发电行业电力监控系统
信息安全保护工作介绍

北京威努特技术有限公司

目 录

01

第一部分

发电行业安全政策和标准介绍

为什么要开展工业控制系统信息安全建设(1/4)

一．互联互通趋势

- 新技术的应用使得原来封闭的工业控制系统网络越来多的纵向开放，在工业4.0、两化融合、智能制造的大趋势下工业控制网络不可避免会遭遇更多的网络威胁。

二．通用设备普及

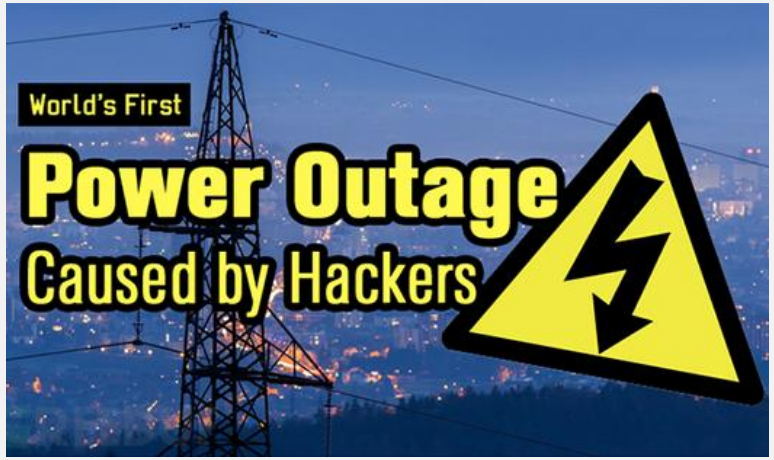
- 工业控制系统逐渐从专用的硬件、软件和通信协议过渡到通用普及的商用软硬件及更开放的TCP/IP协议，传统信息网络的威胁对工控网络变得有效。

为什么要开展工业控制系统信息安全建设(2/4)

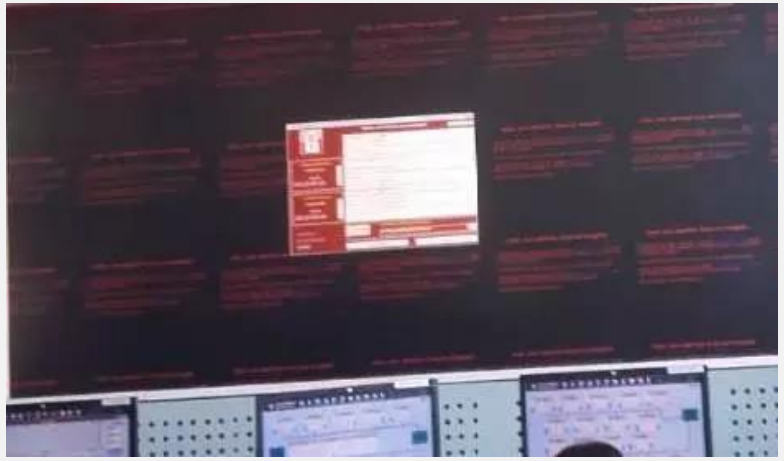
三．重大事件驱动

- 全球工控安全事件高发，2014年245起，2015年295起，2016年278起，平均是2010年伊朗震网事件爆发时的7倍多。

伊朗震网事件



乌克兰电网事件



勒索病毒事件

为什么要开展工业控制系统信息安全建设(3/4)

四． 国家顶层设计

《中华人民共和国网络安全法》
第三章（第二节）

全国人民代表大会
The National People's Congress of the People's Republic of China

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域...**关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。**

《信息安全技术 网络安全等级保护基本要求》
第5部分 工业控制系统安全扩展要求

中国国家标准化管理委员会
STANDARDIZATION ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA

随着信息技术的发展，GB/T 22239—2008在时效性、易用性、可操作性上需要进一步完善，为了适应工业控制系统下网络安全等级保护工作的开展，需对GB/T 22239—2008进行修订，本部分的修订的思路和方法是提出了工业控制系统安全扩展要求。

《关于加强工业控制系统信息安全管理的通知》
《工业控制系统信息安全防护指南》

中华人民共和国工业和信息化部
Ministry of Industry and Technology of the People's Republic of China

工业控制系统信息安全事关经济发展、社会稳定和国家安全。为提升工业企业工业控制系统信息安全（以下简称工控安全）防护水平，保障工业控制系统安全，制定本指南。

国家高度重视工控安全

- 2016年7月首次全国范围的关键信息基础设施网络安全检查工作已经启动，这是落实习近平总书记重要讲话精神的重要举措

中共中央网络安全和信息化领导小组办公室
Office of the Central Leading Group for Cyberspace Affairs

- 2016年11月3日工业和信息化部印发《工业控制系统信息安全防护指南》

中华人民共和国工业和信息化部
Ministry of Industry and Technology of the People's Republic of China

- 2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过《网络安全法》

全国人民代表大会
The National People's Congress of the People's Republic of China

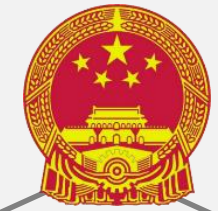
国家工控安全相关政策

国务院

2012年，国务院发布《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）。《意见》明确指出“明确指出保障工业控制系统安全。加强核设施、航空航天、先进制造、石油石化、油气管网、**电力系统**……重要领域工业控制系统的安全防护……”

网信办

2016年7月全国范围关键信息基础设施网络安全检查工作启动，习近平总书记指出：“金融、能源、**电力**、通信、制造等领域是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”，要求“**要全面加强网络安全检查**，摸清家底，认清风险，找出漏洞，通报结果，督促整改”。



工信部

2016年11月3号工信部下发《工业控制系统信息安全防护指南》，指南指出“工业控制系统应用企业应从**安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任**十一个方面做好工控安全防护工作”。

网络安全法具体要求

第三章（第一节）

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务

第三章（第二节）

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域...关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

第三章（第二节）

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估。

第五章

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第六章

第五十九条 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款;对直接负责的主管人员处一万元以上十万元以下罚款。

电力监控系统安全防护总体方案（36号文）

逻辑隔离	安全审计	恶意代码的防范	入侵检查	访问控制
控制区与非控制区之间应采用逻辑隔离措施，实现两个区域的逻辑隔离、报文过滤、访问控制等功能，其访问控制规则应当正确有效。生产控制大区应当选用安全可靠硬件防火墙，其功能、性能、电磁兼容性必须经过国家相关部门的检测认证。	生产控制大区的监控系统应当具备**安全审计系统**，能够及时发现各种违规行为及病毒和黑客的攻击行为。	应当及时更新经测试验证过的特征码，查看查杀记录。禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。**（使用”白名单“安全机制替代传统杀毒软件，更满足工控系统安全防护特点）。**	生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，及时捕获网络异常行为、分析潜在威胁、进行安全审计。	能量管理系统、厂站端生产控制系统、电能量计量系统及电力市场运营系统等业务系统，应当逐步采用电力调度数字证书，对用户登录本地操作系统、访问系统资源等**操作进行身份认证，根据身份与权限进行访问控制，并且对操作行为进行安全审计。**

信息安全等级保护基本要求

网络安全

摘录 7.1.1.2

a) 应在网络边界部署访问控制设备，启用访问控制功能；.....

c) 应对进出网络的信息内容进行过滤，实现对应用层等协议命令级的控制；.....

主机安全

摘录 7.1.3.2

a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

应用安全

摘录 7.1.4.3

a) 应提供覆盖到**每个用户的安全审计功能**，对应用系统重要安全事件进行审计

b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

c) **审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等**；

数据安全

摘录 7.1.5.3

a) 应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；

b) 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；

工业控制系统安全防护指南

4.1 安全软件选择与管理

在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。

4.2配置和补丁管理

做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计。

4.3 边界安全防护

1）通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。

2）通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。

4.4 物理和环境安全防护

拆除或封闭工业主机上不必要的 USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

4.7 安全监测和应急预案演练

1）在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。

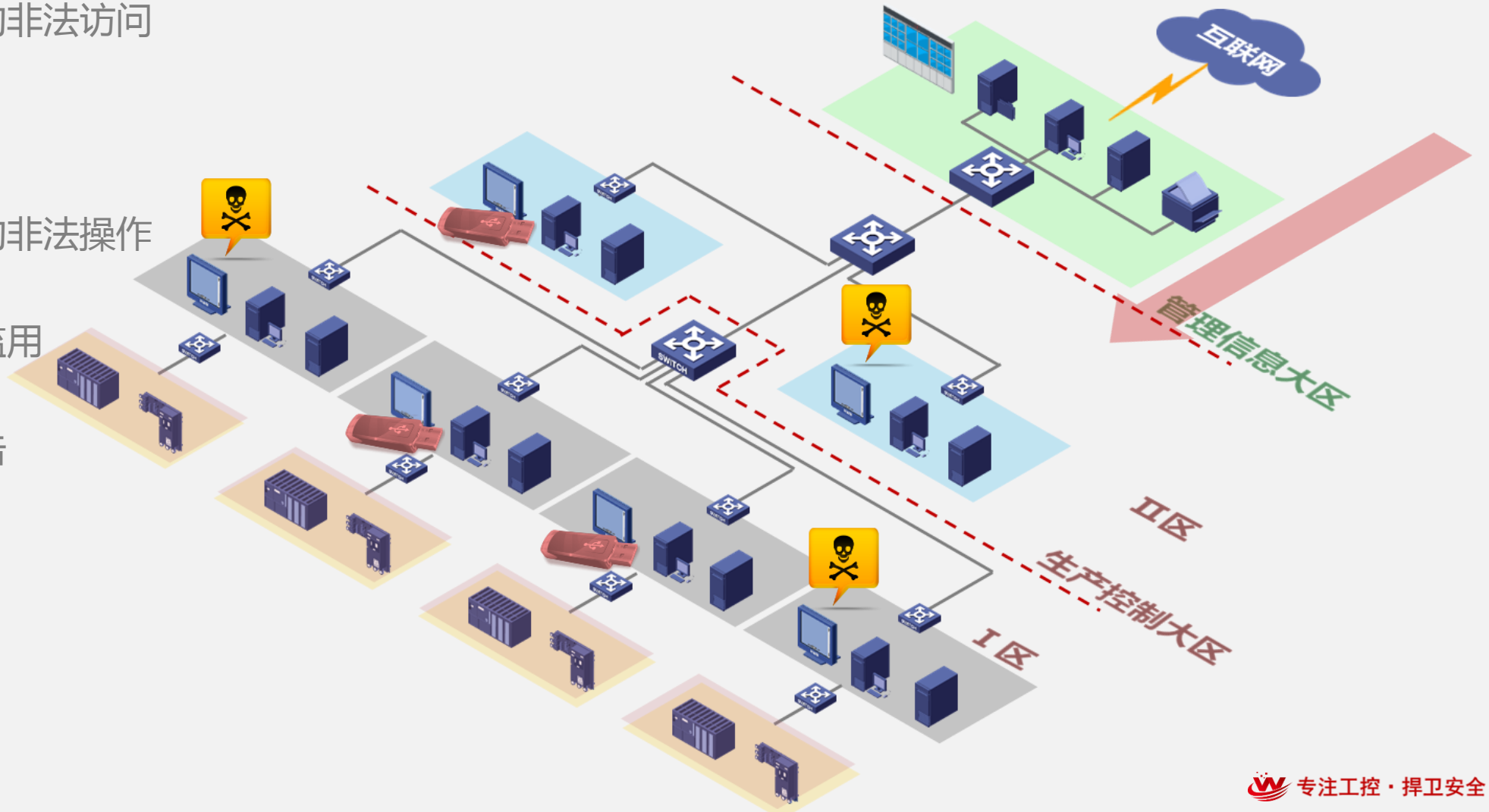
2）在重要工业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。

02

第二部分
发电行业工控安全解决方案

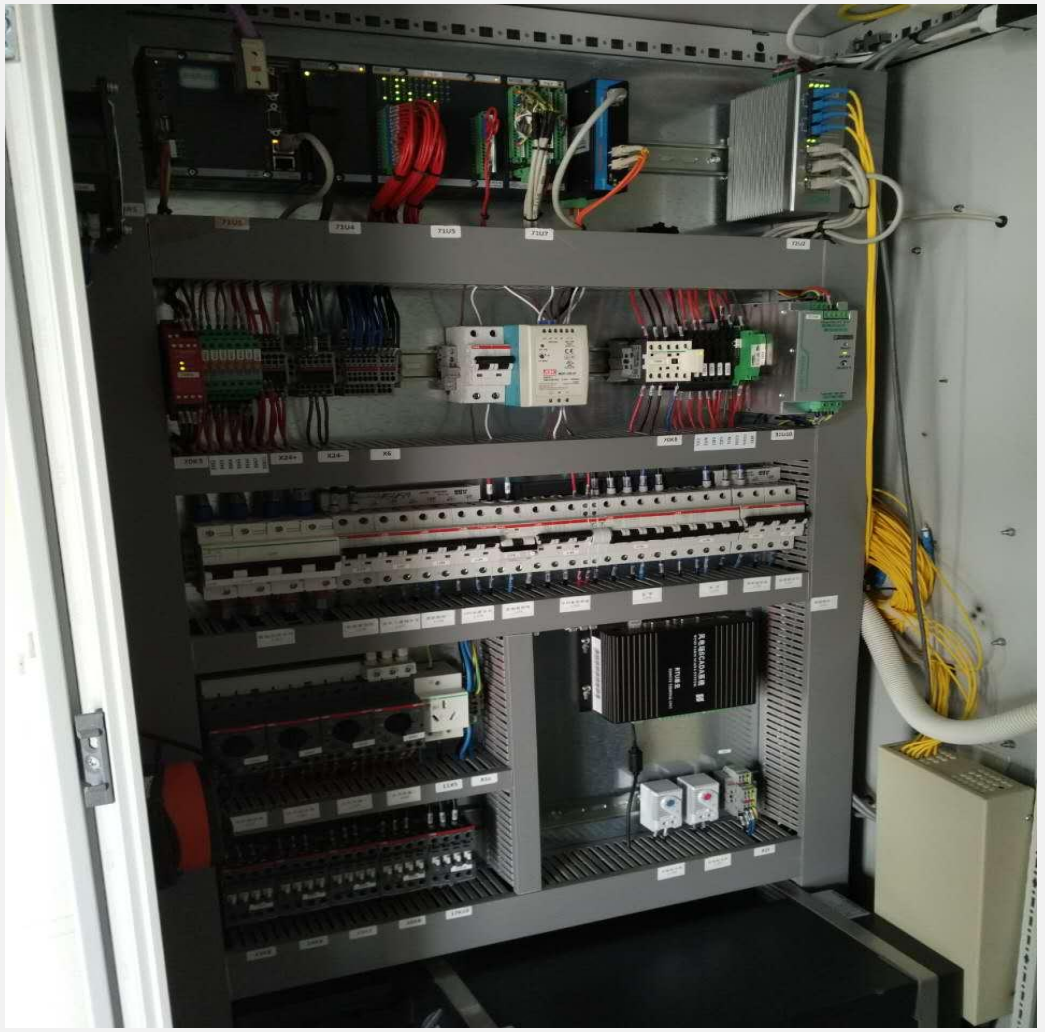
发电厂常见安全威胁

- 从互联网而来的非法访问
- 远程维护通道
- 用户有意无意的非法操作
- 移动存储介质滥用
- 针对漏洞的攻击
- ……



风力发电系统案例

- Bachmann MX213 PLC安全漏洞
  - 该PLC开启了Telnet、FTP、HTTP以及RPC服务，这些服务均存在严重的安全漏洞。
  - 利用FTP漏洞登录后甚至能够获取该PLC内部的任意文件包括Vxworks的内核文件。
- 研华-TPC-651H HMI安全漏洞
  - 该HMI开启了Telnet、RDP远程桌面服务（3389）、windows共享等服务，且部分服务存在严重的安全漏洞。
  - 通过利用这些漏洞可以成功的获取具有系统管理员权限的命令行权限甚至完全控制该设备。



水力发电系统案例

梯调系统中的安全问题

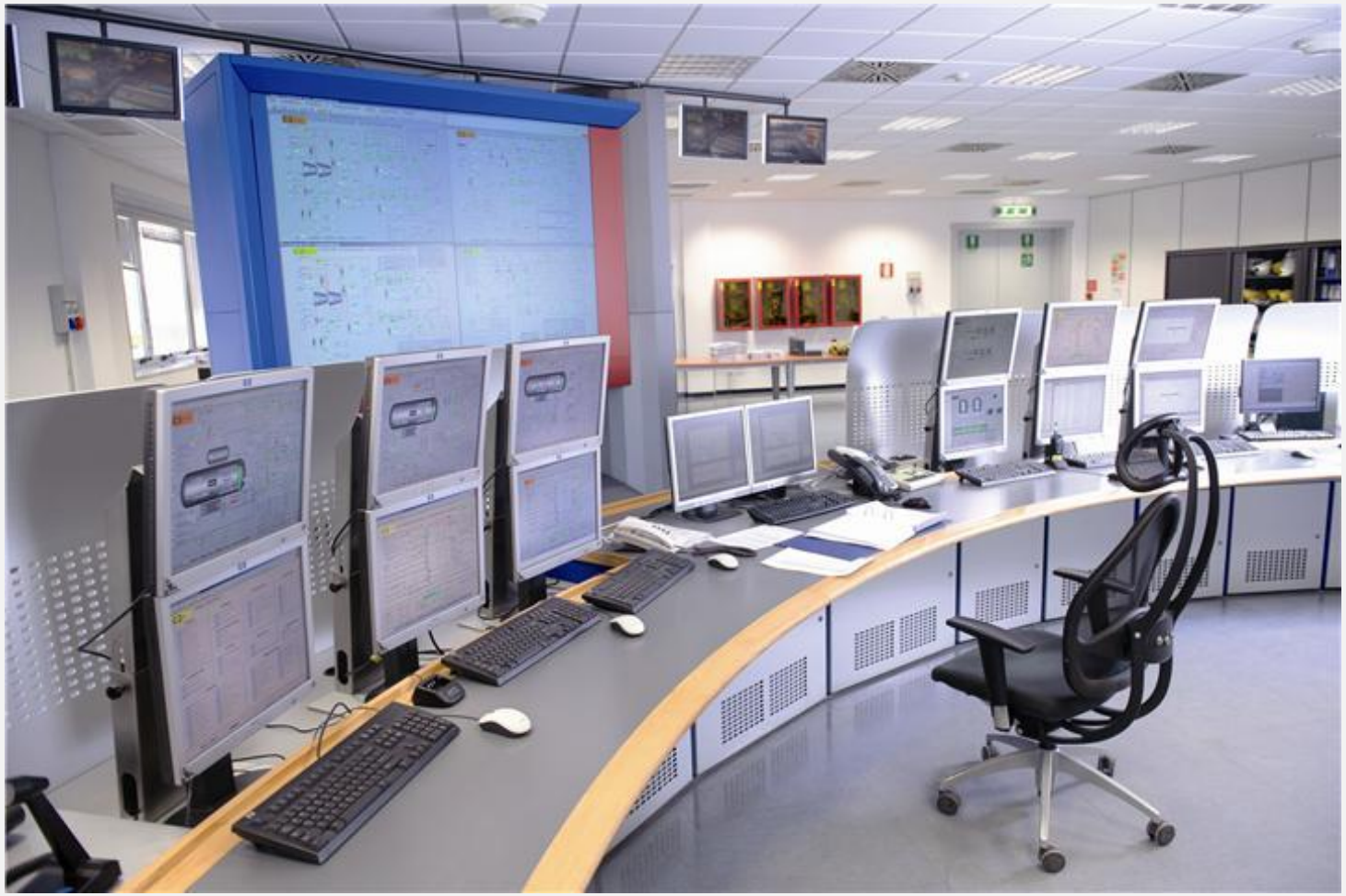
- 某纵向认证设备，用户名、密码明文存储在数据库中。
- 某纵向认证设备，登陆界面存在格式化字符串溢出漏洞，导致设备重启。

船闸系统中的安全问题

- 西门子S7-400 PLC存在安全认证问题，黑客可绕过上位机直接控制该PLC，恶意的CPU-STOP命令可关闭该PLC，导致船闸失控。
- 西门子OSM交换机，snmp服务采用默认的口令admin/admin，web管理员界面的默认口令admin/admin、user/user、登陆可绕过。

火力发电系统案例

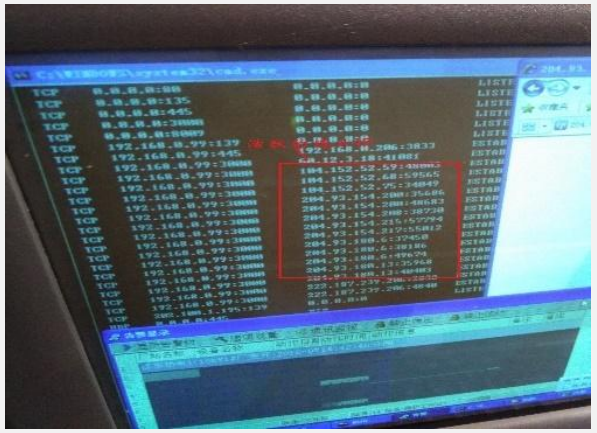
- ABB Symphony系列DCS通讯协议存在设计缺陷
  - 攻击者也能够进行重放攻击改变DCS的工作模式，从而影响工艺的正常运行造成非常严重的后果。
- ABB Symphony系列DCS拒绝服务漏洞
  - 该漏洞被利用将导致IET 800卡件瘫痪并自动重启。在重启过程中所有的以太网数据交互都将受到影响。



现在工控安全都有哪些问题(非法内外联)

■ **案例**

某民营电厂为方便领导实时掌握生产信息，将重要的生产管理服务器违规接入互联网，而同时该服务器又和生产控制系统、办公网络互连。在现场安全检查时，发现该服务器有活跃的境外IP访问，并且有数据的交互。



图：境外IP访问生产服务器

图：上位机安装远程维护工具

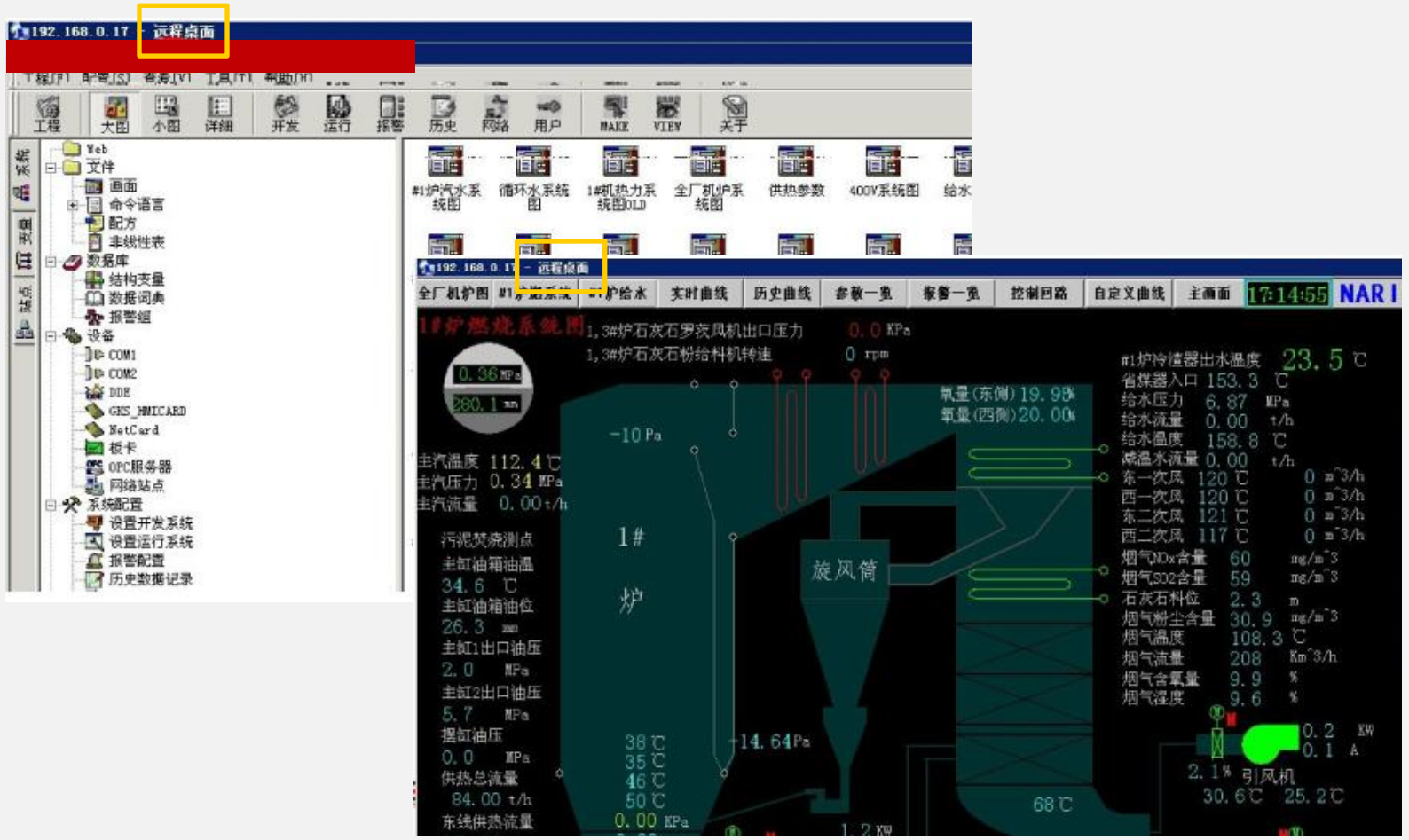
■ **案例**

某新能源企业由于生产现场地理位置比较偏远，设备维护的工程技术人员了方便操作，违规保留远程维护通道，有安全检查时，就将通道临时关闭，打游击战。

现在工控安全都有哪些问题(远程访问)

- **案例**

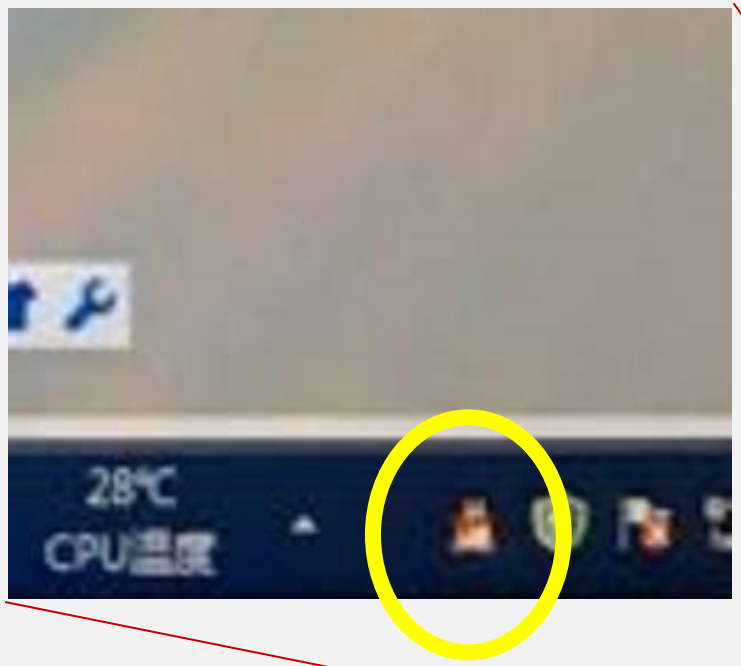
在数个发电厂发现，生产控制大区内部SIS系统和控制系统开启远程桌面服务，此服务的开启为攻击者开辟了一条攻击的路径和权限。

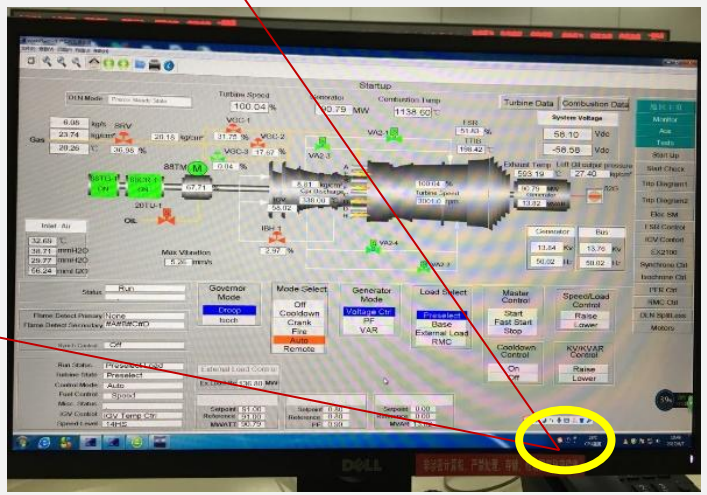


现在工控安全都有哪些问题(私接无线路由)

- **案例**

在华中某热电厂发现，操作员站私接无线WiFi，导致与互联网连通，把整个控制网络暴露在互联网下。





现在工控安全都有哪些问题（病毒泛滥）

案例I

某国有电厂操作员工作站上一方面有病毒感染，另一方面部分安装了游戏娱乐软件。

主机USB接口贴有封条，但是形同虚设，需要时就会揭开使用。

案例II

某城市供水集团的下属水厂的所有操作员站、数据服务器没有任何防护措施，同时生产网和办公网混合，主机等同于直接暴露在公网上。

案例III

某抽水蓄能电站的工程师站和操作员站大部分是Windows XP的操作系统，一方面这些主机运行缓慢，另一方面操作系统已经停止维护。

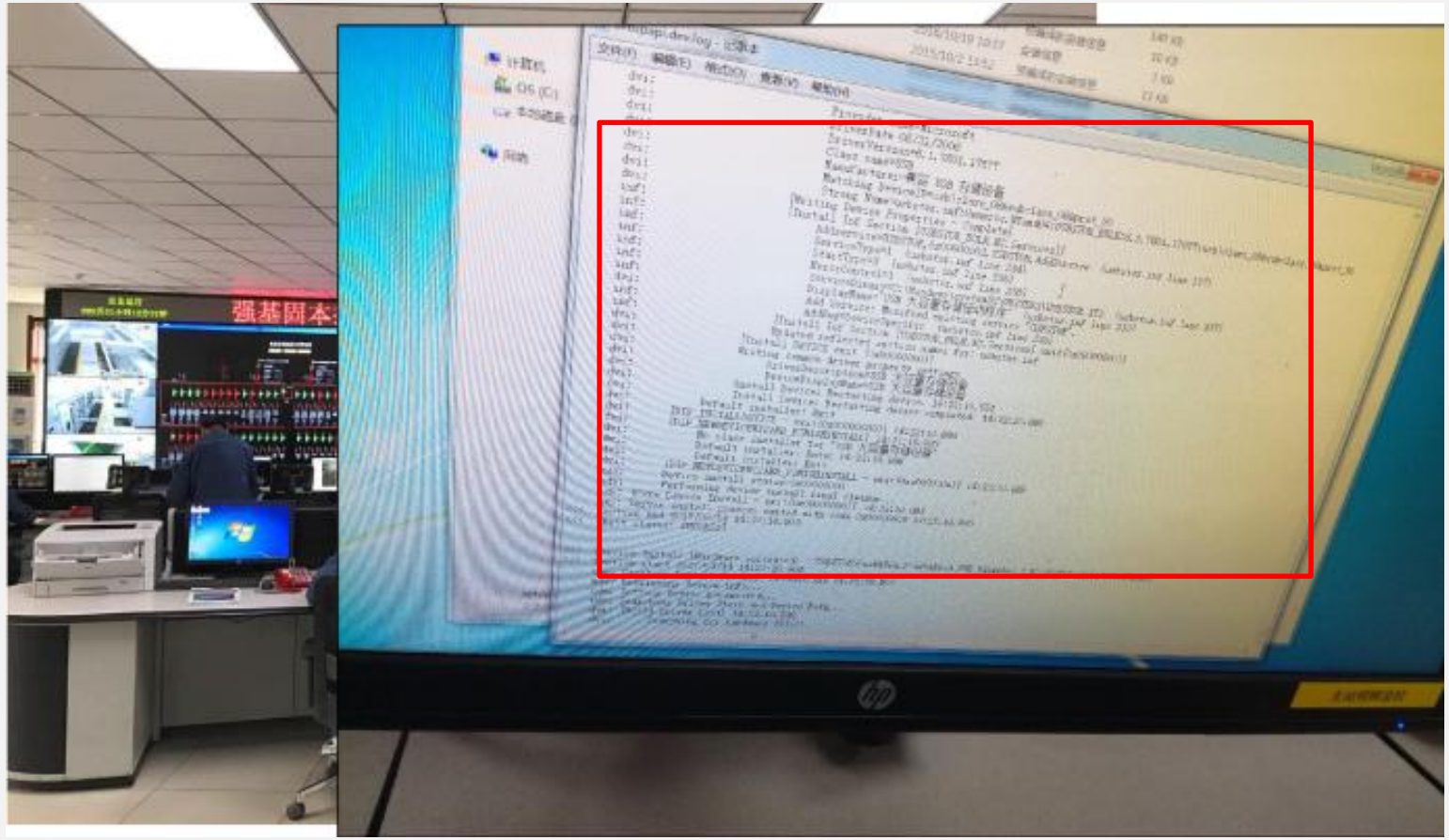
图：现场发现马吉斯病毒

图：Windows XP系统的上位机

现在工控安全都有哪些问题（移动存储介质滥用）

- **案例**

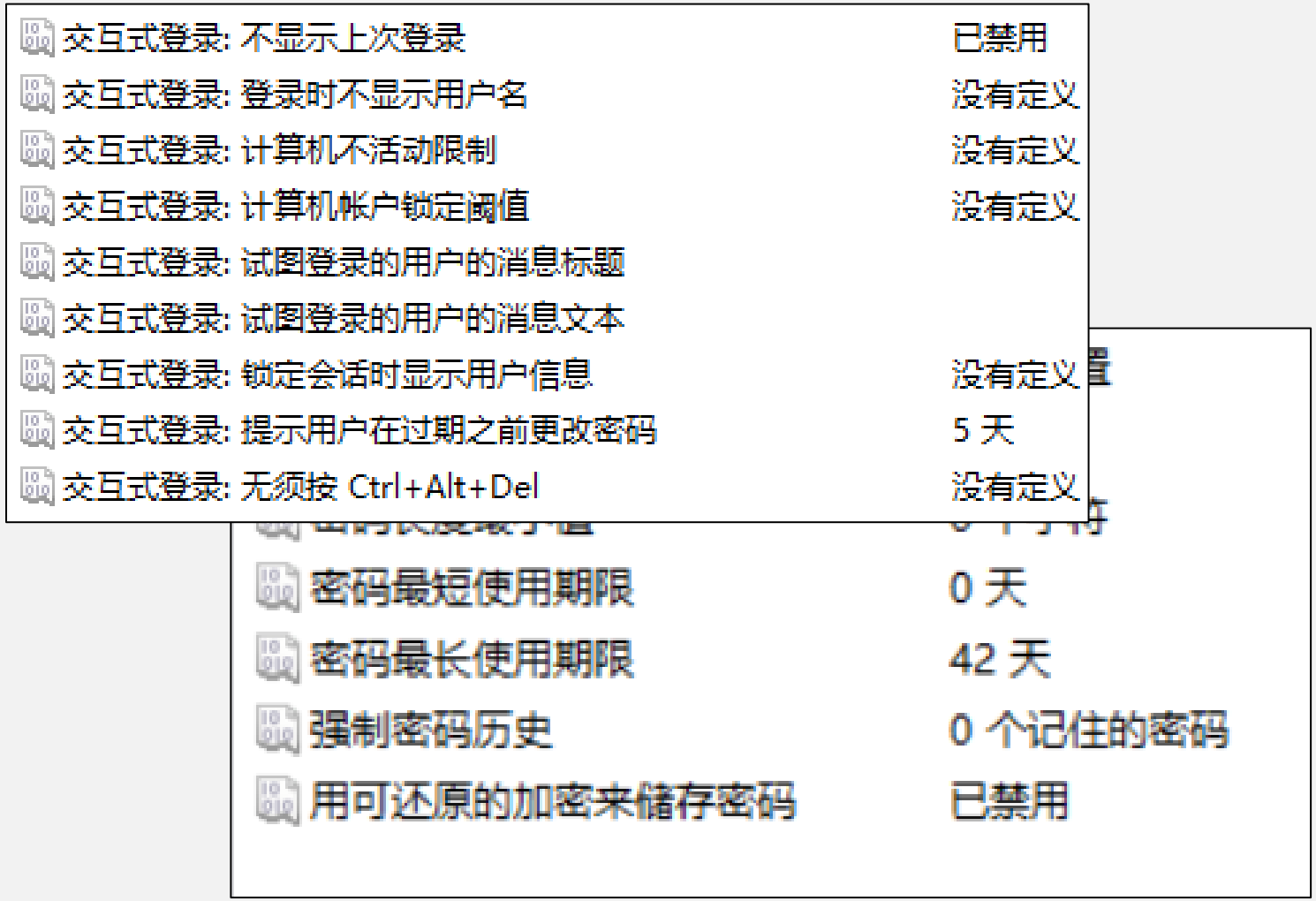
在某变电站,操作主机上发现大量USB插拔记录，用户解释为外协维护工程人员使用U盘，但实际上能看出有大量手机插拔记录。



现在工控安全都有哪些问题（安全配置缺失）

案例

- 在配合执法部门进行安全检查时，在多个行业的现场发现：工业主机操作系统安全配置基本为空白状态，操作用户计算机水平参差不齐，主机自身健康状态堪忧



现在工控安全都有哪些问题（关键控制设备无安全防护）

■ **案例**

在众多工业企业用户现场发现，重要工业控制设备前端无任何安全防护设备，冒用、篡改、攻击都会直接作用于工控设备。

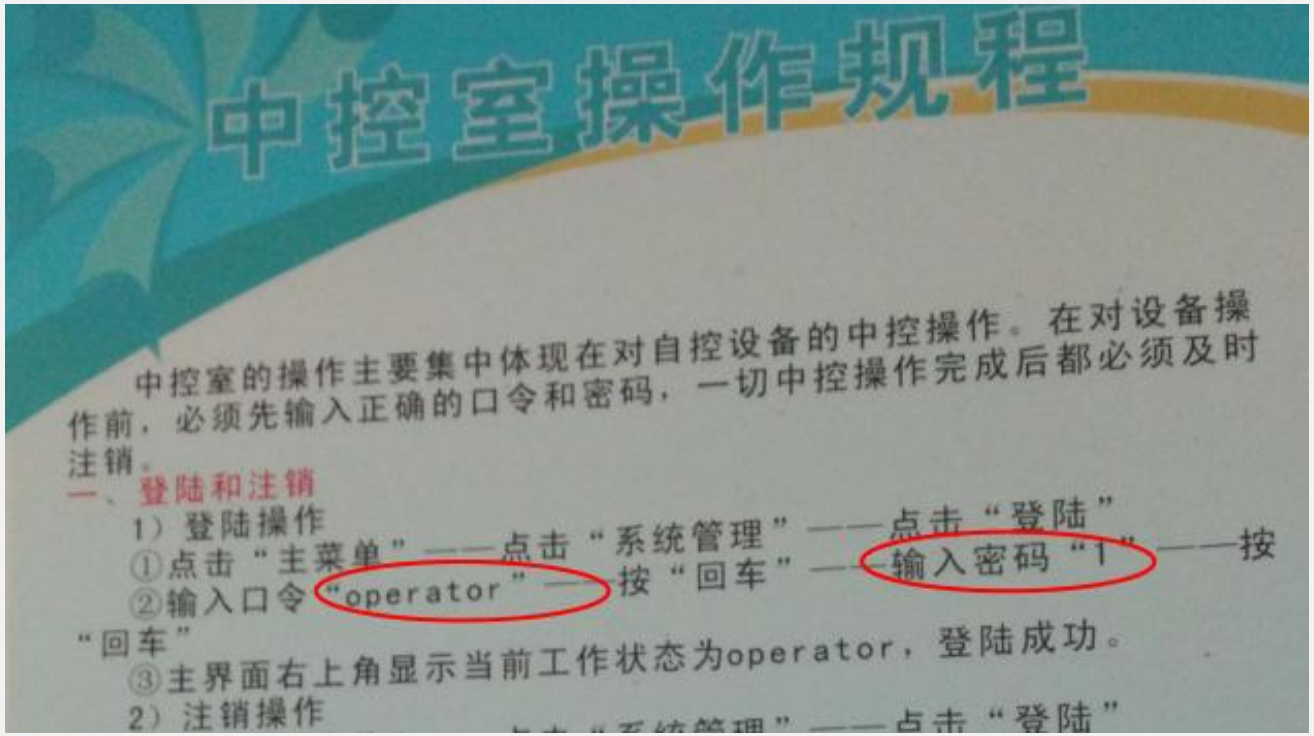
现场控制设备无防护

现场控制设备无防护

现在工控安全都有哪些问题（弱口令问题）

■ **案例**

- 在配合执法部门进行安全检查时，在多个行业的现场发现：工控系统的安全管理制度不完善是个普遍问题（如：弱口令现象普遍存在），人员的安全意识也亟待提升。
- 曾经在不同的工业现场发现重要的密码贴在桌面或者电脑机箱上。



图：控制系统弱口令

解决方案设计依据

发电厂工控网络安全解决方案设计依据

- **《电力监控系统安全防护总体方案》(国能安全[2015]36号文)**
- 《 GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》
- 《 GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求》
- 《 信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求》
- 《 信息安全技术 网络安全等级保护测评要求 第5部分：工业控制系统安全扩展要求》
- 《 信息安全技术 网络安全等级保护安全设计技术要求 第5部分：工业控制系统安全扩展要求》
- 《 工业控制系统信息安全防护指南》

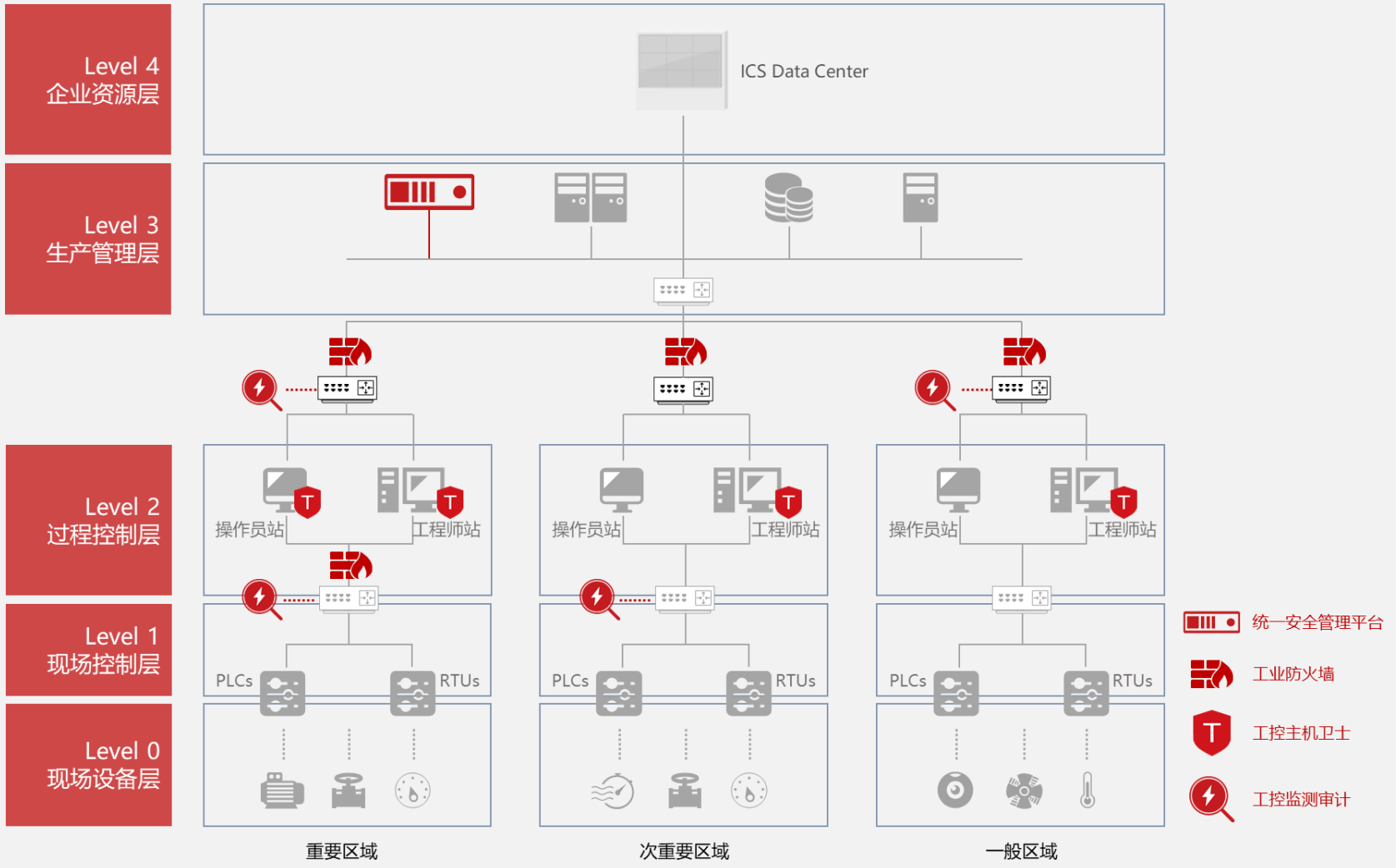
本方案重点解决以上政策标准中的核心问题

威努特工控解决方案模型

国内首家提出工业网络安全“**白环境**”解决方案体系的工控安全厂商，迄今已为上百家关键行业客户建立自主可控、安全可靠的工控安全整体防护体系

核心技术理念：

- 纵深防御
- 白名单机制
- 工业协议深度解析
- 实时监控审计
- 统一平台管理



工业控制系统“白环境”解决方案理念

方案核心安全理念

创新性提出了建立工控系统的**可信任网络白环境**和**工控软件白名单**的理念为客户构筑工控系统“安全白环境”整体防护体系，保护国家基础设施安全。

- 只有可信任的**设备**，才能接入控制网络
- 只有可信任的**消息**，才能在网络上传输
- 只有可信任的**软件**，才允许被执行

技术亮点及创新点

- 从“黑”到“白”
- 从“被动防御”到“主动防护”

国能安全36号文介绍

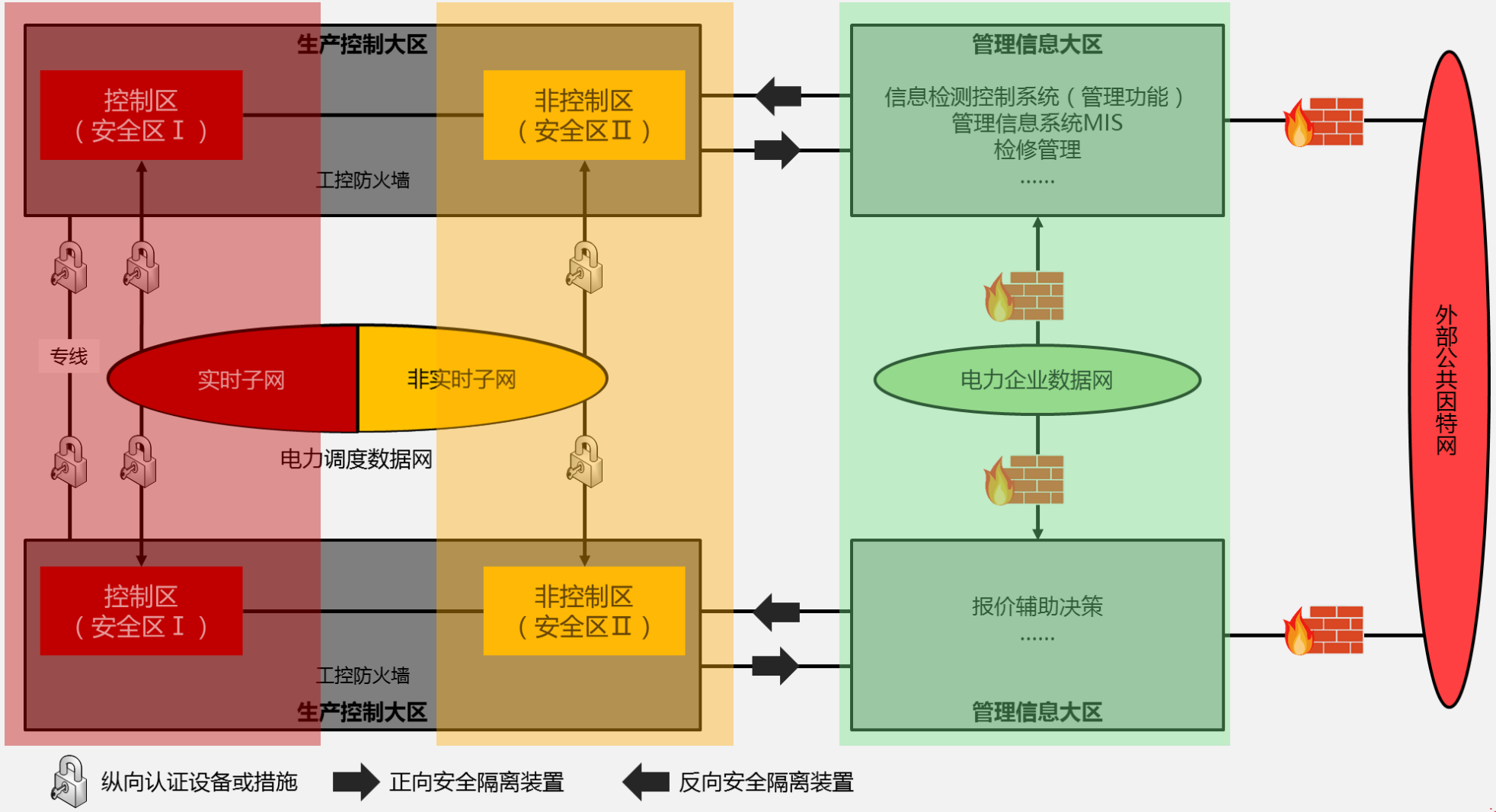
为了加强电力监控系统安全防护工作，根据《电力监控系统安全防护规定》（国家发展和改革委员会2014年第14号），国家能源局制定了《电力监控系统安全防护总体方案》等安全防护方案和评估规范，即国能安全[2015]36号。

国能安全[2015]36号

- **附件1电力监控系统安全防护总体方案**
- 附件2省级以上调度中心监控系统安全防护方案
- 附件3地级调度中心监控系统安全防护方案
- **附件4发电厂监控系统安全防护方案**
- 附件5变电站监控系统安全防护方案
- 附件6配电监控系统安全防护方案
- 附件7电力监控系统安全防护评价规范

附件：
《电力监控系统安全防护总体方案》
《省级以上调度中心监控系统安全防护方案》
《地级调度中心监控系统安全防护方案》
《发电厂监控系统安全防护方案》
《变电站监控系统安全防护方案》
《配电监控系统安全防护方案》
《电力监控系统安全防护评价规范》

安全分区、网络专用、横向隔离、纵向认证



边界安全防护

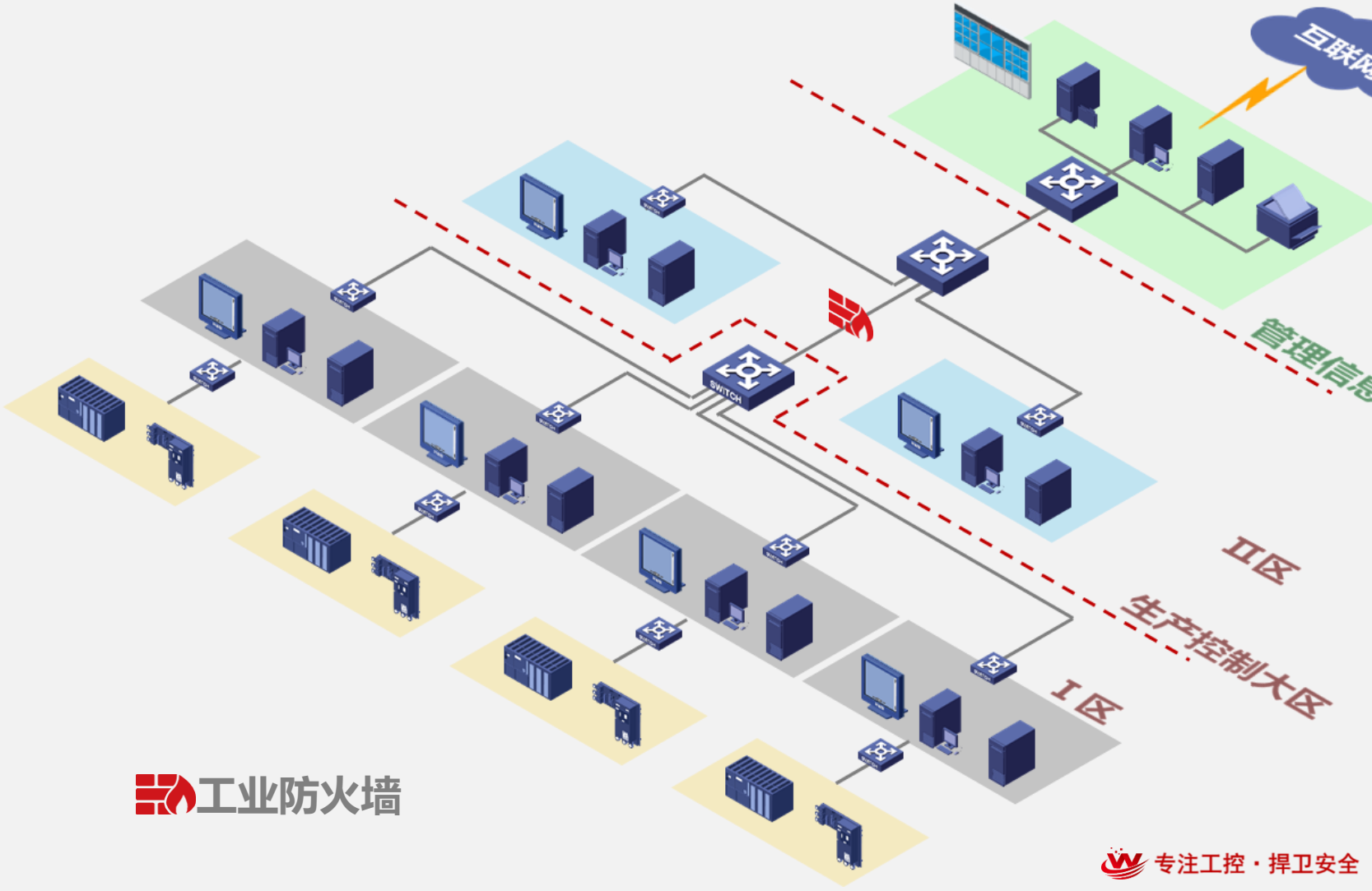
分类		基本要求
国能安全[2015]36号发电厂监控系统安全防护方案 **-4边界安全防护**	4.1横向边界防护	4.1.1 生产控制大区与管理信息大区边界安全防护；
		4.1.2 控制区（安全区I）与非控制区（安全区II）边界安全防护；
		41.3 系统间安全防护 火电厂内同属于控制区的各机组监控系统之间、机组监控系统与控制系统之间、统一机组的不同监控系统之间，同属于非控制区的各系统之间，各不同位置的场站网络之间，采用一定强度的逻辑访问控制措施；
	4.2纵向边界防护	a) 电厂控制大区系统与调度系统通过电力调度数据网进行远程通信时，采用认证、加密访问控制、加密等技术措施实现数据的远方安全传输以及纵向边界的安全防护； b) 参与系统AGC、AVC调节的电厂应当在电力调度数据网的边界配置纵向加密认证装置进行安全防护； c) 对于不具备建立调度数据网的小型火电厂可以通过远程拨号、无线等方式接入相应调度机构的安全接入区。
	4.3第三方边界安全防护	a) 火电厂控制大区中的业务系统与环保、安全等政府部门进行数据通信时，其边界应采用与生产控制大区与管理信息大区之间的防护方式进行隔离； a) 信息管理大区与外部网络之间采用防火墙、VPN等保证边界数据传输的安全; b) 禁止外部系统直接与生产控制大区的业务系统或设置采用远程拨号等方式直接访问，而不经过安全隔离。

边界隔离（Ⅰ区和Ⅱ区之间）

从Ⅱ区而来的非法访问，可能引起Ⅰ区实时网络的异常

部署对工业协议深度解析的隔离阻断装置实现网络分层分区，边界访问控制，避免无授权设备对区域的访问

部署对工业协议深度解析的隔离阻断装置实现基于通信“白环境”边界攻击防御和过滤



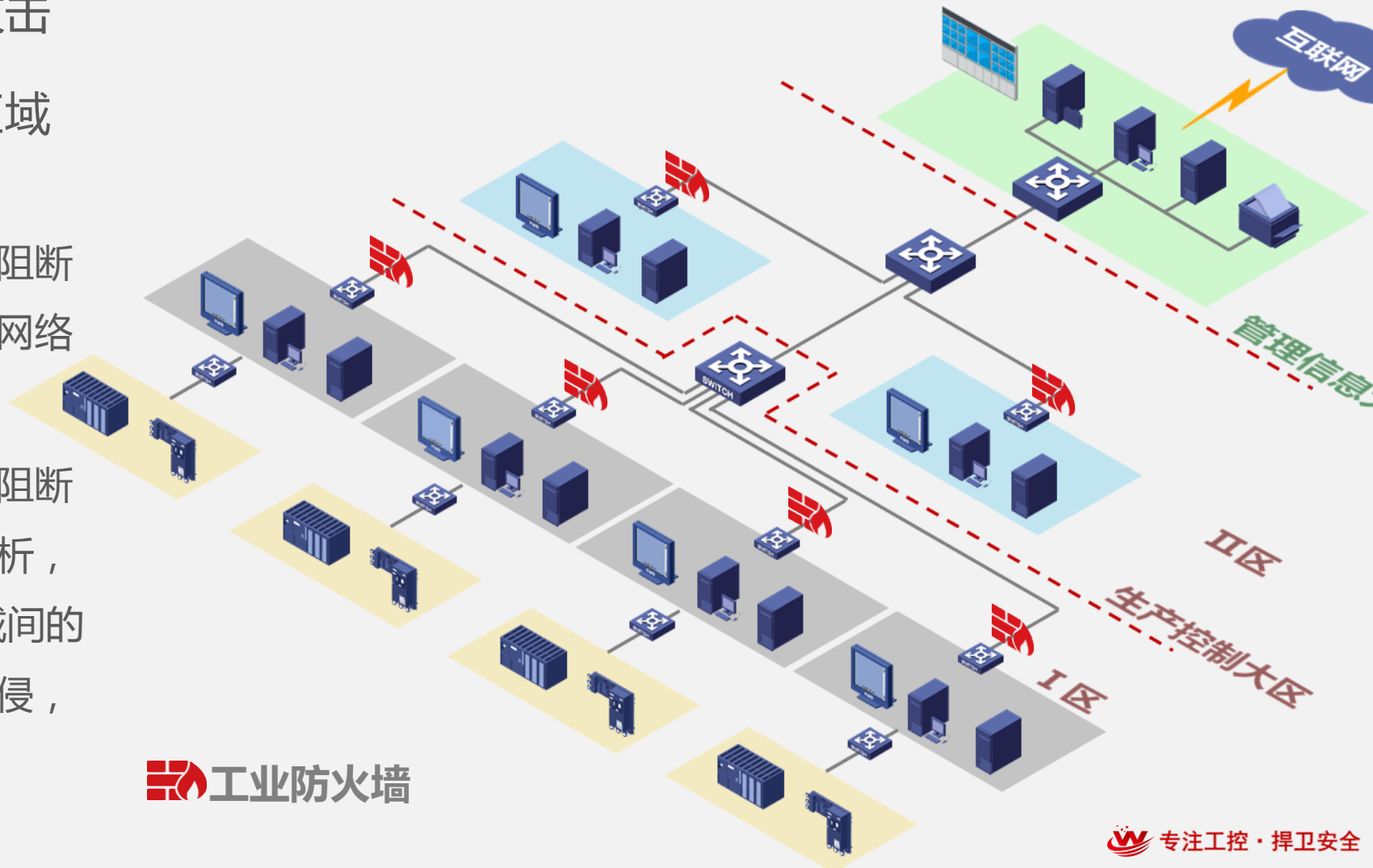
区域隔离（ 生产控制大区内部）

针对某个区域指定的非法攻击

区域内部问题影响至其他区域

部署对工业协议深度解析的隔离阻断装置实现基于区域和功能的区域网络划分及隔离

部署对工业协议深度解析的隔离阻断装置实现对工业专有协议深度解析，建立通讯“白环境“，阻止区域间的越权访问，病毒、蠕虫扩散和入侵，将危险源控制在有限范围内

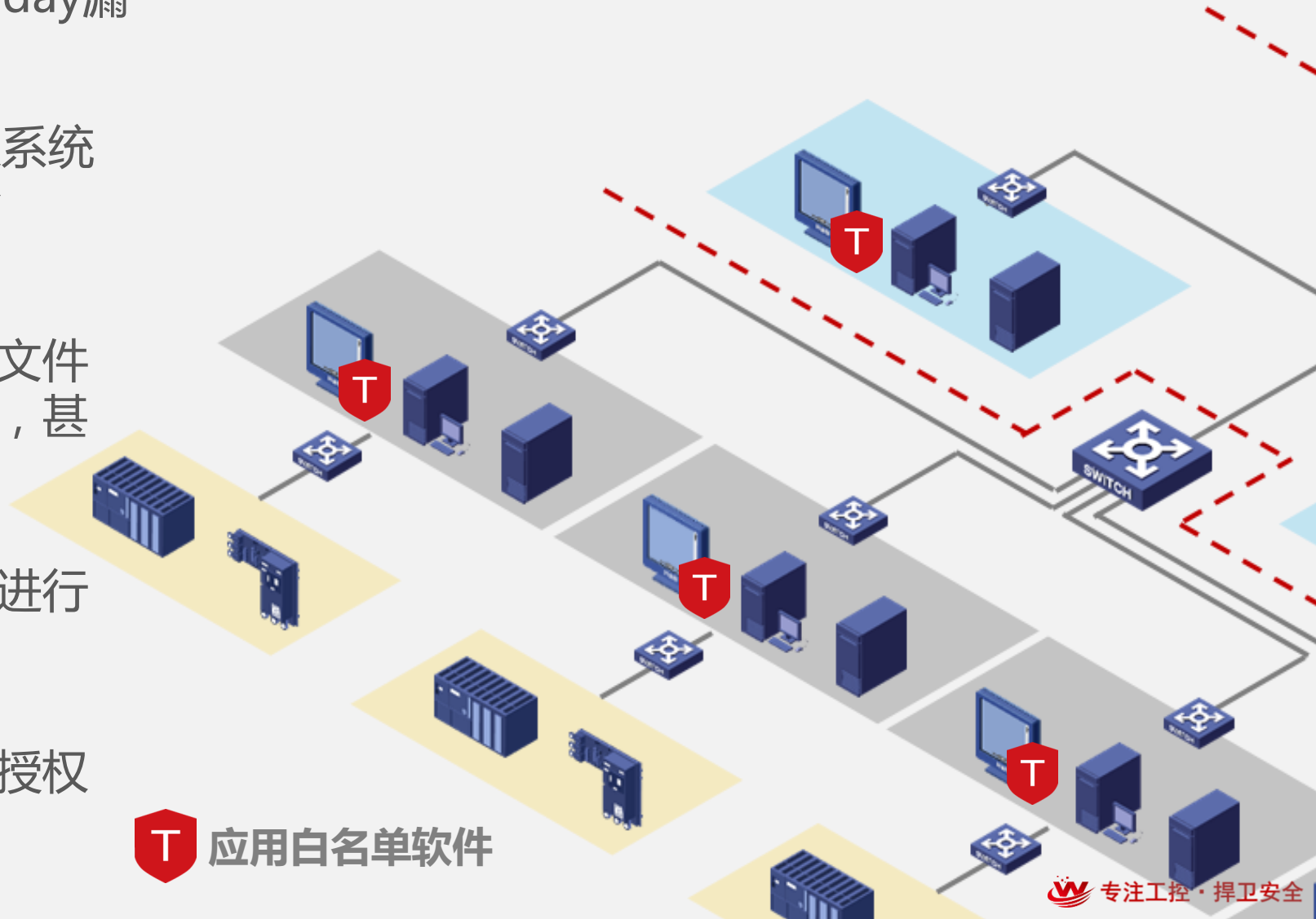


主机与设备安全防护

分类		基本要求
国能安全[2015]36号发电厂监控系统安全防护方案 **-5.2主机与网络设备加固**	主机加固	发电厂厂级信息监控系统等关键应用系统的主服务器，以及网络边界处的通信网关机、web服务器等应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专用软件强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安装应当经过测试。
	网络设备加固	a）非控制区的网络设备与安全设备应当进行身份鉴别、访问权限控制、会话控制等安全配置加固。可以应用电力调度数字证书，在网络设备和安全设备实现支持HTTPS的纵向安全web服务，能够对浏 b）览器客户端访问进行身份认证及加密传输。 生产控制大区中除安全接入区外，应当禁止具有无线通信功能的设备；管理信息大区业务系统使用无线网络传输业务信息时，应当具备接入认证、加密等安全机制。
	外设管控	应当对外部存储器、打印机等外设的使用进行严格管理。

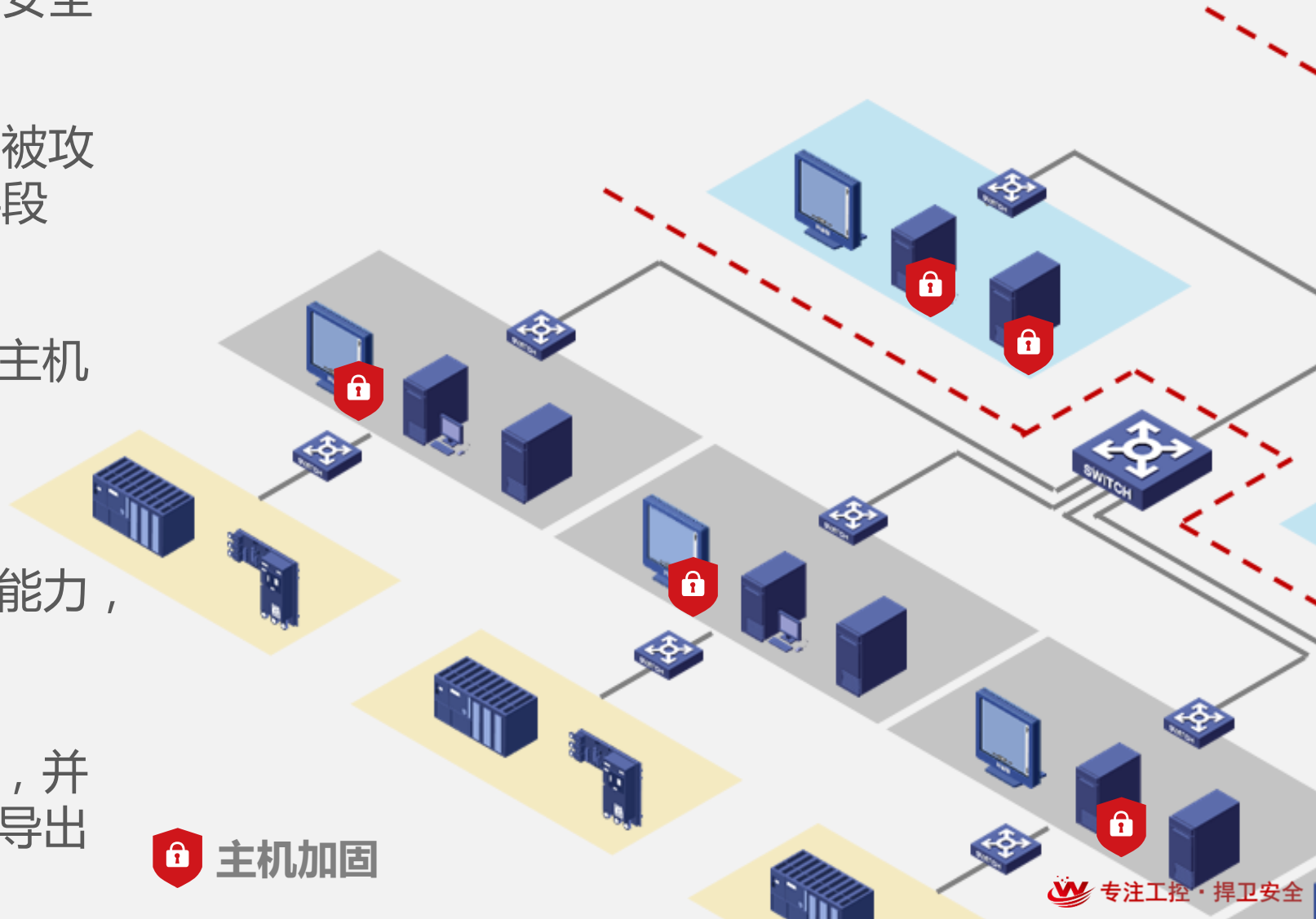
主机安全防护

- 病毒、木马感染上位机，甚至0-day漏洞的利用导致系统不可用
- 上位机系统安全策略缺失，引起系统或用户行为失当，导致安全风险
- 部署应用白名单软件建立可执行文件“白名单”，阻止恶意软件执行，甚至是0-day漏洞的利用
- 通过应用白名单软件对操作系统进行加固，如注册表、配置文件等
- 通过应用白名单软件实现阻止未授权软件的安装



主机加固

- 个人计算机使用水平参差不齐，安全意识存在差异
- 计算机自身安全脆弱，容易成为被攻击的对象，且缺少统一配置的手段
- 通过主机加固类的产品统一工业主机操作系统安全配置
- 提高工业主机操作系统访问控制能力，如提高至强制访问控制
- 对操作事件如登陆、功能停用等，并提供日志的查询、删除、备份和导出



综合安全防护

分类		基本要求
国能安全[2015]36号发电厂监控系统安全防护方案 **-5综合安全防护**	5.1 入侵检测	生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计；
	5.3应用安全控制	发电厂厂级信息监控系统等业务系统应当逐步采用用户数字证书技术，对用户登录失败处理功能，根据身份与权限进行访问控制，并且对操作系统行为进行安全审计。对于发电厂内部远程访问业务系统的情况，应当进行会话控制，并采用会话认证、加密与抗抵赖等安全机制。
	5.4 安全审计	生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析，及时发现各种违规行为以及病毒和黑客的攻击行为。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。
	5.5 专用安全产品的管理	安全防护工作中涉及使用横向单向安全隔离装置、纵向加密认证装置、防火墙、入侵检测系统等专用安全产品的，应当按照国家有关要求做好保密工作，禁止关键技术和设备的扩散。
	5.7 恶意代码防范	应当及时更新特征码，查看查杀记录。恶意代码更新文件的安装应当经过测试。禁止生产控制大区与管理信息大区公用一套防恶意代码管理服务器；
	5.8 设备选型与漏洞整改	发电厂电力监控系统在设备选型及配置时，应当禁止选用经国家相关管理部门检测认定并经国家能源局通报存在漏洞的风险的系统及设备；对于已经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统与设备的运行管理和安全防护。

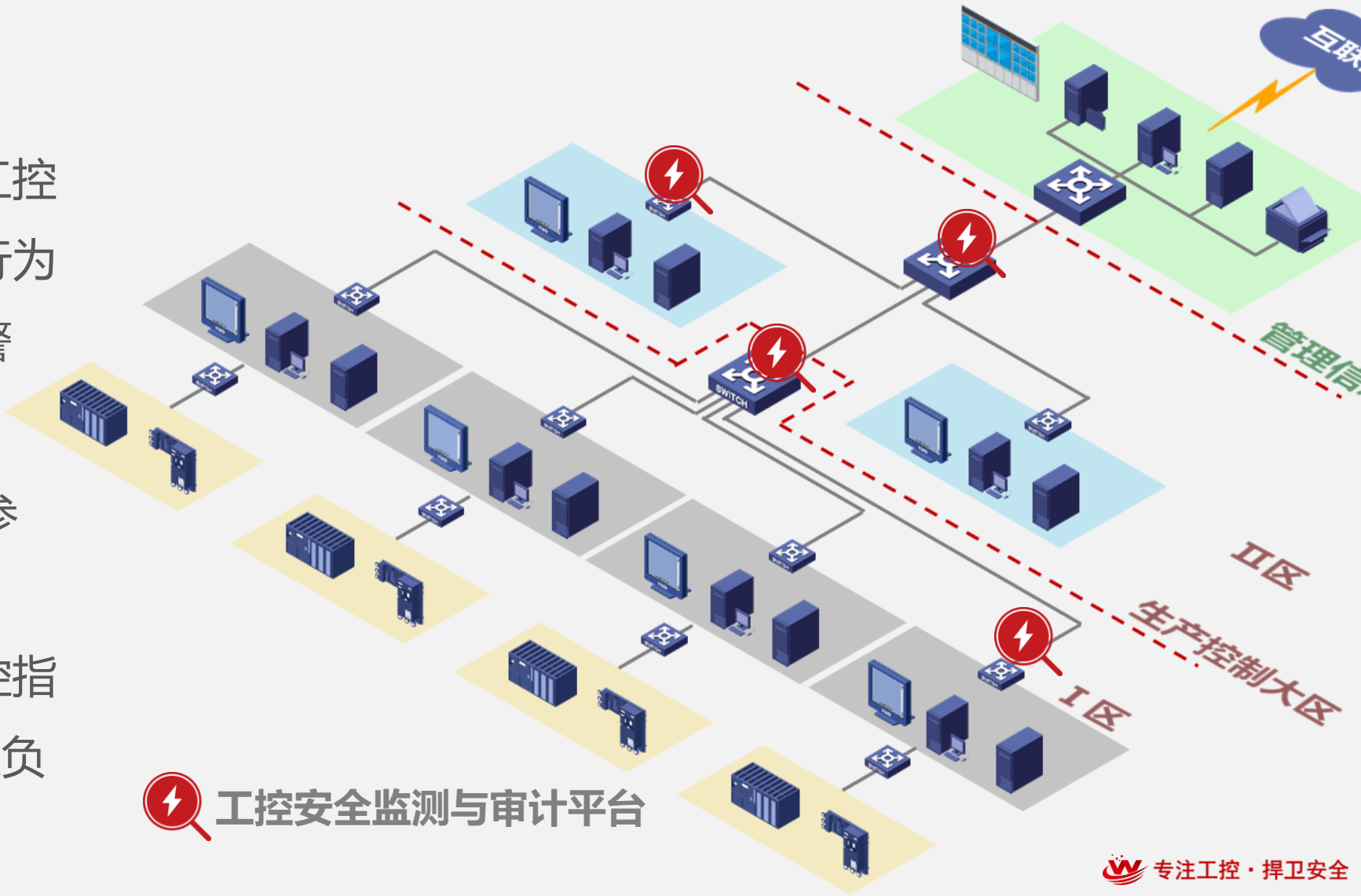
工控网络监测与审计

隐蔽不可知的恶意流量

部署监测与审计平台记录工控协议通信，建立正常通信行为模型，对异常操作进行告警

识别并检测工控协议攻击、TCP/IP攻击、网络风暴、参数阈值检测

对工程师站组态并更、操控指令变更、PLC程序下装以及负载变更等关键事件告警



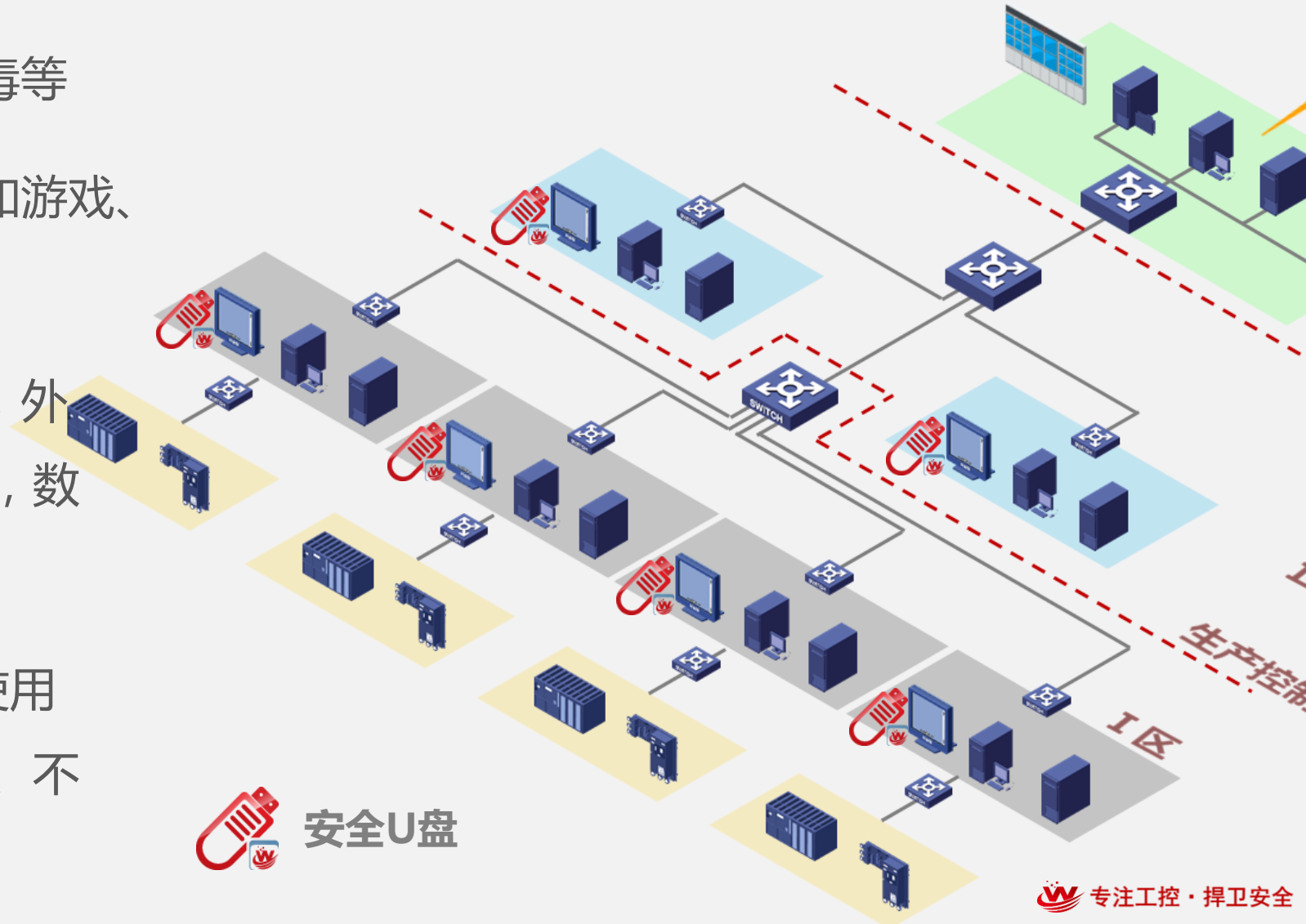
文件安全传递

普通U盘随意插拔，带来未知病毒等

通过U盘带入与工作无关数据，如游戏、视频、程序等，导致系统不可用

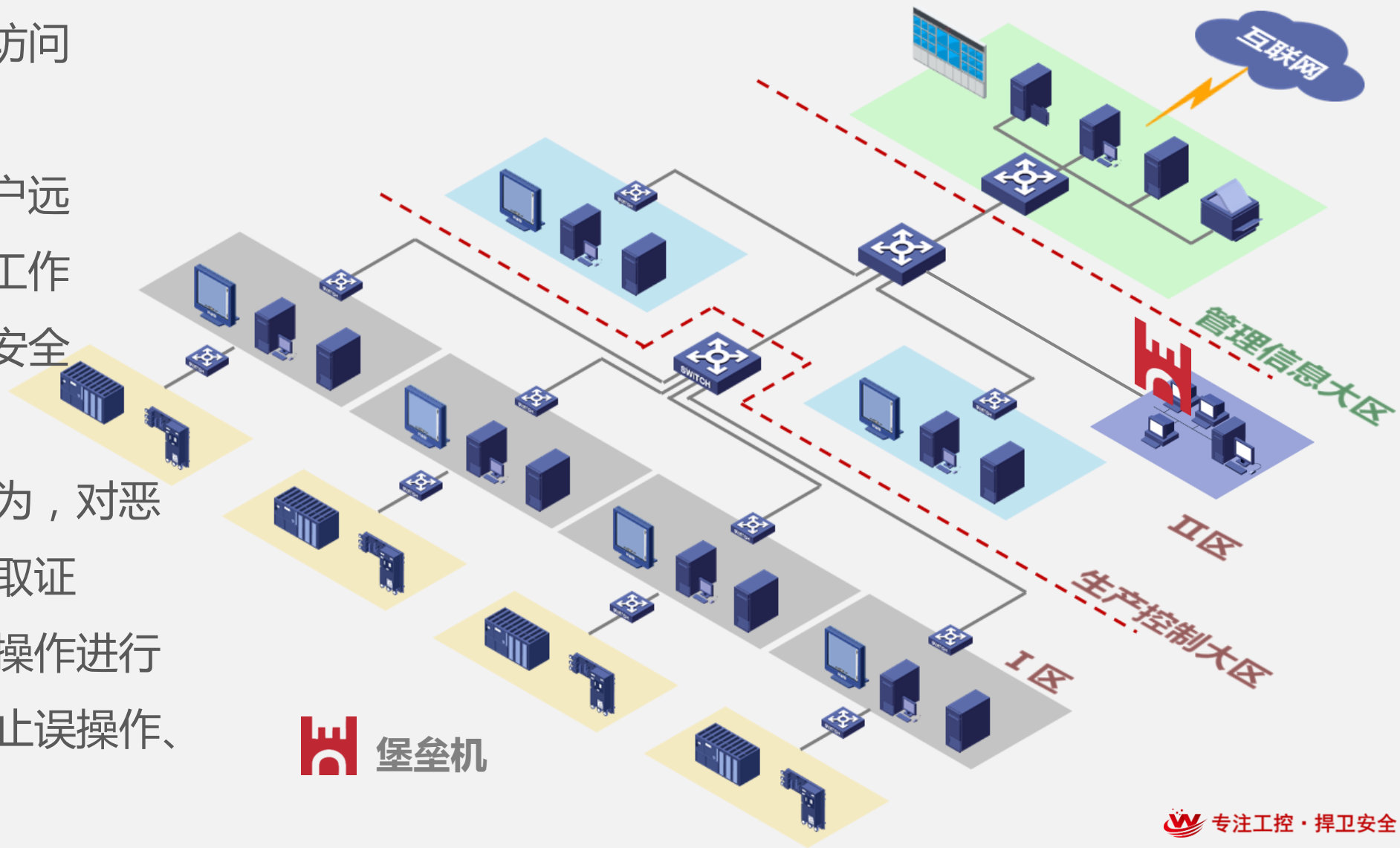
采用安全U盘，仅能在内部使用，外部无法使用，自带硬件安全芯片，数据安全存储

针对普通U盘，控制普通U盘的使用权限，包括禁止使用、只读使用、不控制



应用数据安全之网络设备防护&审计&身份鉴别

- 阻止非授权用户访问网络、安全设备
- 阻止非授权的用户远程维护服务器、工作站、网络设备、安全设备等
- 全程记录维护行为，对恶意维护行为进行取证
- 对远程维护行为操作进行监测、审计，阻止误操作、恶意操作



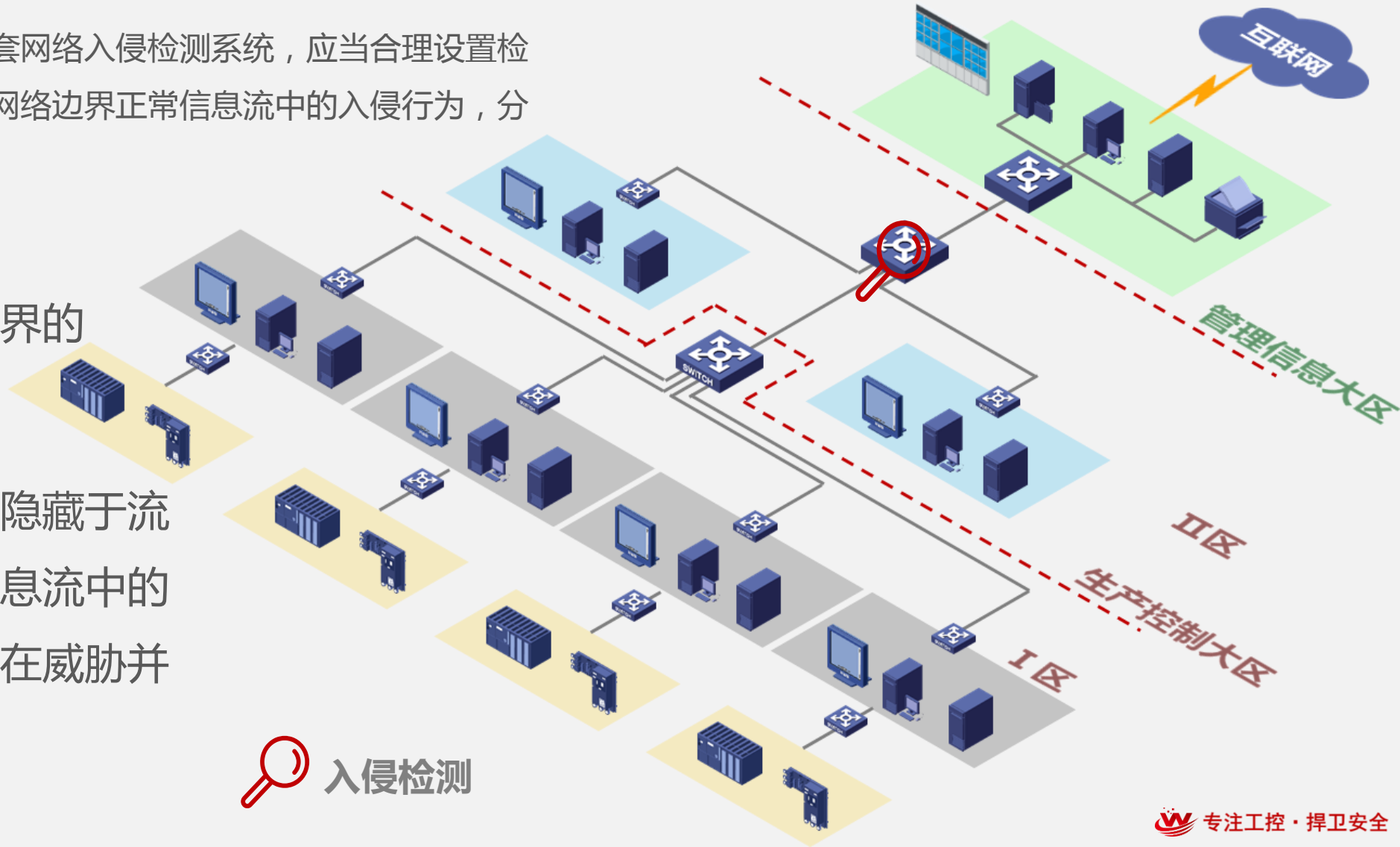
入侵检测

国能安全[2015]36号：

生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计

隐藏于流经网络边界的入侵行为

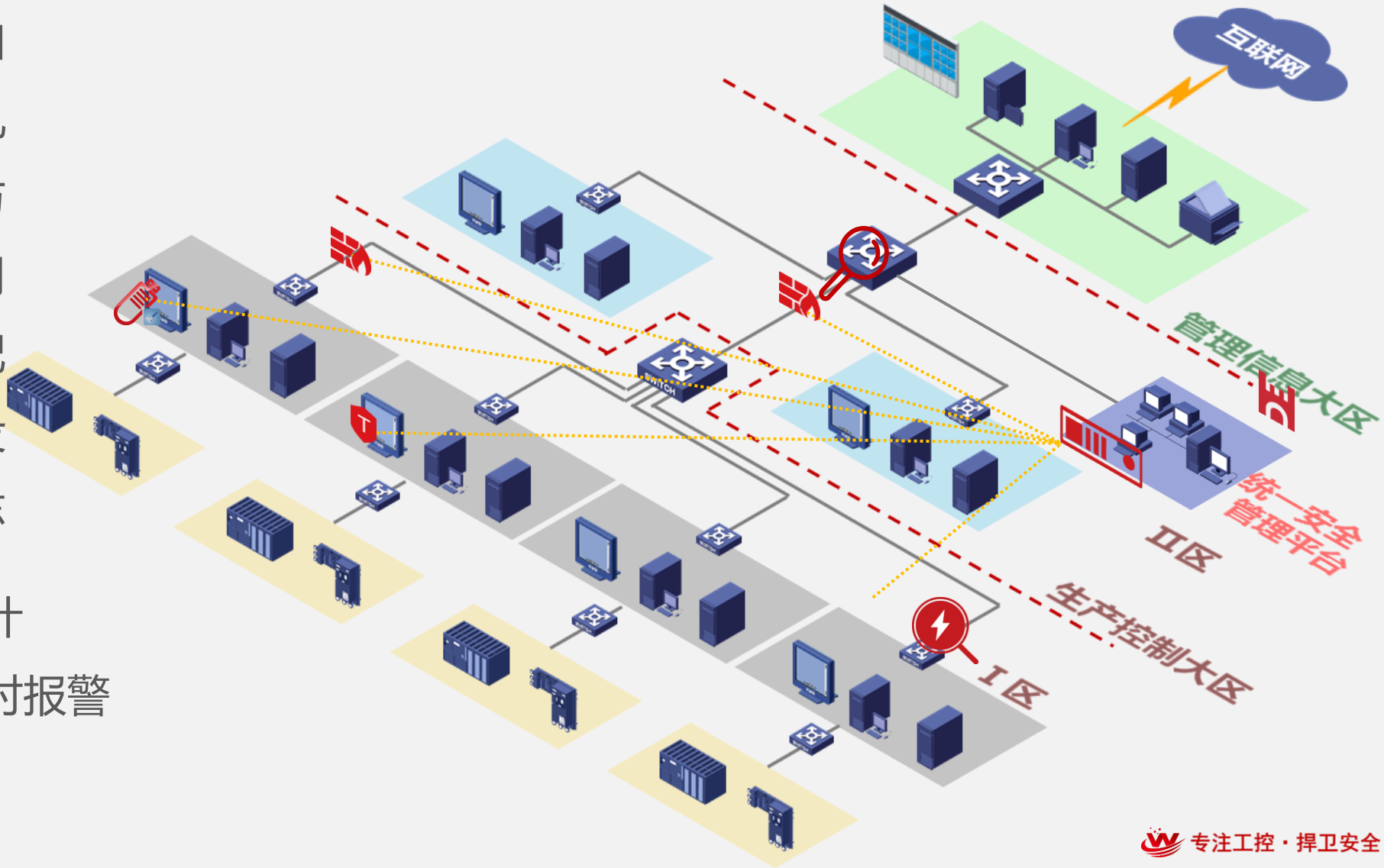
部署入侵检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计



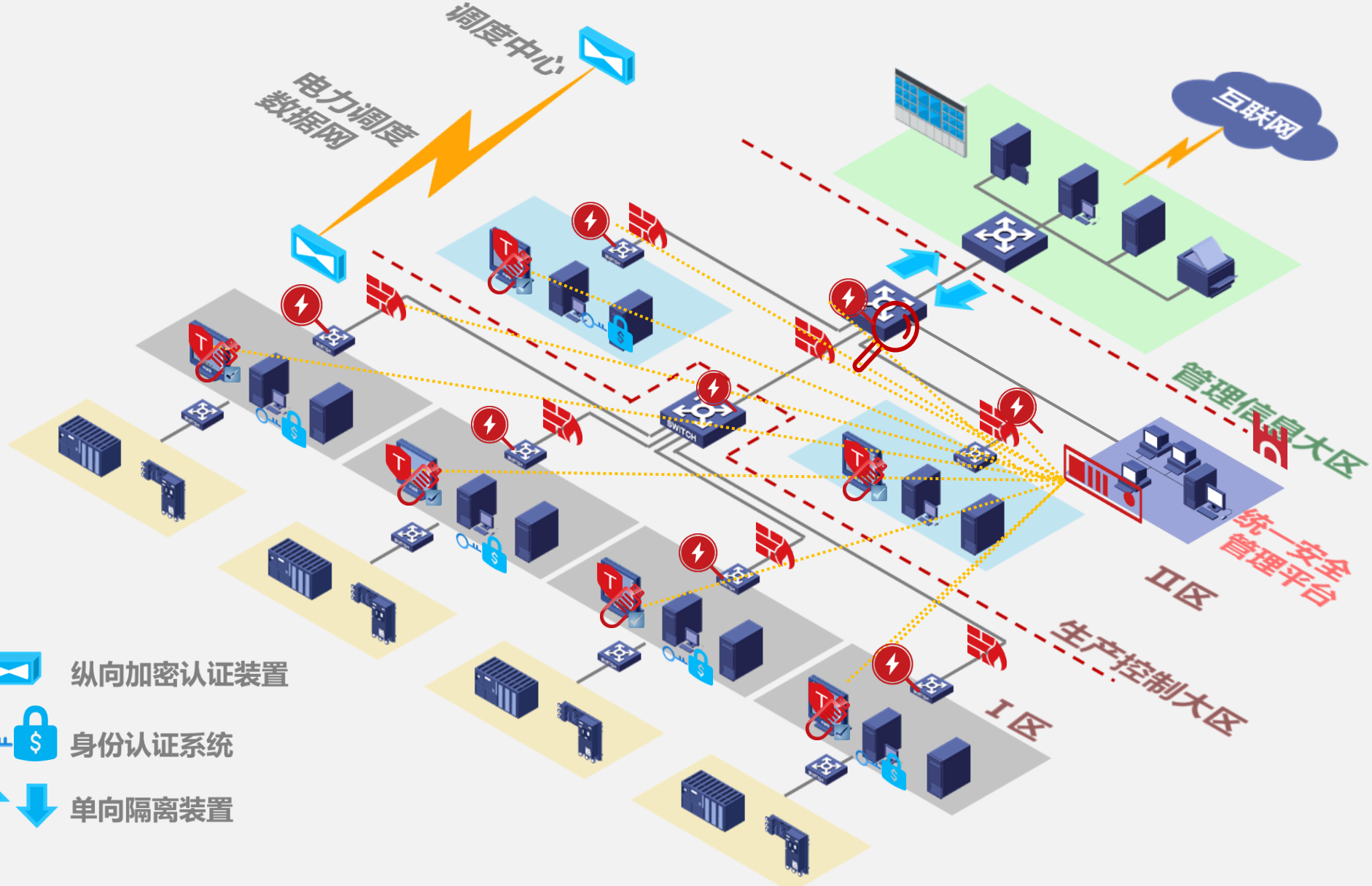
统一安全管理

集中管理安全设备：如工业防火墙、工控主机卫士、工控安全检测与审计平台，实现工控网络的拓扑管理、安全配置及安全策略管理、设备状态监控、告警日志等

- 集中的安全日志审计
- 工作站终端异常实时报警
- 分级分权限管理



网络安全总体防护方案部署示意图



纵向加密认证装置

身份认证系统

单向隔离装置

工业防火墙

工控主机卫士

监测审计平台

统一安全管理平台

堡垒机

入侵检测

网络安全-边界安全防护

《工业控制系统信息安全防护指南》第三条“边界安全防护”

（一）分离工业控制系统的开发、测试和生产环境。

（二）通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。

（三）通过**工业防火墙**、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。

《36号》文附件4《发电厂监控系统安全防护方案》

第四部分 4.1.2 控制区（安全I区）与非控制区（安全II区）边界安全防护

安全I区与安全II区之间应当采用具有访问控制功能的网络设备、安全可靠的硬件防火墙或者相当功能的设备，实现**逻辑隔离**、**报文过滤**、**访问控制**等功能。

《GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求》

应在网络边界部署访问控制设备，启用访问控制功能；.....

应对进出网络的信息内容进行过滤，实现对**应用层等协议命令级的控制**；.....

网络安全-安全审计

《工业控制系统信息安全防护指南》第三条“安全监测与应急演练”

（一）在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。

（二）在重要工业控制设备前端部署具备**工业协议深度包检测功能**的防护设备，限制违法操作。

《36号》文附件4《发电厂监控系统安全防护方案》

第五部分综合防护5.4小节安全审计中明确要求在生产控制大区的监控系统应当**具备安全审计系统**，能够及时发现各种违规行为及病毒和黑客的攻击行为。

《GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求》

7.1.2.3安全审计中相关测试要求明确提出可以对网络设备运行状况、**网络流量、用户行为等进行监测**。

主机安全-恶意代码

《工业控制系统信息安全防护指南》第一条“安全软件选择与管理”

（一）在工业主机上采用经过离线环境中充分验证测试的防病毒软件或**应用程序白名单软件**，只允许经过工业企业自身授权和安全评估的软件运行。

（二）建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。

《36号》文附件4《发电厂监控系统安全防护方案》

第五部分综合防护5.7小节恶意代码防范中明确要求，应及时更新特征码、查看查杀记录。**（使用”白名单“安全机制替代传统杀毒软件，更满足工控系统安全防护特点）**

《GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求》

7.1.3.6恶意代码防范中相关测试要求明确提出可以对主要服务器、**主机等是否安装了实时检测与查杀恶意代码的软件产品。**

主机安全-外部接口

《工业控制系统信息安全防护指南》第四条“物理和环境安全防护”

（一）对重要工程师站、数据库、服务器等核心工控控制软硬件所在区域采用访问控制、视频监控、专人值守等物理安全防护措施。

（二）拆除或封闭工业主机上不必要的USB、光驱、无线等接口。**若确需使用，通过主机外设安全管理技术手段实施严格访问控制”。**

《36号》文附件4《发电厂监控系统安全防护方案》

第五部分综合防护5.2小节主机与网络设备加固中明确要求**“应当对外部存储器、打印机等外设的使用进行严格管理。**

《GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求》

主机安全测评单元也有明确要求“未拆除主机的软盘驱动,光盘驱动,USB接口等”，**如果不能拆除应通过技术手段对外接移动存储设备进行安全管控。**

解决方案总结

	1	2	3	4	5
关键步骤：	安全分区 使用逻辑隔离产品进行安全分区。	重点防护 重要设备使用安全产品进行重点保护。	安全审计 网络全流量、操作行为的监控、记录、审计。	主机防护 配置管理 病毒防护	统一管理 安全产品集中管理
安全产品:	工业防火墙 网闸	工业防火墙 网闸	工控安全监测与审计系统 堡垒主机	工控主机卫士	统一安全管理平台
解决问题：	从互联网而来的非法访问 远程维护通道	远程维护通道 针对漏洞的攻击	用户有意无意的恶意操作	移动存储介质滥用 配置管理、病毒防护	安全产品统一管理

03

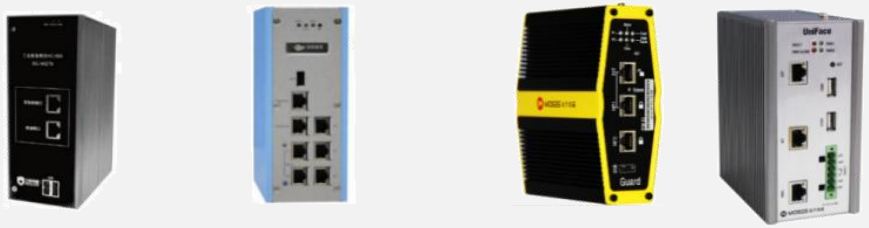
第三部分
工业控系统信息安全产品介绍

工控信息安全专用产品总述

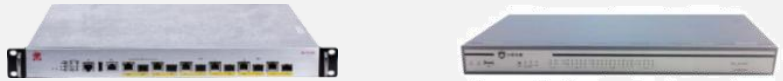
边界防护类-工业防火墙

导轨式工业防火墙

威努特



机架式工业防火墙



威努特

- 此类产品多采用工业级的架构，采用低功耗、无风扇设计，来满足工业现场特殊的环境需求；
- 部署方式通常以串接方式工作，部署在工控以太网与企业管理网络之间、厂区不同区域之间，控制层与现场设备层之间。通过一定的访问控制策略，对工控系统边界、工控系统内部区域进行边界保护；
- 工控防火墙、工控隔离产品均属于边界防护类。

工业防火墙功能特点

传统防火墙基础功能

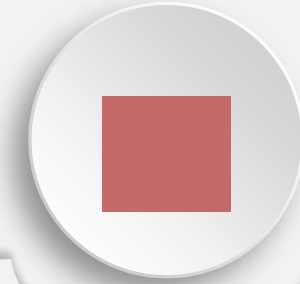
继承传统防火墙的基本访问控制功能，具备对源、目的IP，源、目的端口，协议类型5元组的控制能力

支持工业协议

能够对工业通信协议进行解析，如主流的OPC、Siemens S7、Modbus等协议的深度报文解析，弥补传统IT防火墙对于工业协议解析的空白

白名单机制

大多采用“白名单”机制对边界进行安全防护，即将信任的数据、协议放入到可信列表中，拒绝一切非可信任流量



更符合工业现场特点

一般支持学习、告警、阻断三种工作模式，符合工业用户对边界防护产品的心理需求

对工业防火墙功能认识误区

对于工业防火墙，普遍存在下面2个误区：

1 工业防火墙就是传统防火墙换上工业外壳

一部分用户会认为工业防火墙就是传统防火墙换了工业的外壳，功能没啥区别，换汤不换药，但实际上工业防火墙与传统防火墙在设计原则、工作机制、功能配置等方面有巨大差异，对工业协议的深度解析，对工业网络流量自学习建模的工作机制是工业防火墙独有的特点。

2 过分依赖自学习，缺乏人工配置

自学习确实是形成白名单的一种很好的方式，但却容易受到不固定因素的影响，如学习时间不足、部分业务数据只有在特殊的情况下才能产生，这些因素都直接影响白名单策略的完整性，所以自学习+人工配置形成的白名单策略才能更好的应用于工业现场。

边界防护类-隔离产品

威努特

- 隔离产品一般泛指网闸,目前在电力行业、石油行业应用较多，从功能角度可划分双向隔离网闸和单向隔离网闸；
- 部署方式通常以串接方式工作，部署在生产控制网与管理网之间。如部署在电厂的I,II区与III,IV区之间。满足通用工业控制系统由管理网与办公网之间单项传输的技术要求；
- 目前网闸产品因其功能的特殊性，仅适用于传统网络和工业网络的一些特殊场景。

网闸设备产品特点

架构特殊

网闸设备内部设置两套独立主机，每个主机运行独立的安全操作系统和应用系统，这两套主机分别通过网络连接生产控制区网络和管理信息大区网络

协议隔离

隔离装置的内外网主机之间不提供反向数据通道通信，可以阻断管理信息大区到生产控制大区通信途径，同时支持1bit返回模式，以进行数据验证

关键操作检测

隔离装置通过数据代理的方式来禁止生产控制区网络应用程序与管理信息大区应用程序之间进行直接连接，从而在一定程度上杜绝了病毒及木马携带传输的可能性

网闸VS工业防火墙

网闸产品	工业防火墙产品
■ 以安全为主，在保证安全的前提下，支持尽可能多的应用； ■ 在安全方面，虽然对数据包进行了拆包处理，但对于数据的载荷部分未做深度解析，形成安全空白区； ■ 对于数据的转发延迟性高，不适用于对数据传输低延迟性要求高的场景。	■ 防火墙是以应用为主、安全为辅，在支持尽可能多的应用的前提下，来保证使用的安全； ■ 在安全方面，能够对数据包进行深度解析，甚至做到指令集解析； ■ 对数据转发延迟性小，更适合工业网络环境。

网闸产品与防火墙产品无法衡量其好与坏，更多的区别在于应用场景的不同，防火墙适用于多种业务场景，而网闸产品只适用于对数据延迟性要求不高的业务场景。

监测审计类

导轨式监测审计系统

威努特

机架式监测审计系统

威努特

- 此类产品多采用工业级的硬件架构，采用低功耗、无风扇设计，来满足工业现场特殊的环境需求，如低温、高湿等；
- 此类产品通过镜像接口分析网络流量，及时发现网络流量或设备的异常情况并告警，通常不会主动去阻断通信；
- 旁路的部署方式，也使得这类产品不会因为自身的故障而影响工控系统的正常运行，这样的部署方式更容易让工业用户接受。

监测审计系统功能特点

自学习建立通信模型

利用白名单的方式，建立可信任的业务数据流模型，通过该模型来判断通信的合法性。部分工控协议的解析为指令级,对于工业现场来说，意义较大，可以脱离于系统原有厂商的监控系统，作为第三方监控手段对事后追溯提供依据

无需更新特征库

利用白名单的方式，摆脱原有IT系统中涉及的IDS，IPS需要不断升级“库”来满足安全需求的束缚

关键操作检测

由白名单机制衍生出来的对工业现场业务中的关键操作（如对工程师站组态变更、操控指令变更、PLC下装、负载变更等）违规报警、无流量，异常流量报警等更加符合工业现场需求

对监测审计系统的认识误区

对于监测审计系统，普遍存在下面2个误区：

1 仅是换了一个工业外壳

与工业防火墙面临同样问题，一部分用户会认为监测换了工业的外壳，功能没啥区别，换汤不换药，但实际上其设计原则、工作机制、功能配置等方面有巨大差异，对工业协议的深度解析，对工业网络流量自学习建模的工作机制是工控监测审计独有的特点。

入侵检测系统（IDS）

超低的误报率和漏报率

采用TCP/IP数据重组、目标和应用程序识别、完整的应用层有限状态追踪、应用层协议分析、先进的事件关联分析技术以及多项反IDS逃避技术，提供业界超低的误报率和漏报率。

简单的部署方式

采用旁路部署方式，不会对网络造成任何影响。

强大的分析检测能力

内置丰富的攻击特征库，结合硬件加速信息包捕捉技术来探测包括PLC等控制设备的拒绝服务攻击漏洞、缓冲区溢出攻击漏洞等典型工控漏洞的攻击行为，并及时告警。

丰富的统计报表

能够为用户提供丰富的动态图形报表，以及数十种分析报表模版和向导式的用户自定义报表功能。

主机安全类

工控系统中的主机设备，如工程师站、操作员站等是工控系统的风险点，病毒的入侵、人为的误操作等威胁主要都是通过主机类设备进入工控系统。

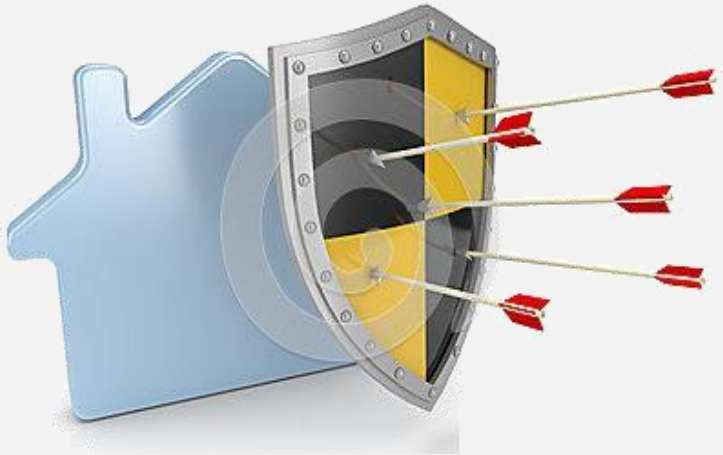
主流主机安全防护产品

白名单防护类

通过在主机上安装客户端程序，确保只有可信的程序、进程才允许运行，防止恶意程序的侵入；

主机加固类

结合等级保护合规性要求，对主机操作系统进行策略性安全加固，增强主机安全防护能力。



主机安全产品功能特点

白名单产品

- 采用「白名单」技术，为工作站即电脑主机创造一个安全可控的环境，主要功能是对可执行文件保护、U盘的使用控制等。因工业现场业务环境相对”确定”，所以白名单产品容易被工业用户接受，既防止了恶意程序的入侵，也避免的传统主机安全防护产品（杀毒软件）误差、漏杀的问题；
- 利用动态跟踪安装包安装技术自动将安装过程中的可执行文件或临时释放的临时可执行文件识别并添加到白名单库中，满足工业现场软件升级的需求。

加固式产品

- 加固式产品主要是对主机的内核级安全加固防护，通过对文件、目录、进程、注册表和服务进行的强制访问控制，制约和分散原有系统管理员的权限，把普通的操作系统从体系上升级，从而满足等级保护标准中对于主机安全的要求。

对主机安全产品的认识误区

对于主机安全防护产品，普遍存在下面2个误区：

1 白名单软件或主机加固软件会不会也如杀毒软件一般，不适用于工业现场

从原理的角度白名单软件是工作在操作系统层面的，是完全没有可能影响系统的运行；而主机加固软件是工作在驱动层面的，那么是否影响系统的运行，还要取决于硬件、软件的驱动。如出现驱动问题，也会出现影响系统运行的情况。

2 也会存在扫描、查杀等动作，影响系统运行

从工作方式、工作原理的角度，白名单软件和主机加固软件采用主动防御的方式，均不存在扫描、查、杀的动作，故不会出现影响系统运行的情况。

监测审计类-堡垒机

威努特

- 堡垒机一般部署在工业网络中管理大区，主要的作用是对运维人员维护过程的全面跟踪、控制、记录、回放，同时对自然人的身份进行统一授权；
- 在工业现场移动设备的交叉使用，把病毒、木马引入到原本脆弱的工控系统；运维人员的不当操作，引起生产事故，以及工控设备配置文件无备份。都给工控系统带来很大的风险，所以在此背景下，为有效解决工业控制系统现场运维风险，堡垒机应运而生。

安全管理类-管理平台

威努特

- 安全管理类产品主要的用途是对部署在工业网络中的安全设备进行集中监测、统一管理，在工业网络中有诸多无人场景，如市政燃气、油田等行业现场均有无人值守站；

- 安全管理类产品一般部署在中心级测，如生产区的机房、管理区的机房，是非高温、非高湿的工作环境，所以安全管理类产品在设计时大多采用传统X86架构。

管理平台的功能特点

安全设备集中管理

集中管理工控网络中的安全设备，包括设备状态监控、拓扑管理、系统配置管理、日志管理等

主机安全统一管理

统一管理工控网络中的主机安全软件，包括模板配置、策略下发、主机状态监测、日志管理等

日志管理分析

对工控网络中的安全日志（如：攻击日志、流量日志、访问日志、主机日志、系统日志）进行汇总、关联分析并形成报告，为工控网络安全事件分析和调查取证提供依据

安全检测类-漏洞挖掘&漏洞扫描

漏洞挖掘平台

威努特

漏洞扫描平台

威努特

- 漏洞挖掘和漏洞扫描产品均属于安全检测类产品，一些厂家将两者合一，以一个产品形态出现；
- 漏洞挖掘其存在的价值在于解决在工业控制系统潜在的未知漏洞，对SCADA系统、DCS系统、PLC控制器等工业控制系统、设备进行漏洞挖掘；
- 漏洞扫描其存在的价值在于检测工业控制系统的已知漏洞，可以支持对西门子、施耐德、GE等工控厂商的SCADA/HMI软件、DCS系统、PLC控制器进行扫描、识别，检测工业控制系统存在漏洞并生成相应的报告，清晰定性安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而在漏洞全面评估的基础上实现安全自主掌控。

漏洞挖掘VS漏洞扫描

漏洞扫描产品

基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算系统（主机、控制器等）的安全脆弱性进行检测，发现可利用的已知漏洞的一种安全检测（渗透攻击）产品。

≠

漏洞挖掘产品

基于模糊测试技术，通过向目标系统提供非预期的输入并监控输出中的异常来发现目标系统的未知漏洞的一种安全检测产品。

安全检测类-工控态势感知

习主席在419会议上提出要对关键信息基础设施进行通报预警，监管单位如经信委是有这方面的需求的。整体行业来看，工业和信息化部部长苗圩2017年2月在“2017工业互联网峰会”表示，工信部正在研究制定工业互联网发展路径，将进一步形成我国工业互联网发展的顶层设计。这也更加促进了“工控态势感知”的发展。

工控态势感知功能特点

工控网络资产在线探测

支持全球工控设备、网络设备、物联网设备、工控网络协议及常规服务的探测与定位

工控系统漏洞感知

实时发现全球互联网上暴露的工业网络漏洞数量，及其严重程度

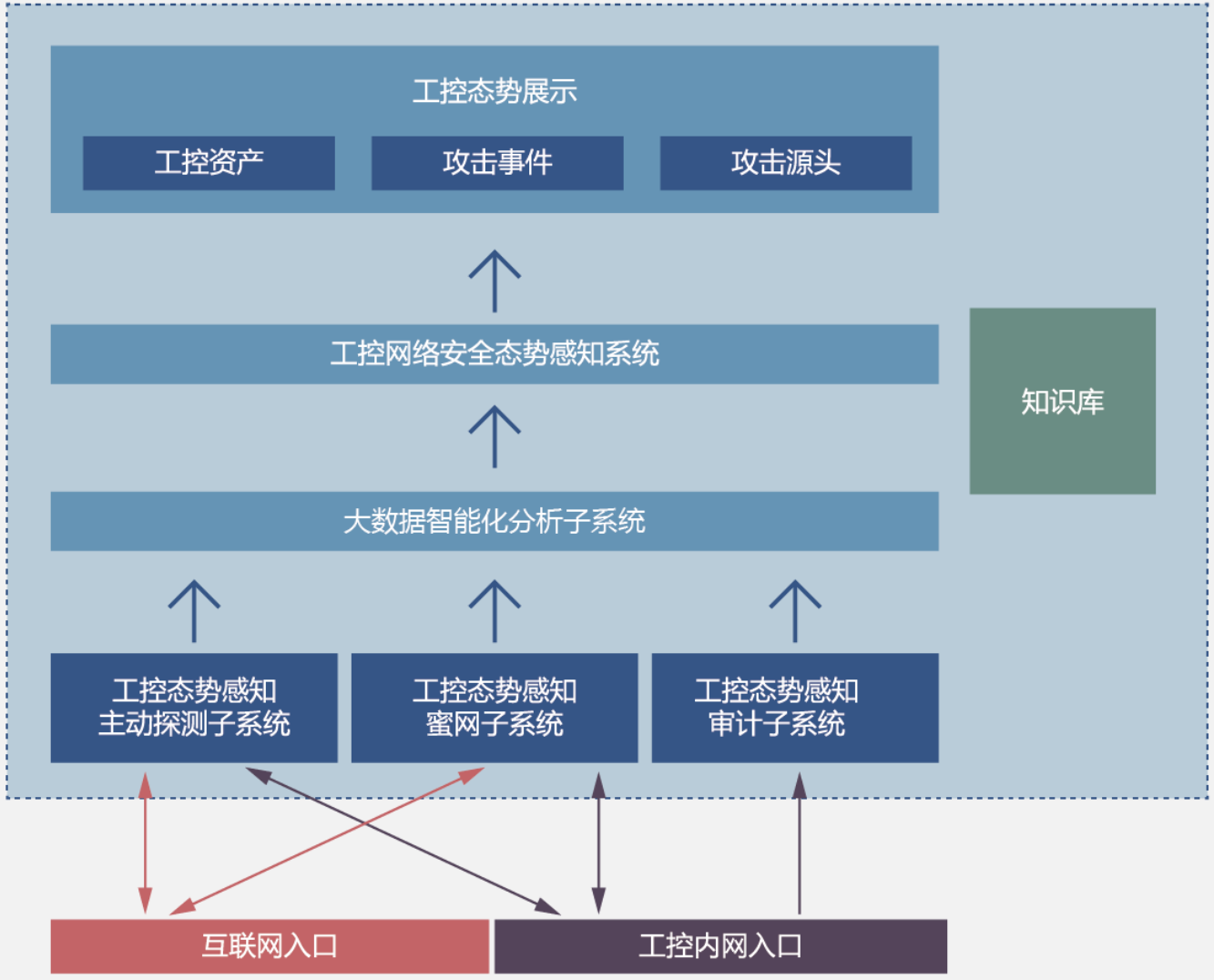
全网威胁态势可视化

多维度展示扫描分析结果，并以地域图、柱状图、饼状图、雷达图等形式展现

工控网络安全态势感知

全面诊断工控系统协议、服务、漏洞及威胁分布，智能分析工控系统资产，客观评估网络安全态势

工控态势感知体系架构



① 工业网络安全态势感知系统需要能够包含企业网络外部和内部的安全感知，能够适用于企业内部网络和企业外部互联网络两种场景下使用

② 在内部部署前端采集装置，在后台系统实现安全态势的收集、分析、展示和预警

③ 系统分工控态势感知主动探测子系统、工控态势感知审计子系统、工控态势感知蜜网子系统三个子系统进行建设

工控安全产品
与
传统信息安全产品的差异

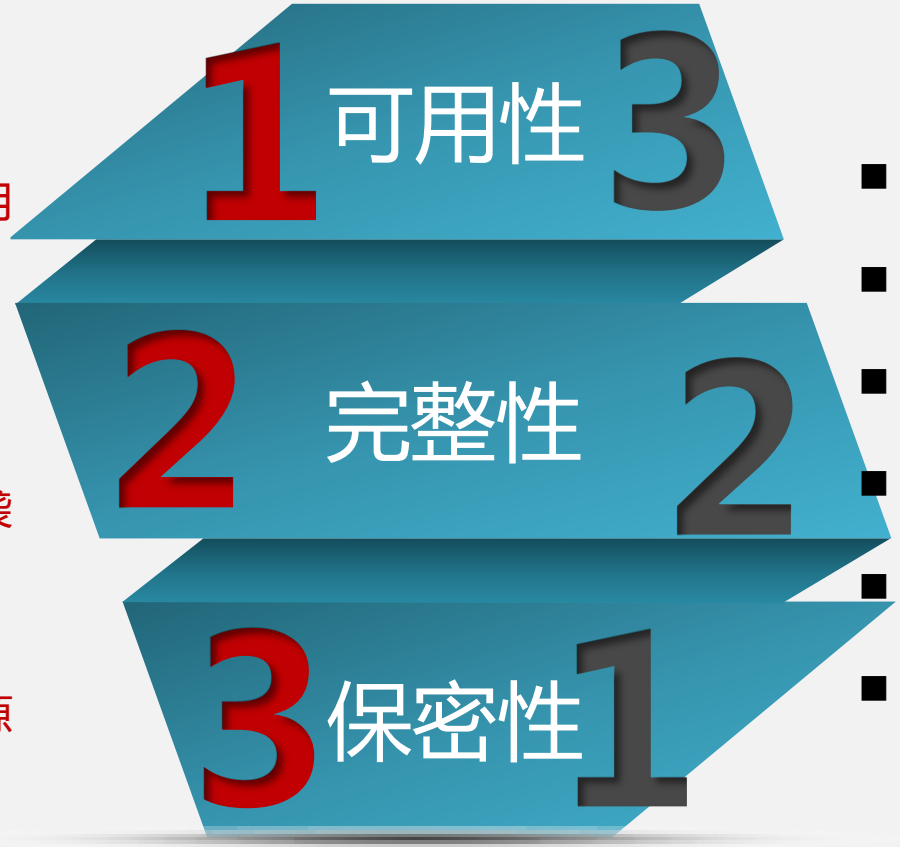
工控安全特殊性

- 网络通讯协议不同：大量的工控系统采用私有协议
- 系统稳定性要求高：网络安全造成误报等同于攻击
- 系统运行环境不同：工控系统运行环境相对落后
- 网络结构和行为相对稳定：不能频繁变动调整
- 安全防护要求高：无法通过补丁来解决安全问题

防护目标区别

工控安全

- 在不利条件下维护生产系统功能正常可用
- 确保信息实时下发传递
- 防范外部、内部的网络攻击
- 保护工控系统免受病毒等恶意代码的侵袭
- 避免工控系统遭受有意无意的违规操作
- 安全事件发生后能迅速定位找出问题根源



- 在不利条件下保证不出现信息泄露
- 保护信息资产的完整性
- 基本不考虑信息传递实时性
- 防范外部、内部的网络攻击
- 保护信息系统免受病毒等恶意代码的侵袭
- 安全事件发生后能迅速定位找出问题根源

传统安全

防护手段区别

VS

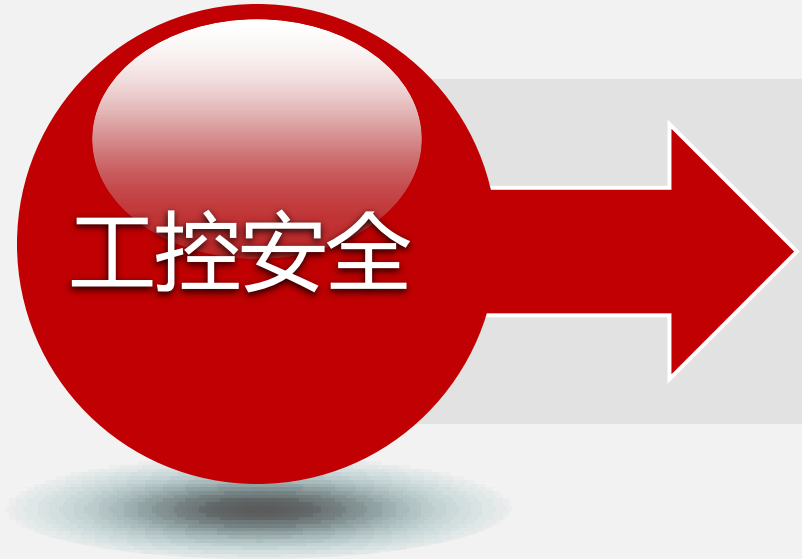
主动防护

白名单机制
旁路机制保证网络畅通
抵御已知未知病毒
学习建立防护策略
五元组+协议解析

被动防御

黑名单机制
冗余热备保证网络畅通
识别清除已知病毒
预先设置防护策略
五元组

网络架构区别



- 网络复杂，多种网络混合，包含有线、无线、卫星通信、无线电通信、移动通讯等
- 通信协议复杂，包含很多专用通讯协议及私有协议
- 设备复杂，网络设备、主机设备、防护设备、控制设备、现场设备种类繁多

- 网络相对简单，多为有线、无线
- 标准TCP/IP通信协议
- 设备类型相对简单，网络设备、主机设备、防护设备为主

数据传输区别

实时性要求高，不允许延迟
基本无加密认证机制
指令、组态、采集数据为主
流向明确基本无交叉

VS

实时性要求不高，允许延迟
加密认证防护
文件、邮件、即时消息为主
数据交叉传输

运行环境区别

工控安全

- 网络相对隔离，不联互联网
- 操作系统老旧，很少更新补丁
- 基本不安装杀毒软件
- 专用软件为主，类型数量不多
- 信息交互通过多通过U盘实现
- 安全漏洞较多，易受攻击

传统安全

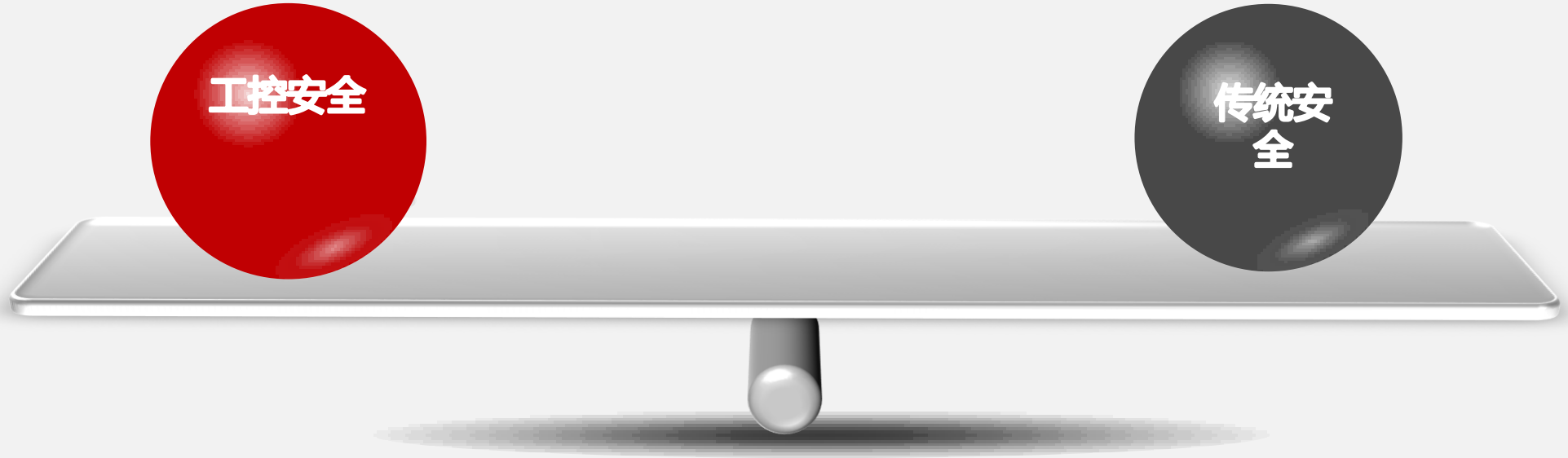
- 网络与互联网相通
- 操作系统新，频繁更新补丁
- 杀毒软件是标配
- 办公软件为主，类型数量繁多
- 信息交互多通过网络实现
- 安全漏洞较少，防护措施完善

物理环境区别

- 一般无机房，直接部署在生产环境
- 无专用散热装备
- 环境条件恶劣，高温、高湿、粉尘大、振动、酸碱腐蚀等
- 基本无监控、登记管理措施

VS

- 配有专用机房，统一放置设备
- 配有空调
- 环境条件优良，温湿度基本恒定，灰尘小，无振动，无腐蚀性
- 配有防盗门、视频监控、出入登记等



防护硬件区别

工控安全

- 工业级设计，全密封
- RISC架构，功耗低
- 自身散热，宽温工作
- 时延100us以下
- 标配Bypass机制
- 深度识别工业协议
- 使用寿命15—20年

传统安全

- 基本无三防设计
- X86架构，功耗高
- 风扇散热，温度范围有限
- 时延毫秒级以上
- Bypass机制非标配
- 基本不支持工业协议
- 使用寿命5—8年

防护软件区别

工控安全

- 白名单机制
- 不需要升级库和补丁
- 操作系统加固
- 抵御已知未知病毒
- 具备自我保护能力
- 运行占用资源少
- 支持老旧系统

VS

传统安全

- 黑名单机制
- 需频繁升级库和补丁
- 不加固操作系统
- 防范已知病毒
- 缺少自我保护
- 支持新版系统
- 运行比较耗资源

管理维护区别

工控安全

- 管理制度不完善甚至缺失
- 缺乏专业技术人员
- 设备维护依赖提供商
- 政策标准文件不完善

VS

传统安全

- 管理制度比较完善
- 配备专业维护技术人员
- 能够实现自我维护
- 标准政策文件完整

工控安全VS传统安全

分类	传统安全	工控安全
性能需求	非实时 响应必须是一致的 要求高吞吐量 高延迟和抖动是可以接受的	实时 响应是时间紧迫的 适度的吞吐量是可以接受的 高延迟和/或抖动是不能接受的
可用性需求	重新启动之类的响应是可以接受的 可用性的缺陷往往可以容忍的，当然要取决于系统的操作要求	重新启动之类的响应可能是不能接受的 中断必须有 计划和前预定时间 高可用性需要详尽的部署前测试
管理需求	数据保密性和完整性是最重要的容错是不太重要的-临时停机不是一个主要的风险 主要的风险影响是业务操作的延迟	人身安全是最重要的，其次是过程保护 容错是必不可少的，即使是瞬间的停机也可能无法接受 主要的风险影响是不合规，环境影响 ，生命、设备或生产损失
体系架构安全焦点	首要集点是保护IT资产，以及在这些资产上存储和相互之间传输的信息。 中央服务器可能需要更多的保护	首要目标是保护边缘客户端（例如，现场设备，如过程控制器） 中央服务器的保护也很重要
未预期的后果	安全解决方案围绕典型的IT系统进行设计	安全工具必须先测试（例如，在参考ICS上的离线），以确保它们不佳影响ICS的正常运作

工控安全VS传统安全

分类	传统安全	工控安全
时间紧迫的交互	紧急交互不太重要 可以根据必要的安全程度实施限制的访问控制	对人和其他紧急交互的响应是关键应严格控制对ICS的访问，但不应妨碍或干扰人机交互
系统操作	系统被设计为使用典型的操作系统采用自动部署工具使得升级非常简单	与众不同且可能是专有的操作系统，往往没有内置的安全功能；软件变更必须小心进行；
资源限制	系统被指定足够的资源来支持附加的第三方应用程序如安全解决方案	系统被设计为支持预期的工业过程，可能没有足够的内存和计算资源以支持附加的安全功能；
通信	标准通信协议 主要是无线网络，附带无线功能的 典型IT网络实践	许多专有的和标准的通讯协议 使用多种类型的传播媒介，包括专有用的有线和无线（无线电和卫星）；网络复杂 ；
变更管理（升级）	软件变更是及时应用的，往往是自动化的程序；	必须进行彻底的测试，以递增方式部署到整个系统；中断必须有计划；
管理支持	允许多元化的支持模式	服务支持通常是依赖单一供应商
组件生命周期	3-5年的生存期	15-20年的生存期
组件访问	组件通常在本地，可方便地访问	组件可以是隔离的，远程的，需要大量的物力才能获得对其的访问

威努特 WINICSSEC

专注工控·捍卫安全