开始语

- 《SP 800—82 ： 工业控制系统(ICS)安全指南》于2010年1O月发布，是NIST依据2002年联邦信息安全管理法 、2003年国土安全总统令HSPD-7等编制而成。它遵循《OMB手册 》的要求“保障机构信息系统 ，为联邦机构使用，同时允许非政府组织自愿使用，不受版权管制。”
- SP 800—82有逻辑地给出了ICS安全保护的建议和指导， 若能有效地满足这样的需求,ICS系统就可达到更安全的（secure），即系统处在一种特定状态，可有效地抵御所面临的不可接受的风险。

NIST SP 800-82 概述

- 该指南为保障工业控制系统ICS提供指南，包括监控与数据采集系统(SCADA)、分布式控制系统（DCS)和其他完成控制功能的系统。它概述了ICS和典型的系统拓扑结构，指出了这些系统的典型威胁和脆弱点所在，为消减相关风险提供了建议性的安全对策。同时，根据ICS的潜在风险和影响水平的不同，指出了保障ICS安全的不同方法和技术手段。该指南适用于电力、水利、石化、交通、化工、制药等行业的ICS系统。

主要内容

- 工业控制系统概论
- ICS特性、威胁和脆弱性
- ICS系统安全程序开发与部署
- 网络结构
- ICS安全控制

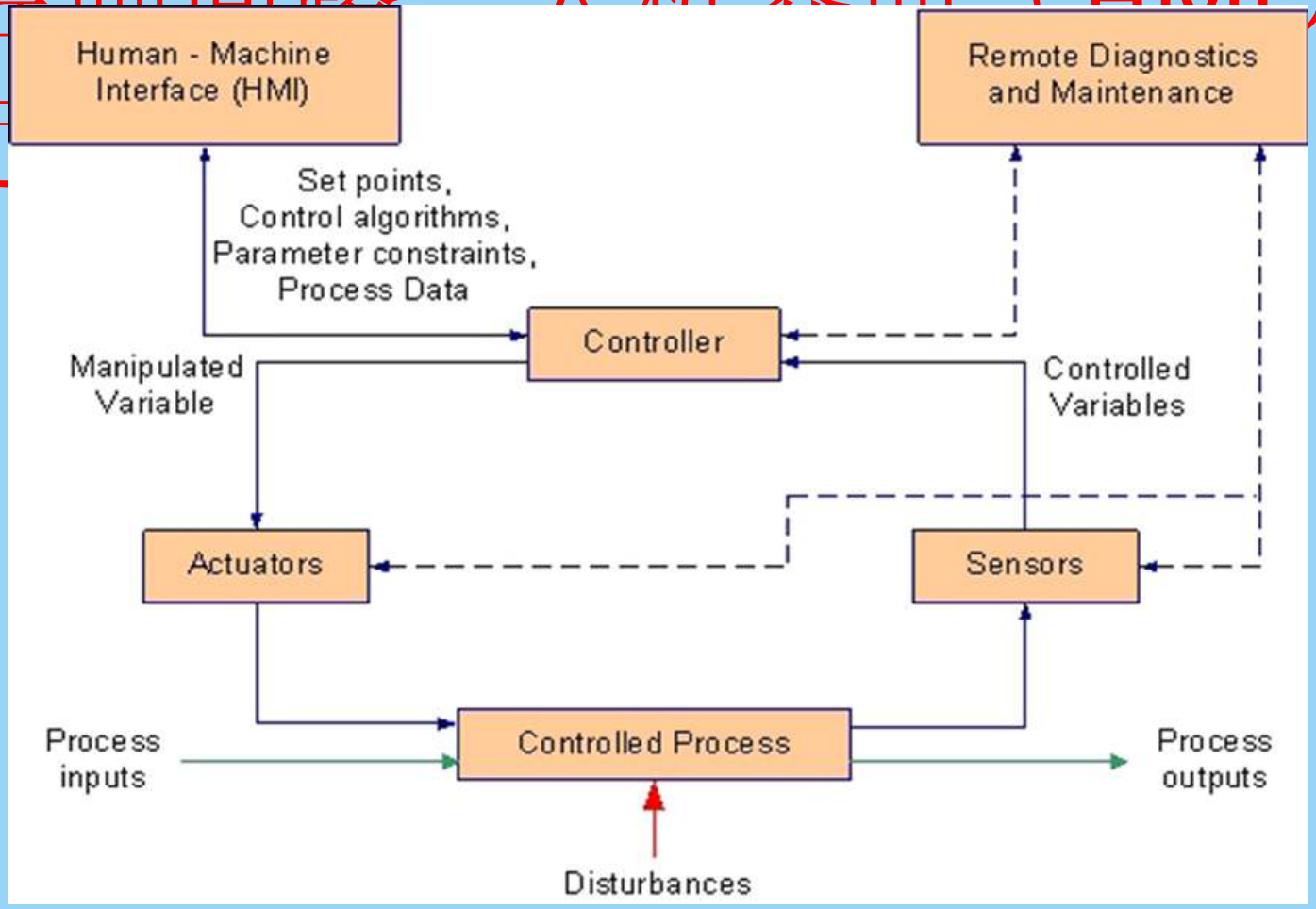
工业控制系统概论

工业控制系统

- 监控和数据采集系统(SCADA)
- 分布式控制系统（DCS)
- 可编程逻辑控制器（PLC)

ICS操作关键组件

- 控制回路、人机界面（HMI）、远



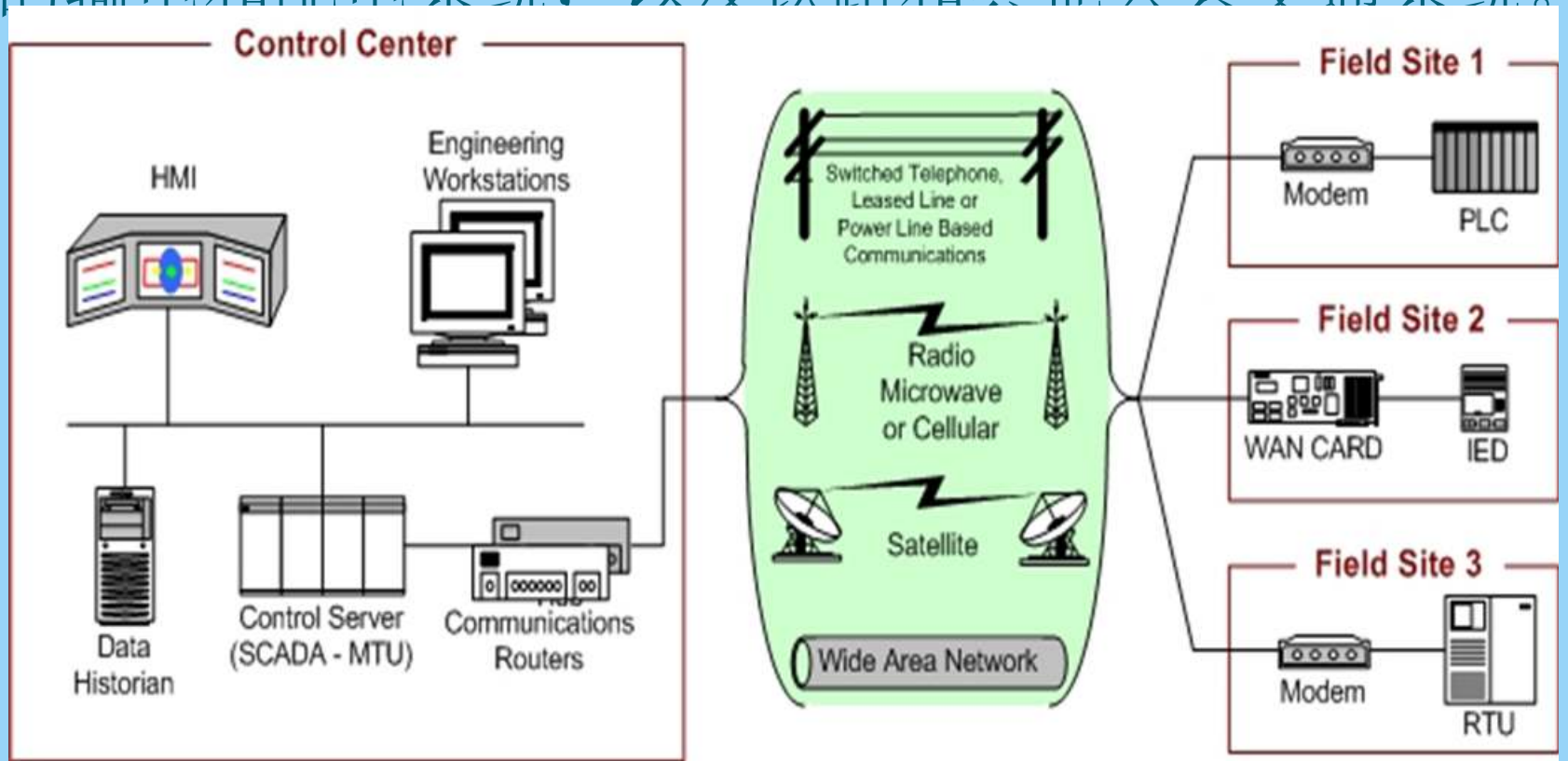
主要ICS元件

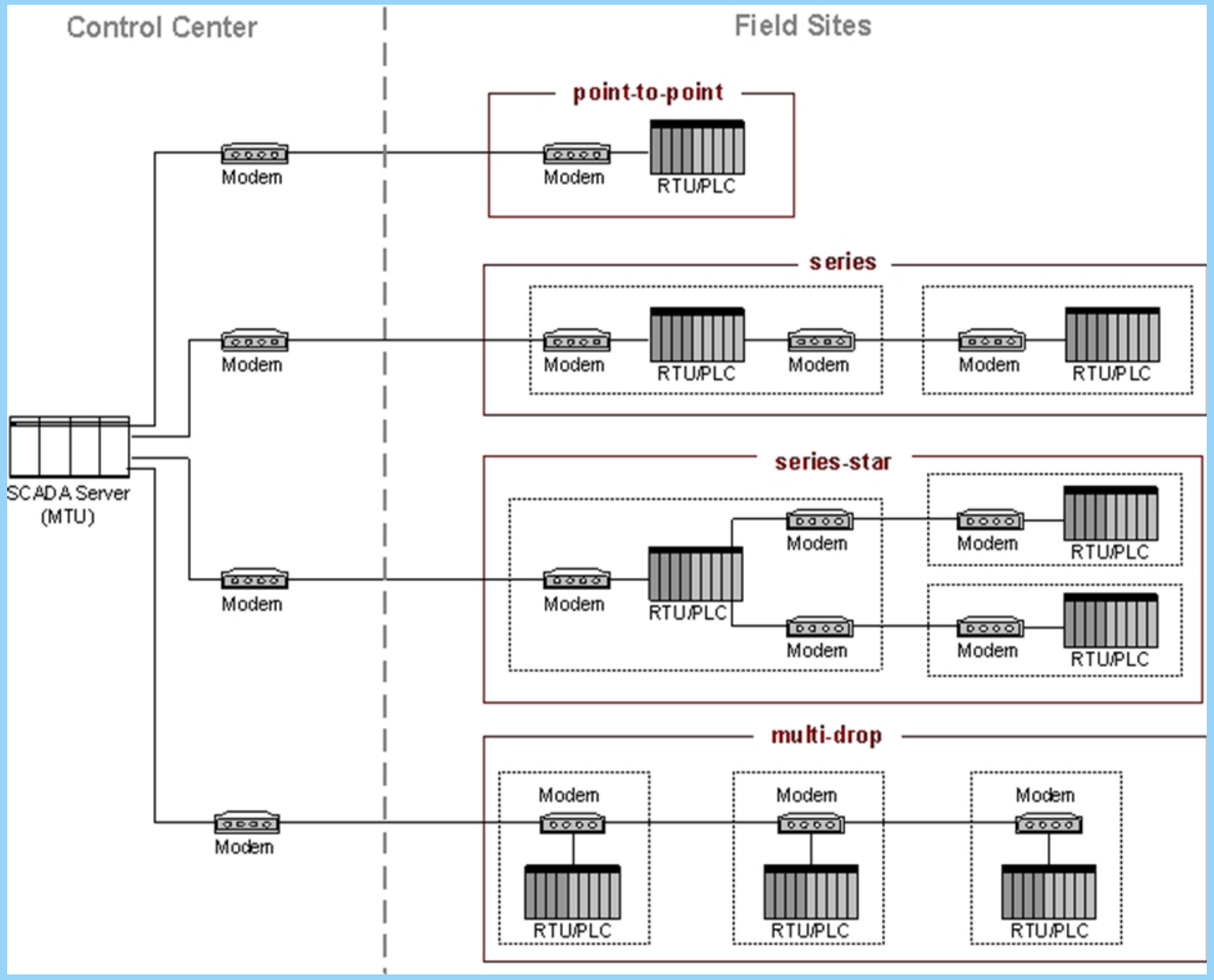
- 控制元件：控制服务器、SCADA服务器或主终端单元（MTU）、远程终端装置（RTU）、可编程逻辑控制器（PLC）、智能电子设备（IED）、人机界面（HMI）、历史数据、输入/输出（IO）服务器；
- 网络组件：现场总线网络、控制网络、通讯路由器、防火墙、调制解调器、远程接入点。

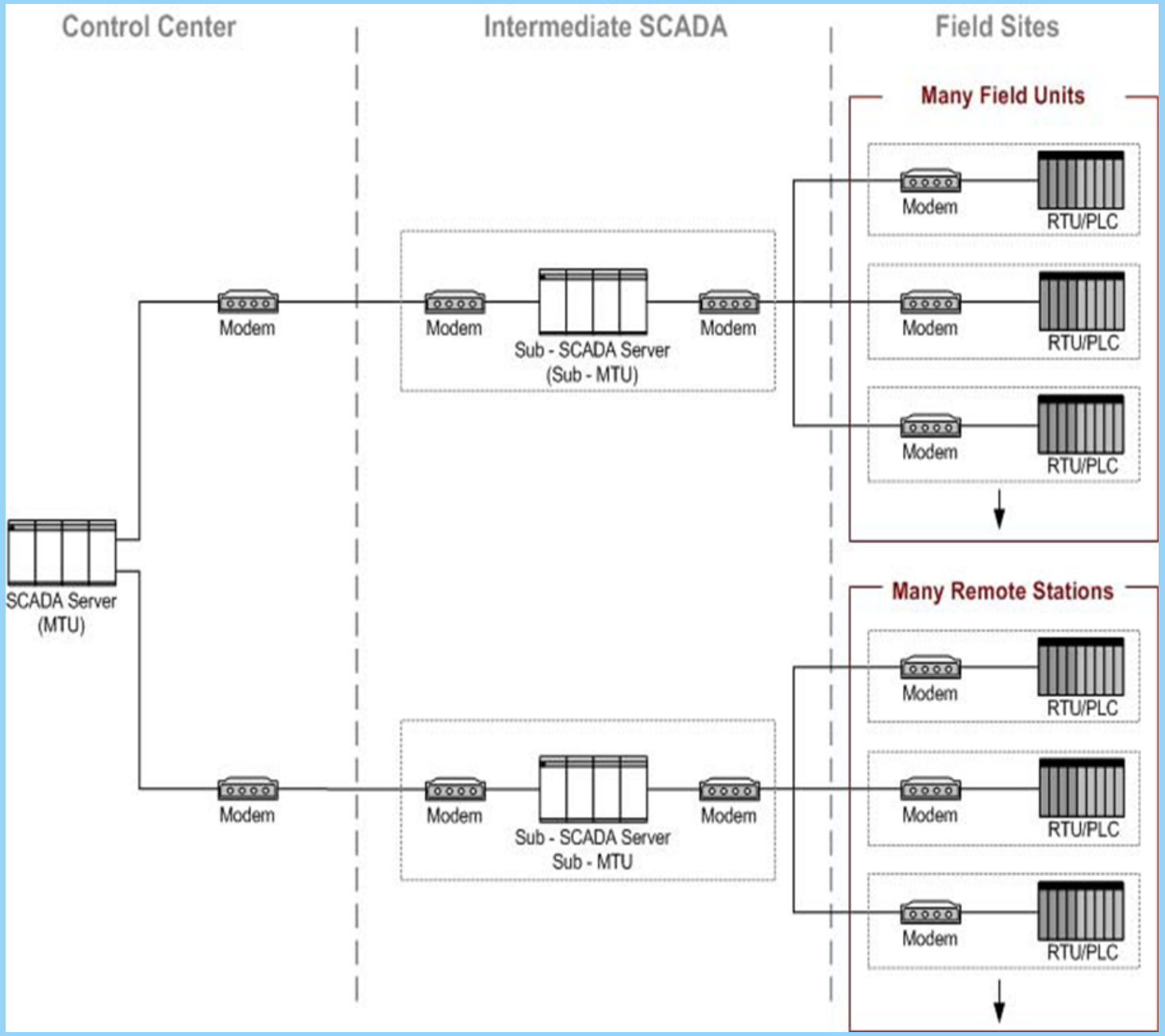
SCADA系统

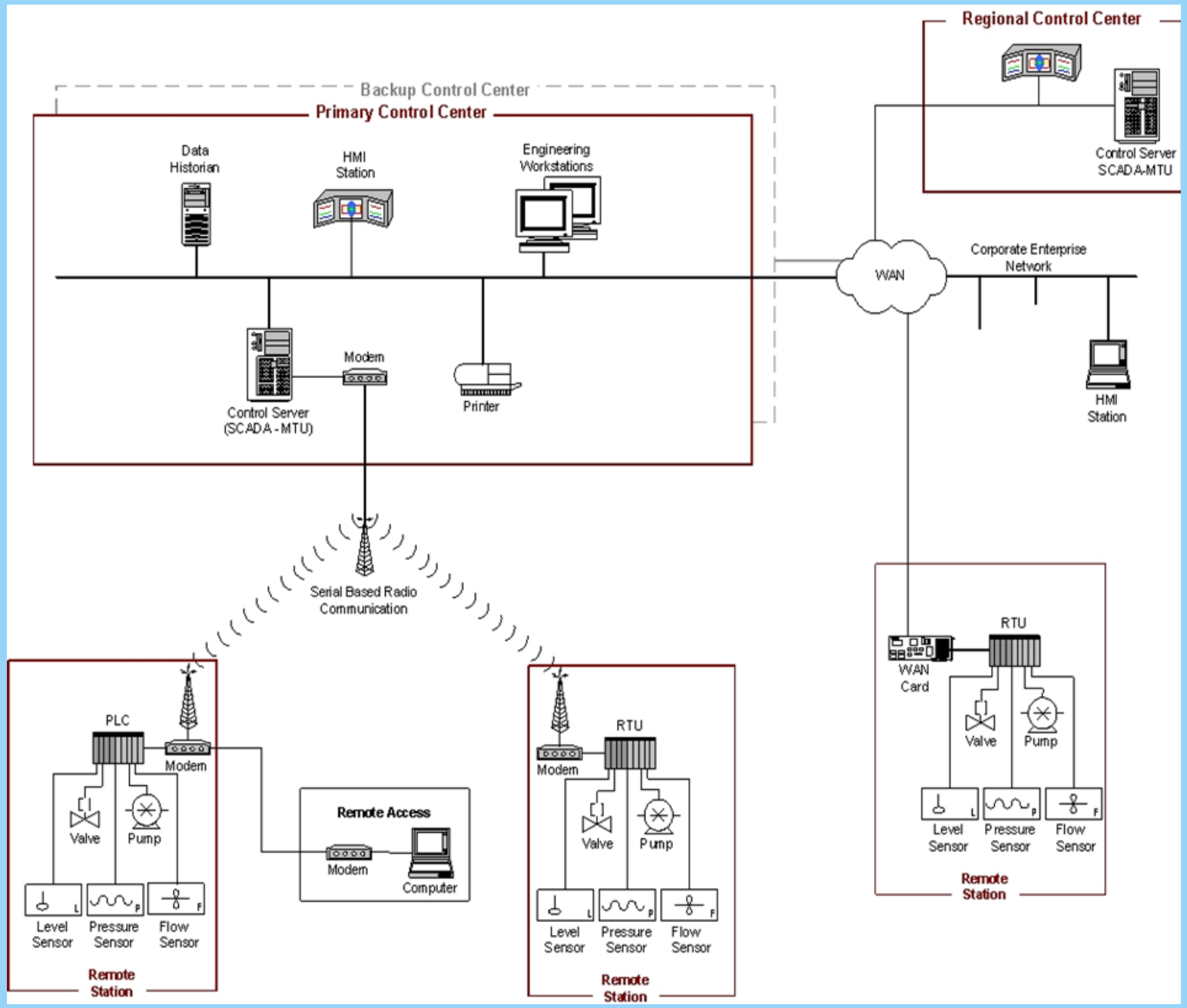
- SCADA系统是用来控制地理上分散的资产的高度分布式的系统，往往分散数千平方公里，其中集中的数据采集和控制是系统运行的关键。这些系统被用于配水系统和污水收集系统，石油和天然气管道，电力设施的输电和配电系统，以及铁路和其他公共交通系统。

总体结构



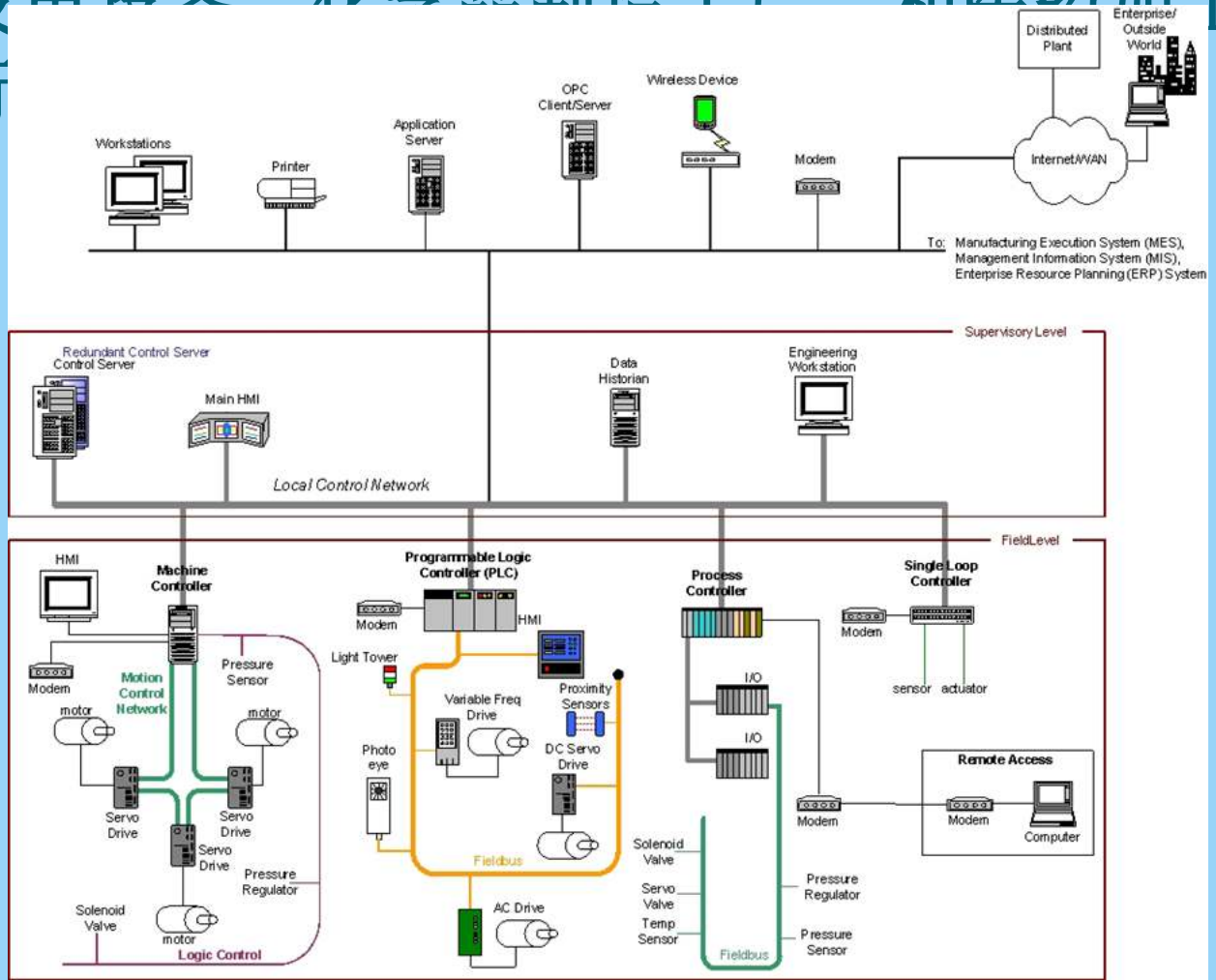

Control Center
Field Sites
point-to-point
series
series-star
multi-drop
SCADA Server
(MTU)
Modem
RTU/PLC


Control Center
Intermediate SCADA
Field Sites
Many Field Units
Modem
RTU/PLC
Modem
RTU/PLC
Modem
RTU/PLC
Modem
Modem
Sub - SCADA Server
(Sub - MTU)
Modem
SCADA Server
(MTU)
Many Remote Stations
Modem
RTU/PLC
Modem
RTU/PLC
Modem
RTU/PLC
Modem
Modem
Sub - SCADA Server
Sub - MTU
Modem


Regional Control Center
Control Server
SCADA-MTU
Backup Control Center
Primary Control Center
Data
Historian
HMI
Station
Engineering
Workstations
Modem
Control Server
(SCADA - MTU)
Printer
WAN
Corporate Enterprise
Network
HMI
Station
Serial Based Radio
Communication
PLC
Modem
Valve
Pump
Level
Sensor
Pressure
Sensor
Flow
Sensor
Remote
Station
Remote Access
Modem
Computer
RTU
Modem
Valve
Pump
Level
Sensor
Pressure
Sensor
Flow
Sensor
Remote
Station
RTU
WAN
Card
Valve
Pump
Level
Sensor
Pressure
Sensor
Flow
Sensor
Remote
Station

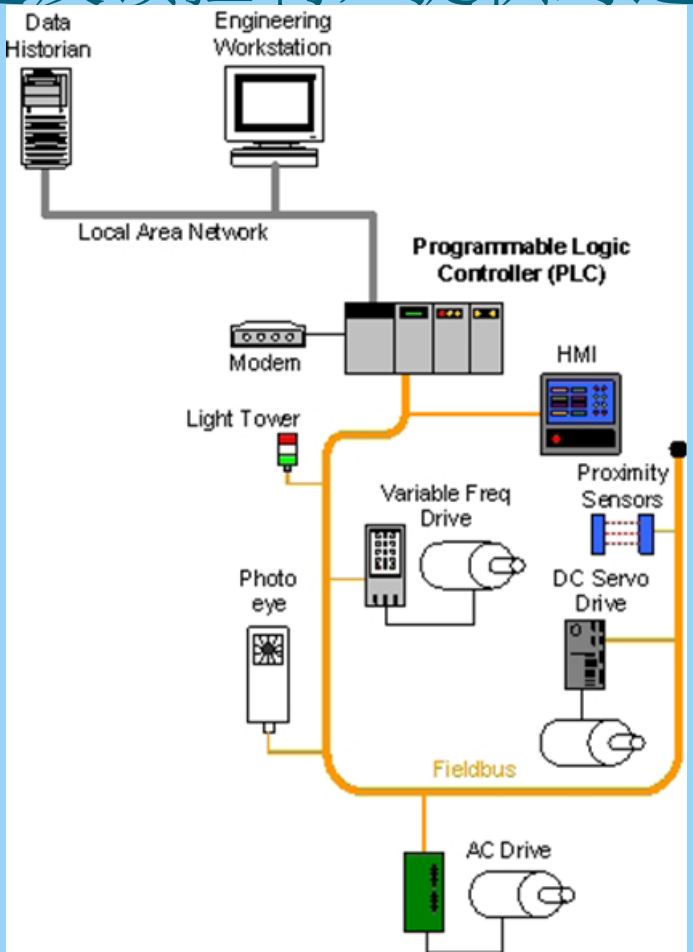
分布式控制系统（DCS）

- DCS系统用于控制在同一地理位置的生产系统，被用来控制工业生产过程，如炼油厂，水和污水处理，发电设备，化学品制造工厂，和医药加工设施等行



可编程逻辑控制器（PLC）

- PLC可用在SCADA和DCS系统中，作为整个分级系统的控制部件，通过反馈控制，提供对过程的本地管理。



ICS特性，威胁和脆弱性

ICS特性

- 本文中ICS特性主要是通过与IT系统的区别而列举出来的。

起初，ICS与IT系统并无相似之处，随着ICS采用广泛使用的、低成本的互联网协议（IP）设备取代专有的解决方案，以促进企业连接和远程访问能力，并正在使用行业标准的计算机、操作系统（OS）和网络协议进行设计和实施，它们已经开始类似于IT系统了。但是，ICS有许多区别于传统IT系统的特点，包括不同的风险和优先级别。其中包括对人类健康和生命安全的重大风险，对环境的严重破坏，以及金融问题如生产损失和对国家经济的负面影响。

表3-1 IT系统和ICS的差异总结

分类	信息技术系统	工业控制系统
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，因为过程的可用性要求 可用性要求可能需要冗余系统 中断必须有计划和提前预定时间（天/周） 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	首要焦点是保护 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），以确保它们不会影响 ICS 的正常运作
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严格限制的访问控制	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，通常是由软件供应商操作，因其专用的控制算法，以及可能要修改相关的硬件和软件
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 主要是有线网络，稍带一些本地化的无线功能的 典型的 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，包括专用的有线和无线（无线电和卫星） 网络是复杂的，有时需要控制工程师的专业知识

变更管理	在具有良好的安全策略和程序时，软件变更是及时应用的。往往是自动化的程序。	软件变更必须进行彻底的测试，以递增方式部署到整个系统，以确保控制系统的完整性。 ICS 的中断往往必须有计划，并提前预定时间（天/周）。 ICS 可以使用不再被厂商支持的操作系统。
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

- 其中首要的区别在于：IT系统的目标和过程控制系统的目标有根本性的区别， IT系统通常将性能、保密性和数据完整性作为首要需求，而ICS系统则将人类和设备安全作为其首要责任，因此，系统的可用性和数据完整性的具有较高核心级。

ICS面临的威胁

- 控制系统面临的威胁可以来自多种来源，包括对抗性来源如敌对政府、恐怖组织、工业间谍、心怀不满的员工、恶意入侵者，自然来源如从系统的复杂性、人为错误和意外事故、设备故障和自然灾害。