某DCS系统历史站操作系统与数据库权限未分离。

（4）测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在。

目前状况：DCS系统监控软件通常分为运行人员权限、操作员权限、工程师权限、管理员权限，部分DCS操作员权限采用共享账户的方式。

问题与建议

（5）测评指标：应提供访问控制功能，对登录的用户分配账户和权限。

目前状况：某DCS系统操作员权限可访问并修改工程师权限才能修改的数据表。

（6）测评指标：应遵循最小安装的原则，仅安装需要的组件和应用程序。

目前状况：某DCS系统通信站安装了无线网卡驱动和Team Viewer远程管理软件。

问题与建议

（7）测评指标：应关闭不需要的系统服务、默认共享和高危端口。

目前状况：某DCS系统服务器开启25/80/3389/445高危端口。控制器开启21端口。

（8）测评指标：应采用免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施。

目前状况：部分DCS厂商已实现了与系统兼容的可信验证机制防恶意代码软件。部分DCS厂商由于兼容性问题还无法部署防恶意代码软件。

问题与建议

（9）测评指标：应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

目前状况：DCS系统虽然自身不具备异地实时备份功能，重要程序文件、组态文件、系统文件通过移动介质备份。

（10）测评指标：应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

目前状况：DCS系统与办公系统通过单向隔离装置物理隔离，能够阻断基于TCP/IP协议的传输， DCS系统不采用邮件服务，此项不适用。

问题与建议

2、如何统一各机构对等保2.0标准的理解和对结果的判定？

建议1：深入开展工控系统等级保护测评培训

建议2：形成工控漏洞评价标准

建议3：应用统一的工控系统测评工具

提升

1. 建议建立完善各品牌工控系统问题库和知识库

2. 深入研究工具接入对工控系统的扰动机理

3. “测”与“评”的结合

提升

1. 建议建立完善各品牌工控系统问题库和知识库

序号	安全层面	和利时	艾默生	ABB	新华	日立
1	安全区划分	网络分区隔离	网络分区隔离	网络分区隔离	网络分区隔离	网络分区隔离
2	边界安全防护	防火墙 / 单向隔离	防火墙 / 单向隔离	防火墙 / 单向隔离	防火墙 / 单向隔离	单向隔离
3	入侵检测	NIDS	NIDS	NIDS	/	/
4	主机与网络设备加固	主机白名单、服务最小化	PM补丁管理	漏洞扫描和补丁管理	主机白名单、服务最小化	/
5	安全审计	日志和审计（自主产品）	SIEM安全事故事件管理（自主产品）	日志和审计	日志和审计	日志
6	移动介质管理	光盘 / 终端管理	光盘	光盘 / 终端管理	光盘	光盘
7	恶意代码防范	白名单	防病毒软件	防病毒软件 / 白名单	防病毒软件	/

2. 深入研究工具接入对工控系统的扰动机理

研究工具接入对系统的扰动机理，有利于进一步研制工控系统接入测评工具，辅助测评工作，实现自动化测评。

3. “测”与“评”的结合

以“测”促“评”，以“评”带“测”，“测”“评”结合。“测”是客观的，对标；“评”是分析评价。

谢　谢!

中国电子信息产业集团有限公司第六研究所
工业控制系统信息安全技术国家工程实验室
工控系统安全检测中心　王绍杰
Tel：158 1103 1546