

中控·SUPCON

工业控制系统内建安全设计与防护

浙江中控技术股份有限公司

陆卫军 副总设计师

居高思远，
域无限



WWW.SUPCON.COM



1. 引言

2. 工控安全特殊性

3. 内建安全设计

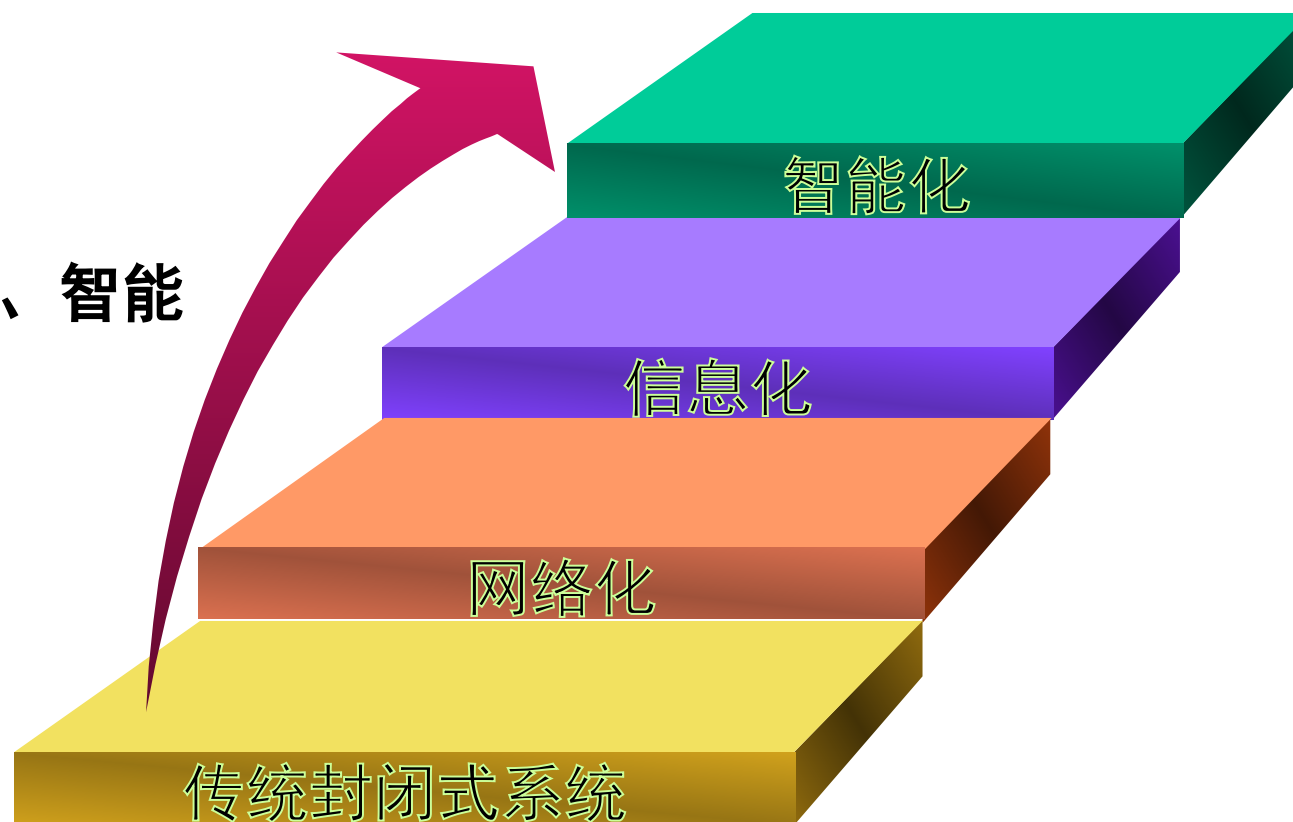
4. 安全应用实践



- 从传统封闭式系统演变到开放式的网络系统
- 从信息孤岛演变到过程控制和企业信息系统的集成

工业4.0

开放、互联、智能





- 2010年6月，发现了第一个专门攻击真实世界中基础设施的Stuxnet病毒
- Stuxnet病毒已经感染了全球45000个以上的大型网络环境，其中伊朗6成以上个人电脑感染了这种病毒。据报道称该病毒可以改变离心机的转速从而破坏离心机，并向控制台仍发出离心机工作正常的信号
- 该病毒造成伊朗约20%的离心机(1000多台)失控，线速度从1225千米/小时提高到1620千米/小时，直到报废，使得布什尔核电站一再推迟发电计划

中控·SUP

互联网网



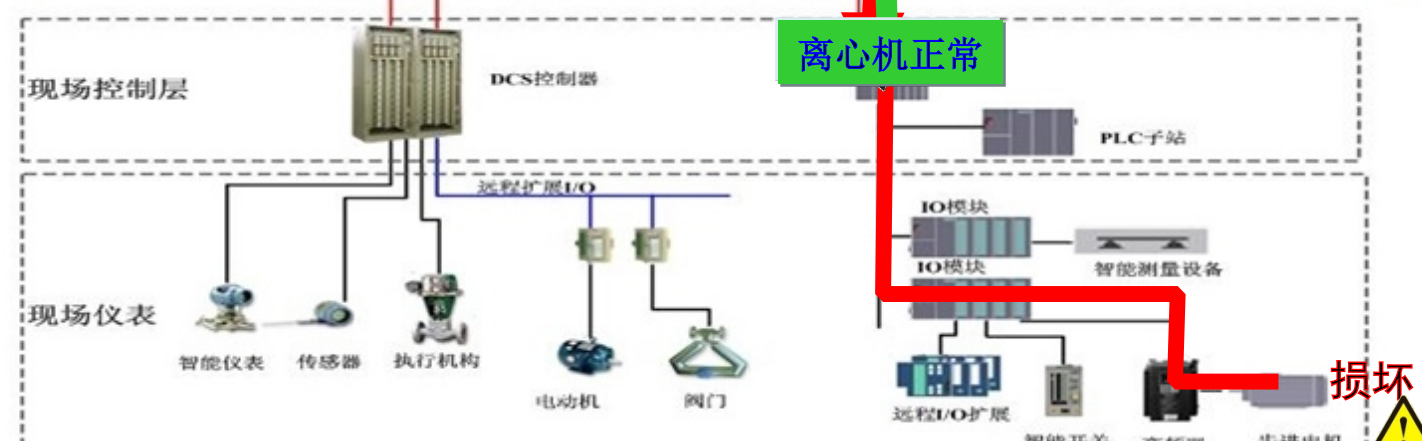
企业管理网



车间监控网



现场控制网



1. Stuxnet 散布到互联网，感染计算机和U盘
2. 带有Stuxnet 的U盘，插入ICS计算机，传染给控制系统网络
3. 找到控制系统组态软件后，利用其漏洞，替换原有S7otbxdx.dll文件

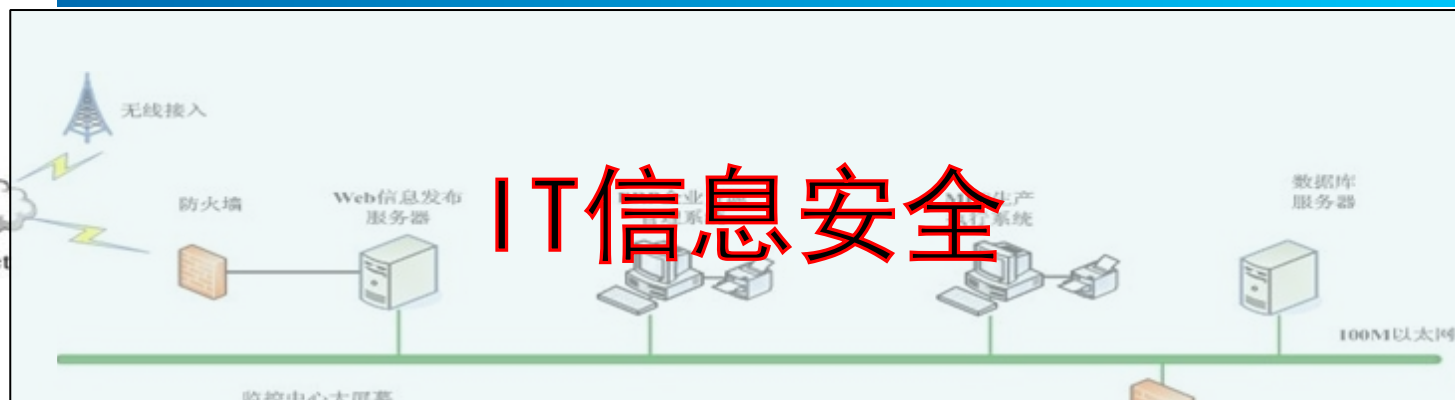
4. 借助组态软件，向PLC控制器注入恶意控制程序DB890
5. PLC向离心机发送恶意控制指令，使其超速；向控制室发送欺骗性的“正常”数据



互联网网



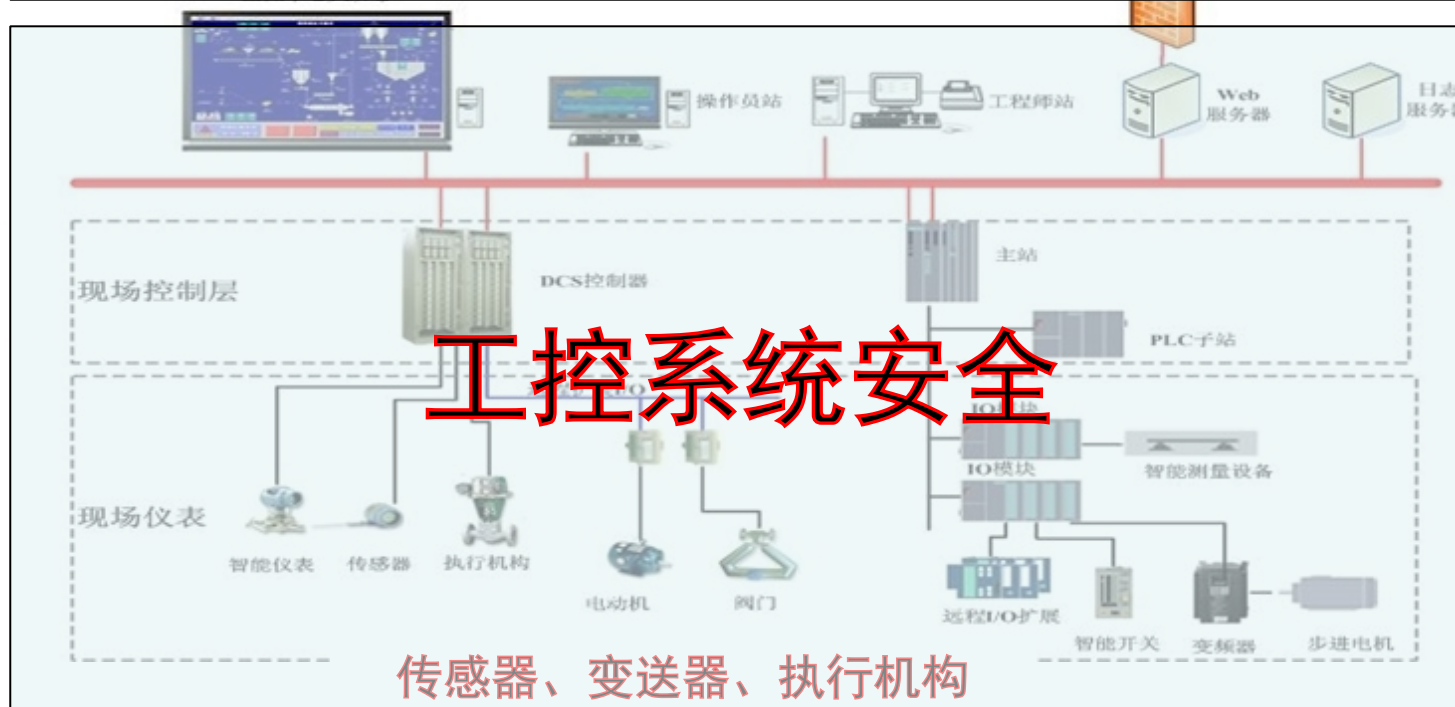
企业管理网



IT信息安全

车间监控网

现场控制网





1. 引言

2. 工控安全特殊性

3. 内建安全设计

4. 安全应用实践



传感器



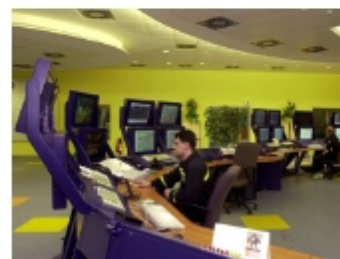
控制阀



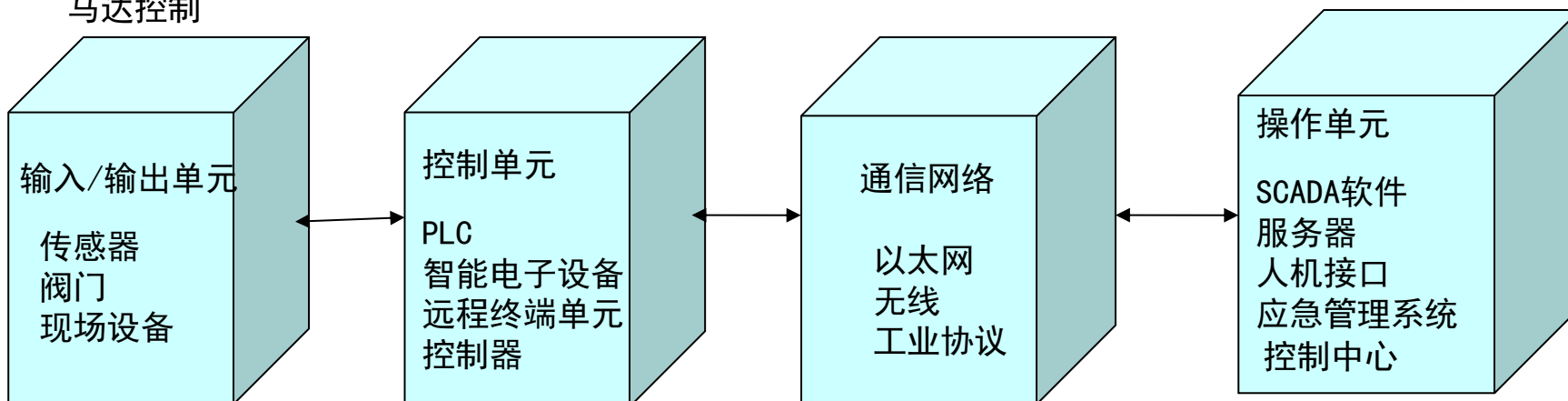
可编程逻辑
控制器



人机界面 (HMI)
和操作显示



马达控制





- 可用性要求特别高，10年×365天×24小时不停车，可用性>99.99%
- 危害更大，例如核电站、西气东输等，爆炸会导致重大安全事故，以人员安全、过程保护为核心
- 平台特殊，嵌入式系统+私有协议+15年维护周期+环境严重受限

LV1: 局部失效或间隙中断

- 单一操作站/网络/硬件故障或损坏

LV2: 全线停车

- 网络全面瘫痪、控制站故障
- 设备报废、基础设备损坏

LV3: 人身伤亡

- 对人员（雇员、社区群众）的伤害
- 财产的损失（数据的丢失）、……

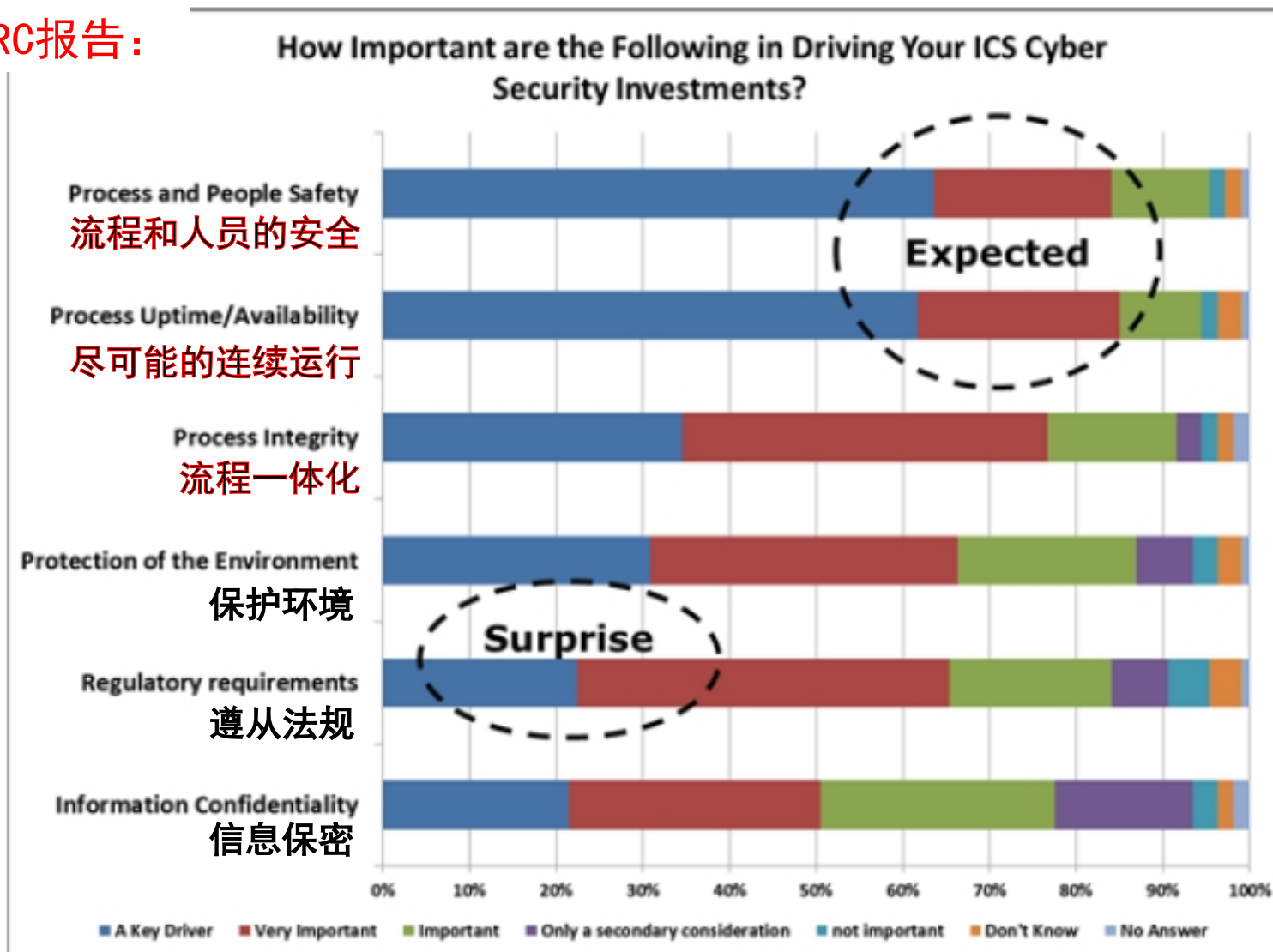
LV4: 安全事故及环境破坏

- 爆炸等安全事故
- 人民生活资源（水、电、气）的污染
- 有毒、危险物质的无序排放、非法转移使用

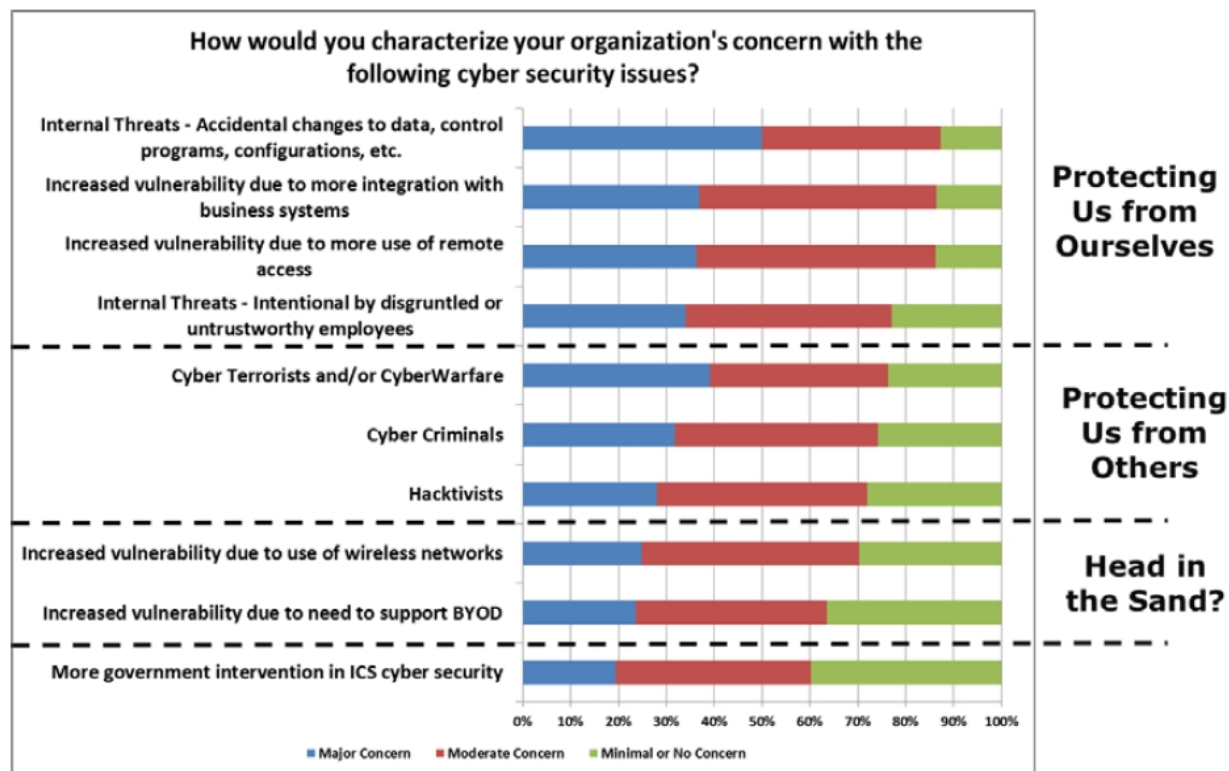




引自ARC报告：



- 硬件物理失效
- 软失效SER
- 软件缺陷
- 系统漏洞
- 误操作
- 工艺环境威胁
- 病毒攻击
- 黑客或敌对势力攻击
- 内部人员恶意破坏



引自ARC报告



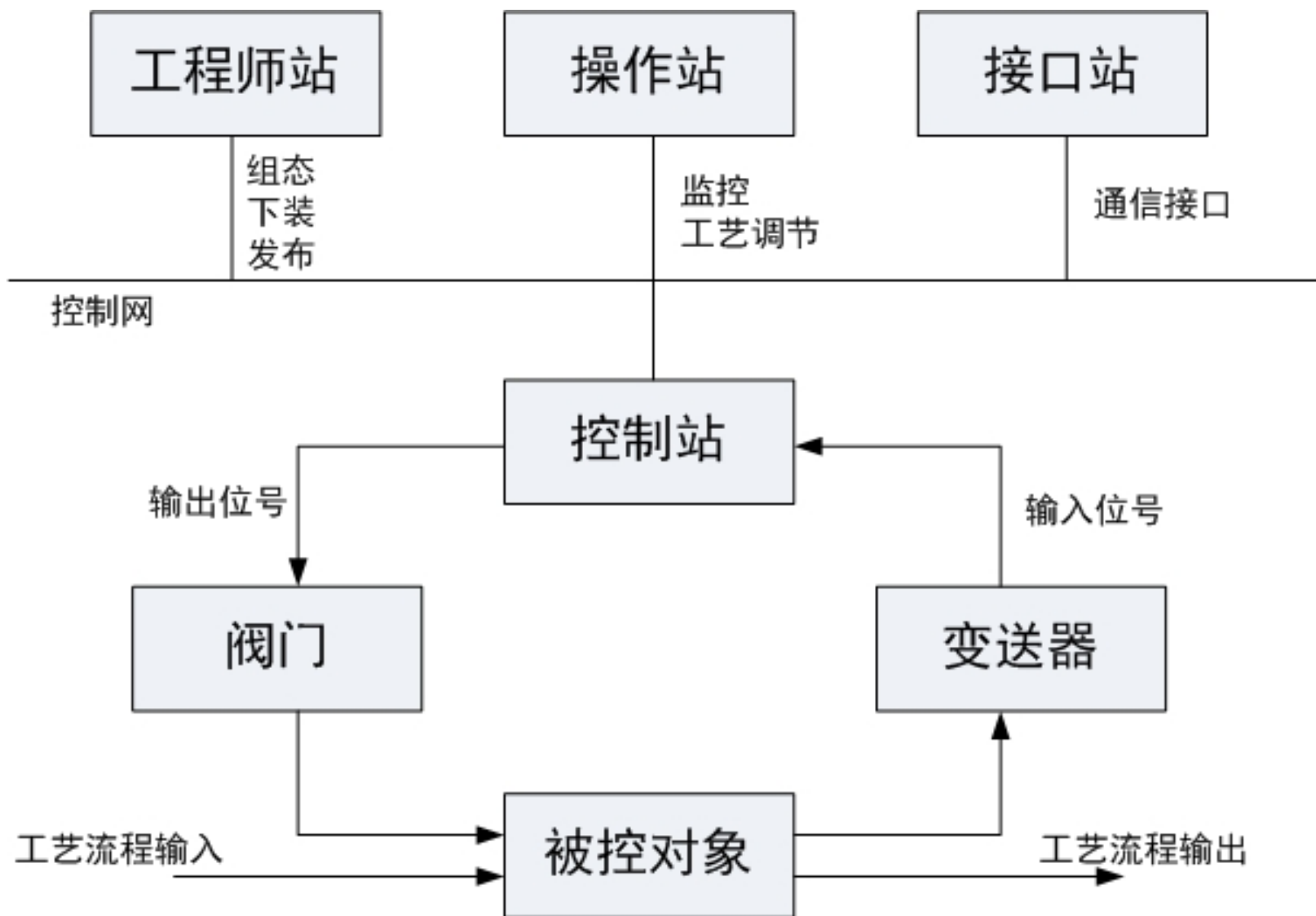


1. 引言

2. 工控安全特殊性

3. 内建安全设计

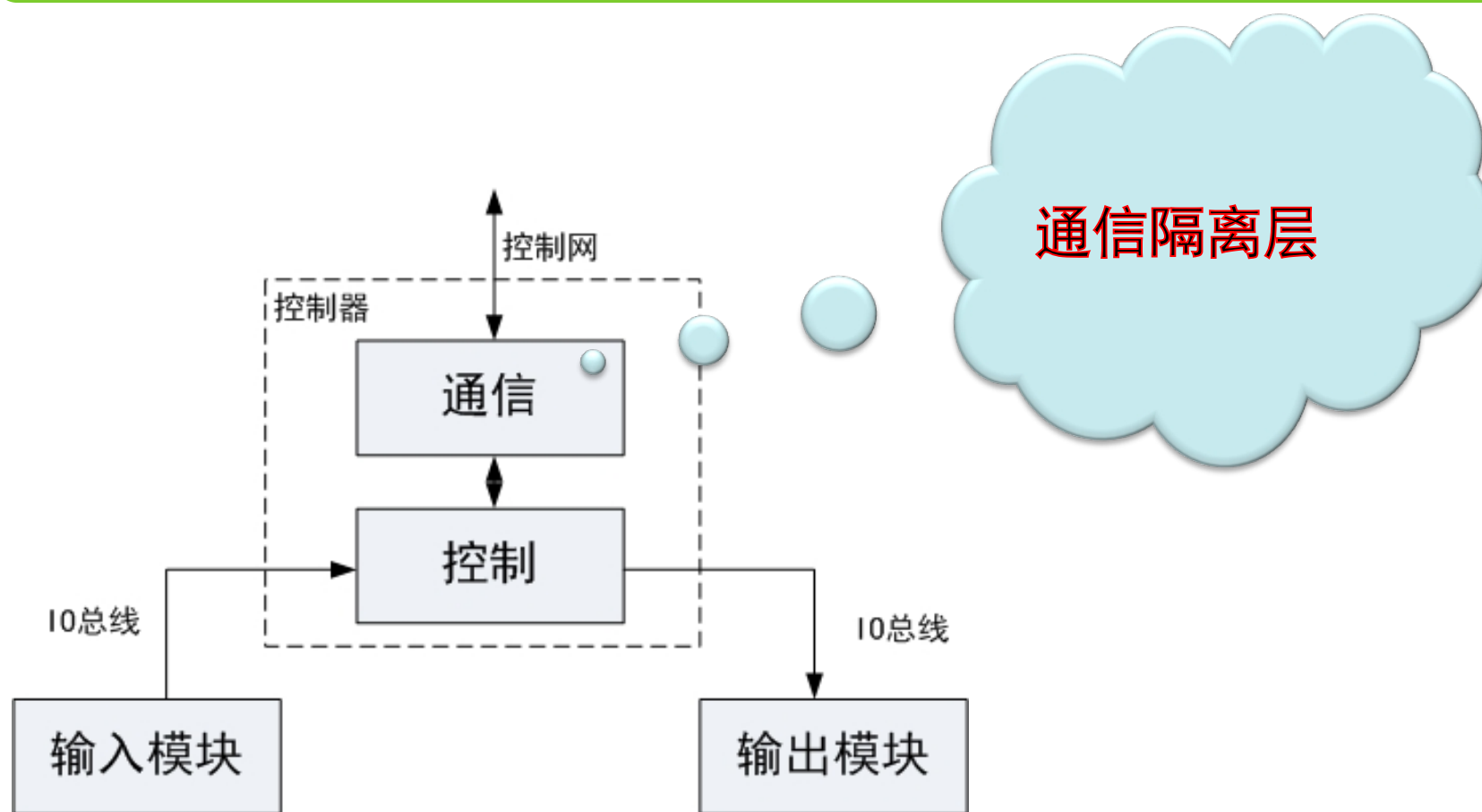
4. 安全应用实践



中控·SUPCON 内建安全设计：控制与通信安全隔离技术

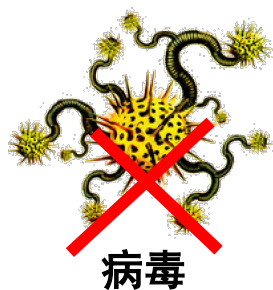


控制站通信隔离层设计，控制与通信安全隔离，保证控制可信运行





病毒运行依赖黑客对于嵌入式操作系统的了解，对控制器也是如此



病毒

不基于通用系统

无运行环境



自主研发



黑客

协议、接口私有、受限

无进入机会



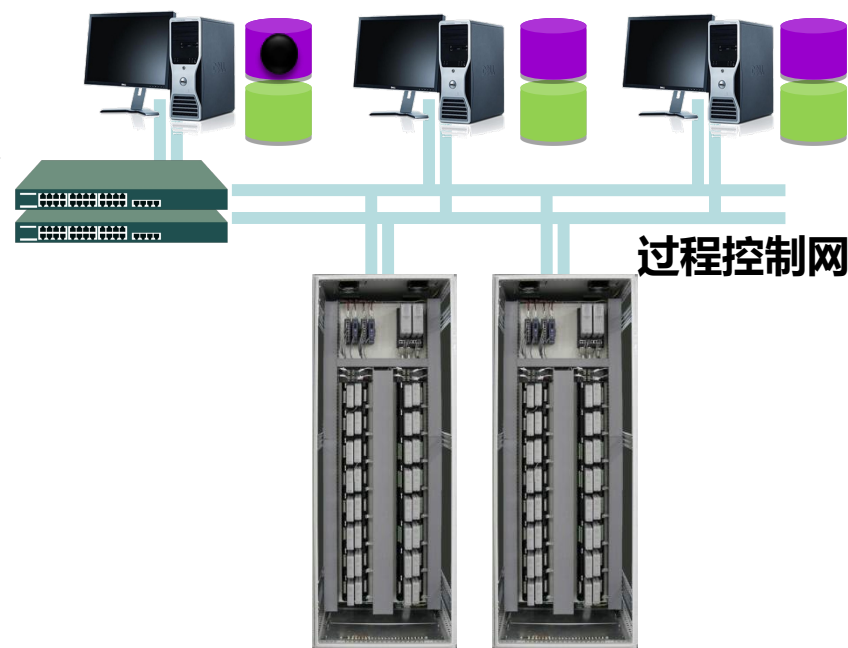
全系统冗余和关键数据备份设计，保证控制系统实时诊断与恢复

- 全系统冗余设计

- 工程师站、服务器、控制网、控制器、IO总线、IO模块
- 单一故障不影响工业控制系统正常运行

- 关键数据备份设计

- 工程师站/操作站：组态文件、历史数据
- 控制站：硬件组态、位号组态、控制算法





通过多层次数据加密和防护技术，保证数据的完整性和机密性

- 操作层
- 网络层
- 控制层
- 现场总线/无线层

SCnet

控制网络

DO=1



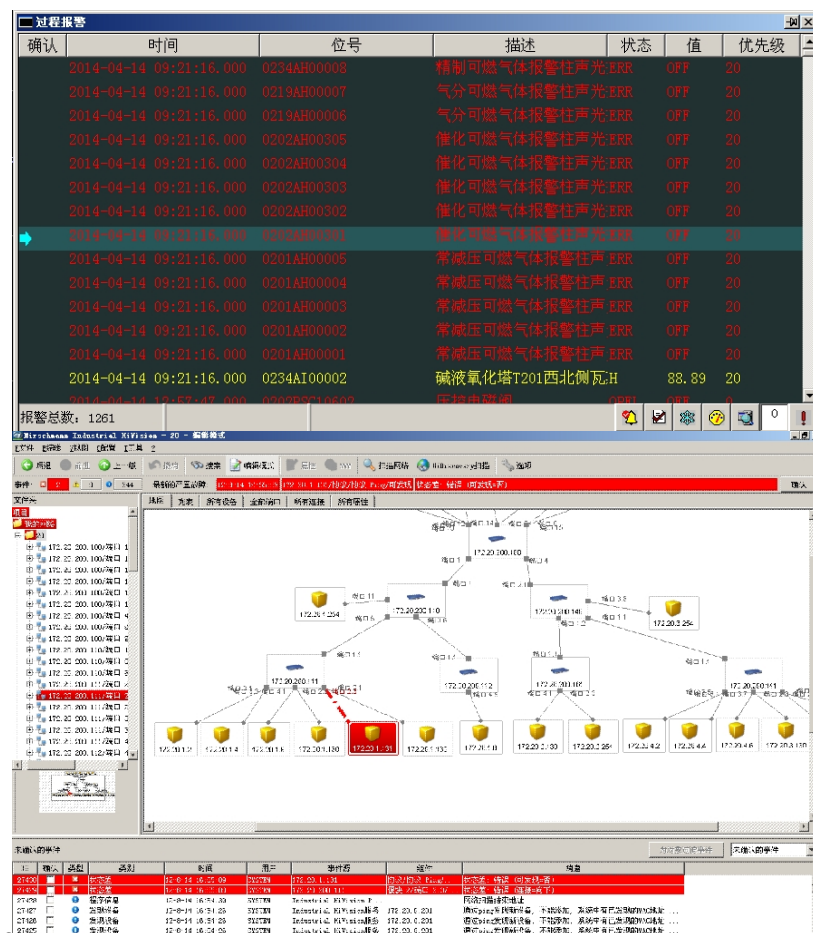
非明码传输，防止窃听和篡改

中控·SUPCON 内建安全设计：全面报警与审计技术



完善的报警功能和审计功能，让行为不可抵赖，故障不被隐藏

- 过程报警（工艺报警）
- 系统报警
- 详细诊断
- 全网诊断
- 设备管理与智能诊断
- 操作记录与安全事件记录
- 工艺建模/行为建模/预测管理

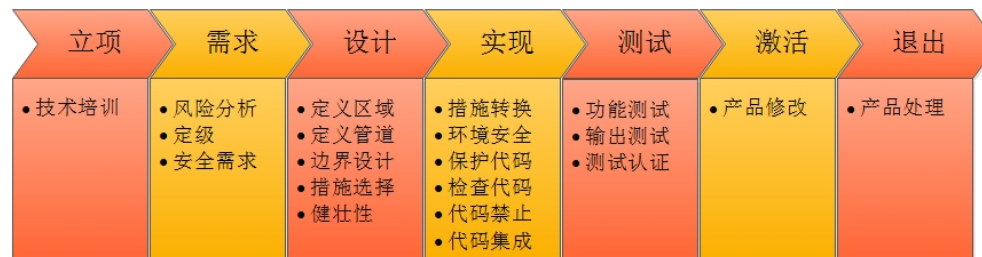


中控·SUPCON 内建安全设计：安全V&V验证技术



通过安全开发程序和安全V&V验证措施，保证工控系统整体安全

- 安全开发程序
- 开发环境与过程安全
- 安全功能验证技术与测试平台



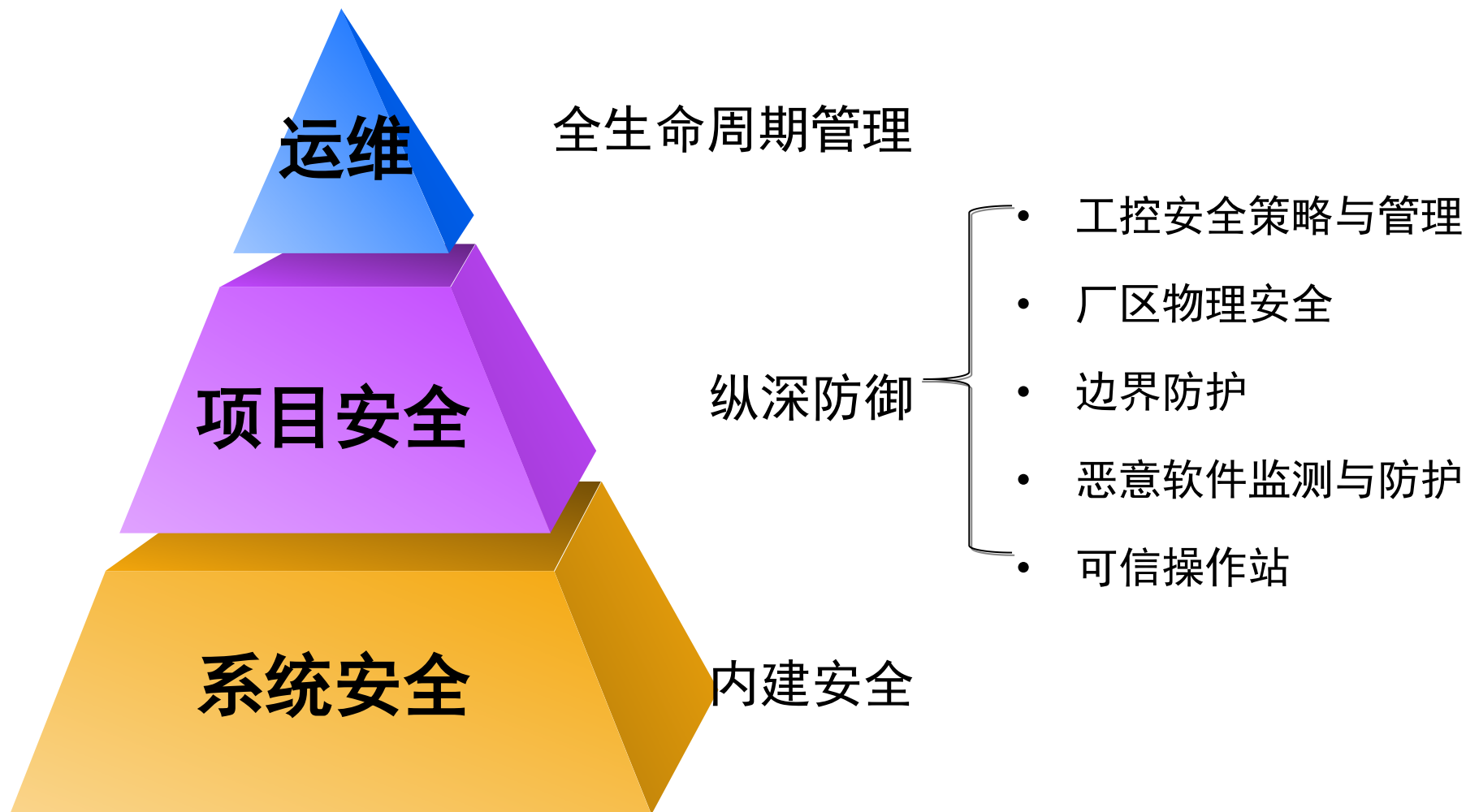


1. 引言

2. 工控安全特殊性

3. 内建安全设计

4. 安全应用实践

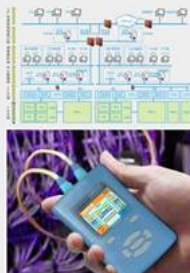


测试中心 | TESTING CENTER

中控·SUPCON

**LARGE SCALE
NETWORK LABORATORY**
大规模网络实验室

分析验证工业大规模组网方案



测试内容

- 大规模网络性能测试
- 网络流量 网络延迟 网络丢包率
- 网络可靠性 网络扩展性 网络安全

测试方法

- 网络解决方案验证
- 网络集成方案 无线接入方案
- 网络冗余方案 组网通信方案

测试工具

- 选点抽样测试
- 环境模拟测试
- 网络压力测试
- 对比分析测试

Certificate Of Compliance

This is to certify that the:

WebField ECS-700
FCU712-S01

Manufactured by:

Zhejiang Supcon Technology Co.,Ltd.

Is in compliance with the requirements set forth by:

Achilles Level II Certification

This certificate is restricted to the specified version of the referenced Device (including model number, hardware/firmware/software version, and control protocol) set forth in this Certificate. Any change to the Device might impact the Device's ability to pass the standards referenced in this Certificate. This Certificate is based upon limited testing, and is not a complete or comprehensive certification of the security of the Device. The Device may contain security vulnerabilities and deficiencies that are not covered by the standards referenced in this Certificate. This Certificate is subject to rescission by Worldtech Security Technologies Inc.

More information regarding this Certificate and the Achilles Communications Certification Standard is available at www.worldtech.com and upon request from Worldtech Security Technologies Inc.

CERTIFICATE NO. CERT-194-020714

FCU712-S_V11.1x.00

HARDWARE VERSION

FCU712-S_V11.1x.00

FIRMWARE VERSION

N/A

CONTROL PROTOCOL

Embedded Device

CATEGORY



Nate Kube, CTO

worldtech
A GE Company



国家信息安全测评 信息安全服务资质证书 (安全工程类一级)

证书号: CNITSEC2014SRV-1-401

浙江中控技术股份有限公司

注册地址: 杭州市滨江区六和路308号
工商注册登记号: 330000000005204
组织机构代码: 72008294-9

符合《信息安全服务资质评估准则》一级(基本执行级)(A类)要求。
特发此证

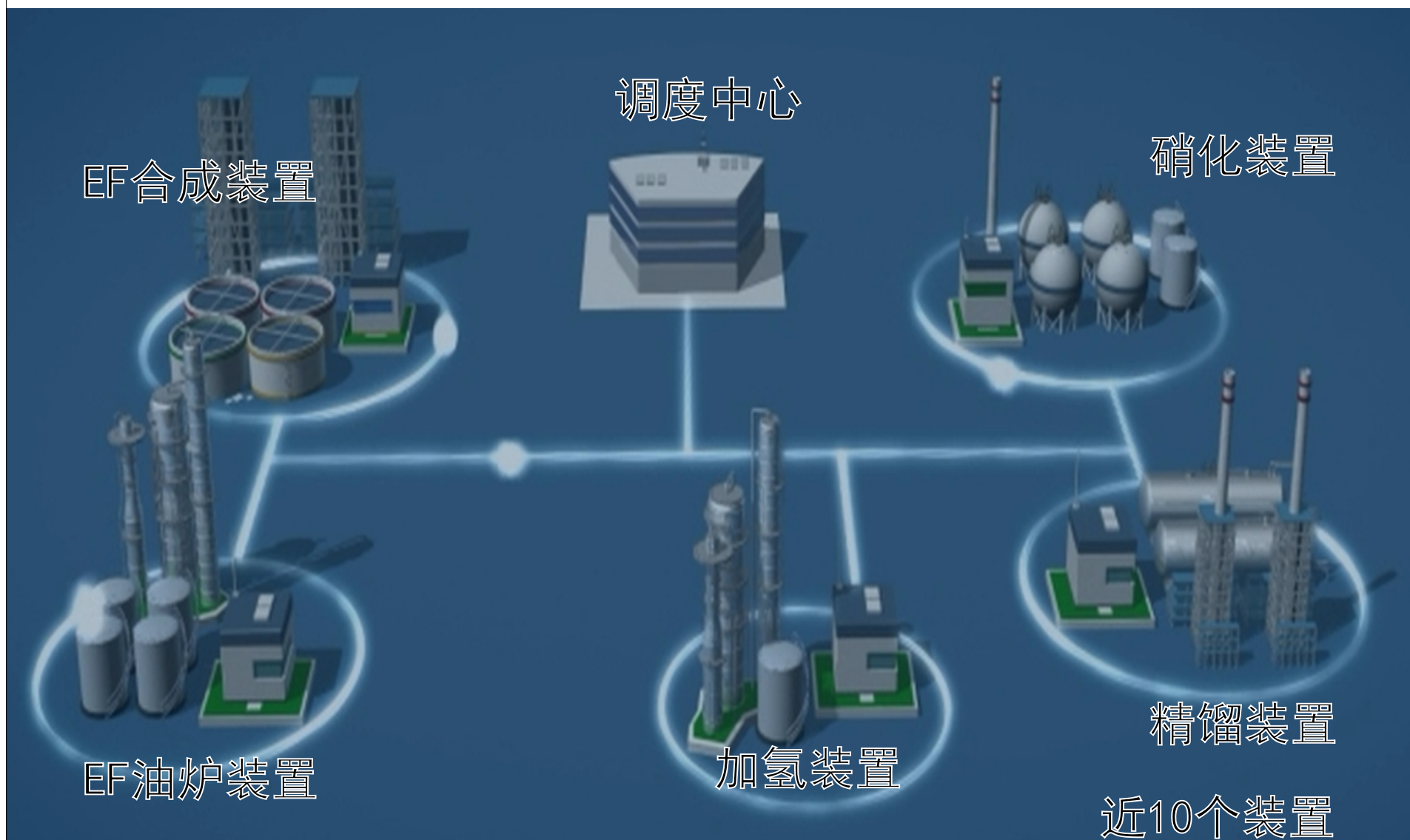
本证书签发日期: 2014年6月12日

有效期至: 2017年6月11日

批准人:

中国信息安全测评中心

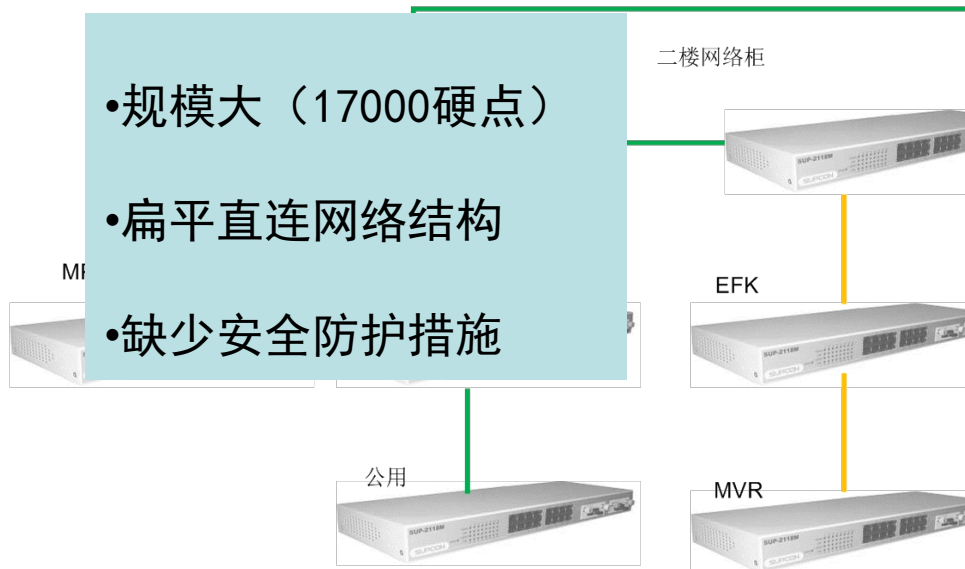






网络特征

- 规模大（17000硬点）
- 扁平直连网络结构
- 缺少安全防护措施



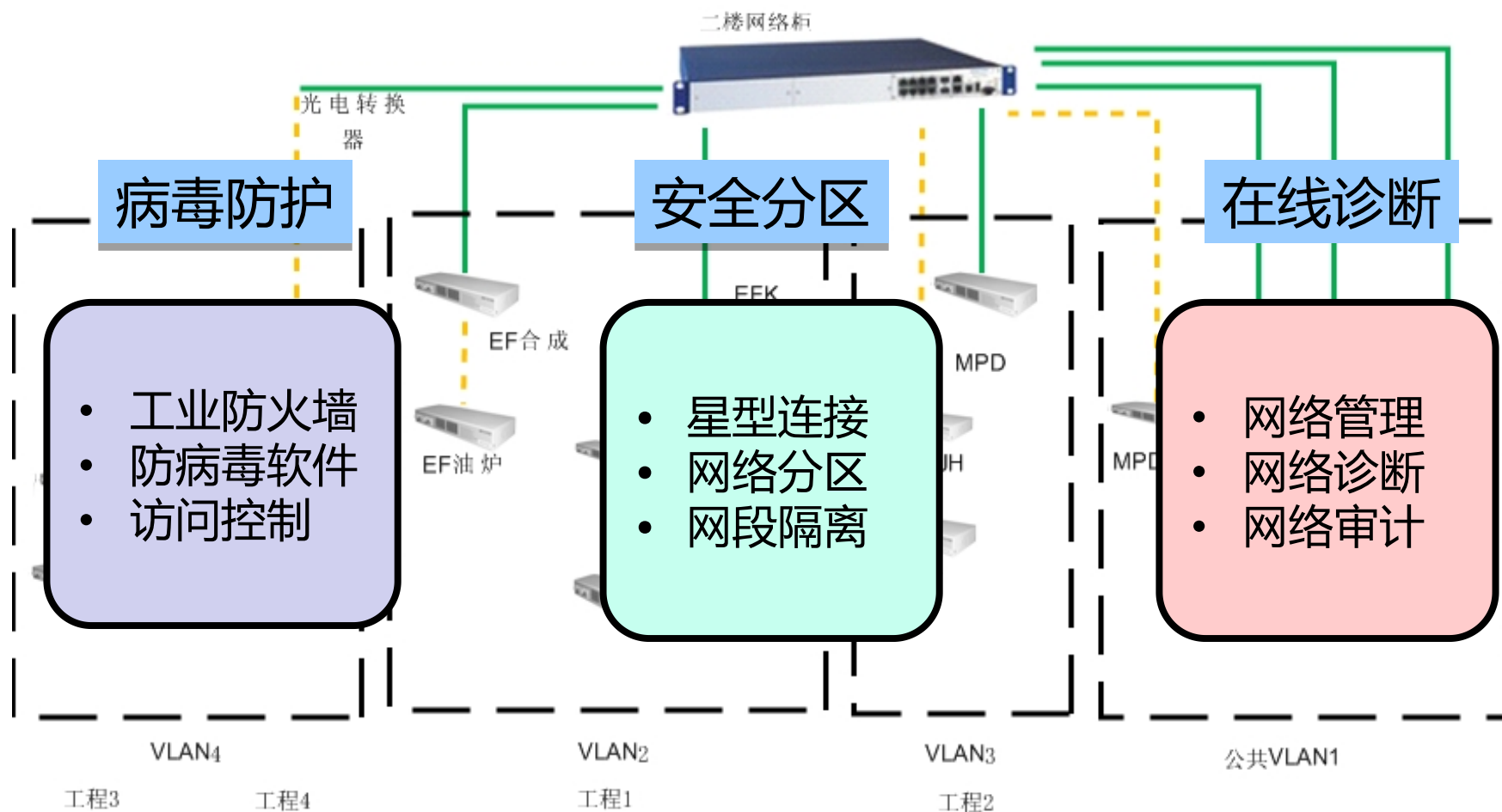
存在问题

- 网络规模大，风险集中
- 易发生网络风暴
- 装置不隔离，易故障扩散
- 网络不分层
- 存在网络乱接情况
- 存在随意使用U盘情况
- 存在随意连接手机情况
- 操作站未防毒处理





- 部分有限度的升级控制系统，提升安全能力
- 改进网络结构，实现网络隔离，提高网络安全；
- 部署基于白名单的防病毒解决方案和工业防火墙，防范病毒蔓延及外部攻击；
- 实现全网诊断功能，实时监控网络状态；
- 实现基于硬件GPS的时间同步，提高时间同步精度。



TECHONOLGY WINS DREAMS

IONOLOGY WINS DREAMS

感谢支持!

TECHONOLGY WINS DREAMS

TECHONOLGY WINS DREAMS

中控 · SUPCON