工业控制系统的安全分析

安天实验室—微电子与嵌入式研发中心
赵世平（TBsoft）

提纲

- 工业控制系统简介
- 工控系统中的安全薄弱点
- 如何分析工控系统的安全性
- 工控系统安全设计部分准则
- 结束语

工业控制系统简介

工业控制系统及其应用简介

- 现代工业控制系统的应用范围：
  - 钢铁、化工、电力等重化工业（应用多年）
  - 轻工业
  - 工业控制系统衍生而来的家电自动控制系统
  - 物联网（可见的将来）

工业控制系统发展的三条主线

- 逻辑控制或者程序控制——PLC
  - 应用实例：生产流水线上的自动控制
- 遥测遥控系统的发展——SCADA（数据采集与监控）
  - 应用实例：电力系统SCADA（人工调度）
- 连续过程闭环控制——PCS（过程控制系统）
  - 应用实例：化工行业温度、压力、流量等

PLC

- 西门子S7-300系列PLC
- 目前PLC除用于逻辑控制和程序控制之外，也用于SCADA和PCS。

SCADA

➢ 电力系统SCADA

远程连接层

人机界面（HMI）层

工控计算机、HMI设备……

站控层（站内层）

工业以太网、交换机、集线器、网关、现场总线……

间隔层（隔离层）

远程终端单元（RTU）、智能电子设备（IED）、PLC……

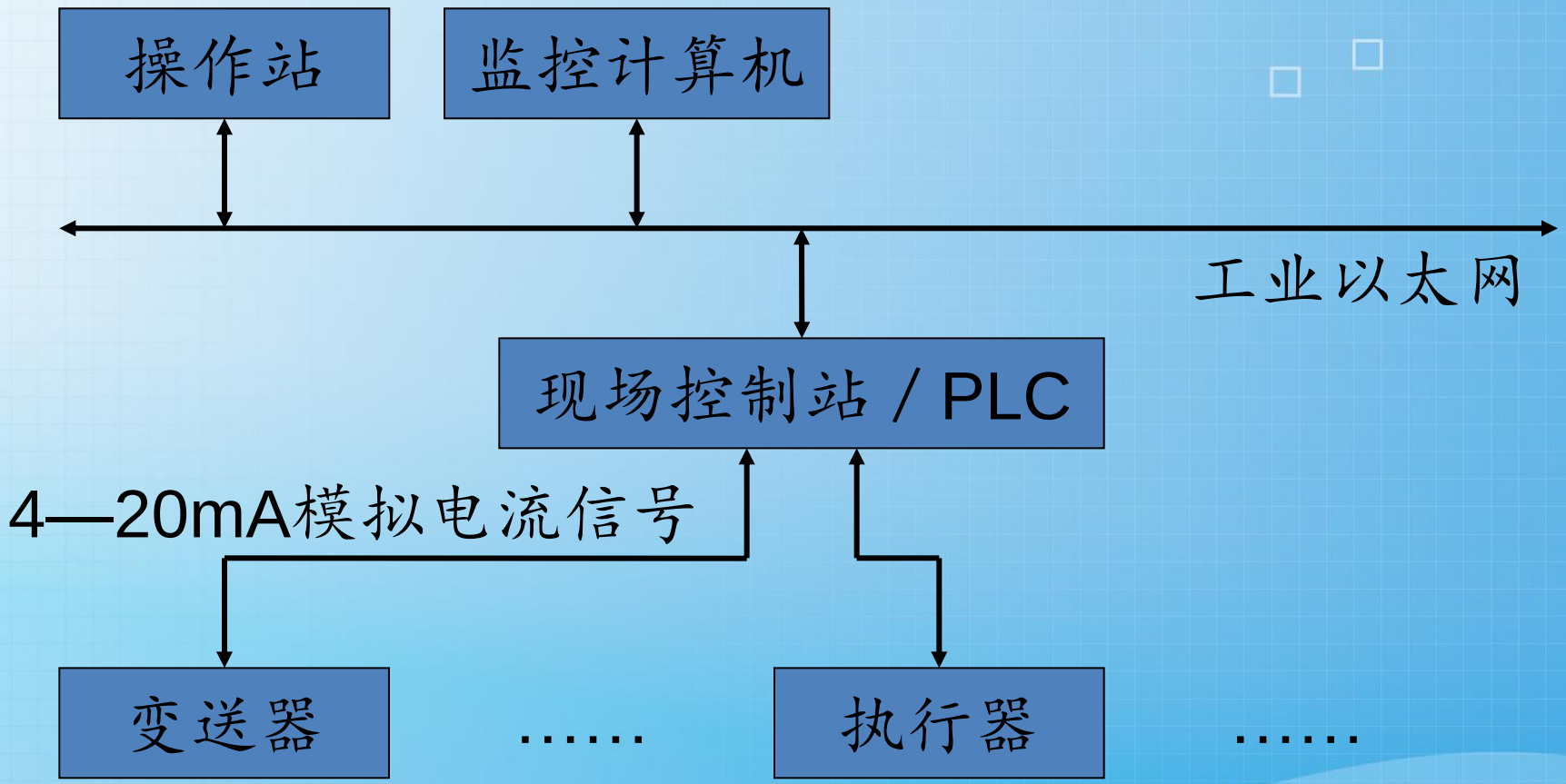
过程层（执行层）

电压互感器（PT）、电流互感器（CT）、开关……

过程控制系统的发展

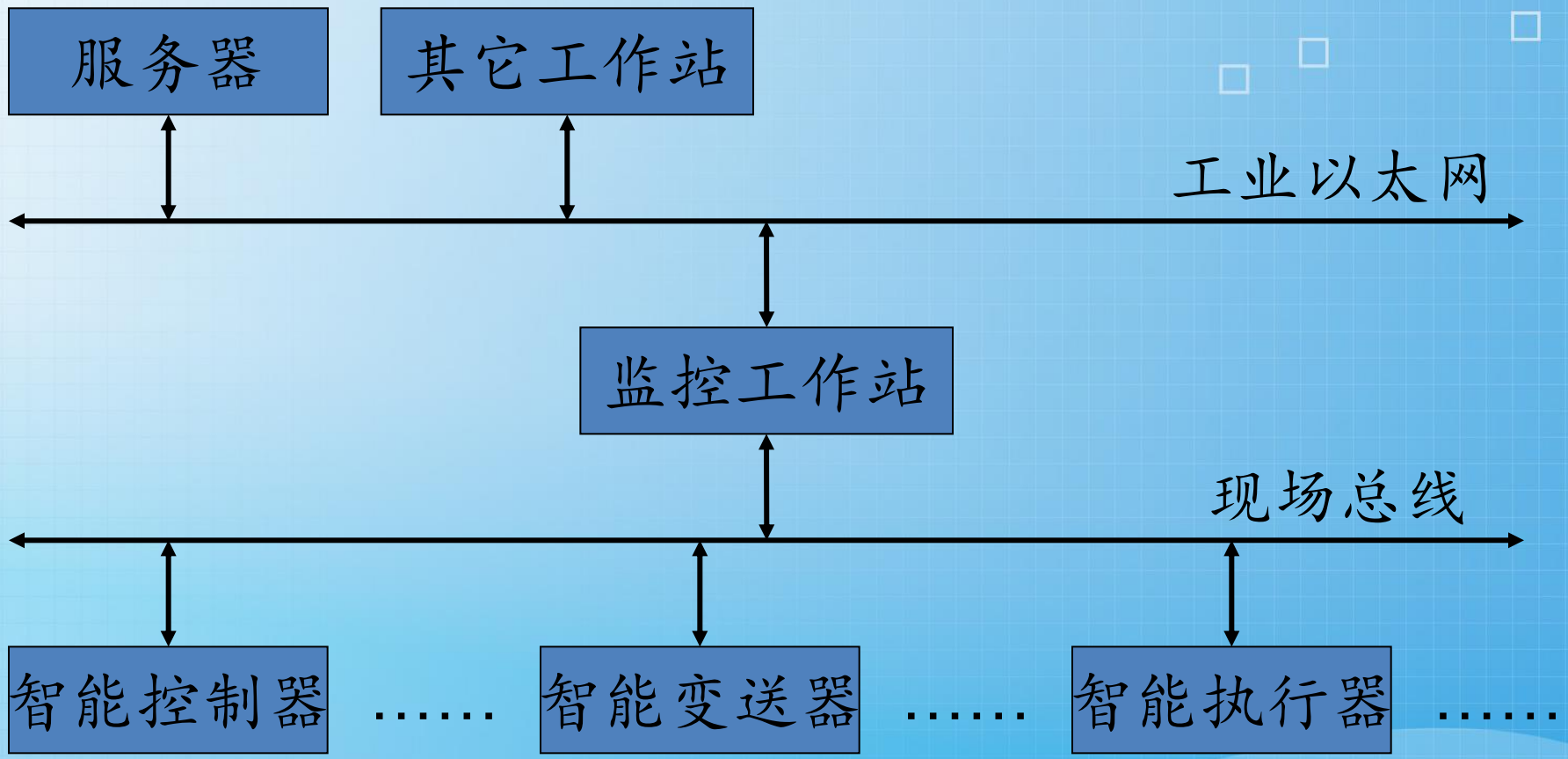
- 模拟单元组合仪表阶段（基本已被淘汰）
- 集散控制系统（DCS）阶段（目前使用广泛）
- 现场总线控制系统（FCS）阶段（目前和今后的发展方向）

集散控制系统（DCS）简介



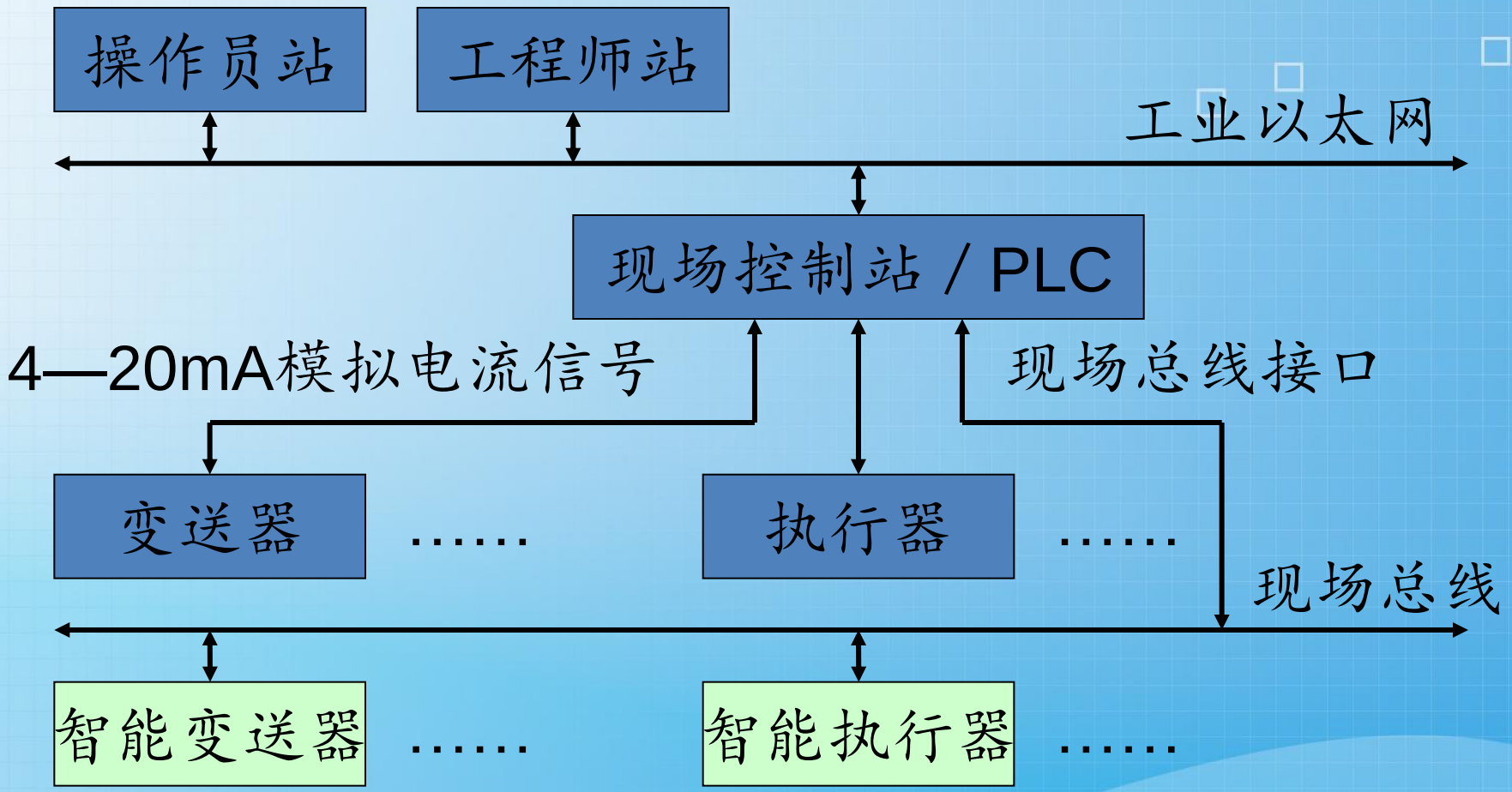
- 特点：工业以太网数字通信，现场仪表模拟通信。

现场总线控制系统（FCS）简介



- 特点：工业以太网和现场总线全数字通信

目前实际的DCS、FCS和现场总线应用



工控系统中的安全薄弱点

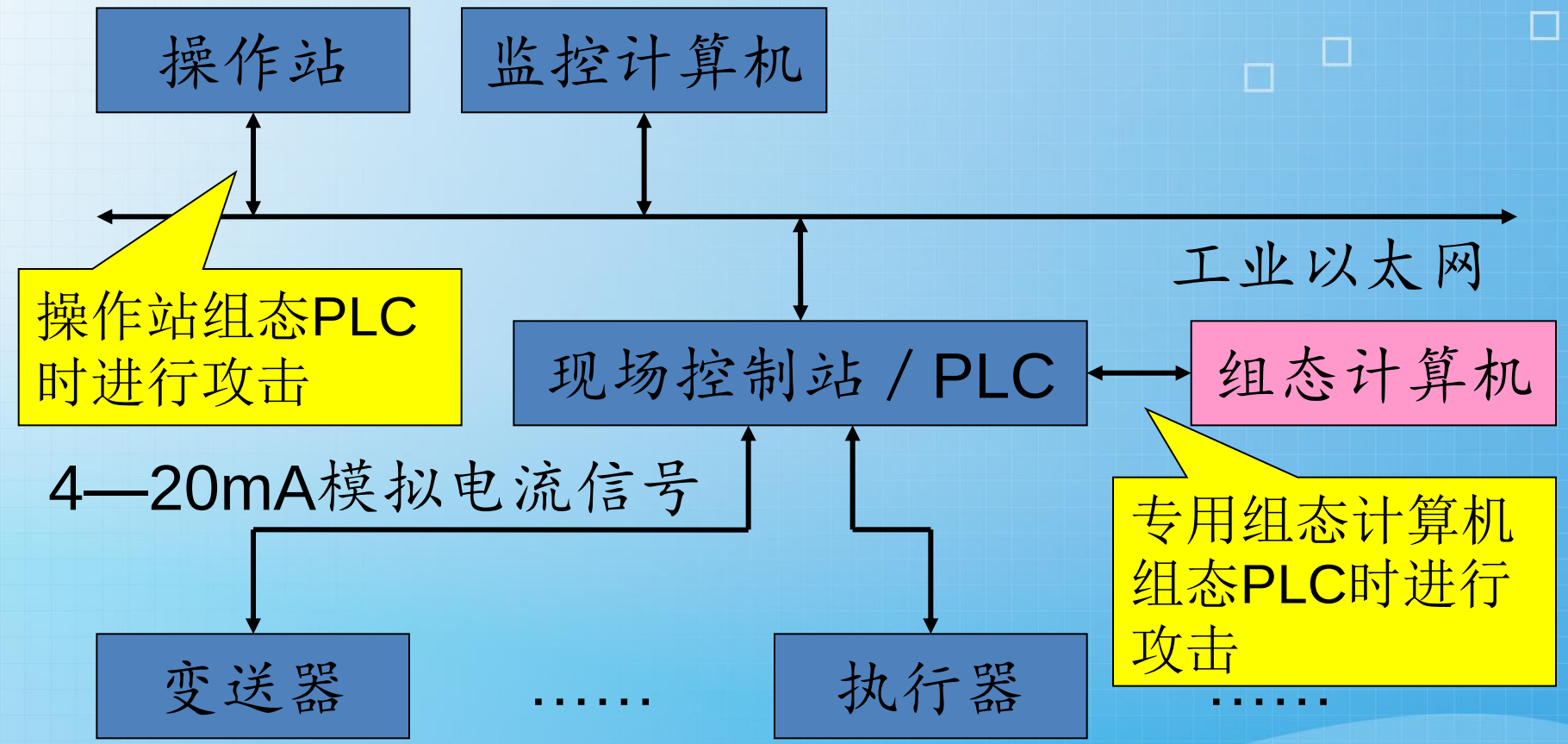
对DCS的攻击实例——震网（Stuxnet）蠕虫攻击伊朗核设施

- 来自安天实验室《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》
  - 目标：伊朗核电站提炼浓缩铀的设施
  - 目的：干扰浓缩铀提取过程，降低成品浓度，使之无法用于核武器
  - 方法：渗透至工业内网，利用工业控制系统的安全漏洞，改变相关设施的运行参数
  - 结果：成功！使伊朗核工业陷入停滞
- 攻击目标为DCS中的西门子WinCC HMI / 组态软件、STEP7组态软件以及S7-300 / 400系列PLC（某些型号），采用与攻击渗透民用以太网相似的方法。

DCS中的PLC

- S7-300 / 400系列PLC（某些型号）是Stuxnet蠕虫攻击的重要目标。
- PLC程序由PLC指令构成，PLC指令相当于CPU指令，因此PLC程序相当于一种CPU的机器语言程序。
- 目前流行PLC的指令格式基本是公开或者半公开的，其程序下载（组态）机制基本也是半公开的，因此编写感染PLC程序的恶意代码，并组态到PLC中并不存在很高的技术门槛。这种PLC恶意代码与PC病毒一样，可以长期潜伏在PLC中实施隐蔽性破坏，也可以通过外部条件触发实施突发性破坏，对于正常测控的破坏威力相当大。

攻击DCS中的PLC

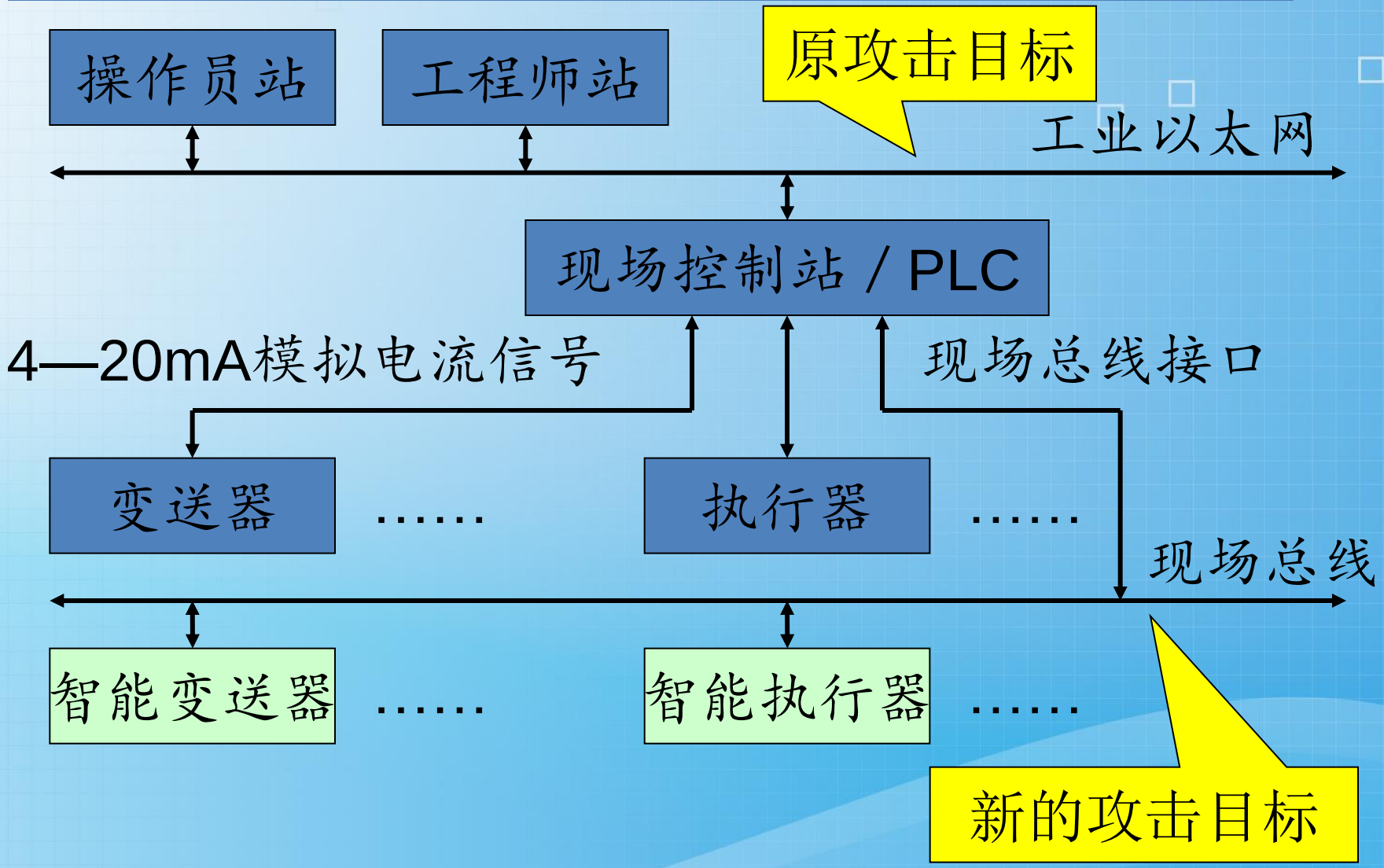


- 先感染操作站等PC，在PLC组态时写入恶意代码。

从DCS到FCS——现场总线带来的安全性问题

- 数字化通信下移到现场测控仪表
- 为了实现数字化通信，现场测控仪表必须是基于单片机和嵌入式系统的智能仪表。每一个现场仪表上都运行着嵌入式软件。
- 数字化通信和软件的下移，导致攻击目标下移，传统针对以太网的攻击发展成为针对现场总线网络和现场测控仪表的攻击。

攻击目标下移



现场总线简介

- 现场总线（Fieldbus）是将自动化最底层的现场控制器和现场智能仪表、设备互连的实时控制通信网络，遵循ISO的OSI开放系统互连参考模型的全部或者部分通信协议。

- 为了支持数字通信，现场总线控制系统中的变送器、执行器等仪表都必须是基于微控制器（单片机）的智能仪表，智能仪表可以直接实现控制，也可以由监控工作站（监控计算机）实现控制，相当于使用计算机软件实现虚拟控制器。

常用现场总线标准

- Profibus（石化行业）
- FF（石化行业钻井平台）
- CAN / DeviceNet（汽车工业、铁路工业）
- MODBUS（原为用于控制器的通用通信语言，现已发展成为现场总线协议，中小企业应用极为广泛）
- 短程无线通信协议（Zigbee等）

现场总线协议与OSI模型的对应关系

- 以MODBUS为例

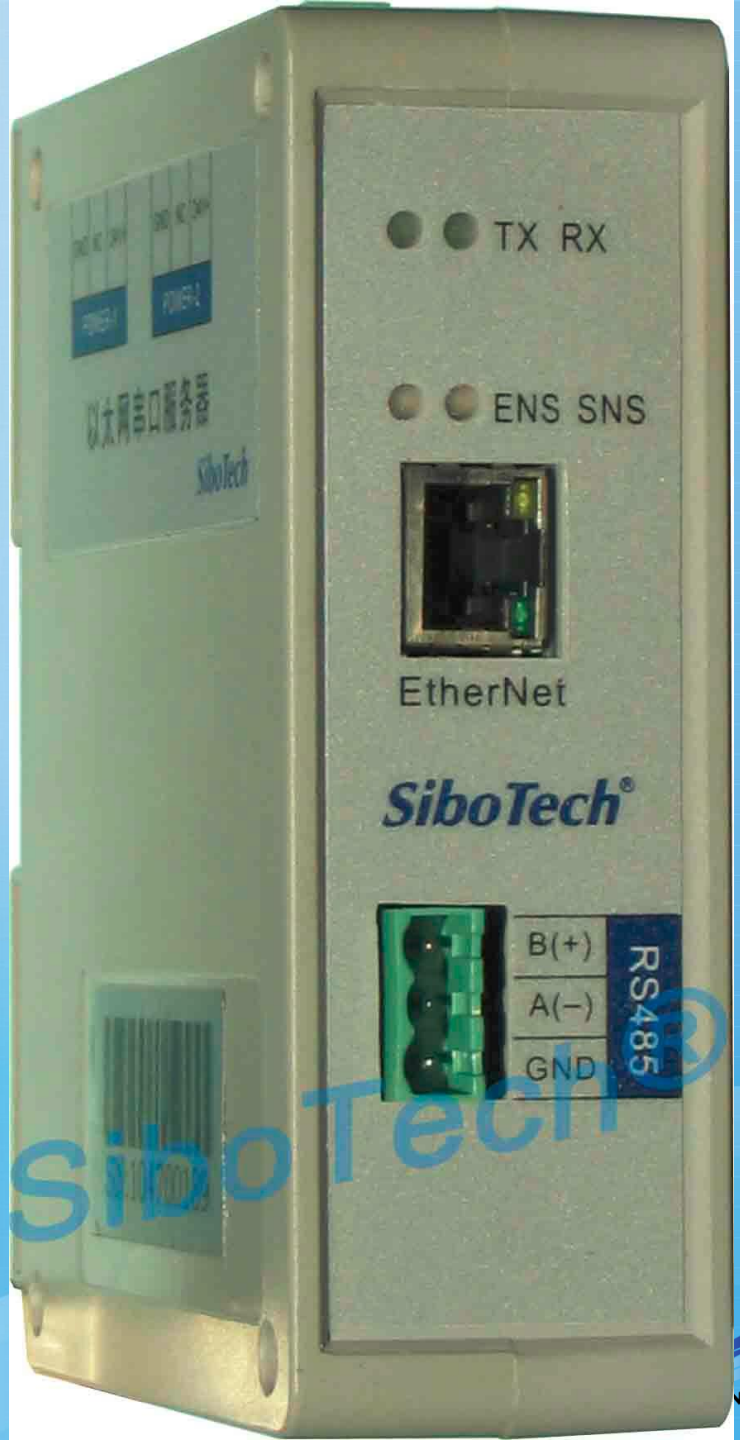
应用层	MODBUS应用层	MODBUS应用层
表示层		
会话层		
传输层		TCP
网络层		IP
数据链路层	MODBUS串行链路	Ethernet
物理层	RS-485总线	Ethernet物理层
OSI模型	串行链路上的MODBUS协议	MODBUS/TCP

目前现场总线协议存在的安全性问题

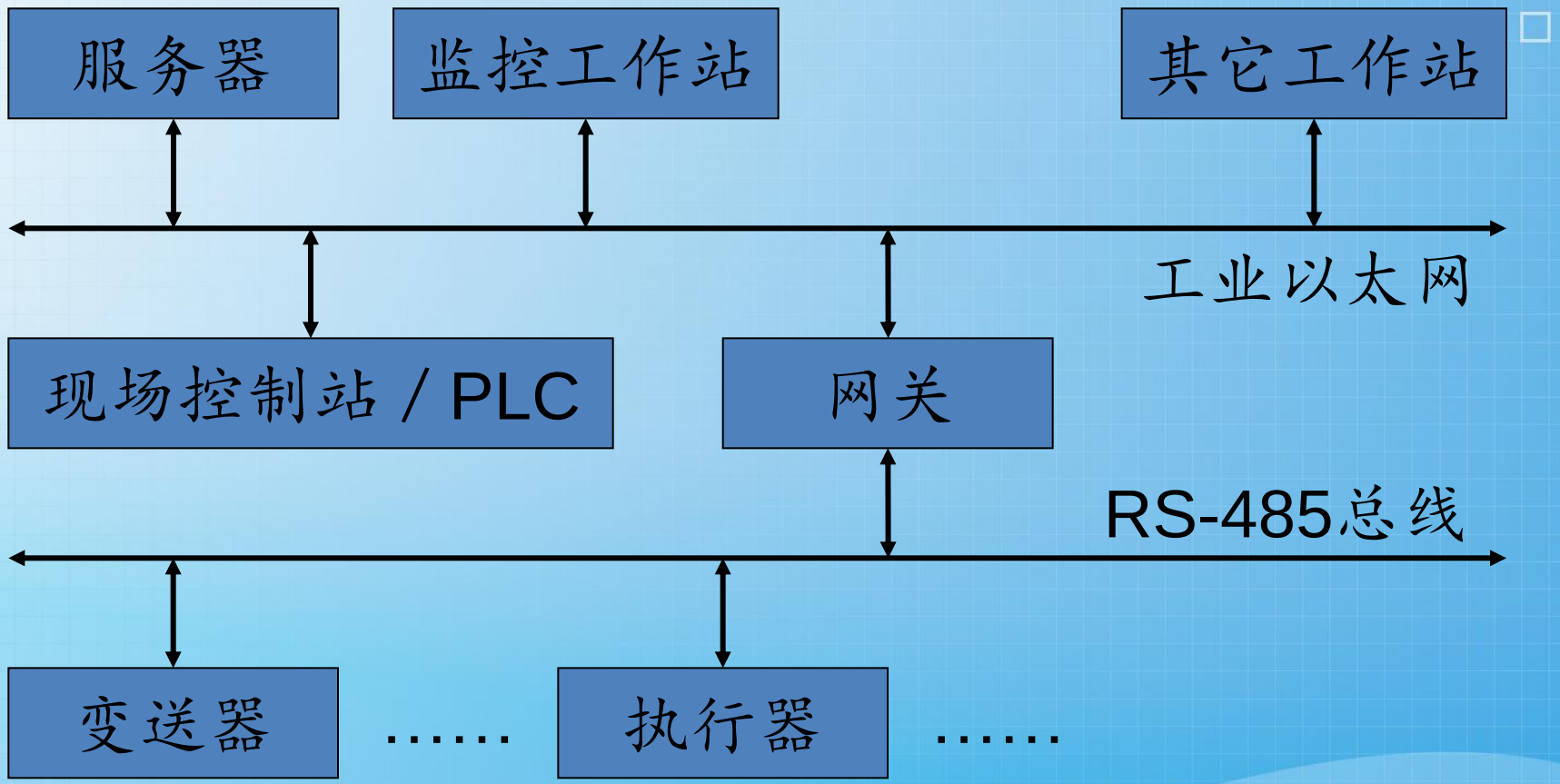
- 几乎所有的现场总线协议都是明码通信（传统工业内网与互联网物理隔离）
- 基于RS-485总线物理层的现场总线协议，例如Profibus-DP、MODBUS串行链路协议等，由于传输媒质成本低（两线）而被广泛使用。基于RS-485总线进行的通信是广播方式，连接在RS-485总线上的任意一个设备发送数据，可以被连接在同一总线上的所有其它设备接收。
- MODBUS等现场总线协议，其应用层协议可同时适用于以太网和RS-485总线，以太网和RS-485总线之间的连接只需要简单的网关设备。

MODBUS/TCP转RS-485/MODBUS网关

- 产品功能：
  - 实现MODBUS/TCP与RS-485/MODBUS（包括RTU模式和ASCⅡ模式）互相转换的网关设备，可以轻松实现MODBUS设备的互联。

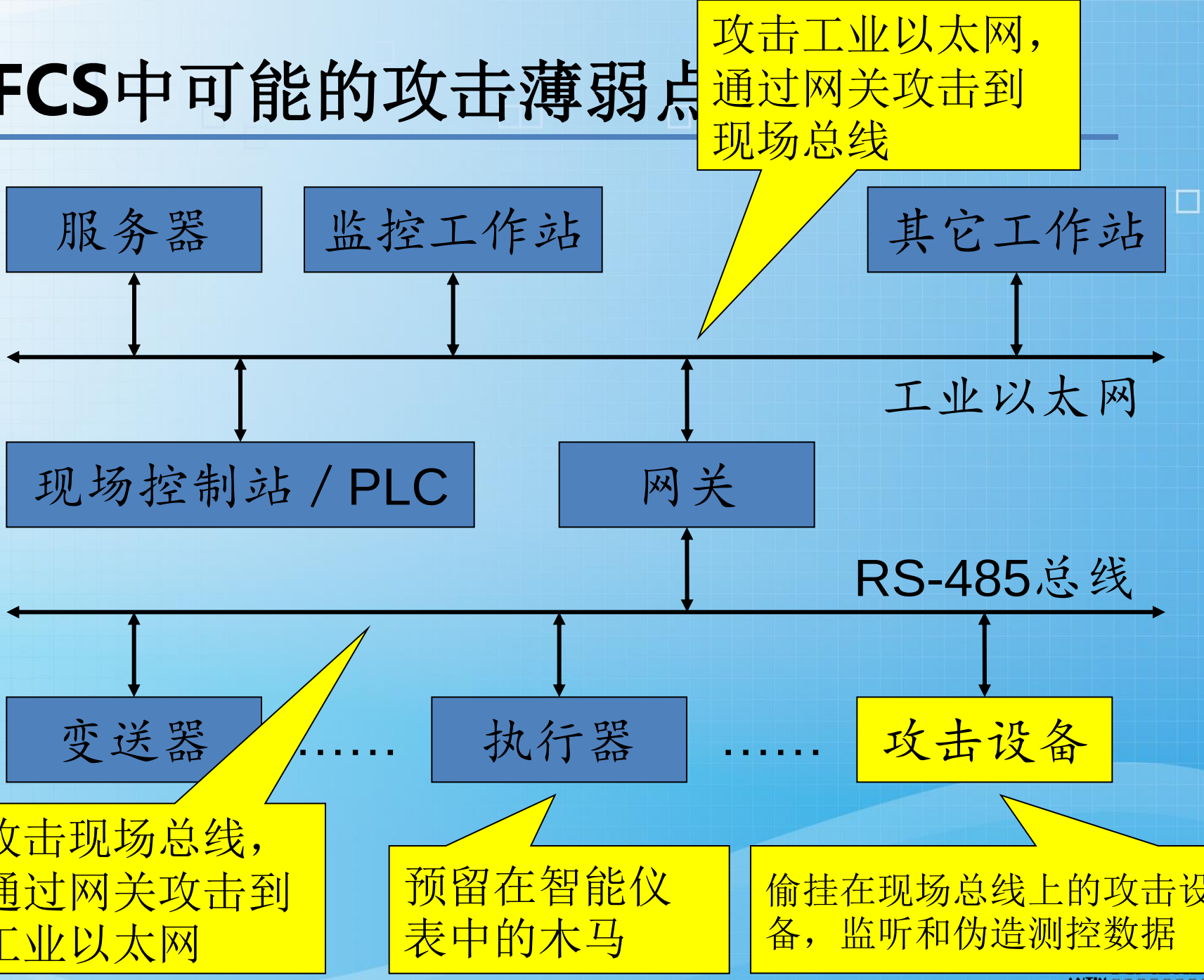


网关在FCS中的应用



- 带来问题：以太网和RS-485总线之间的攻击通道

FCS中可能的攻击薄弱点



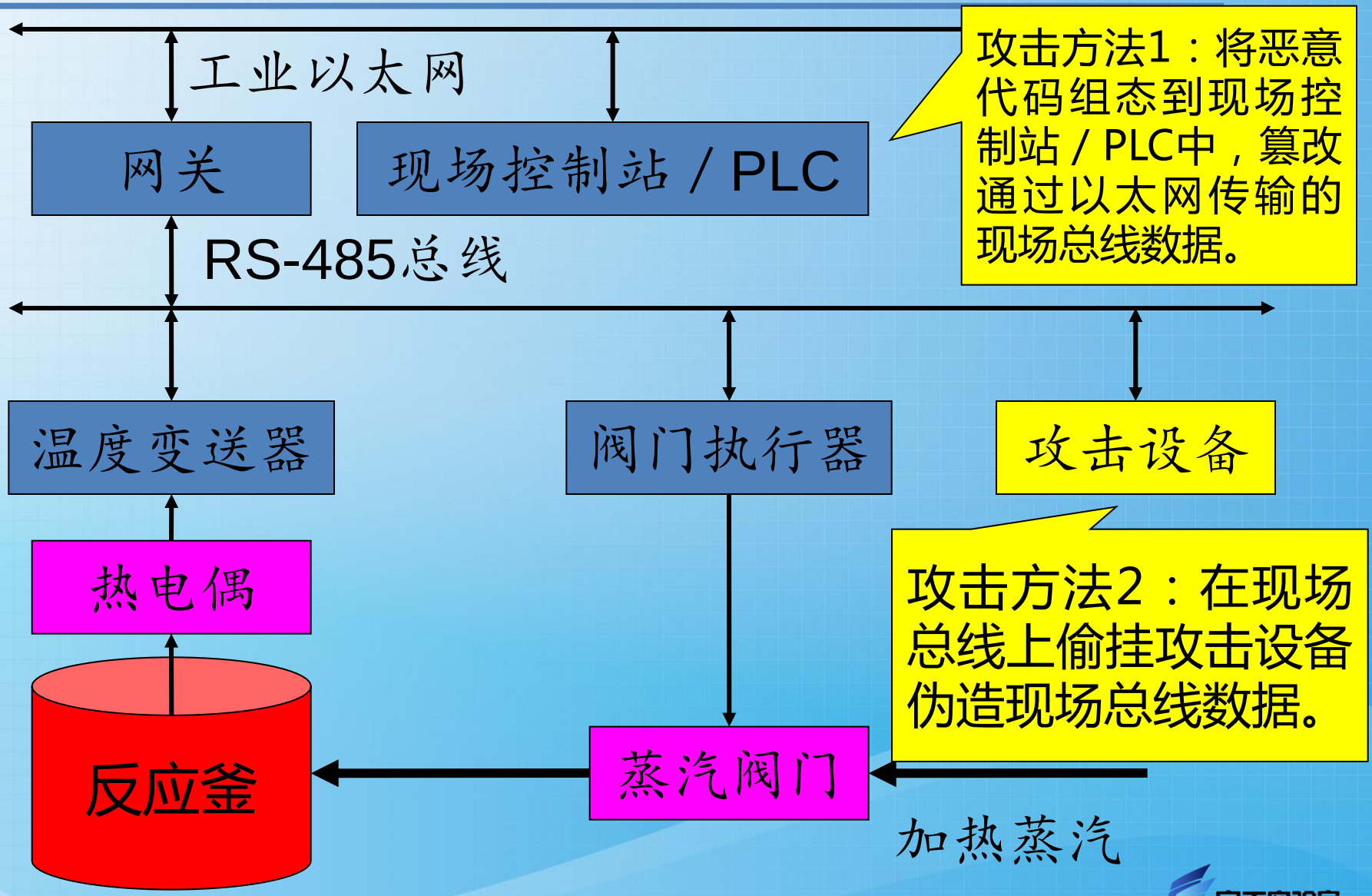
短程无线通信芯片——被忽视的安全薄弱点

- 2.4GHz短程无线通信目前广泛应用于无线传感器等场合，用于不便于架设现场总线线路的环境。
- 2.4GHz短程无线通信方案
  - Zigbee（较成熟，有一定安全性）
  - 厂商自定义无线通信协议（安全性可能存在问题）
- 目前广泛使用的NORDIC公司nRF24L01 2.4GHz短程无线通信芯片存在很大的安全性隐患。
- 安天实验室曾于2009年成功地针对基于nRF24L01的短程无线通信产品进行了监听。

短程无线通信芯片——被忽视的安全薄弱点

- 国内一些小企业生产的“无线传感器”等测控仪表，其无线通信部分大量采用nRF24L01 2.4GHz短程无线通信芯片，连基本的通信数据加密都没有使用，可以说毫无安全性可言，极易遭到窃听和攻击，如果使用，将成为现场总线中极易被攻击的薄弱点。

例：攻击化工厂反应釜的温度测控



例：攻击化工厂反应釜的温度测控

- 攻击演示说明
  - 在基于RS-485总线的现场总线上挂接攻击设备
  - 截获RS-485/MODBUS现场总线数据报
  - 伪造RS-485/MODBUS现场总线数据报
  - 伪造虚假的反应釜温度

例：攻击化工厂反应釜的温度测控

- 攻击效果：反应釜无法获得正确的温度测量数据，只能得到一个较低的虚假测量温度，导致加热蒸汽在反应釜温度已经超标的情况下仍然对反应釜持续加热，温度测控失灵。
- 最终结果：反应釜超温导致冲料、起火甚至爆炸，导致人员伤亡和次生灾害（有害化学物质泄漏等）。

如何分析工控系统的安全性

工控系统漏洞的三种类型

- 运行工控系统相关软件所需平台（操作系统）的漏洞
  - 例：Stuxnet利用MS10-046、MS08-067和MS10-061漏洞
- 工控系统相关软件的常规漏洞
- 工控环境中的特有漏洞
  - 例：Stuxnet利用未加密的西门子S7-300/400 PLC组态协议
  - 对工控系统安全的威胁最为严重

上述三类漏洞的特点

- 在一次完整的攻击或者APT事件中：
  - 第1、2类漏洞起到“路径”、“跳板”、“倍增器”等辅助作用
  - 第3类漏洞完成“致命的最后一击”
- 第3类漏洞对工控系统威胁最大也是最根本性的漏洞

传统安全企业对工控系统漏洞的挖掘

- 主要集中在上述第1、2类漏洞
- 第2类漏洞是传统安全企业的主要目标
  - 与一般软件漏洞挖掘类似
  - 传统安全企业的强项
  - 可以不需要专门的环境和设备

第3类漏洞的特点

- 围绕工控通信协议出现
- 设计协议时带来的而非软件开发中的疏漏
  - Stuxnet之前很少考虑到工控针对性恶意代码、APT甚至信息武器会把工控系统作为破坏目标
  - 设计工控协议时就很少考虑安全性问题
- 挖掘和封堵第3类漏洞是目前国内工控安全研究中最为欠缺的

例1：协议本身的漏洞挖掘

- 以MODBUS协议为例
  - 串行链路（RS-485总线）上的MODBUS协议仅涵盖OSI模型中的1、2、7层

OSI模型与串行链路上的MODBUS协议

应用层
表示层
会话层
传输层
网络层
数据链路层
物理层

OSI模型

MODBUS应用层
MODBUS串行链路
RS-485总线

串行链路上的MODBUS协议

MODBUS协议会话机制中的漏洞

1. 主节点发送请求，请求数据帧中包括子节点地址，请求被所有子节点接收到，但只有与子节点地址相符合的子节点处理接收到的请求数据帧；

2. 主节点发送请求后等待响应；

3. 相应子节点处理请求数据帧后，发送响应数据帧；

4. 主节点接收到响应数据帧后，会话完成，如果主节点等待响应时间超时仍未接收到响应，认为会话失败，放弃本次会话。

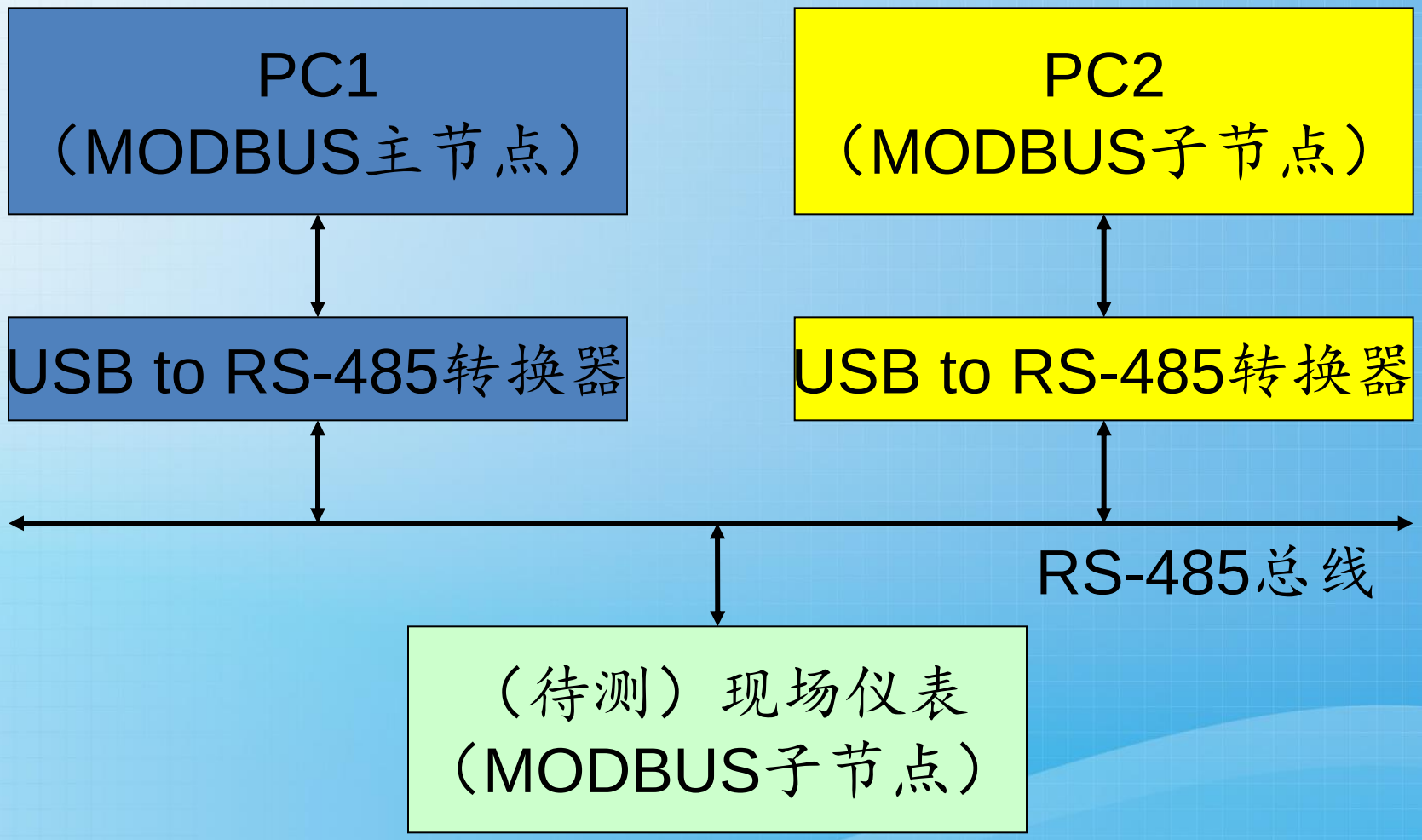
MODBUS协议会话机制中的漏洞

1. RS-485总线上，任意一个节点发送的数据帧，可以被除这个节点外的所有节点接收到，任何一个节点都可以监控RS-485总线所有通讯数据帧。

2. 主节点并不知道真正是哪个子节点在处理请求数据帧。

3. 主节点仅通过是否超时来判断会话是否成功，如果子节点处理请求数据帧的速度较慢，另一子节点完全可以伪造响应数据帧结束会话，使得主节点收到错误响应。或者通过干扰RS-485总线阻止主节点收到响应，使得主节点认为超时而放弃会话。

漏洞挖掘方法



漏洞挖掘方法（续）

1. 将两台PC连接到同一条RS-485总线上，并同时连接上现场仪表，一台PC作为MODBUS主节点，另一台PC和现场仪表都作为MODBUS子节点；

2. 使用MODBUS通信测试软件，在作为MODBUS主节点的PC上不断发出符合现场仪表通信协议要求的请求；

3. 在作为MODBUS子节点的PC上，使用串口监控软件（或者MODBUS通信监控软件）监控所有数据帧；

漏洞挖掘方法（续）

4. 如果发现请求数据帧和响应数据帧之间有较长的时间间隔，说明这种现场仪表可能引发MODBUS协议漏洞；
5. 在作为MODBUS子节点的PC上，开发并运行攻击程序，接收请求数据帧并快速发送伪造的响应数据帧，检查作为MODBUS主节点的PC是否收到了伪造的响应数据帧，如果收到表示攻击成功，现场仪表存在引发MODBUS协议漏洞的可能。

例2：对协议处理的漏洞

- 以MODBUS协议为例
  - 无论是上位机HMI功能软件、现场控制站／PLC嵌入式软件还是现场仪表嵌入式软件，都必须处理MODBUS协议数据报或者数据帧。
  - 一般来说，正常的MODBUS协议数据报（帧）处理不会存在问题，但异常的数据报（帧）同样可能引发缓冲区溢出等漏洞，可以从不同角度构造异常的MODBUS协议数据报（帧），以进行漏洞发现或者扫描。

构造异常的MODBUS数据报或者数据帧

- 不正常的功能码
- 不正常的地址（例如248—255）
- 超长数据（最容易引发缓冲区溢出漏洞）
- 错误的CRC或者LRC

开发漏洞扫描工具

- 挖掘对协议处理的漏洞
- 代替人工测试挖掘
- 智能化
- 适合工业通信协议

工控系统安全设计部分准则

安全通信设计

- 现场控制站以及PLC的组态协议
  - 加密通信
  - 抗篡改机制
- 现场总线协议
  - 不能只考虑“本质安全”而忽视“通信安全”
  - 设计抗攻击的会话层协议
  - 加密通信
- 加密通信的设计
  - 加密算法的选择
  - 密钥管理

选择集中控制还是分布式控制？

- 基于PC的集中控制软件开发简单
- 分布式控制风险小
  - 理想的FCS实际并不实用
  - 目前实际FCS多在DCS现场控制站或者PLC上添加现场总线接口
  - 分散的现场控制站有效降低了风险
- 无论集中控制还是分布式控制都应该使用冗余设计

7·23高铁事故的启示

- 事故前
  - 既有线（160km/h以下）基于ZPW-2000A轨道电路移频自动闭塞，分散的轨道继电器控制各地面信号机显示信号，同时控制机车信号。
  - 提速既有线（200km/h）和客专基于CTCS-2（中国列车运行控制系统2级），通过CAN总线连接列控中心，列控中心实现集中控制信号。
- 事故当晚
  - 雷击损坏列控中心设备，导致列控中心集中控制出现异常，信号错误升级（红灯→绿灯）。
  - 追尾事故！

7·23高铁事故的启示（续）

列控中心集中控制的该信号错误变成绿灯，引起D301次列车错误冲入区间，最终导致惨烈追尾事故！

7·23高铁事故的启示（续）

- 事故后
  - 所有动车与现有客货列车混跑的既有线，限制动车速度不得超过160km/h。
  - 客专和高铁线路也进行了降速

结束语

提高工控系统安全性

- 工控针对性恶意代码、APT和信息武器将越来越多地攻击工控系统
- 目前工控系统的安全基础存在先天不足
- 传统的内外网物理隔离措施不能有效地保证工控系统安全

提高工控系统安全性

- 工控相关通信协议，例如PLC组态协议和现场总线协议应该进行安全改造。
- 研制适用于工业以太网和现场总线的防火墙以及IDS、VDS等，以多种策略检测和阻断针对性攻击，但不应该影响工控系统的实时性。
- 加强要害部门设备和通信网络物理层的安全保卫措施。
- 加快重要工控核心设备的国产化。
- 选择可信任的制造商制造的测控仪表，包括短程无线通信协议的正确选择。
- 加强工控安全设计的研究和应用。

谢谢大家！