能源行业生产控制系统等保测评技术和实践分享

电力行业信息安全等级保护测评中心第一测评实验室
北京卓识网安技术股份有限公司
华北电力大学信息安全工程实验室

目 录

能源行业典型生产控制系统组成

能源工业是指对能源资源进行开发、加工、输送和利用的燃料动力工业，包括电力、石油、天然气、煤炭、核、新能源等类型。

工业生产过程控制：
是工业生产的核心大脑

关键信息基础设施运行控制：
能源工业控制系统是战略性基础设施的关键组成部分

什么是工业控制系统？

是国家关键基础设施控制系统的重要组成部分。

工业控制系统概念

工业自动化和控制系统（IACS)：包括人员、硬件、软件和工业过程操作的策略，其中策略可能影响工业过程的安全、信息安全和可靠性操作。（GB/T 35673-2017(62443-3-3)）

工业控制系统包括但不限于：

1）工业控制系统包括分布式控制系统（DCS）、可编程逻辑控制器（PLC）、智能电子设备（IED）、监视控制与数据采集（SCADA）系统，运动控制（MC）系统、网络电子传感和控制，监视和诊断系统等。

2）相关的信息系统，例如先进控制或者多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、制造执行系统（MES）等。

3）相关的部门、人员、网络或机器接口，为连续的、批处理、离散的和其他过程提供控制、安全和制造操作功能。

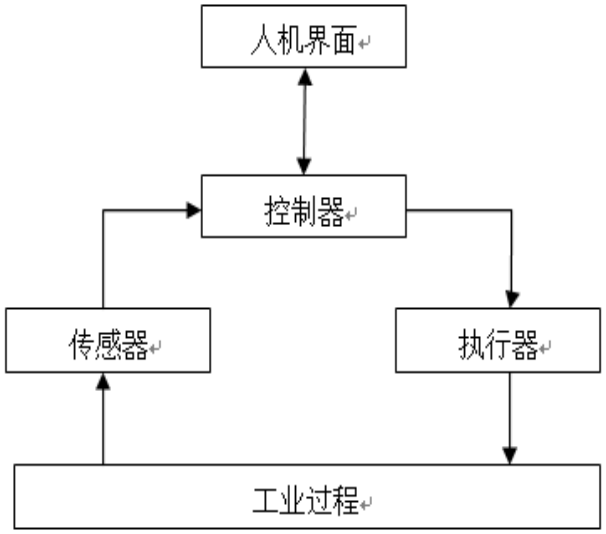
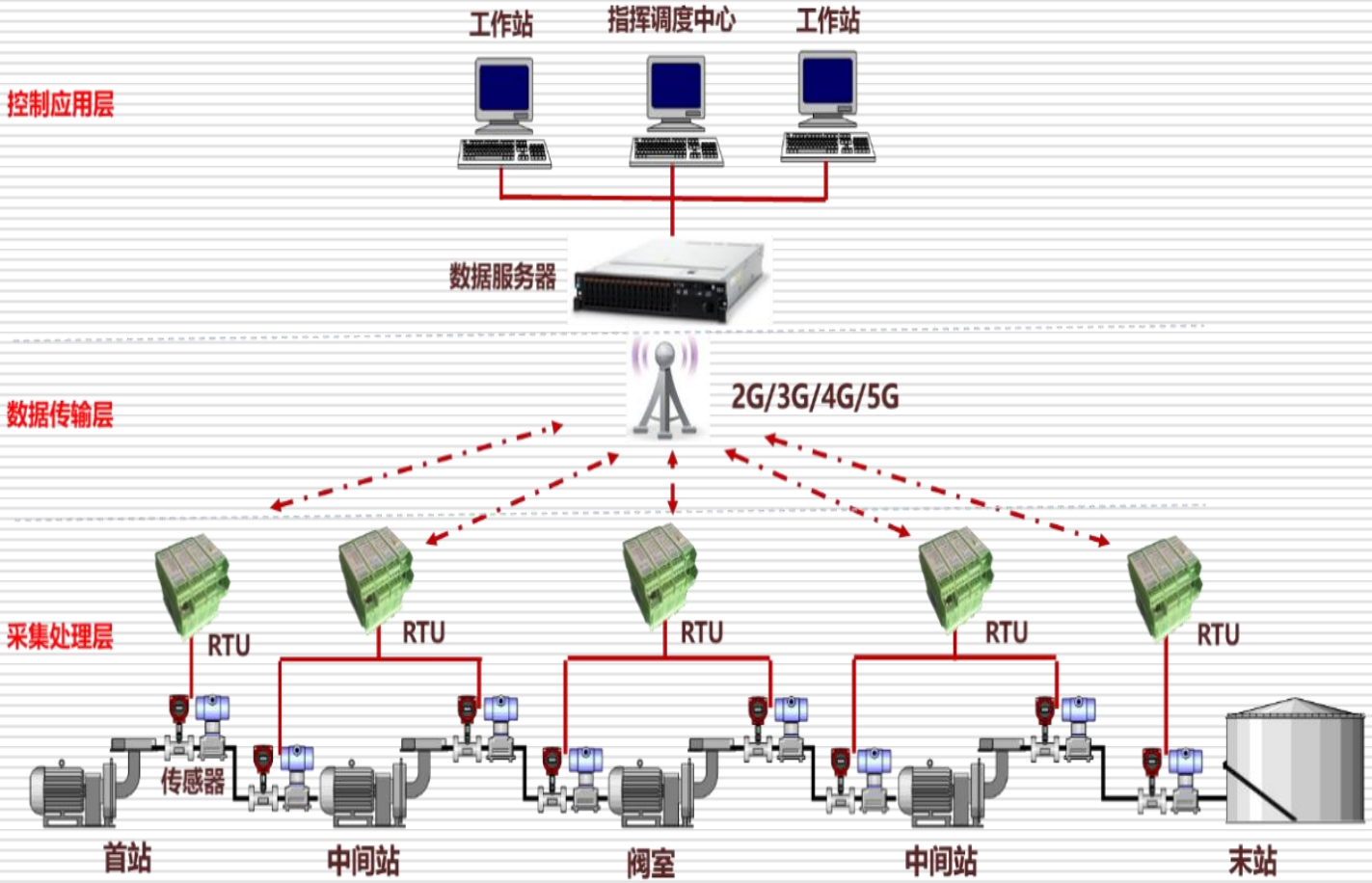


图 1 ICS 的典型操作

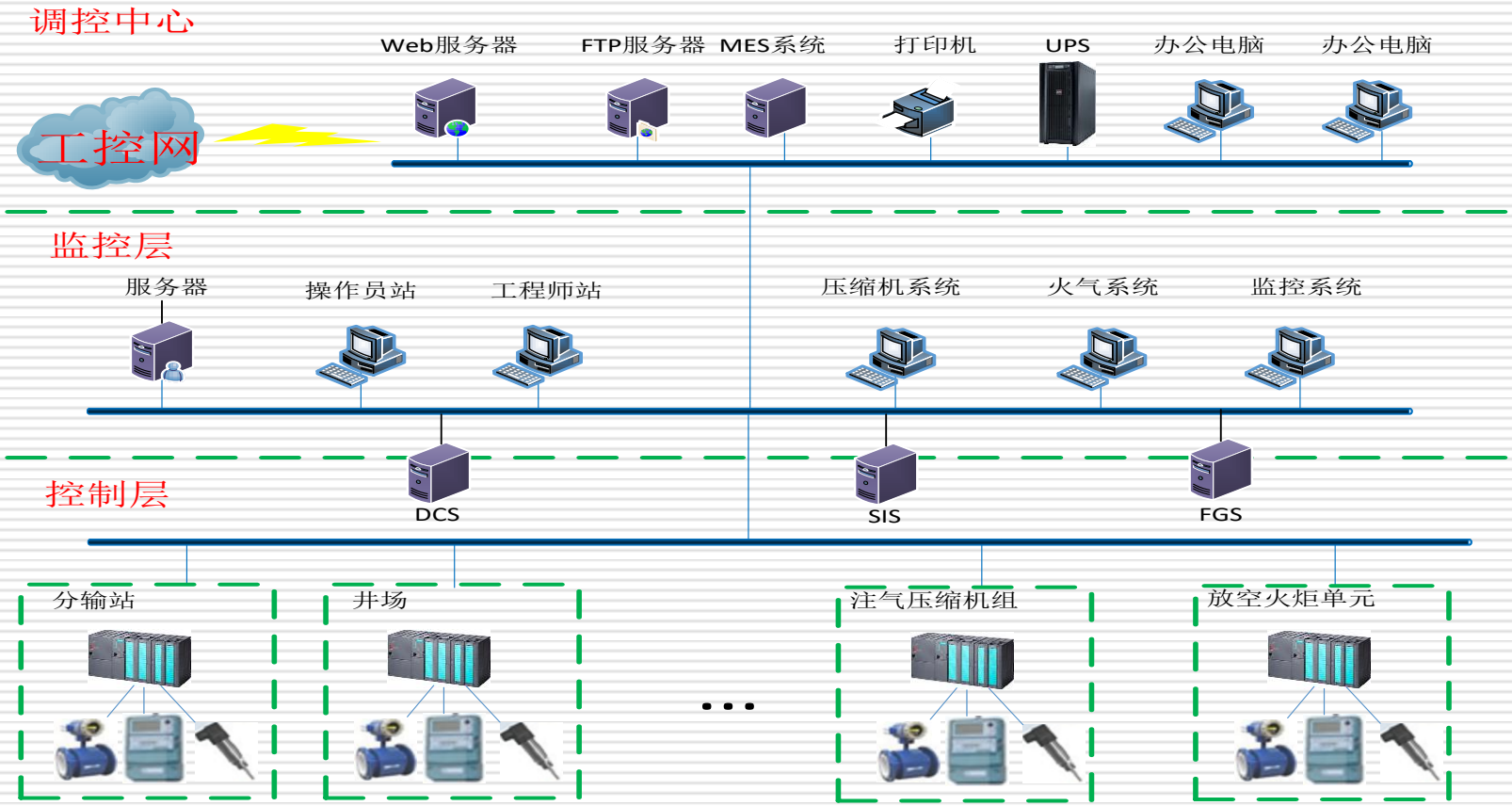
例：油气开采控制系统


生产管理子系统
生产动态实时监控
生产信息统计分析
生产工况实时诊断
工艺流程智能优化
关键告警集中展示
生产动态KPI展示
数据传输子系统
WiFi
WiMax
GPRS
3G
4G
卫星
压力
温度
流量
电量
功图
视频
可燃气体
有毒气体
RFID
数据采集与监控子系统
油井
气井
注水井
阀组
计量间
原油联合站
天然气处理厂

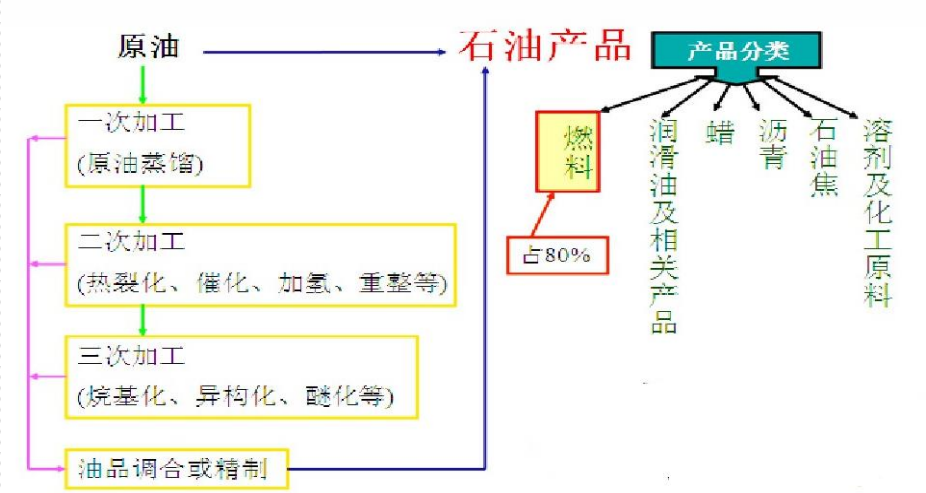
例：油气输送控制系统


工作站
指挥调度中心
工作站
控制应用层
数据服务器
数据传输层
2G/3G/4G/5G
采集处理层
RTU
RTU
RTU
RTU
RTU
传感器
首站
中间站
阀室
中间站
末站

例：储气库控制系统

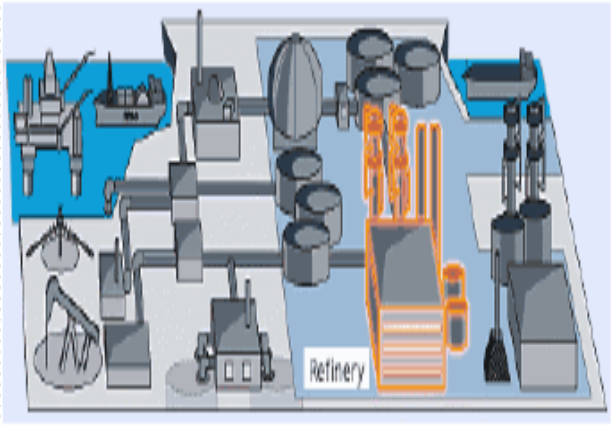

调控中心
Web服务器
FTP服务器
MES系统
打印机
UPS
办公电脑
办公电脑
工控网
监控层
服务器
操作员站
工程师站
压缩机系统
火气系统
监控系统
控制层
DCS
SIS
FGS
分输站
井场
注气压缩机组
放空火炬单元

例：石油炼制系统



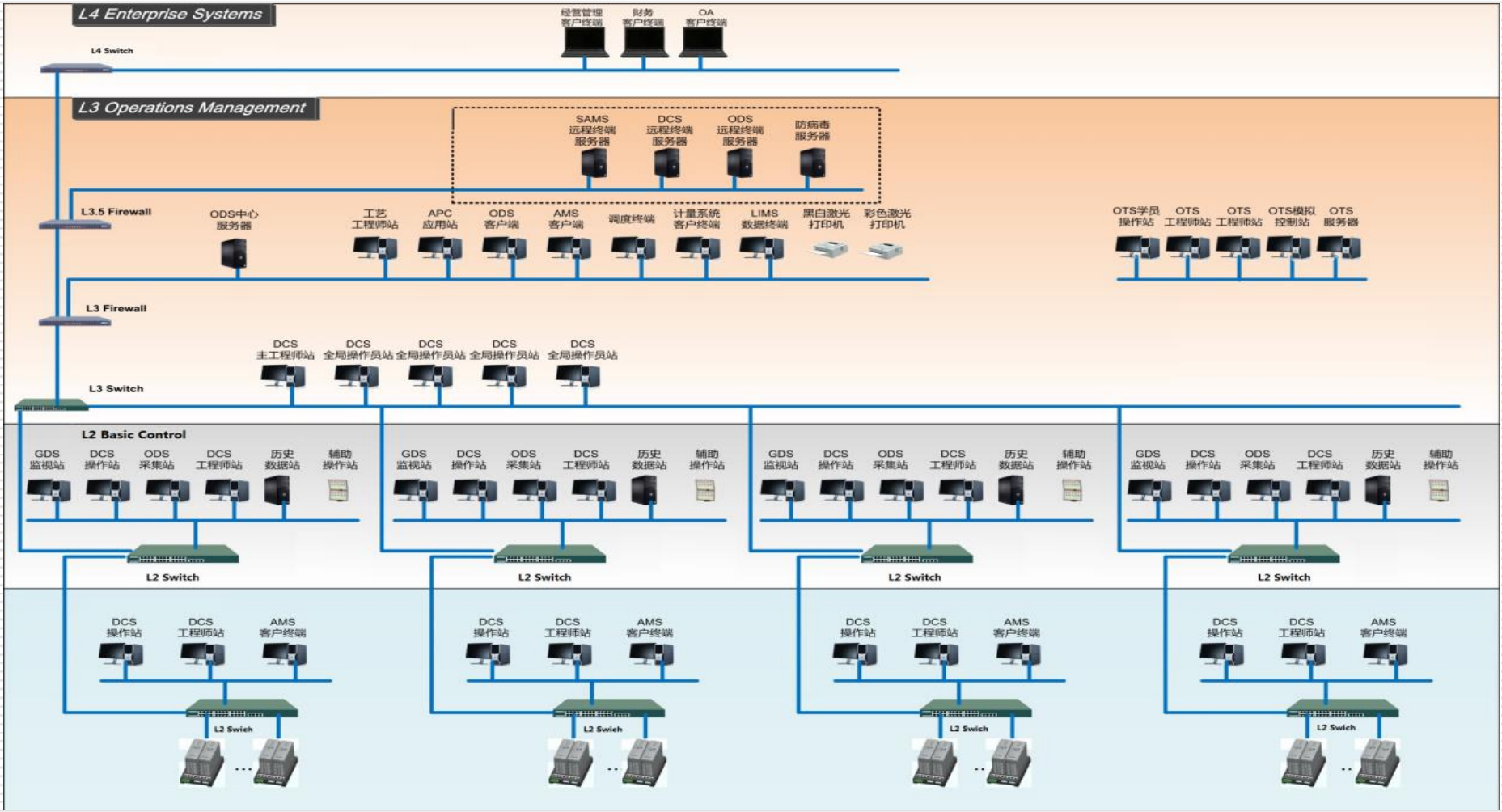
- 化学反应过程只能通过控制测量仪表和自动系统来间接监控；
- 生产过程往往是连续生产线，某一工序出现问题都会影响到全局；
- 水、电、蒸汽、氮气、燃料气、压缩空气等辅助公用系统保障生产装置平稳操作；

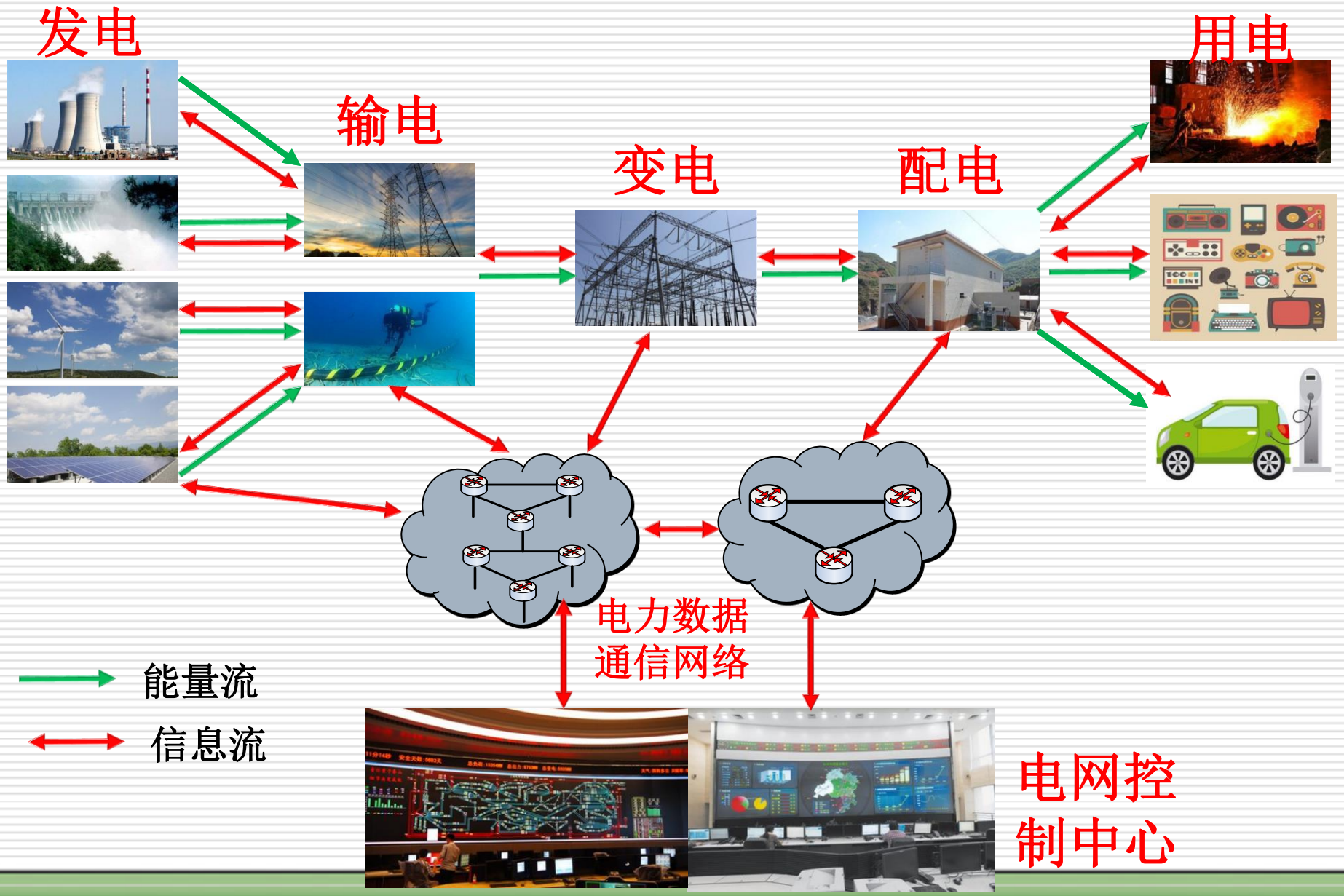
炼油

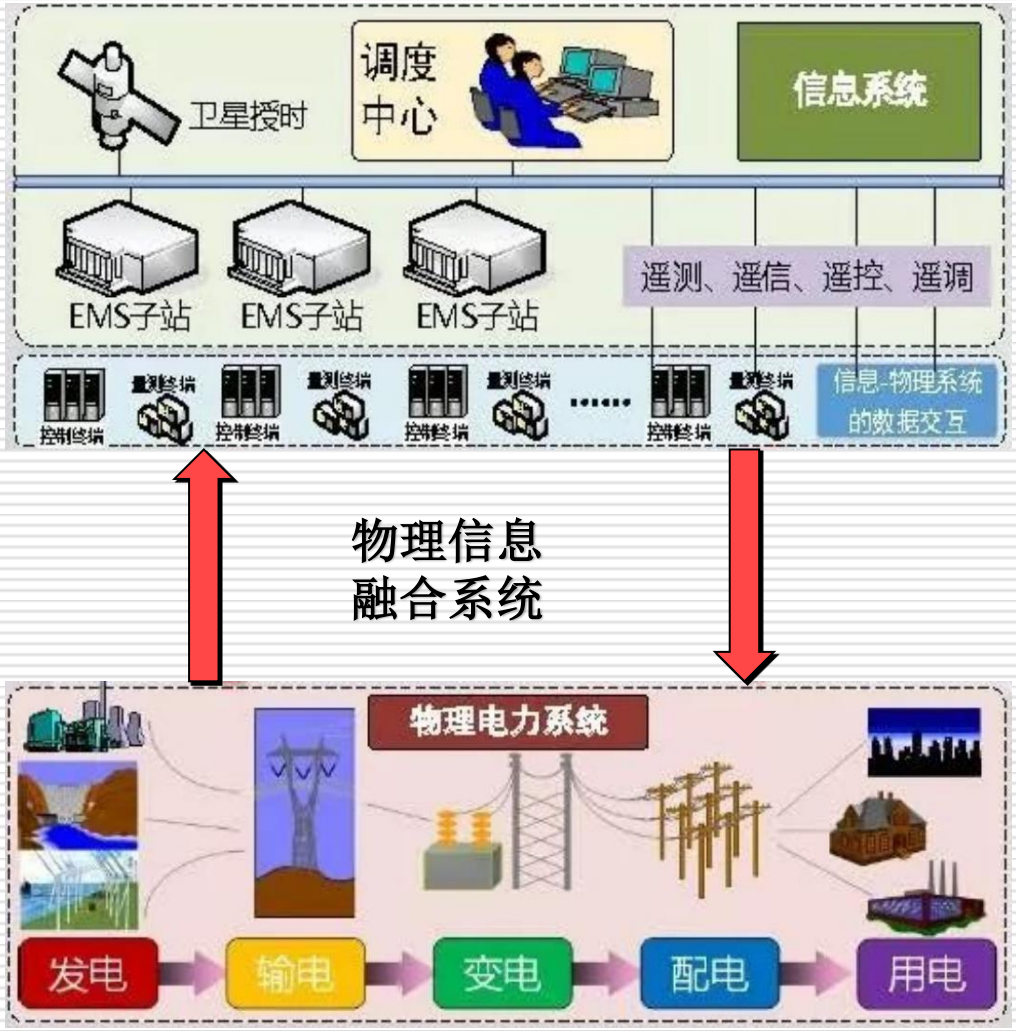


装置	应用
常减压装置	压缩机、在生风机
芳烃联合装置	鼓风机、引风机、空冷器
蜡油加氢装置	循环泵、风机
渣油、柴油加氢装置	循环泵、风机
重油催化裂化装置	油泵、风机
芳烃抽提	风机
空分装置	压缩机
灌区	泵

例：某石化工业控制系统


L4 Enterprise Systems
经营管理客户终端
财务客户终端
OA客户终端
L4 Switch
L3 Operations Management
SAMS远程终端服务器
DCS远程终端服务器
ODS远程终端服务器
防病毒服务器
L3.5 Firewall
ODS中心服务器
工艺工程师站
APC应用站
ODS客户端
AMS客户端
调度终端
计量系统客户终端
LIMS数据终端
黑白激光打印机
彩色激光打印机
OTS学员操作站
OTS工程师站
OTS工程师站
OTS模拟控制站
OTS服务器
L3 Firewall
DCS主工程师站
DCS全局操作员站
DCS全局操作员站
DCS全局操作员站
DCS全局操作员站
L3 Switch
L2 Basic Control
GDS监视站
DCS操作站
ODS采集站
DCS工程师站
历史数据站
辅助操作站
L2 Switch
DCS操作站
DCS工程师站
AMS客户终端
L2 Swich


发电
输电
变电
配电
用电
电力数据
通信网络
能量流
信息流
电网控
制中心



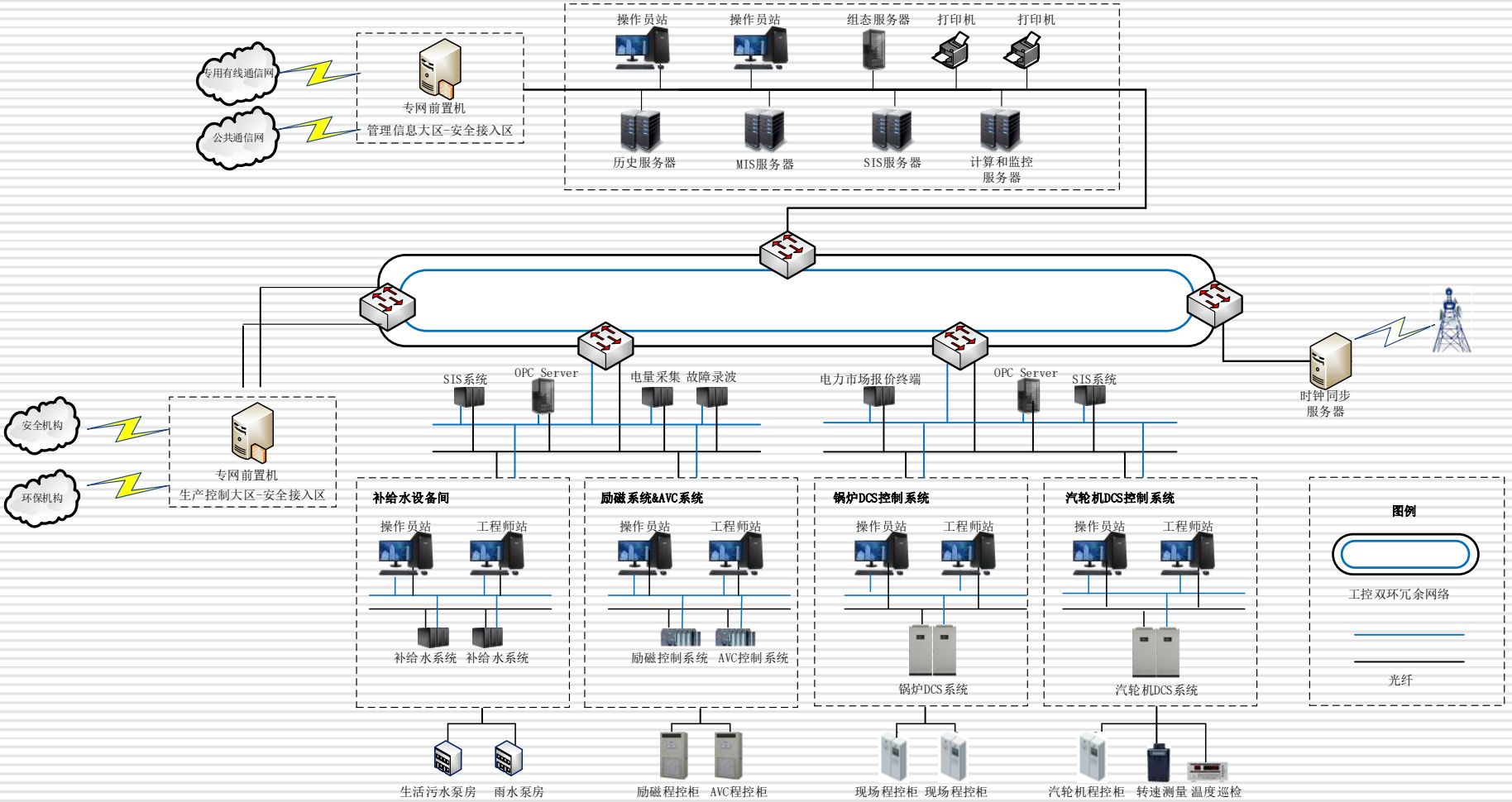
二次系统：

对一次系统进行监视，控制，测量和保护的系统，称为二次系统。如保证其安全可靠运行的继电保护装置、安全自动装置、调度自动化系统（主要有SCADA、EMS/DMS、WAMS等）和电力通信等相应的辅助系统

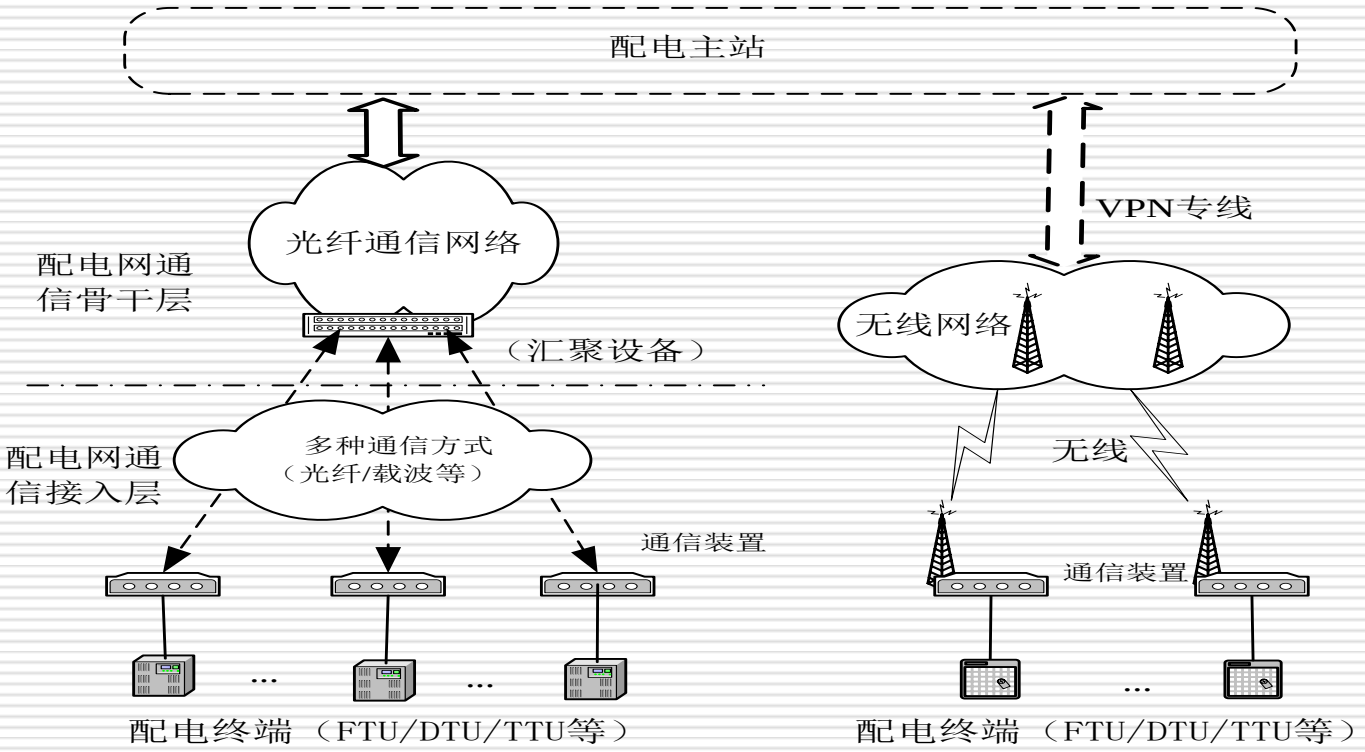
一次系统：

担负电能输送和分配任务的系统称为一次系统。如发电机、变压器、断路器、隔离开关、母线、线路、电动机等。

例：火力发电厂工业控制系统



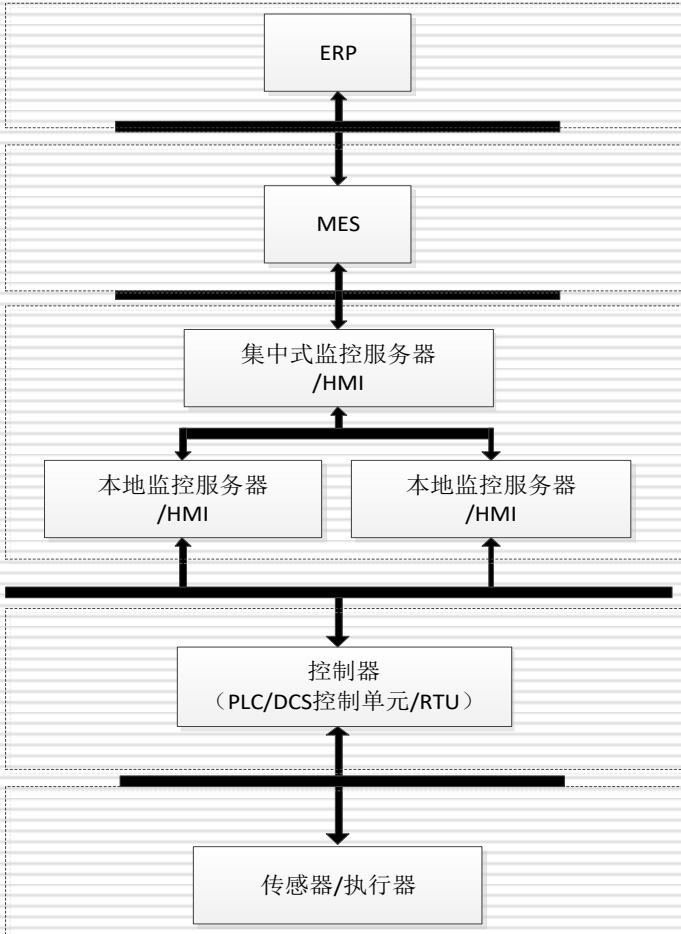
例：配电监控系统


配电主站
光纤通信网络
配电网通
信骨干层
（汇聚设备）
VPN专线
无线网络
多种通信方式
（光纤/载波等）
配电网通
信接入层
无线
通信装置
通信装置
配电终端（FTU/DTU/TTU等）
配电终端（FTU/DTU/TTU等）

	SCADA系统	DCS系统	PLC系统	RTU系统
主要特点	利用远程通信技术将地理位置分散的远程测控站点进行集中监控	利用局域网对控制回路进行集中监视和分散控制,用于连续变量、多回路的复杂控制	逻辑控制功能强，用于数字量、开关量的控制	对远程站点的现场数据测量功能强
地理范围	地理位置高度分散	地理位置集中（如工厂或以工厂为中心的区域)	地理位置集中	危险、恶劣的远程生产现场
应用领域	远程监控行业（如石油和天然气管道、电力电网	过程控制行业（如发电、炼油)	工业自动化，如生产线等	远程监控行业
通信技术	广域网、广播、卫星和电话或电话网等远程通信技术	局域网技术	局域网技术	远程通信技术
规模大小	大规模系统，现场站点多	控制回路复杂，测控点数多		作为SCADA系统的组成部分

工控控制系统测评对象的选择

层次模型—功能



层级4 企业资源层
该层级主要通过ERP系统为企业决策层及员工提供决策运行手段。

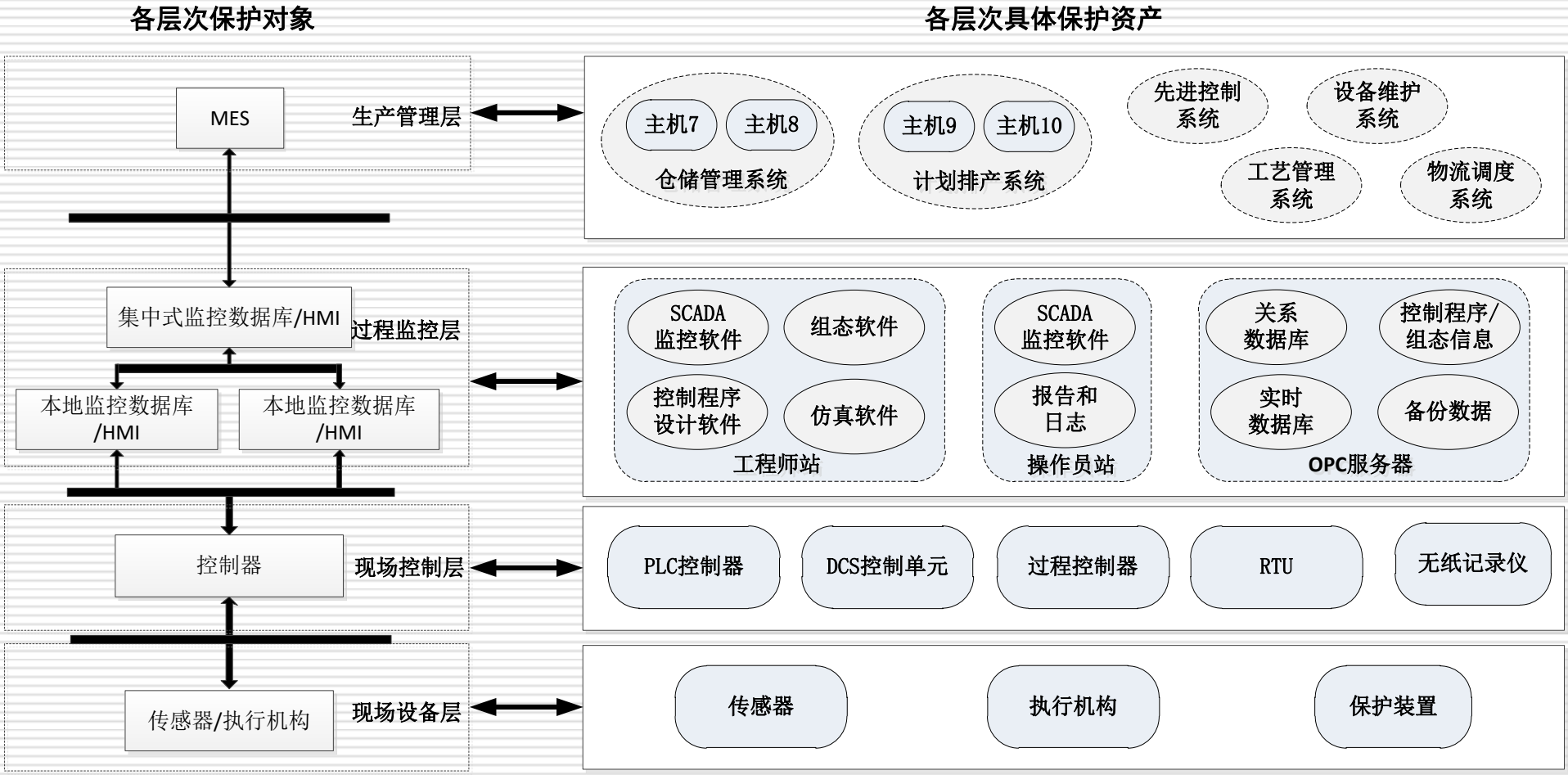
层级3 生产管理层
该层级主要通过MES系统为企业提供包括制造数据管理、计划排程管理、生产调度管理等管理模块。

层级2 过程监控层
该层级主要通过分布式SCADA系统采集和监控生产过程参数，并利用HMI系统实现人机交互。

层级1 现场控制层
该层级主要通过PLC、DCS控制单元和RTU等进行生产过程的控制。

层级0 现场设备层
该层级主要通过传感器对实际生产过程的数据进行采集，同时，利用执行器对生产过程进行操作。

层次模型—资产

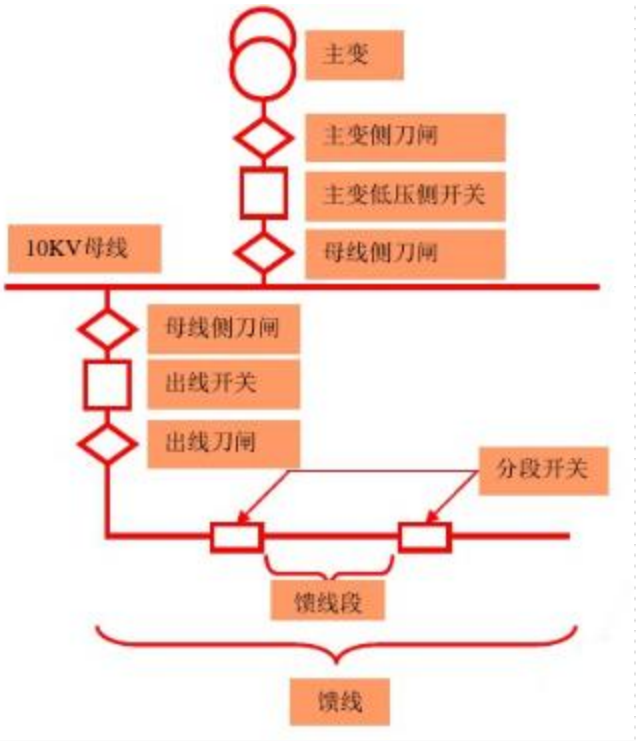

各层次保护对象
各层次具体保护资产
MES
生产管理层
主机7
主机8
仓储管理系统
主机9
主机10
计划排产系统
先进控制系统
设备维护系统
工艺管理系统
物流调度系统
集中式监控数据库/HMI
过程监控层
本地监控数据库/HMI
本地监控数据库/HMI
SCADA监控软件
组态软件
控制程序设计软件
仿真软件
工程师站
SCADA监控软件
报告和日志
操作员站
关系数据库
控制程序/组态信息
实时数据库
备份数据
OPC服务器
控制器
现场控制层
PLC控制器
DCS控制单元
过程控制器
RTU
无纸记录仪
传感器/执行机构
现场设备层
传感器
执行机构
保护装置

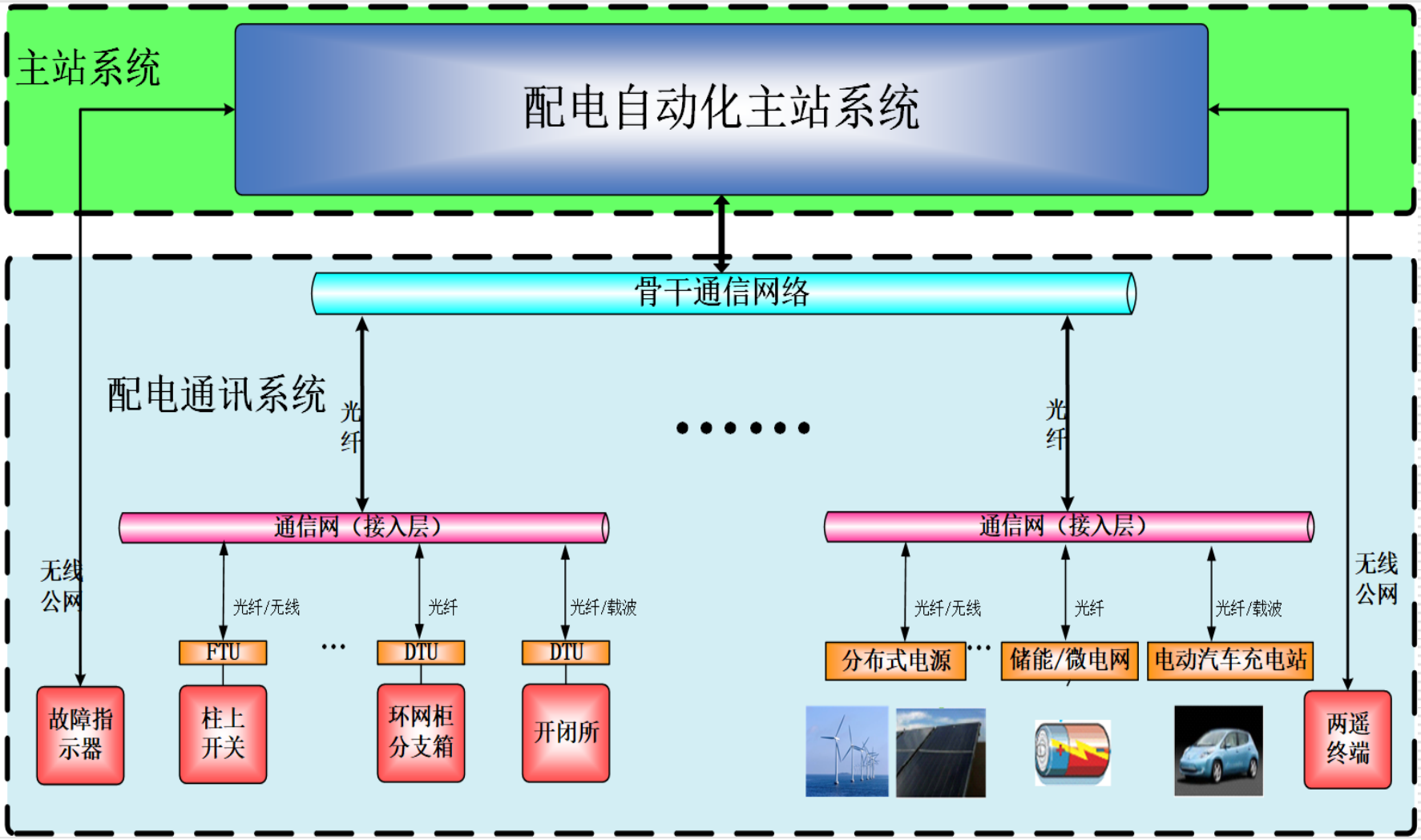
典型的测评对象（示例）

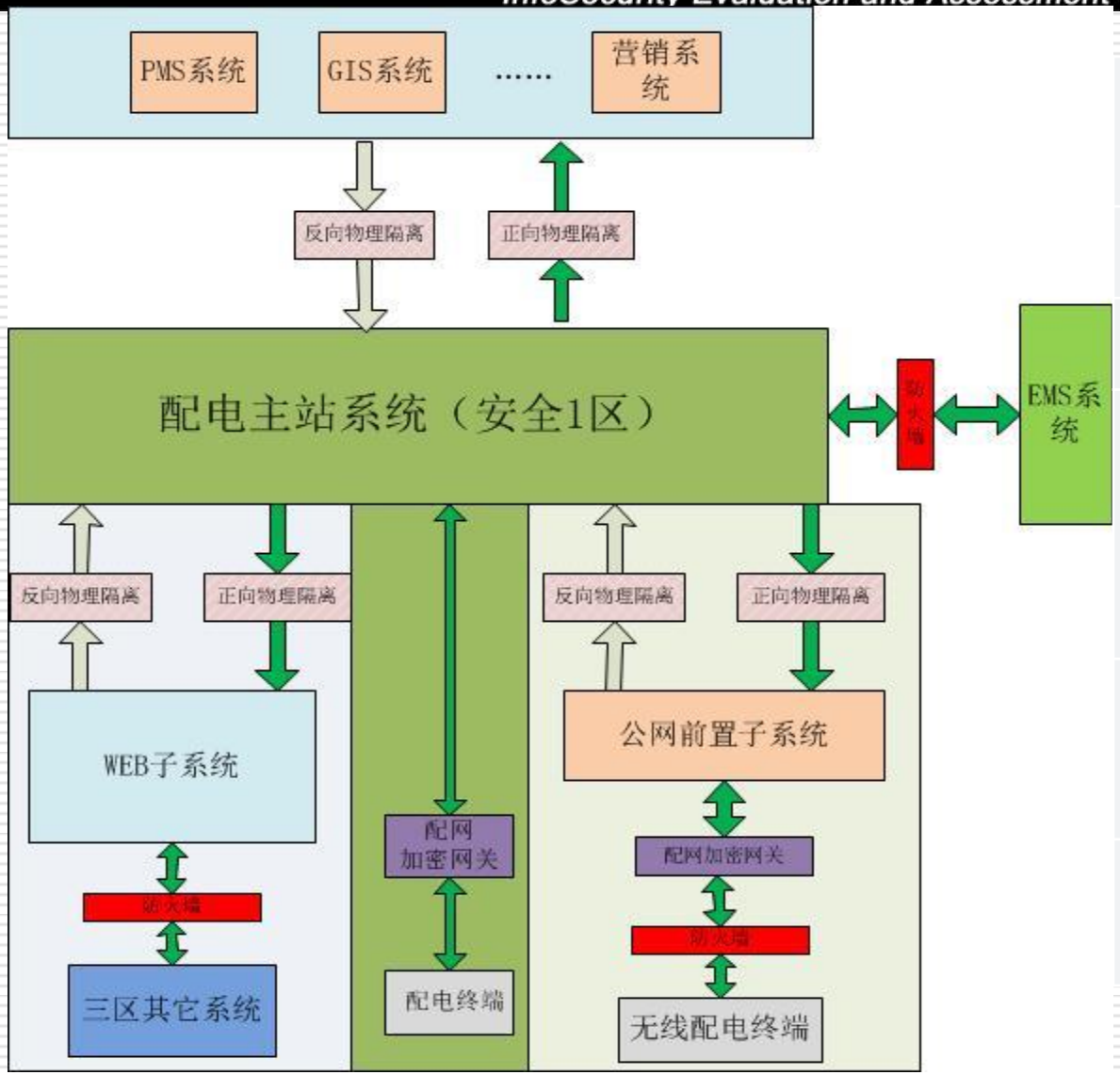
安全类或层面	测评对象
安全物理环境	系统机房、集控室、无人值守监控室等物理场所【1】
安全通信网络	● 交换机【2】、路由器等网络设备 ● 防火墙、网闸、加密装置等安全设备
安全区域边界	● 数传电台、无线网关等网络设备 ● 网闸、防火墙、IDS、IPS、防病毒检测、安全审计等安全设备
安全计算环境	● 服务器、操作终端 ● 磁盘阵列等存储设备等 ● 控制设备、智能仪表、带以太网通讯的远程子站 ● MES系统、EMS系统、APC系统等生产管理层软件【3】 ● SCADA软件、DCS监控软件、OPC通讯软件、实时/历史数据库软件、网络管理软件等 ● PLC编程软件、DCS组态软件、SIS编程软件、通讯配置软件、固件升级软件等 ● 操作系统、防恶意代码软件等 ● 网络互联设备和网络安全设备等。
安全管理中心	安全运营中心、态势感知平台、审计系统等

例： 配电自动化系统

配电系统化系统主要指10kV中压系统，一般从变电站的主变低压侧和低压母线开始，直到电力用户为止。配电自动化主要处理中压网的一次设备（开闭所、环网柜、柱上开关、变压器）的监测与控制，以及基于地理信息系统的设备管理。



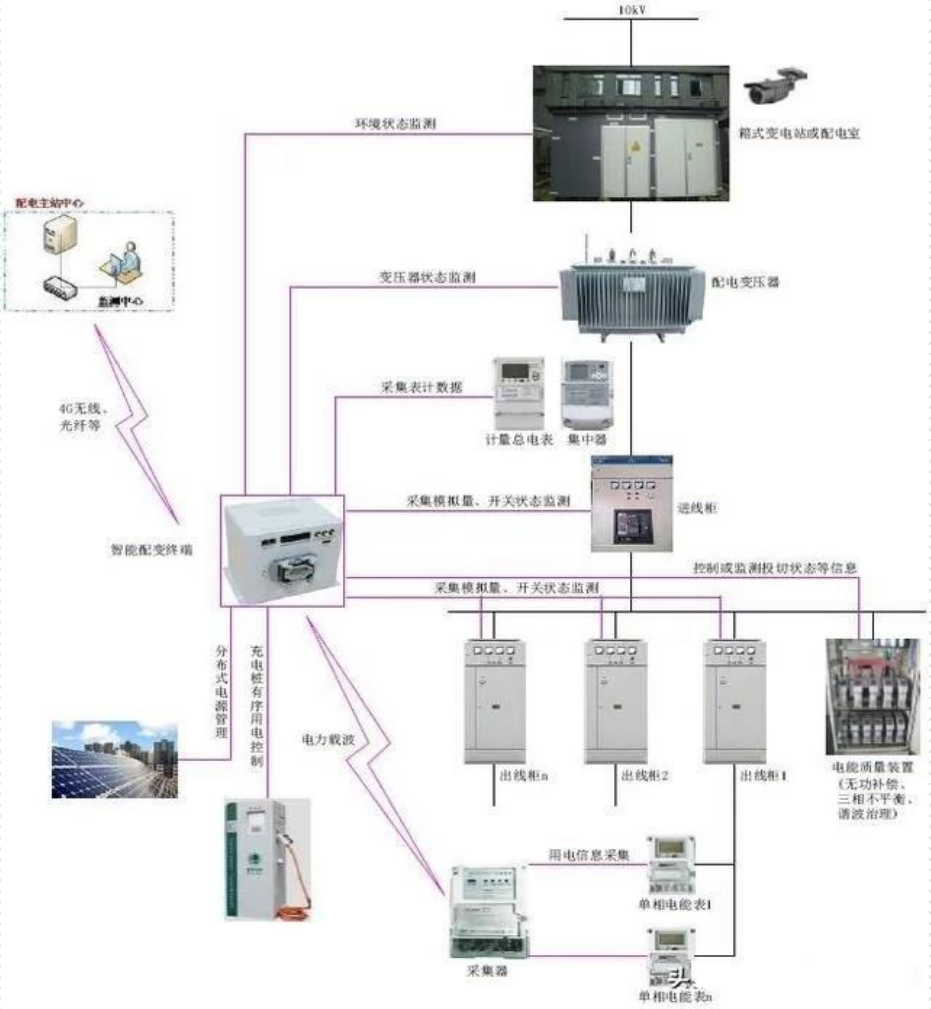

主站系统
配电自动化主站系统
骨干通信网络
配电通讯系统
光纤
光纤
通信网（接入层）
通信网（接入层）
无线公网
光纤/无线
光纤
光纤/载波
光纤/无线
光纤
光纤/载波
无线公网
FTU
DTU
DTU
分布式电源
储能/微电网
电动汽车充电站
故障指示器
柱上开关
环网柜分支箱
开闭所
两遥终端



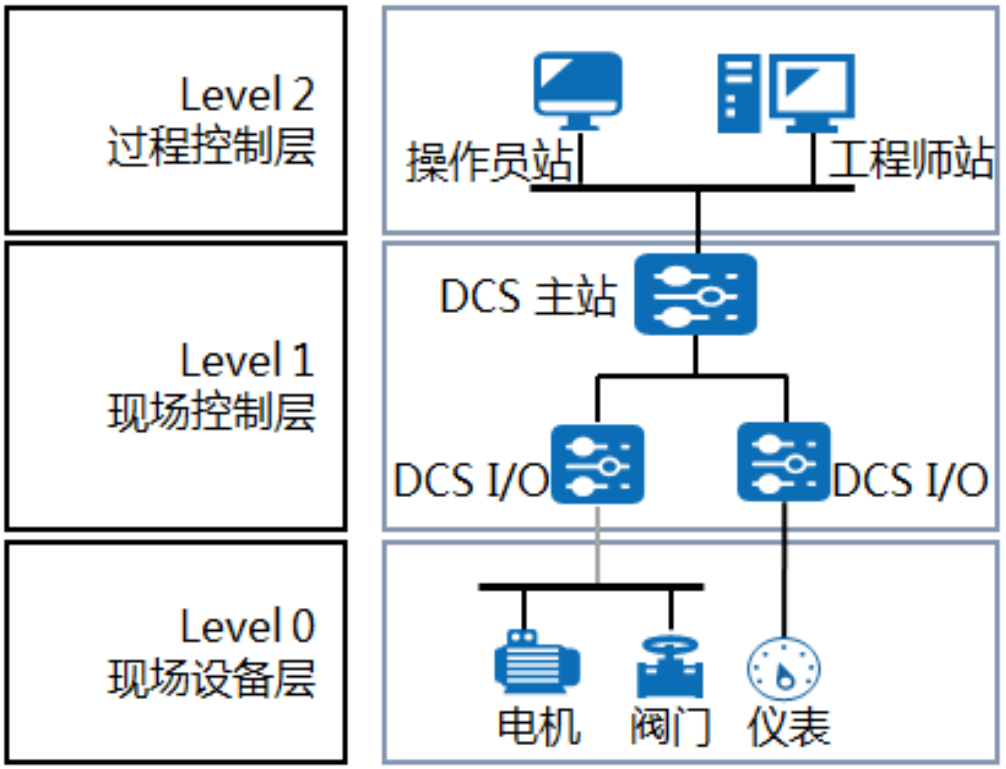
功能层次	资产
企业资源层	不涉及
生产管理层	不涉及
过程监控层	配网主站系统、WEB子系统、公网前置子系统、配网加密网关及网络、安全设备
现场控制层	FTU、DTU、TTU、网络设备、安全设备等
现场设备层	出线开关、柱上开关、环网柜、开闭所（开关站）、配电变压器

安全区	硬件配置	功 能 说 明
生产控制大区	数据采集服务器	完成配电SCADA数据采集、系统时钟和对时的功能。
	SCADA服务器	完成配电SCADA数据处理、操作与控制、全息历史/事故反演、多态多应用、模型管理、权限管理、告警服务、报表管理、系统运行管理、终端运行工况监视等功能
	配网应用服务器	完成馈线故障处理、电网分析应用、配网实时调度管理、智能化应用等功能。在主站系统处理负载率符合指标的情况下，可以将配网应用服务器与SCADA服务器合并。
	历史数据库服务器	完成数据库管理、数据备份与恢复、数据记录等功能。
	接口适配服务器	完成与外部系统的信息交互功能。
	工作站	包括配调工作站、检修计划工作站、报表工作站、维护工作站等。
管理信息大区	公网数据采集服务器	完成公网配电通信终端（FTU、TTU等）的实时数据采集。
	WEB服务器	完成安全I区配电SCADA数据信息的网上发布功能。
	时间序列数据库服务器	完成全息历史数据的处理和存储，供WEB应用分析使用。

现场控制层&现场控制层

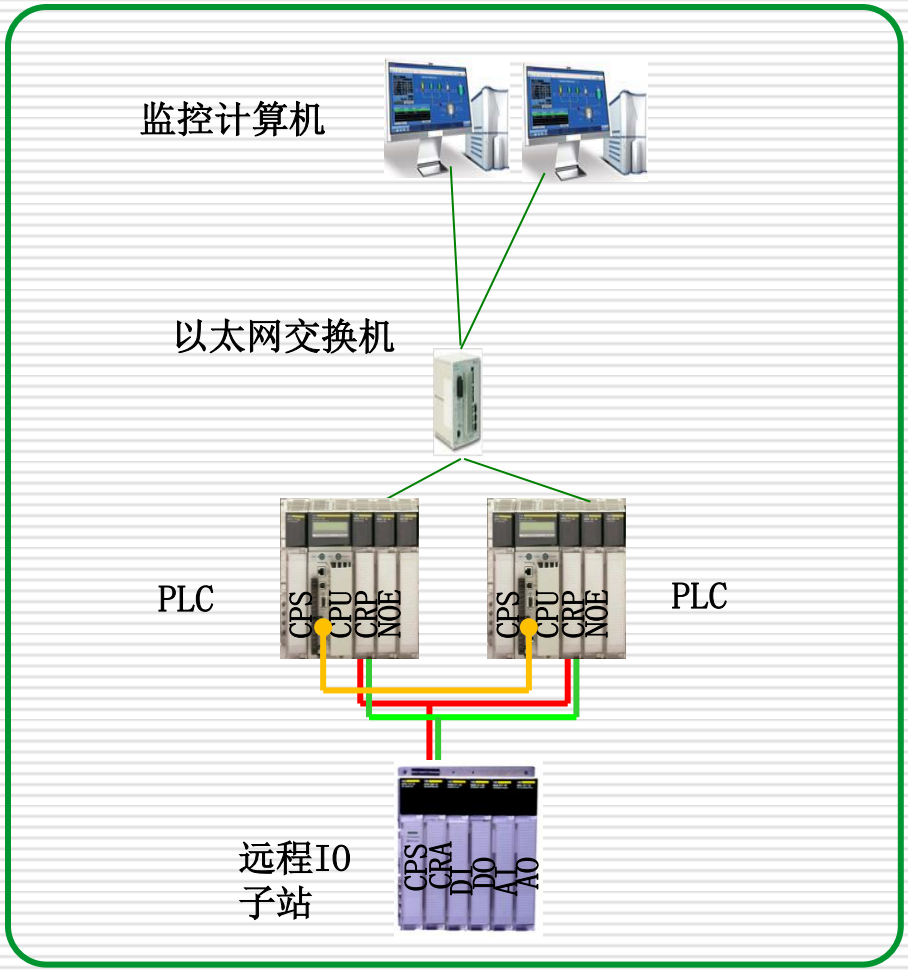

10kV
环境状态监测
箱式变电站或配电室
配电主站中心
监测中心
变压器状态监测
配电变压器
采集表计数据
计量总电表
集中器
4G无线、光纤等
采集模拟量、开关状态监测
进线柜
智能配变终端
控制或监测投切状态等信息
采集模拟量、开关状态监测
分布式电源管理
充电桩有序用电控制
电力载波
出线柜n
出线柜2
出线柜1
电能质量装置（无功补偿、三相不平衡、谐波治理）
用电信息采集
单相电能表1
采集器
单相电能表n

例：典型的DCS系统


Level 2
过程控制层
Level 1
现场控制层
Level 0
现场设备层
操作员站
工程师站
DCS 主站
DCS I/O
DCS I/O
电机
阀门
仪表

功能层次	资产
企业资源层	不涉及
生产管理层	不涉及
过程监控层	服务器、工控机、交换机、操作系统、应用软件
现场控制层	DPU、网络设备
现场设备层	电机、阀门、仪表

例： 典型的 PLC系统



功能层次	资产
企业资源层	不涉及
生产管理层	不涉及
过程监控层	监控计算机
现场控制层	PLC、网络设备
现场设备层	电机、阀门、仪表

工业控制系统安全扩展要求

-- 以第三级为例

工业控制系统的测评时应同时依据安全测评通用要求和安全测评扩展要求，本部分仅涉及工业控制系统安全扩展要求。

序号	控制点	第一级	第二级	第三级	第四级
1	室外控制设备防护	2	2	2	2
2	网络架构	2	3	3	3
3	通信传输	0	1	1	1
4	访问控制	1	2	2	2
5	拨号使用控制	0	1	2	3
6	无线使用控制	2	2	4	4
7	控制设备安全	2	2	5	5
8	产品采购和使用	0	1	1	1
9	外包软件开发	0	1	1	1

安全物理环境--室外控制设备物理防护

a) 室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；

测评实施要点：

核查是否放置在采用铁板或其他防火材料制作的箱体或装置中，并紧固于箱体或装置中；

核查箱体或装置是否具有透风、散热、防盗、防雨和防火能力

安全物理环境--室外控制设备物理防护

b）室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

测评实施要点：

访谈管理员，了解室外设备附近强电磁、强热源情况；

核查室外控制设备是否远离强电磁干扰、强热源等环境，如雷电、沙暴、大功率启停设备、高压输电线等强电磁干扰环境，以及加热炉、蒸汽等强热源环境；

对于无法远离强电磁干扰、强热源等环境的室外控制设备，应核查是否具有应急处置及检修维护记录。

安全通信网络—网络架构

a) 工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段;

b) 工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段;

c) 涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离

测评实施要点：

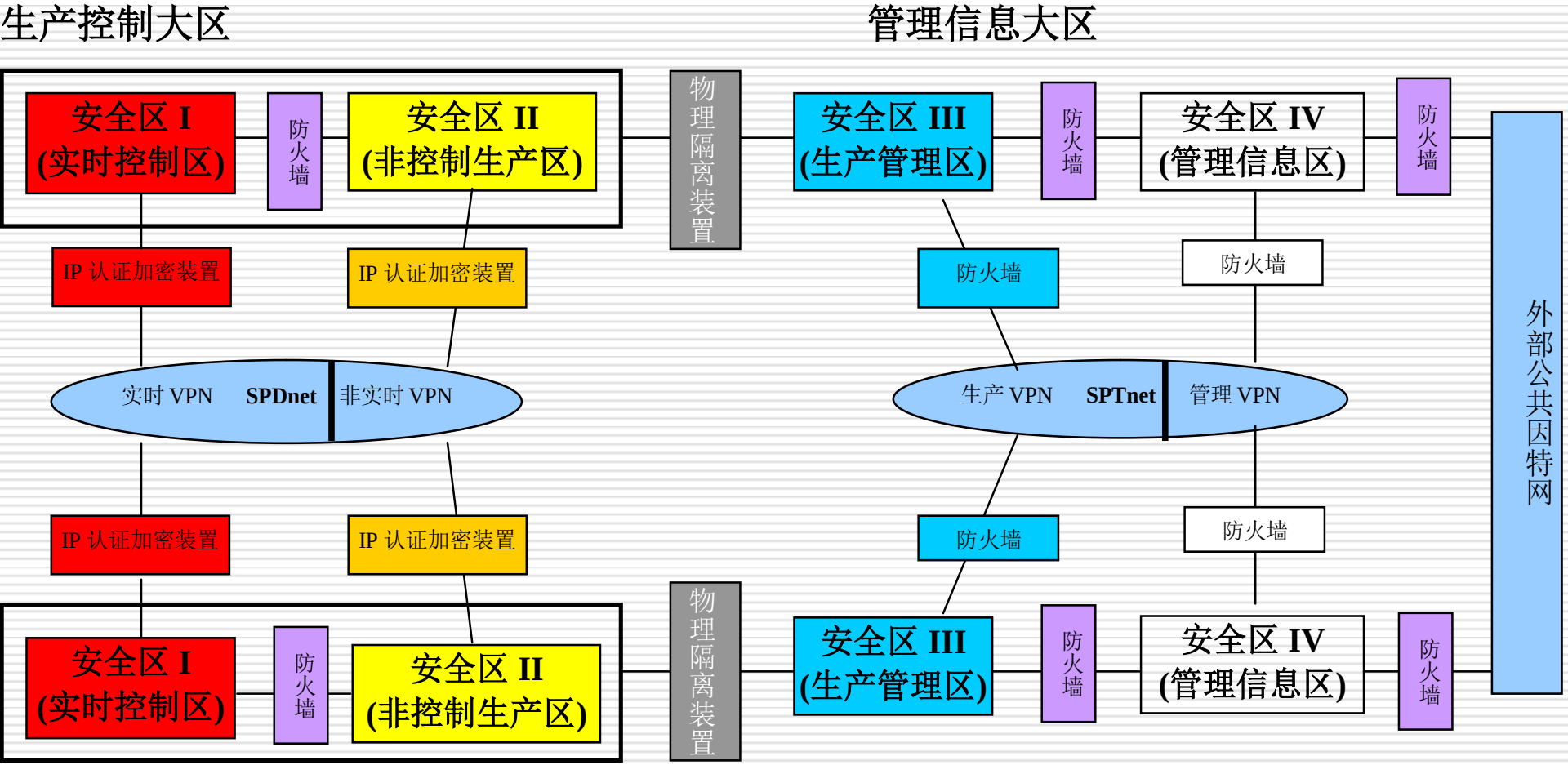
核查工业控制系统边界是否存在与企业其他系统进行通信的情况，采用何种方式通信；采用何种访问控制的设备或技术手段实现单向隔离，是否有效；

了解网络拓扑结构，工控控制系统的业务特点和安全域划分原则；核查不同安全域、各层级之间是否采用具有访问控制功能的设备，并核查其访问控制策略的有效性；

了解被测工业控制系统是否涉及实时控制和数据传输；核查涉及实时控制和数据传输的工业控制系统是否在物理层面上独立组网，且与其他系统或非实时业务无共用设备。

核查工业控制系统的无线通信方式。

电力监控系统安全防护总体方案



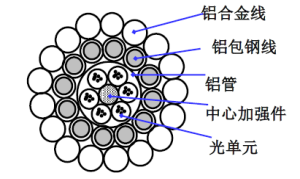
安全分区、网络专用、横向隔离、纵向认证

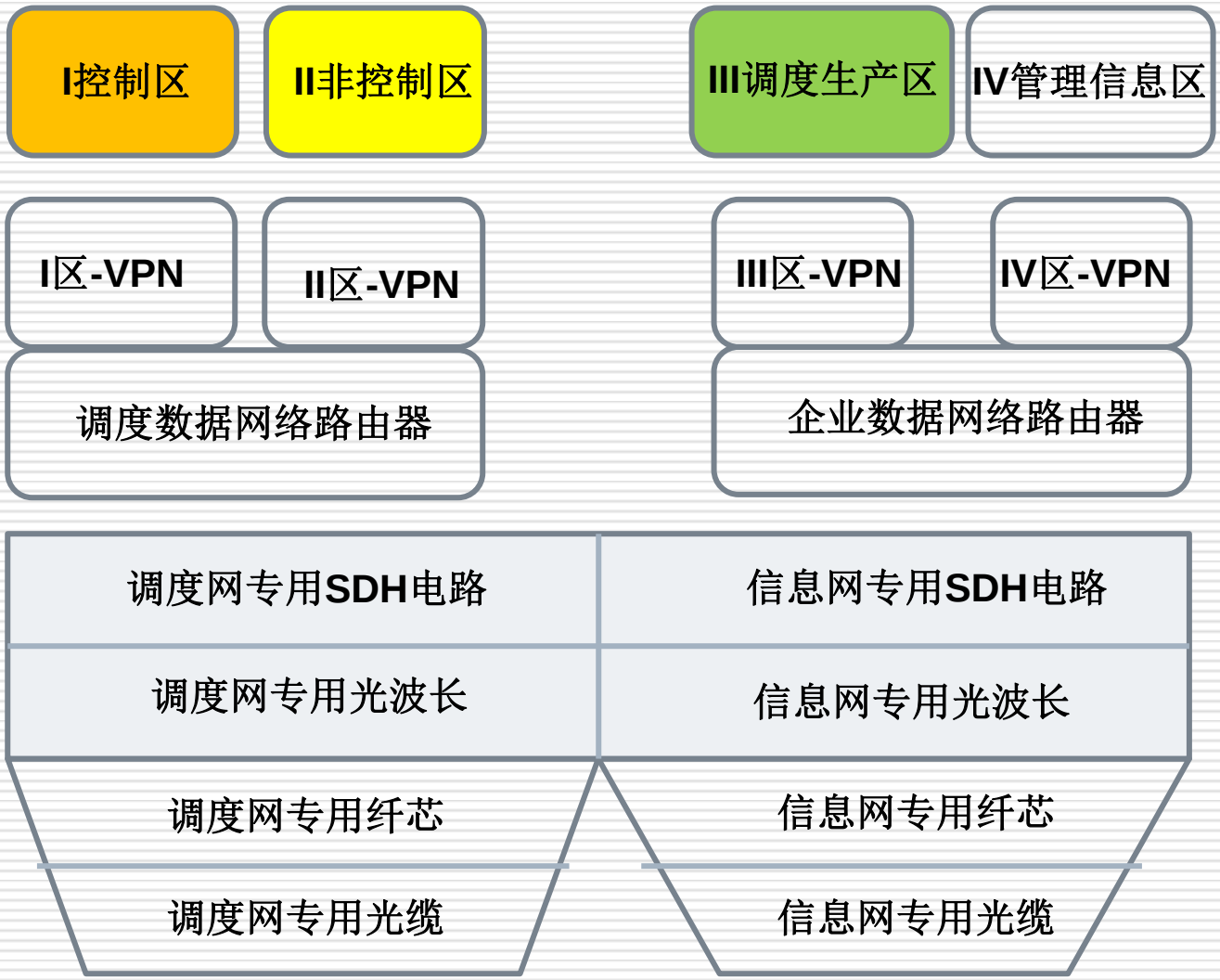
网络专用

ATM异步传输模式和PTN网路传输协议属于统计复用，不满足网络专用的安全要求。

控制系统尽量不用无线通信。如采用无线换用通信必须基于改进的安全隔离架构LTE设备

电力特种光缆：OPGW

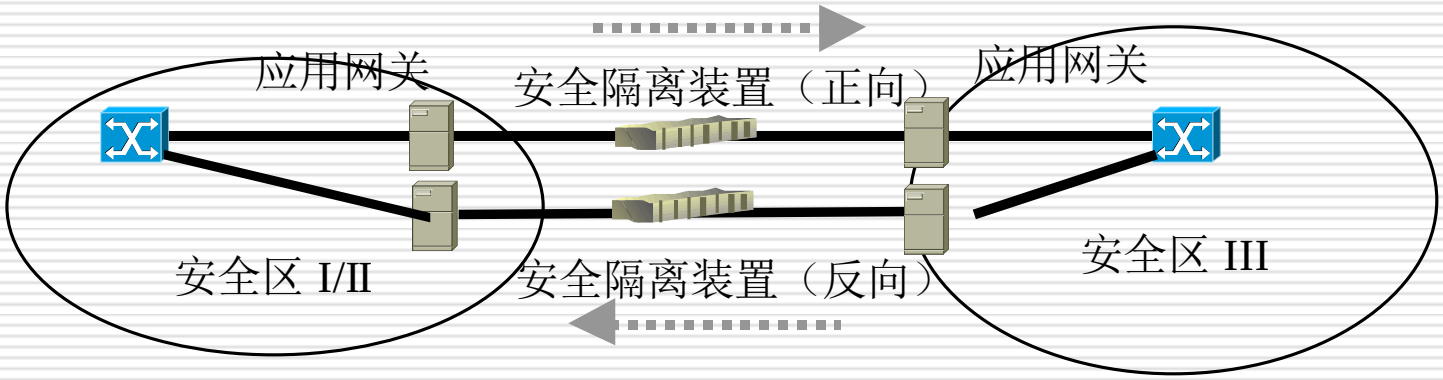




横向隔离

- 电力专用安全隔离装置作为安全区I/II与安全区III的必备边界，要求具有最高的安全防护强度，是安全区I/II横向防护的要点。
- 安全隔离装置（正向）用于安全区I/II到安全区III的单向数据传递；安全隔离装置（反向）用于安全区III到安全区I/II的单向数据传递。

安全隔离装置的部署：



安全通信网络—通信传输

a）在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

测评实施要点：

访谈网络管理员，了解工业控制系统是否具有与广域网进行控制指令或相关数据交换需求，识别是否具有通过广域网传输的控制指令；

核查工业控制系统与广域网是否使用加密认证设备，并查看设备是否配置加密策略；

测试验证所使用的加密认证技术手段的有效性。在条件允许的情况下（如停机检修），可通过技术手段验证数据是否为密文传输。

安全区域边界—访问控制

a）应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务；

b）应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

测评实施要点：

访谈网络安全管理员工业控制系统与企业其他系统之间是否部署访问控制设备（防火墙、隔离设备），访问控制设备是否开启访问控制策略；

现场核查访问控制设备的访问控制策略，是否禁止通用网络服务；

对边界网络进行渗透测试，确认不存在绕过访问控制措施的方法；

示例

在安全域边界和安全层级之间布置工业防火墙、网络隔离设备等，并设置相应的访问控制规则，禁止任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务。

安全区域边界—拨号使用控制

a）工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别好访问控制等措施；

b）拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施

测评实施要点：

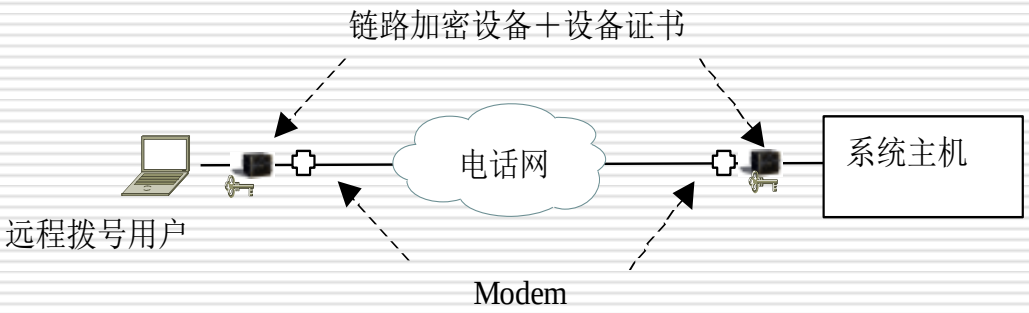
现场核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施；

如采用VPN接入进行拨号访问，查看是否采取的访问控制措施。

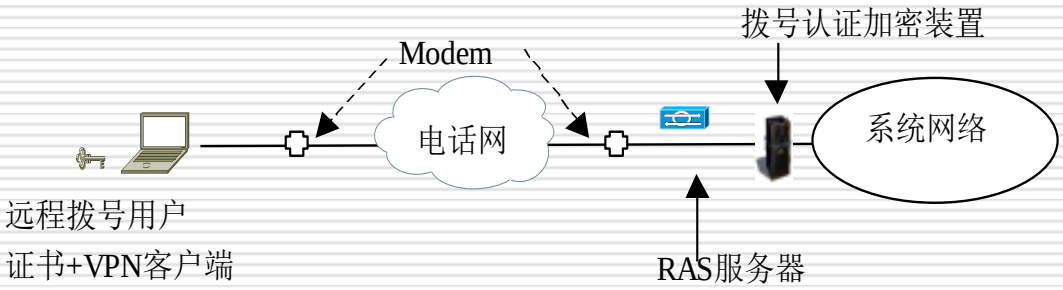
访谈并现场核查拨号服务器和客户端使用经安全加固的操作系统，关闭了不需要的端口和服务，启用登录失败处理功能，设置密码策略，访问控制列表。

访谈并核查数据通信采用数据证书认证方式，服务器与客户端通信过程部署加密认证装置或服务器密码机方式进行加密通信。

示例： 远程拨号访问防护



远程拨号访问防护－链路方式



远程拨号访问防护－网络方式

链路保护措施：

使用专用链路加密设备，实现以下安全功能：

- 两端链路加密设备相互进行认证
- 对链路帧进行加密

网络保护措施：

采用远程访问VPN方式。在RAS与本地网络之间设置拨号认证加密装置，结合用户数字证书，对远程拨入的用户身份进行认证，通过认证后，在远程拨入用户与拨号认证加密装置之间建立IPSecVPN，对网络层数据进行机密性与完整性保护。

相关的安全产品包括：用户端的IPSecVPN客户端插件及相应的加密卡、RAS端的拨号认证加密装置（包括相应的加密设备）。拨号认证加密装置可以是单独的设备，置于RAS与本地网络之间，也可以与RAS集成在一个物理设备中。

安全区域边界—无线使用控制

a）应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

b）应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；

测评实施要点：

现场核查无线通信的用户在登录时是否采用了身份鉴别措施，如账户/口令、生物识别等，通信设备，应通过唯一标识进行识别，如MAC地址、设备串号等；

现场核查用户身份标识是否具有唯一性。

访谈网络安全管理员是否对无线通信过程中是否对用户进行授权；

现场核查无线通信过程中是否对用户进行授权，核查具体权限是否合理，核查未授权的使用是否可以被发现及告警。

安全区域边界—无线使用控制

c）应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

d）对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为

测评实施要点：

访谈网络安全管理员无线通信传输中是否采用加密传输的措施，系统中所采用的无线通信技术类型；

现场核查无线通信传输中部署加密认证设备或加密模块进行加密传输，数据加密处理，保证传输报文的机密性

访谈网络安全管理员工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；

现场核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备，发现未经授权的无线设备及时告警，并可以对试图接入的无线设备进行屏蔽。

安全计算环境--控制设备安全

a）控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制。

测评实施要点：

DCS控制单元、PLC控制器、RTU、过程控制器、测控装置等

（1）访谈设备管理员或安全管理员，控制设备是否具备安全功能；

（2）核查设计文档、说明文档

（3）测试：控制设备在线测试 或 实验室环境测试后现场验证固件版本号

（4）与上位机构成控制系统，验证控制设备

建议：在实验室进行相应控制设备的测评，建立设备测评数据库

安全计算环境--控制设备安全

b）应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作;

测评实施要点：

（1）访谈负责控制设备日常更新的管理员，控制设备是否具备补丁升级、固件升级的条件；是否有关补丁管理相关文档，涉及安全补丁更新的管理和批准、设备供应商补丁升级的获取渠道、补丁测试、按照流程等。

（2）控制设备的漏洞发现可以通过漏洞扫描、关注漏洞发布平台或跟踪官方补丁发布等方式或设备制造商发布的信息，建议形成《补丁管理文档》，增加可用的安全补丁列表，补丁测试等信息。

（3）关注在设备版本、补丁及固件更新前，测试评估更新对系统安全稳定性的影响，如在备用控制设备上进行测试验证或在搭建的测试环境中进行，查看测试验证记录。

（4）查验补丁升级相关的管理文档，若有，查看补丁测试报告、补丁更新批准文档。

安全计算环境--控制设备安全

c）应关闭或拆除控制设备的软盘驱动、光盘驱动、USB接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；

测评实施要点：

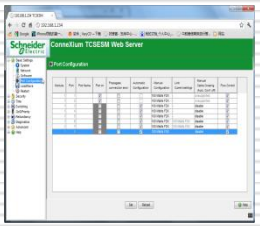
（1）访谈安全管理员或设备管理员
（2）核查控制设备具备哪些硬件接口或驱动，如软盘驱动、光盘驱动、USB接口、串行口或多余网口等，哪些接口或驱动必须保留使用；
（3）确需保留接口或驱动的原因应足够充分，并记录其用途；监控管理措施包括控制设备锁在保护箱并有破坏报警装置，或通过运维监控系统针对接口或驱动的使用情况进行监控报警。

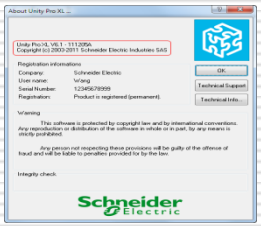
安全计算环境--控制设备安全

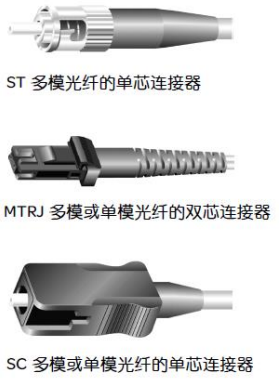
d）应使用专用设备和专用软件对控制设备进行更新；

测评实施要点：

(1)访谈安全管理员或设备管理员，更新控制设备所使用的专用设备和专用软件的品牌型号、软件版本，通常由其上位管理或控制设备中的服务程序实现；
(2)核查专用设备和专用软件的更新记录，确认其正常工作。







安全计算环境--控制设备安全

e) 应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。

测评实施要点：

控制设备固件存在被预置恶意代码程序的可能性；
（1）控制设备上线前应事先在离线环境中进行专项安全性测试与验证，其中，离线环境指的是与生产环境物理隔离的环境，实施安全性检测的机构应为具备国际或国际授权认可，如具有CNAS资质的检测机构；
（2）关注安全检测报告中针对控制设备固件恶意代码的检测部分。

举例

CPU 和 NOE 模板的固件文件

安全建设管理—产品采购和使用

a)工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

测评实施要点：

(1) 核查系统使用的工业控制系统重要设备及网络安全专用产品是否通过专业机构的安全性检测，是否有通过专业机构出具的安全性检测报告；

(2) 核查检测机构是否具有符合国家规定或相关部门规定的要求

如 重要设备可参考国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制订的《网络关键设备和网络安全专用产品目录》。

安全建设管理—外包软件开发

应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容

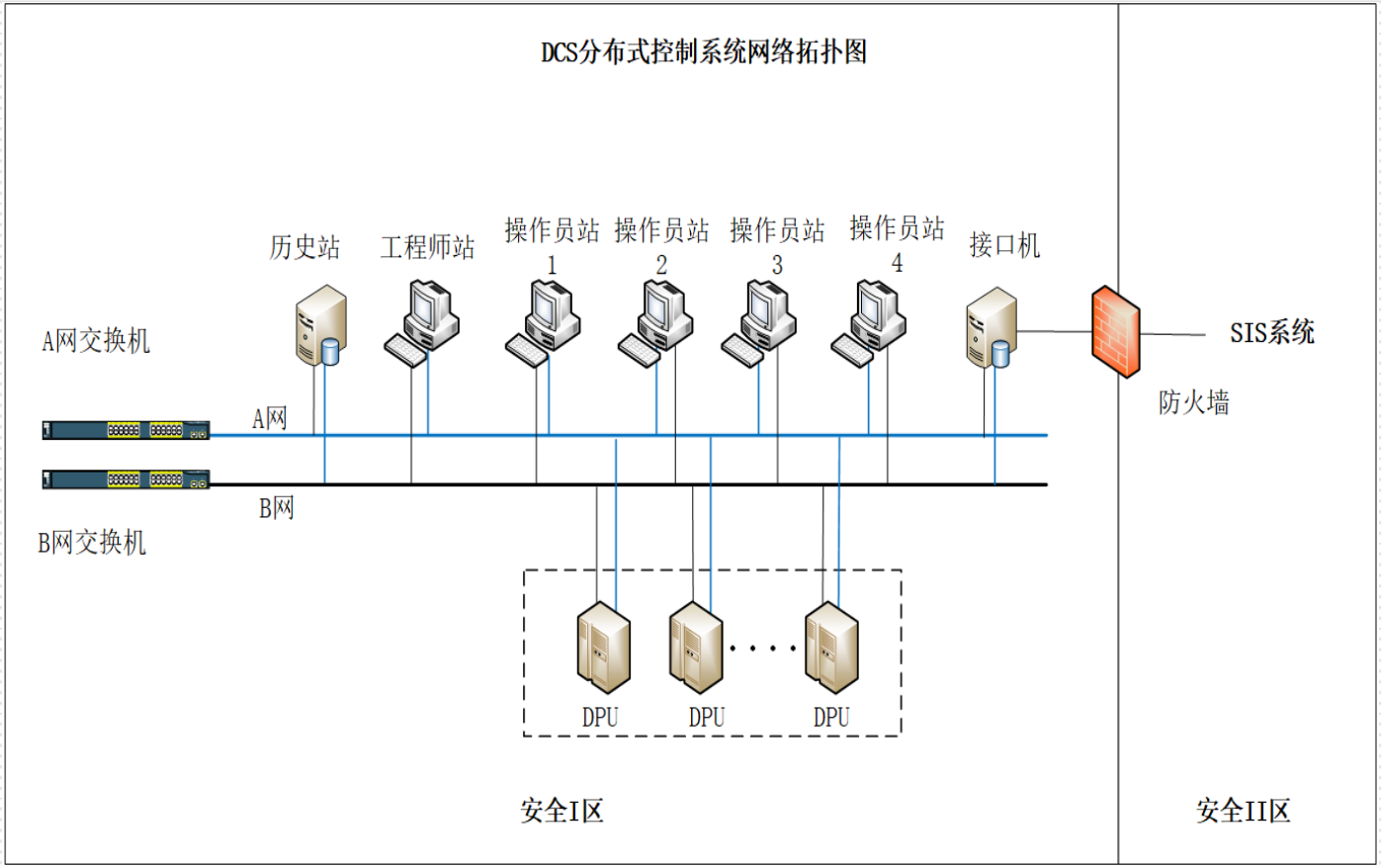
测评实施要点：

核查外包开发合同，合同中是否规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。

典型生产控制系统测评实践

1. 测评对象选择

DCS分布式控制系统为三级系统（S3A3G3）



（1）机房
（2）网络设备
（3）安全设备
（4）服务器、终端
（5）业务应用软件
（6）控制设备
（7）安全相关人员和安全管理文档等

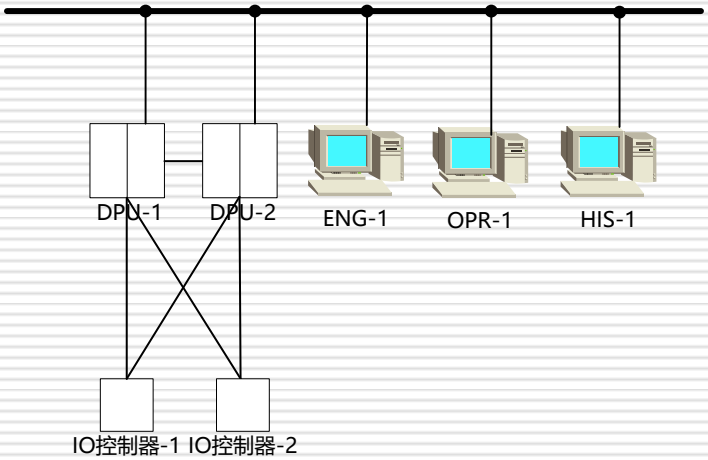
2. 测评指标的选择

- 安全通用要求+工业控制系统安全扩展要求
- 某些要求项不适用于所有测评对象，也可能不适用于特定对象，不适用项需要细分及慎重选择。
- 安全设备种类比较多，不适用项需具体分析

2. 工业控制系统安全扩展要求不适用项讨论

安全类	安全控制点	不适用项	原因说明
安全物理环境	室外控制设备物理防护	a)室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；	无室外控制设备
		b)室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。	无室外控制设备
安全通信网络	通信传输	a)在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。	无广域网进行数据通信
安全区域边界	拨号使用控制	a)工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别和访问控制等措施；	不允许使用拨号访问服务
		b)拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施；	不允许使用拨号访问服务
		c)涉及实时控制和数据传输的工业控制系统禁止使用拨号访问服务。	不允许使用无线通信
	无线使用控制	a)应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；	不允许使用无线通信
		b)应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；	不允许使用无线通信
		c)应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；	不允许使用无线通信
		d)对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。	不允许使用无线通信
安全建设管理	外包软件开发	a)应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。	无外包软件开发

3 现场控制设备的测评方法

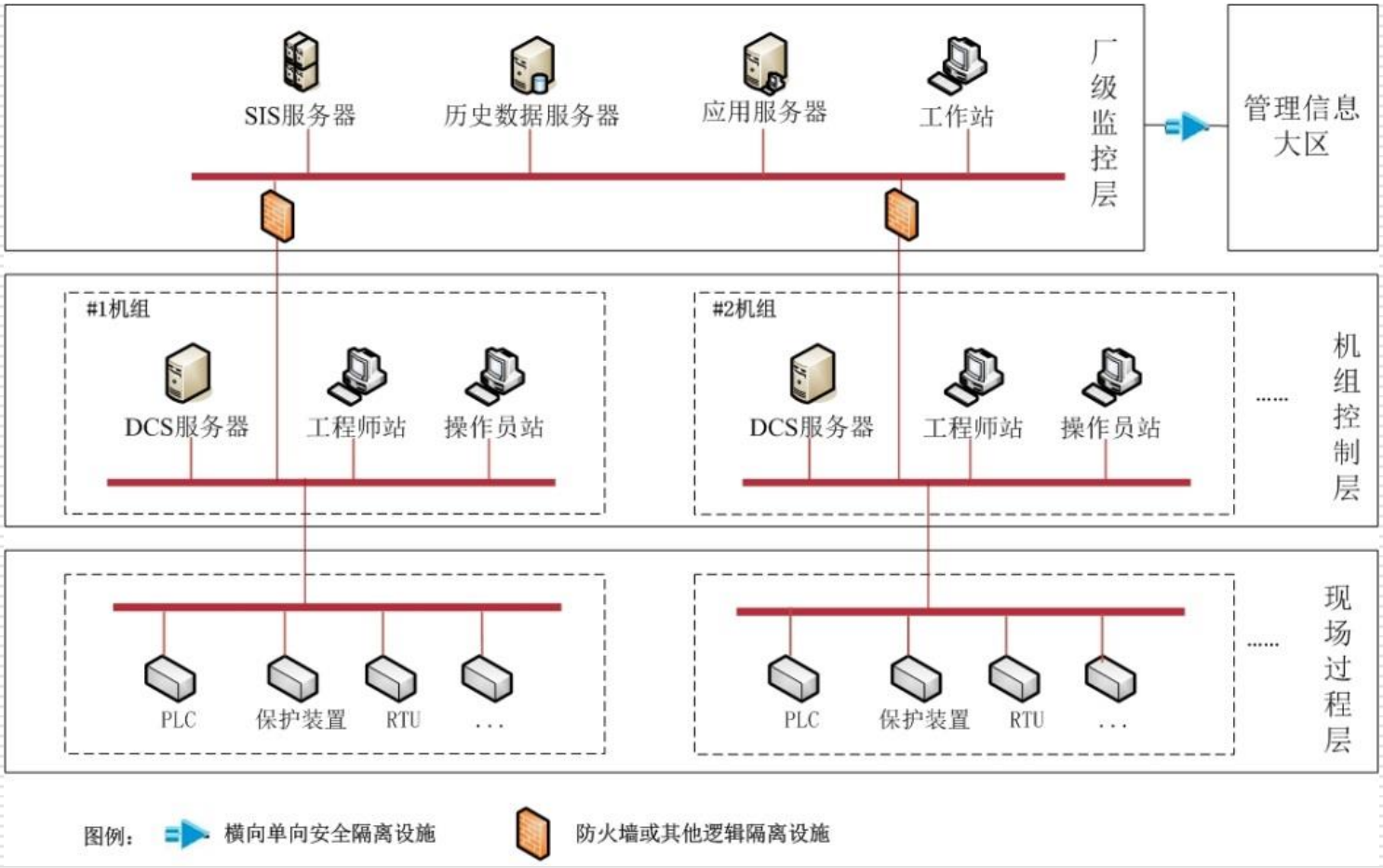


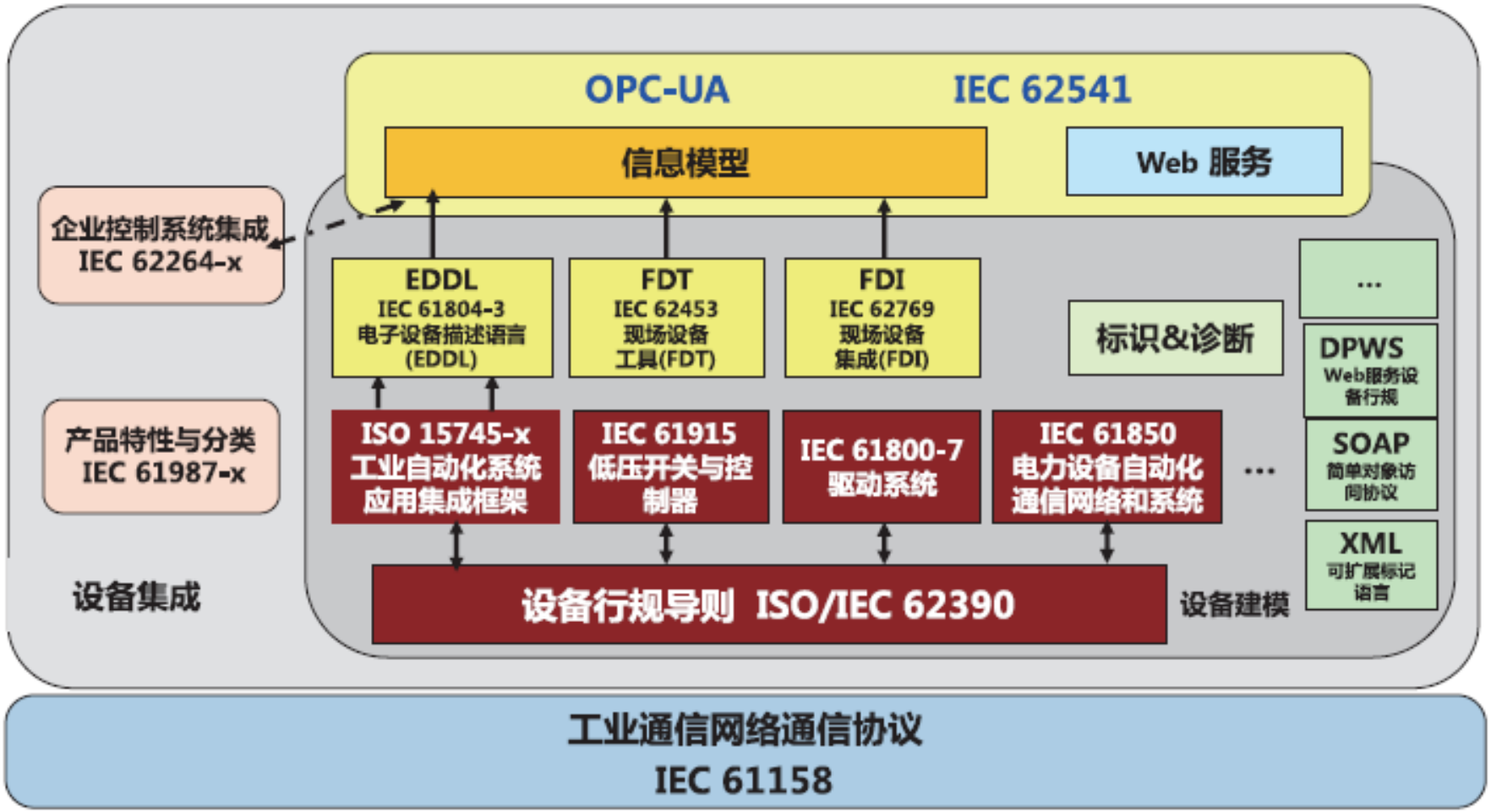
抽样与测试方式

被评估方通过搭建模拟仿真测试环境，在不对现场工业控制系统的正常运行造成影响的基础上进行安全验证工作，评估工业控制系统系统整体安全状况、潜在的安全威胁、可行的技术措施及工具等。

1. 端口探测
2. 特定版本的漏洞
3. 结合上位机的测试
4. 总线协议分析

4 安全区域边界的测评方法




OPC-UA
IEC 62541
信息模型
Web 服务
企业控制系统集成
IEC 62264-x
EDDL
IEC 61804-3
电子设备描述语言
(EDDL)
FDT
IEC 62453
现场设备
工具(FDT)
FDI
IEC 62769
现场设备
集成(FDI)
标识&诊断
...
DPWS
Web服务设备行规
SOAP
简单对象访问协议
XML
可扩展标记语言
产品特性与分类
IEC 61987-x
ISO 15745-x
工业自动化系统
应用集成框架
IEC 61915
低压开关与控制器
IEC 61800-7
驱动系统
IEC 61850
电力设备自动化
通信网络和系统
...
设备集成
设备行规导则 ISO/IEC 62390
设备建模
工业通信网络通信协议
IEC 61158

感谢聆听

刘韧
13601156975