

电厂自动化发展与信息安全防护

许继刚

中国能源建设集团工程研究院

2017年5月11日 北京展览馆

目 录

- 一、发电行业现状
- 二、电厂自动化技术的发展
- 三、电厂信息安全的三道重要防线
- 四、关键控制系统的信息安全防御
- 五、主要信息系统的信息安全防御

一、发电行业现状

一、发电行业现状

1 装机容量

截至到2017年3月底，全国总装机容量达到16.1亿千瓦，其中火电达到10.6亿千瓦，占全部装机容量的65.84%。

百万千瓦大型机组的数量牢牢稳居世界首位。

一、发电行业现状

2 煤耗

2016年全国运行火电机组的平均供电标准煤耗率为
312g/kW·h。

新投产大型机组的煤耗都在300g/kW·h以下。

目前世界上煤耗最低、运行效率最高的机组在中国。

一、发电行业现状

序号	项目	机组容量	机组参数	设计机组热效率 (%)	设计厂用电率 (%)
1	丹麦 Nordjyllandsvaerk et #3机组	1×385MW 超临界	29MPa/ 582° C/582° C/ 82° C	47	6.5
2	日本橘湾电厂1、2号机组	2×1050MW超超临界	25MPa/ 600° C/610° C	44	4.9
3	日本矶子电厂1号机组	600MW 超超临界	25MPa/ 600° C/600° C/	44	5.4
4	日本 Hitachinaka(常陆那珂)电厂	1×1000MW超超临界	24.5MPa/ 600° C/600° C/	45.1	5
5	德国 Niederaussem 电厂	1×1027MW超超临界	29MPa/ 580° C/600° C/	45.2	实际供电煤耗 292g/kWh

一、发电行业现状

国内部分超超临界机组技术指标汇总表

序号	项目	机组容量	机组参数	设计机组热效率 (%)	设计发电煤耗 (g/kWh)	设计厂用电率 (%)	2012年厂用电率 (%)	2012年供电煤耗 (g/kWh)
1	华能玉环电厂一、二期	4×1000MW 超超临界	26.25MPa/ 600℃/ 600℃	45	272	6.5	4.17-4.38 (不含脱硝)	285.08-289.19
2	华电邹县电厂四期#7、8机组	2×1000MW 超超临界	25MPa/ 600℃/ 600℃	45.46	272.9	5.34	4.26-4.37 (不含脱硝)	285.71-286.11
3	外高桥第三电厂	2×1000MW 超超临界	27MPa/ 600℃/ 600℃	45.58	269.9	5.5	3.8	275.85-276.44
4	华能威海电厂三期#5、#6机组	2×680MW 超超临界	25MPa/ 600℃/ 600℃	44.8	274	5.6	3.75-4.1	289.97-291.71

二、电厂自动化技术的发展

二、电厂自动化技术的发展

1 采用多机一控的控制方式是技术发展的必然趋势

- × 传统的机组控制方式

 - 单元机组一机一控

 - 单元机组两机一控

- × 多机一控的发展

- × 多机一控的典型实例

 - 国华宁海电厂4X600MW

 - 华能玉环电厂4X1000MW

- × 多机一控的优势

二、电厂自动化技术的发展

2 辅助系统的高度集中化控制已愈来愈成熟

× 煤、灰、水三个独立集中点

如典型项目：2000年示范项目益阳电厂

煤控制点：输煤、燃油、煤水处理

灰控制点：除灰、除渣、除尘等

水控制点：补给水处理、凝结水处理等

× 煤、灰、水三个独立集中点，预留集中监控的可能

× 煤、灰、水三个辅助点加主控室集中点

× 煤独立集中点，灰、水在主控室集中

× 煤、灰、水全部在主控室集中

二、电厂自动化技术的发展

3 空冷控制系统纳入单元机组DCS已具备条件

- × 空冷控制系统与空冷工艺系统的关系

 - 方案一：空冷控制系统随空冷工艺系统统一供货

 - 方案二：空冷控制系统单独采购

- × 空冷控制系统与DCS的关系

 - 方案一：独立控制系统分别与DCS通讯

 - 方案二：直接纳入DCS

- × 需设计注意的问题

二、电厂自动化技术的发展

4 采用脱硫分散控制系统是目前脱硫设计的主流

× 脱硫控制方式

方案一：独立脱硫控制室

方案二：脱硫与灰渣合并控制室

方案三：脱硫与输煤等其它系统合并控制室

方案四：先在就地过渡，然后引入机组主控室

方案五：脱硫在机组主控室控制

二、电厂自动化技术的发展

5 脱硝系统宜由单元机组值班人员统一监控

- × 脱硝控制方式

- × 脱硝控制系统与DCS的关系

方案一：独立控制系统分别与DCS通讯

方案二：直接纳入DCS

- × 设计需注意的问题

脱硝区域的闭路电视监视系统

脱硝系统的液氨泄漏检测

改造项目与DCS的配合

二、电厂自动化技术的发展

6 基于现场总线的分散控制系统已开始规模化应用

✘ 目前较大范围应用FCS并已投入运行的电厂主要有：

华能金陵电厂二期 $2 \times 100\text{MW}$ 机组工程、

华能九台电厂 $2 \times 600\text{MW}$ 机组工程、

华能秦岭电厂 $1 \times 600\text{MW}$ 机组工程、

国电肇庆热电公司 $2 \times 350\text{MW}$ 机组工程等。

二、电厂自动化技术的发展

7 机组自启停系统愈来愈受到关注

- 德国Altbach HKW1 1x(465MWeI+280MWth) Altbach电厂, 1985投运
- 德国RDK Block 7 1x(550MWeI+220MWth) Karlsruhe电厂1985 投运
- 澳大利亚Stanwell 4x350MW Queensland电厂, 1994投运
- 澳大利亚Callide C 2x450 MW Biloela电厂, 2001投运
- 德国Wilhelmshafen 1x756 MW Wilhelmshafen电厂, 2002投运
- 德国BOA1 Niederaussem 1x1012MW Bergheim电厂, 2003投运
- 澳大利亚Muja Stage C&D 2x200MW+2x227MW Perth电厂, 2009投运等等

二、电厂自动化技术的发展

7 机组自启停系统愈来愈受到关注

- × 国内成套引进的机组如华能福州电厂、华能大连电厂、阳城第一发电厂、上海石洞口二电厂、华能山东日照电厂、山西河津电厂一期、宝钢电厂、上海外高桥电厂、广东珠海电厂等均设计了此功能，且发挥了较好作用。
- × 上海外高桥2X900MW机组、华能玉环电厂4X1000MW机组、国电江苏泰州电厂2X1000MW机组、国电双鸭山电厂2X600MW机组、阳城一厂二期工程2X600MW机组、华能鹤岗三期2X900MW机组、浙江国华宁海2X1000MW机组、国华台山2 X600MW机组、国华黄骅2X600MW机组、华润常熟3X600M机组、山东黄岛2 X600MW、华能海门电厂2x1000MW超超临界等

二、电厂自动化技术的发展

7 机组自启停系统愈来愈受到关注

× 国电泰州电厂二期2x1000MW二次再热机组设置的断点:

- 1、启动准备
- 2、上水准备
- 3、上水清洗
- 4、点火升温
- 5、汽机冲转
- 6、自动并网
- 7、升负荷1
- 8、升负荷2

二、电厂自动化技术的发展

7 机组自启停系统愈来愈受到关注

× 国电泰州电厂二期2x1000MW二次再热机组设置的断点:

- 1、降负荷断点A
- 2、降负荷断点B
- 3、机组解列



二、电厂自动化技术的发展

8 安全相关系统逐步得到规范

✘ 国标《大中型火力发电厂设计规范》 15.6.2 条：

发电厂锅炉和汽轮机的跳闸保护系统，可采用电子逻辑系统或继电器硬逻辑系统，系统宜采用经认证的、SIL3级及以上的安全相关系统。安全相关系统应符合《电气/电子/可编程电子安全相关系统的功能安全》GB/T20438和《过程工业领域安全仪表系统的功能安全》GB/T21109.

二、电厂自动化技术的发展

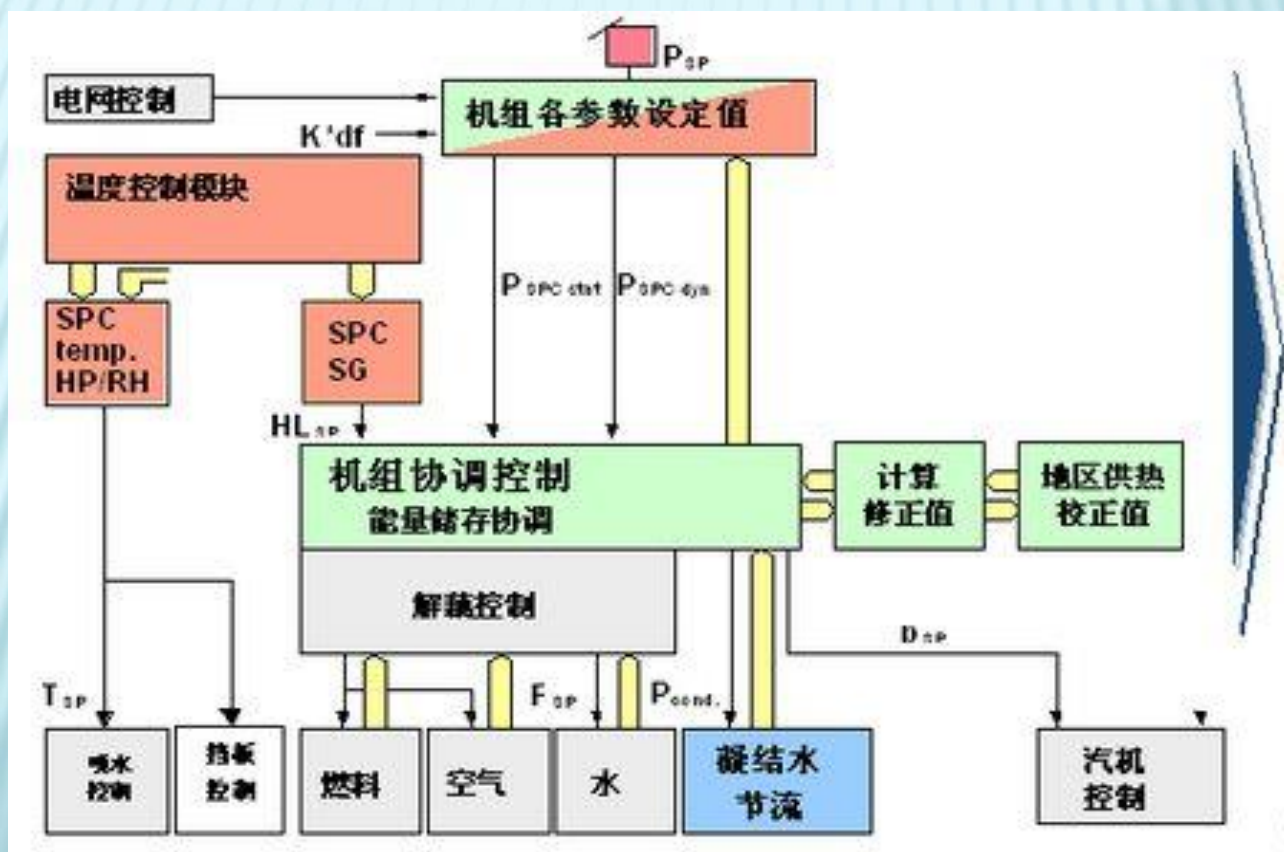
9 优化控制软件是节能减排的有效手段

- 西屋Smart Process™优化控制软件
- 西门子电站优化软件Profi
- Honeywell优化软件UES-SIS
- ABB公司的Optimax软件包
- GE公司的NtelliMax

二、电厂自动化技术的发展

9 优化控制软件是节能减排的有效手段

西门子优化控制软件PROFI在国华宁海电厂的应用



二、电厂自动化技术的发展

9 优化控制软件是节能减排的有效手段

- 华中科技大学的优化控制系统
- 华北电力大学的优化控制系统
- 华北电科院的优化控制系统
- 浙江电科院的TOP系统
- 云南电科院的厂网协调优化系统
- 神华国华研究院的优化控制系统

二、电厂自动化技术的发展

10 无线控制技术已开始发挥作用

- × 英国E. ON发电厂，装机容量为1940 MW，采用了艾默生公司的智能无线技术对水处理流量进行监视和测量。
- × 美国宾夕法尼亚州PPL发电厂，采用了智能无线技术测量锅炉给水泵系统的压力、温度、油位等相关信号。
- × 美国Nebraska电站采用无线技术用于监视远方的油罐工况。
- × 美国LCRA下属的SGPP（3X650MW机组）电厂和LPPP（545MW燃气蒸汽联合循环机组）电厂采用无线控制系统实现两厂异地的数据共享和通信管理等。

二、电厂自动化技术的发展

10 无线控制技术已开始发挥作用

- × 张家口发电厂全厂共有 $8 \times 300\text{MW}$ 机组，其水源地共有26口深井，在水源地每个井位布置1台远方遥控箱，实现无线远方控制。
- × 广东茂名电厂200MW机组的叶轮给煤机，采用进口无线遥控系统。
- × 华能上海石洞口第一发电厂2008年对除灰系统进行无线控制技术改造，包括四台锅炉的气力输灰、灰库、灰浆系统。

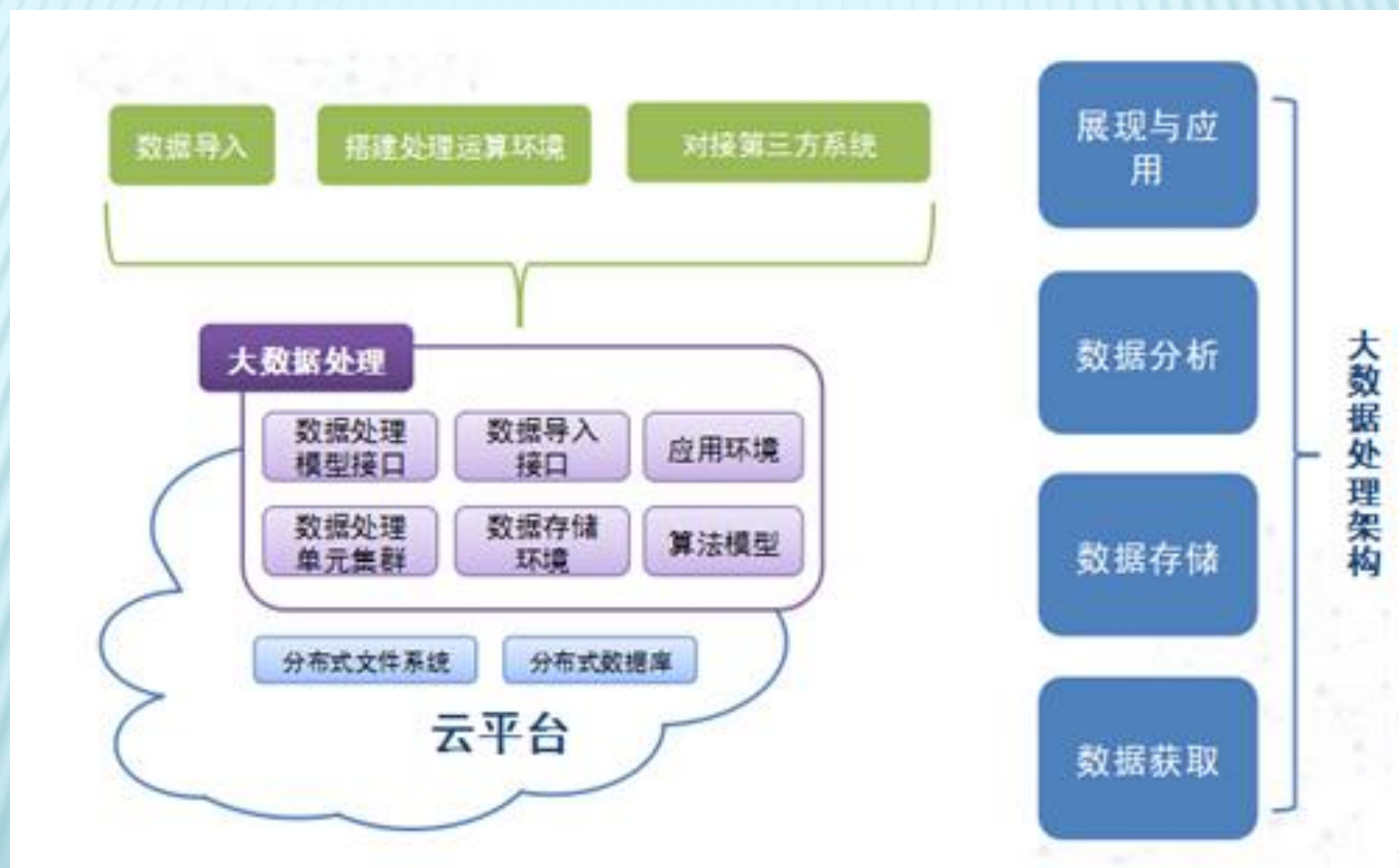
二、电厂自动化技术的发展

11 大数据已在发电集团公司发力

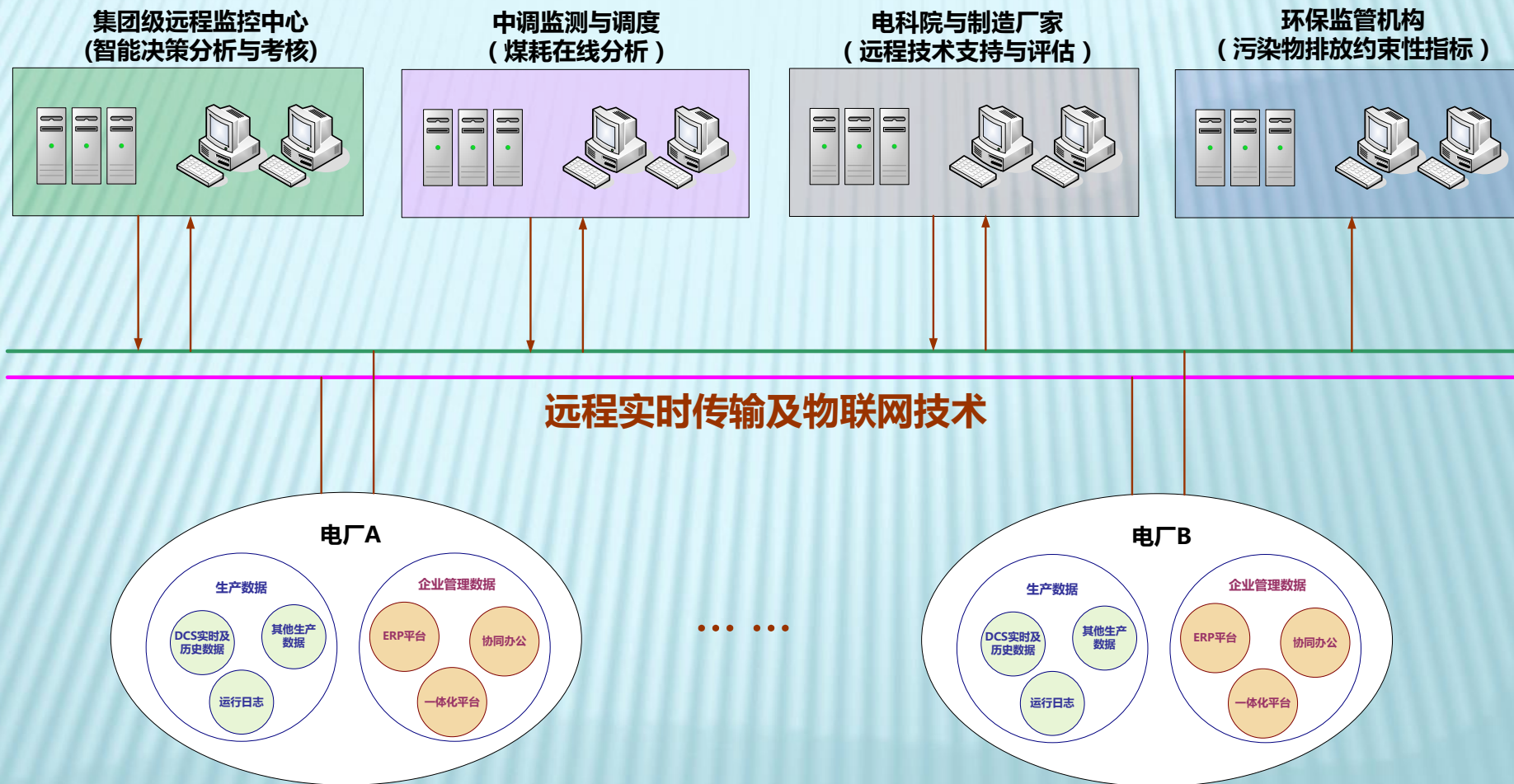
运用大数据和云计算深度挖掘机组和设备运行数据，提高机组和设备的运行维护水平。

- × 国华电力“一横一纵三层次”设备数据库平台已初步形成规模，2016年又科研立项“利用大数据开发电厂知识库”。
- × 粤电集团委托广东省电科院对全集团机组进行数据分析和诊断。
- × 国电2016年科技项目立项“集团大数据平台开发”，计划最终囊括200多台机组数据。

三、电厂自动化技术的发展



二、电厂自动化技术的发展



二、电厂自动化技术的发展

12 智能诊断和维护技术向三维可视化发展

利用三维可视化模型，在三维空间中准确定位工艺和设备，标注相关参数，为准确查找故障，提高机组运行水平奠定基础。

- ✘ 京能高安屯数字化电厂项目是目前国内数字化电厂建设最先进的电厂。已经成功开发了三维可视化施工模型，三维可视化模拟培训系统等，下一步将开发三维可视化设备诊断和维护系统。

二、电厂自动化技术的发展

13 移动和远程监控技术已开始应用

将手机等移动设备和电厂有关自动化系统进行联接，在保证运行安全的前提下，提高机组运行和维护的灵活便捷性。通过手机等移动监控机组运行状态并发布控制命令。

- ✘ 浙能温州电厂2014年就将移动设备成功应用于电厂设备维护。
- ✘ 神华集团2016年科研立项，将移动设备应用于发电机组远程监控。

二、电厂自动化技术的发展

14 视频监控技术向智能化迈进

将视频监控系统、门禁管理系统、火灾探测与报警系统等进行联网升级，形成全厂范围内的动态全息可视化监视系统，通过大屏幕实时监视全厂各个方位、各个设备以及有关进入人员的状况，无论是设备发生状况，还是人员发生状况，都能快速跟踪与定位，为处理紧急状况提供手段。

- ✘ 故宫博物院：2012年5月08日，故宫文物被盗震惊世界。目前，65面大屏幕，1500个摄像头，4000个火灾探测器，近万个安防报警器。形成三维全息安防系统。

三、电厂自动化技术的发展



三、电厂自动化技术的发展



二、电厂自动化技术的发展

15 无人机技术将在电厂找到用武之地
利用无人机进行巡检。

- ✘ 电网已经开始使用无人机进行巡检，应用于跨江线路、特高压输电线路等。
- ✘ 神华国能集团2016年科研立项，准备开发风电场巡检用无人机。

三、电厂自动化技术的发展



三、电厂自动化技术的发展



二、电厂自动化技术的发展



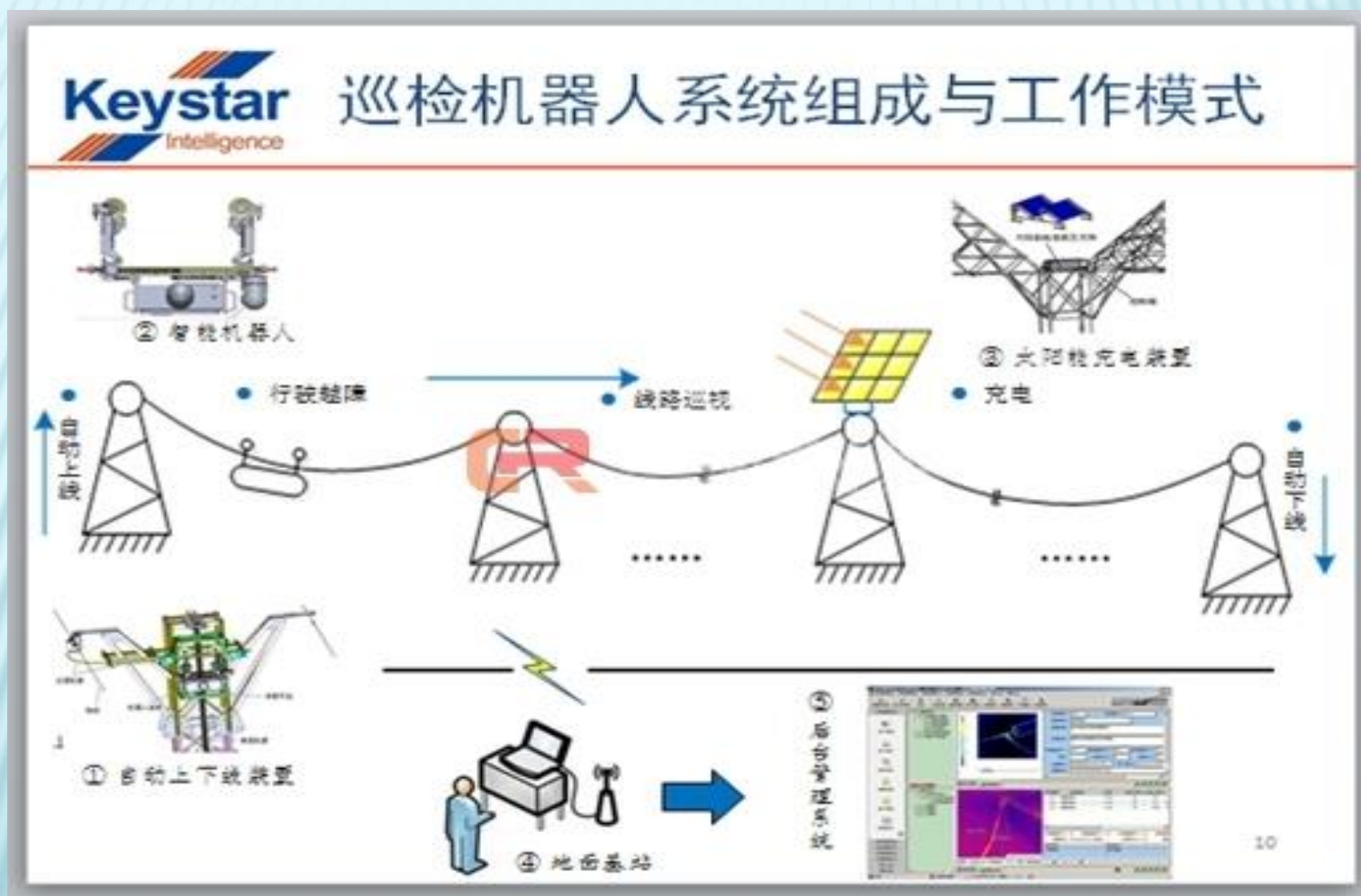
二、电厂自动化技术的发展

16 机器人已登上电厂舞台

利用机器人进行维护、检修以及危险场所的紧急操作。

- × 电网输电线路已开始使用机器人进行巡检。
- × 变电站已开始使用机器人进行巡检，可以应用到电厂升压站。
- × 目前已成功开发出凝汽器在线清洗机器人。
- × 目前已成功开发出管道巡检机器人、电缆隧道巡检机器人。

三、电厂自动化技术的发展



二、电厂自动化技术的发展



二、电厂自动化技术的发展



二、电厂自动化技术的发展



二、电厂自动化技术的发展

17 智能测量技术的应用范围不断扩伸

采用各种先进和智能化的测量手段对煤质、炉膛燃烧、烟气成分等进行测量，促进节能减排。



二、电厂自动化技术的发展

智能测量技术

煤质在线
测量技术

- ④ 脉冲中子源煤质在线分析；
- ④ 基于LIBS技术的煤质在线分析；
- ④ 同位素中子源煤质分析。

炉膛温度
场测量
技术

- ④ CCD三维可视化技术
- ④ 超声波测量技术
- ④ 激光等离子体温度测量

先进传感技术

烟气测量
技术

- ④ 智能烟气在线分析仪
- ④ 基于信息融合的软测量技术
- ④ 基于LIBS技术的烟气测量技术

二、电厂自动化技术的发展

18 VR技术开始融入电厂仿真

- × 在线仿真技术

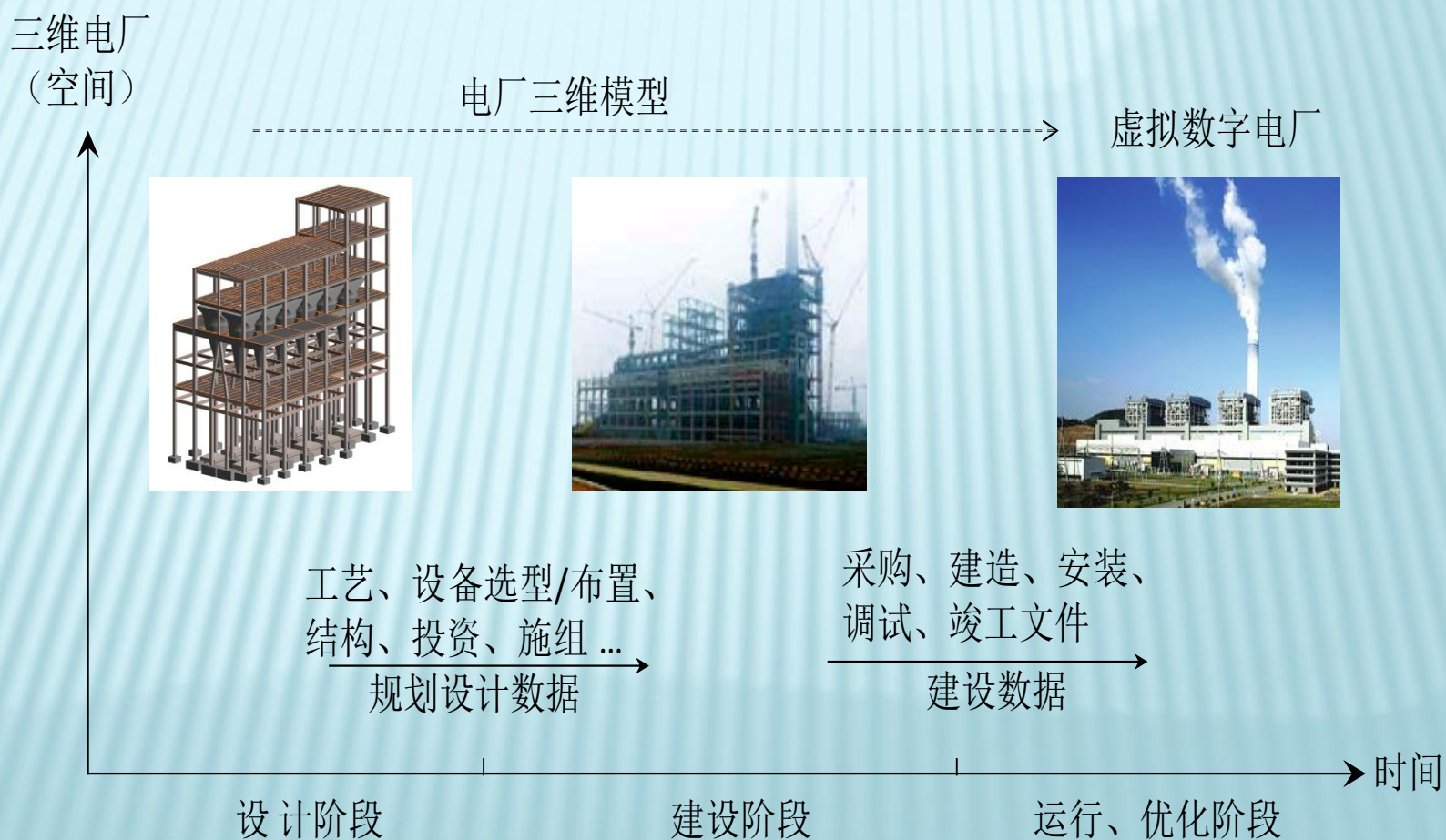
大唐托克托电厂已开发高精度在线仿真系统。

- × 三维VR仿真技术

京能高安屯电厂已开发出三维模拟仿真系统，并已经应用VR技术。

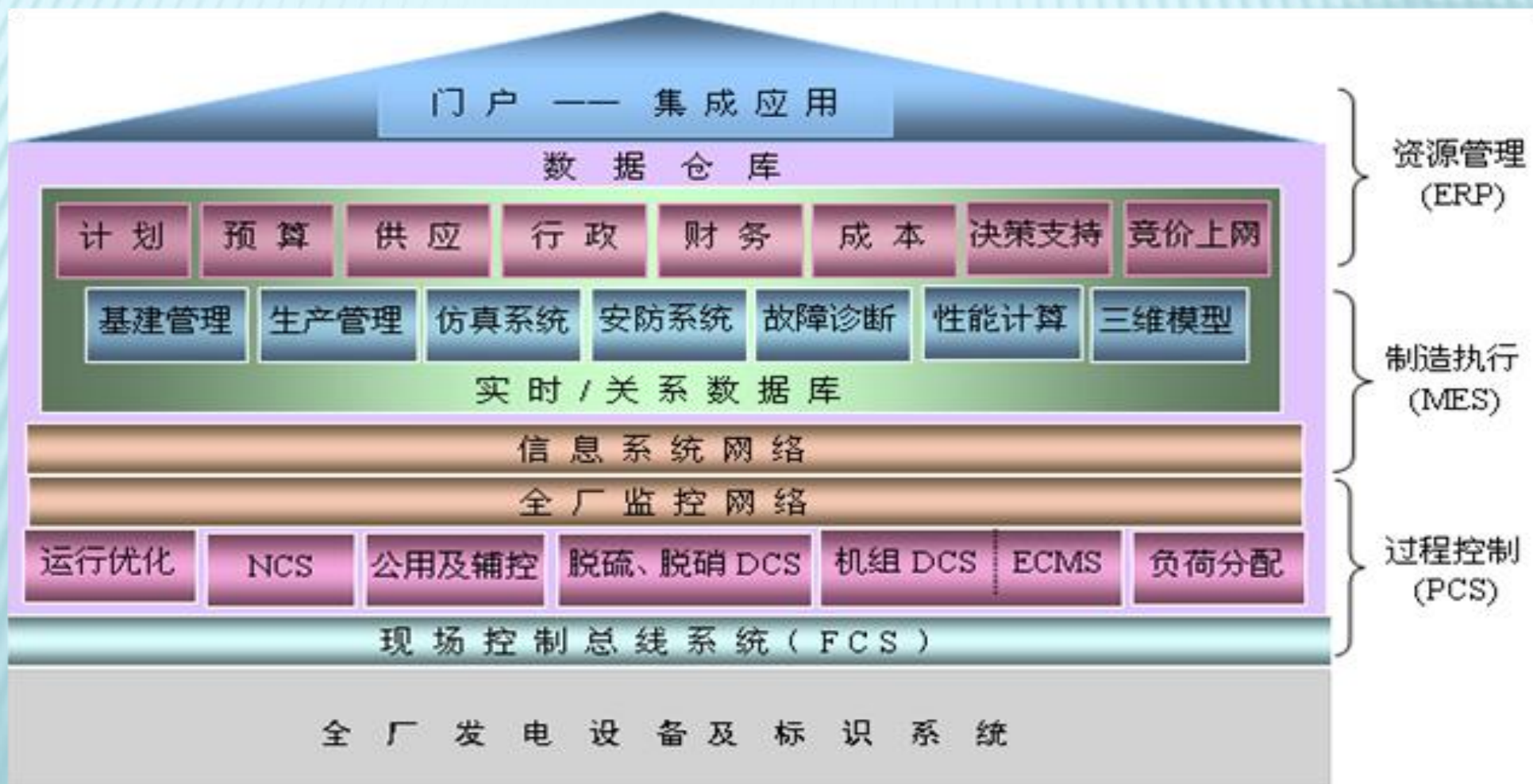
二、电厂自动化技术的发展

19 智能电厂是当前发展的目标



二、电厂自动化技术的发展

19 智能电厂是当前发展的目标



二、电厂自动化技术的发展

智能电厂与智慧电厂

电厂智能化是电厂信息化过程中，在基本达到数字化基础上，采用模糊控制、神经网络、专家系统、遗传算法、自组织控制、自学习控制以及数据挖掘等智能控制和智能分析技术对信息进行处理和加工（算法高度智能，数据深度挖掘），并尽可能在最大范围内代替人实现闭环反馈输出，达到高度自动化，使电厂处于安全、经济和环保等方面综合最优的状态。

二、电厂自动化技术的发展

智慧是一种拟人化的具有自我感知和判断能力的高级生物特征。智慧让人可以深刻地理解人、事、物、社会、宇宙、现状、过去、将来，拥有思考、分析、探求真理的能力。

智慧电厂是在自动化电厂、信息化电厂、数字化电厂、智能化电厂基础上更聪明、并具有自我感知和判断能力的电厂。

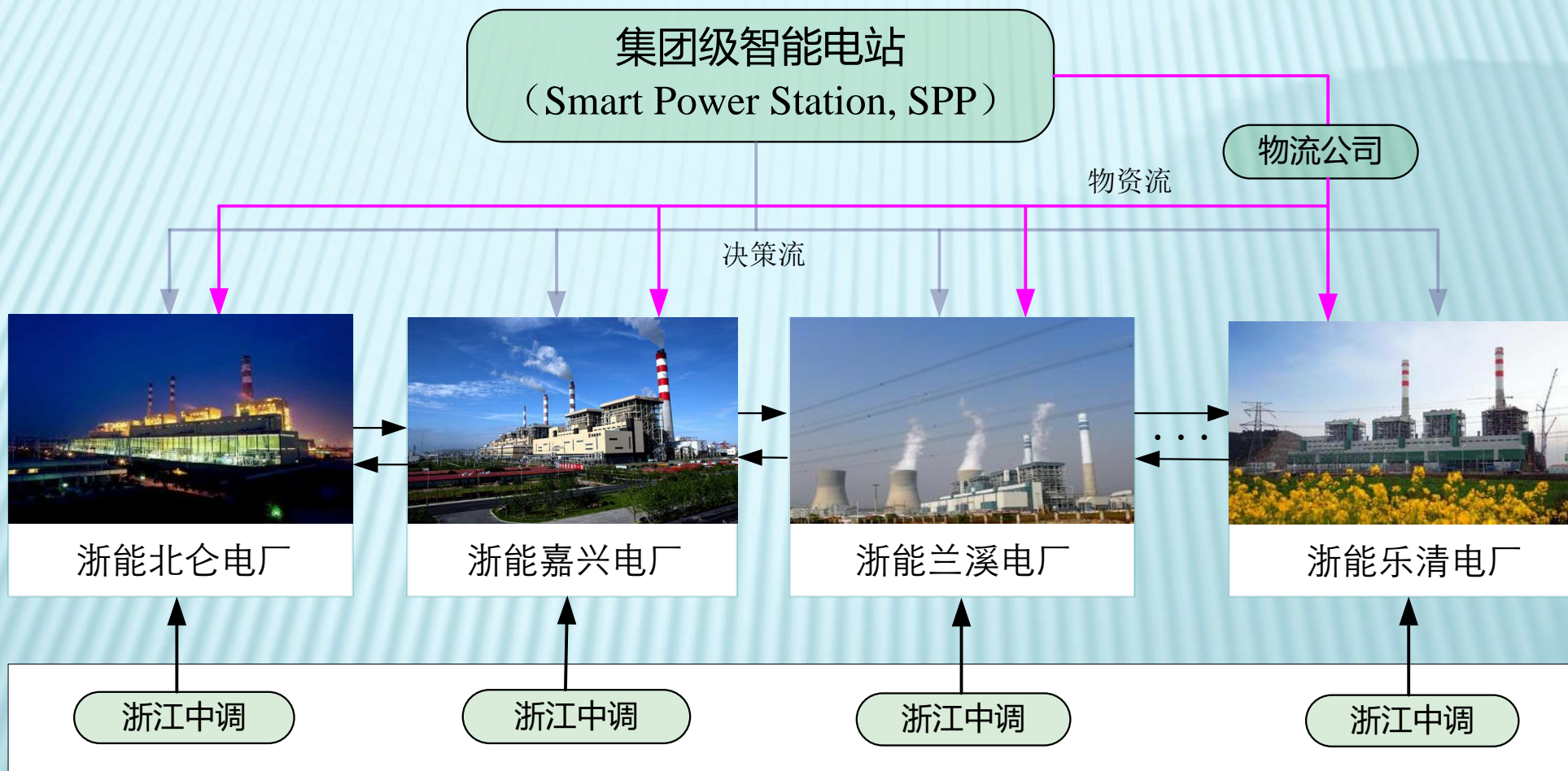


二、电厂自动化技术的发展

20 无人值守与集团控制中心将会出现

- × 澳洲电力Station F超临界电厂，单按钮实现温态、热态启动至满负荷。AGC全自动范围：30%--110%超负荷。操作和维护人员携带口袋式呼叫报警装置，实现无人值守运行方式。

二、电厂自动化技术的发展



二、电厂自动化技术的发展

目标：智慧电厂、智慧电网、智慧城市有机融合，实现中国梦！



三、电厂信息安全的三道重要防线

三、电厂信息安全的三道重要防线

电厂自动化系统的两个层次：

- × **第一个层次是控制系统**，所有直接参与生产过程测量与控制的自动化系统均划归该层次，包括机组分散控制系统（DCS）、汽机数字电液控制系统（DEH）、辅助车间控制系统等。
- × **第二个层次是信息系统**，将电厂与信息有关的，不直接参与过程控制的自动化系统均归到信息系统，包括管理信息系统（MIS）、厂级监控信息系统(SIS)、视频监视系统、视频会议系统、门禁管理系统等。

三、电厂信息安全的三道重要防线

按照两个大区进行安全分区：

- × 第一个层次的所有系统都化归为生产控制大区，
- × 第二个层次的所有系统都化归为管理信息大区。

三、电厂信息安全的三道重要防线

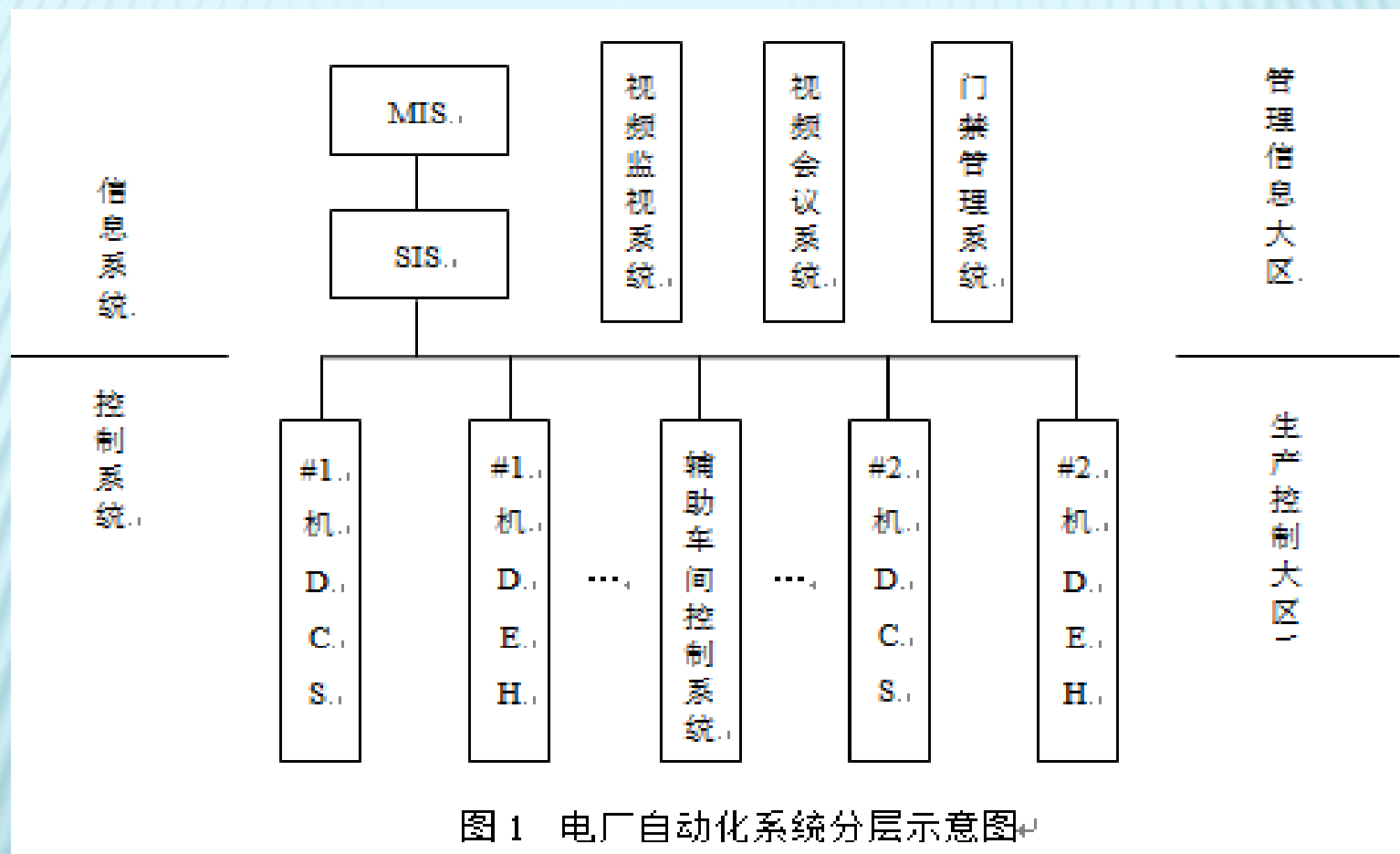


图 1 电厂自动化系统分层示意图

三、电厂信息安全的三道重要防线

- ✘ 我国将计算机信息系统的安全等级化分为五个等级：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级，安全保护能力从第一级到第五级逐级增强。
- ✘ 电厂第一个层次的所有系统都是第五级，也就是访问验证保护级。
- ✘ 电厂第二个层次系统中，SIS、视频监视系统和门禁管理系统与生产运行的关系较为密切，可以化归为第四级，MIS、视频会议系统与生产运行不直接发生关系，则可以化归为第三级。

三、电厂信息安全的三道重要防线

电厂信息安全的防范重点是设置好三道重要防线。

- × **第一道安全防线**：电厂信息系统与外部系统的安全防线，也就是管理信息大区内系统与外部联系的防线。
- × **第二道安全防线**：电厂控制系统与产品供货商的安全防线，也就是生产控制大区内系统与各自供货商的防线。
- × **第三道安全防线**：电厂控制系统与电厂信息系统的安全防线，也就是生产控制大区内系统与管理信息大区内系统的防线。

四、关键控制系统的信息安全防御

四、关键控制系统的信息安全防御

1 DCS的安全防御重点

- ✘ 电厂机组普遍采用DCS。DCS是电厂覆盖工艺系统最多，控制面最广的控制系统。DCS直接参与生产过程控制，是电厂安全运行的基本保障。
- ✘ 对于DCS来说，信息安全的防御点主要在三个方面，一是DCS与供货厂商之间的安全防御，二是DCS与其他系统之间的安全防御，三是DCS人机交互的安全防御。

四、关键控制系统的信息安全防御

1.1 DCS与供货厂商之间的安全防御

- × 首先讨论DCS与供货厂商之间的安全防御。随着计算机技术、网络技术、通讯技术的迅猛发展，DCS厂商可以轻而易举地获取由其提供DCS的所有数据，也可以采取一定的手段对其所供DCS进行远程控制，存在不可避免的安全隐患。尤其是目前一些百万千瓦机组的DCS多采用国外进口产品，其中隐含的安全问题不容忽视。该安全不仅仅涉及电厂本身，一旦遇到战争等国际社会动荡，还会危及地区和国家的安全。妥善处理并杜绝电厂DCS与产品供货商之间的信息安全隐患，是当前容易忽视的问题，需要提醒电厂建设方和设计方高度重视。

四、关键控制系统的信息安全防御

1.2 DCS与其他系统之间的安全防御

- × 其次讨论DCS与其他系统之间的安全防御。DCS是机组的主要控制系统，但并不是覆盖全部机组工艺的系统。比如DEH、旁路控制系统（BPS）、汽机危机遮断系统（ETS）等。如果这些控制系统未能纳入DCS，则与DCS之间就有数据接口，但由于这些系统和DCS一样处于同一个安全大区，来往数据已经严格过滤，因此无需特别防御。

四、关键控制系统的信息安全防御

1.2 DCS与其他系统之间的安全防御

需要特别防御的是DCS与SIS之间的信息传输。DCS与SIS之间有大量的数据交换信息。目前的设计方案是，SIS与DCS之间应配置数据单向传输的专用隔离装置，严禁SIS向DCS发送除采集数据所需通讯协议以外的任何信息。DCS的数据可以上传至SIS,但SIS的数据不能直接下传到DCS。

四、关键控制系统的信息安全防御

1.2 DCS与其他系统之间的安全防御

对于SIS需要完成负荷分配控制功能的电厂而言，必须满足一定的前提条件并采取特别的设计方案。

前提条件是：电网调度必须是调厂而不是直接调机组。

设计方案是：此时的负荷控制命令应当由值长判断决定后才能发送到DCS,而且必须由值班操作员确认后才能执行。负荷控制命令宜通过硬接线方式下达。

四、关键控制系统的信息安全防御

1.2 DCS与其他系统之间的安全防御

目前有的项目开始设置厂级DCS或其他厂级控制系统。如果设置了厂级控制系统，则机组DCS就不会直接与厂级信息系统发生数据联系，需要设置专用隔离装置的防御点上移到了厂级控制系统。

四、关键控制系统的信息安全防御

1.3 DCS人机交互的安全防御

DCS人机交互设备主要有操作员站和工程师站，在个别没有设置SIS的项目中还设置了值长站。

- ✘ 值长站可以通过显示器进行监视，但不能操作。操作员站可以通过显示器监视并按设定的程序进行操作，但不能对系统进行任意修改和组态。值长站和操作员站没有对外的数据接口，不需要特别防御。
- ✘ 工程师站是对DCS进行维护并可以修改组态的装置，也是外部入侵DCS的可能关口。对于工程师站来说，防御的主要措施，一方面是制定好电厂的管理机制，另外就是要设计好系统身份识别、访问控制机制和密码安全机制等。

四、关键控制系统的信息安全防御

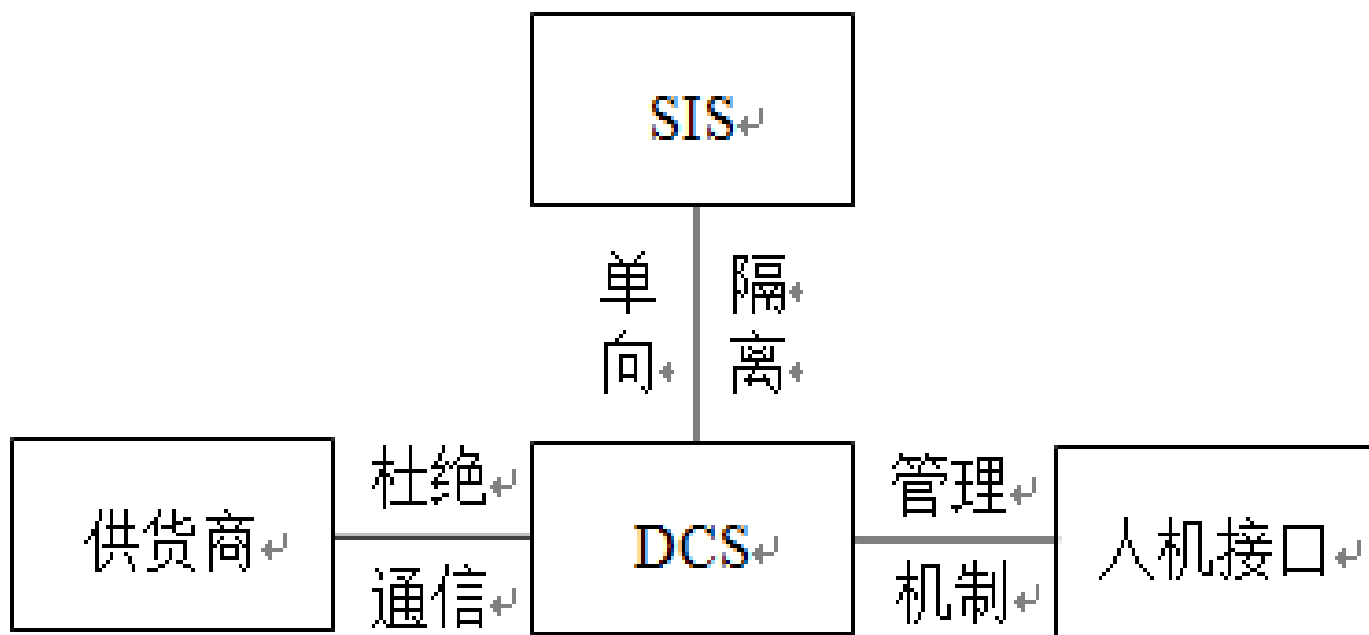


图 2 DCS 安全防御重点示意图

四、关键控制系统的信息安全防御

2 DEH的安全防御重点

- × DEH是电厂机组控制系统中和DCS一样重要的系统，而且在大多数项目中，DEH已经和DCS融为一体。对于DEH已经纳入DCS的系统，其安全防御由DCS统筹，无须特别设计。
- × 对于DEH独立设置的系统，其安全防御重点和DCS一样，也分三个方面：一是DEH与供货厂商之间的安全防御，二是DEH与其他系统之间的安全防御，三是DEH人机交互的安全防御。
- × 和DCS有所区别的是，DEH不会接受SIS的任何指令，SIS的负荷分配控制指令通过DCS对DEH进行控制。

四、关键控制系统的信息安全防御

3 其他机组控制系统的安全防御重点

- ✘ 除了DCS和DEH外，电厂机组还有其他一些主要的控制系统，比如旁路控制系统（BPS）、汽机危机遮断系统（ETS）和锅炉炉膛安全监控系统(FSSS)。

四、关键控制系统的信息安全防御

3.1 其他机组控制系统的安全防御重点 BPS

- ✘ 目前绝大多数BPS已经纳入DCS，对于已经纳入DCS的系统，不需要特别考虑安全防御措施。
- ✘ 对于少数独立设置的BPS来说，需重点考虑的问题只有一个，就是切断BPS与供货商之间的信息联络。和BPS发生信号联系的都是DCS、DEH等控制系统，BPS不直接与SIS等信息系统发生联系，所以只需要设置常规的逻辑隔离，无须采取特别防御。由于BPS不设置独立的操作员站、工程师站等人机接口设备，因此也不存在人机交互的安全防御问题。

四、关键控制系统的信息安全防御

3.2 其他机组控制系统的安全防御重点 ETS FSSS

- × ETS和FSSS是电厂核心保护系统。FSSS目前基本上都纳入DCS，由DCS统一进行防护。ETS除与DCS和DEH有信号联系外，基本不与外界发生信号联系，需要防护的主要是防止ETS与供货商之间的信息联络，像所有其他控制系统一样，切断有可能的远程控制，防止电厂被攻陷。

四、关键控制系统的信息安全防御

4 辅助车间控制系统的安全防御重点

- ✘ 电厂至少有十几个辅助车间，早期的辅助车间控制系统是各自独立的，目前正在设计和运行的发电厂，集中度较低的基本上只有三个集中控制网络，即煤、灰、水集中控制网络。集中度高的，全厂辅助车间统一为一个辅助车间集中控制网络。
- ✘ 下面以全厂设置一个辅助车间集中控制网络为例进行讨论。虽然辅助车间控制系统没有前面讨论的机组控制系统那么重要，但是仍然处在第一个层次，即生产控制大区。辅助车间集中控制网络的安全防御重点和DCS一样，也分三个方面：一是辅助车间集中控制网络与供货厂商之间的安全防御，二是辅助车间集中控制网络与其他系统之间的安全防御，三是辅助车间集中控制网络人机交互的安全防御。

四、关键控制系统的信息安全防御

4 辅助车间控制系统的安全防御重点

和DCS有所区别的是，辅助车间集中控制网络不会接受SIS的任何指令，辅助车间的运行根据机组的运行需要确定。

五、主要信息系统的信息安全防御

五、主要信息系统的信息安全防御

1 SIS的安全防御重点

SIS是电厂的运行数据中心，处于电厂所有自动化系统的中心位置，它主要的部件是实时/历史数据库，实时/历史数据库需要采集电厂绝大多数自动化系统的主要数据，又将部分数据传给MIS和其他管理系统。

五、主要信息系统的信息安全防御

1.1 SIS与其他系统之间的安全防御

- × SIS防御的重点是，必须切断所有从实时/历史数据库读取数据的用户系统对SIS的入侵，这些系统包括MIS、上级主管单位的生产管理系统、在线仿真系统等。在实时/历史数据库与所有读取数据的系统之间应配置数据单向传输的专用隔离装置，他们可以从实时/历史数据库读取数据，但绝不允许反向输入数据。

五、主要信息系统的信息安全防御

1. 2 SIS人机交互的安全防御

SIS的人机交互设备和DCS不太一样,SIS有功能站、值长站、工程师站和监视终端设备等。

五、主要信息系统的信息安全防御

1.2 SIS人机交互的安全防御

- × **功能站**可以按照功能分为负荷分配调度站、计算与性能分析站、网络管理维护站、应用软件管理维护站等，这些功能站只要有
人机交互，如计算与性能分析站，就需要注意防御，一方面是制
定好电厂的管理机制，另外还要设计好系统身份识别、访问控
制机制和密码安全机制等，防止一般人员擅自进入并改变程序。
- × **值长站**可以通过显示器进行监视，但不能操作。监视终端设备
同样也只能通过显示器进行监视而不能操作。值长站和监视终
端设备没有对外的数据接口，不需要特别防御。
- × **工程师站**是对SIS进行维护并可以修改组态的装置，也是外部入
侵SIS的可能关口。对于工程师站来说，需要采取和功能站一样的
防御措施。

五、主要信息系统的信息安全防御

2 MIS的安全防御重点

- × 相对于SIS而言，MIS的安全等级略低，可以采取和其他工业企业相同的信息安全防御措施。
- × MIS对外的联系主要有：与上级主管单位进行信息交换，与地区政府部门进行环保数据对接，与公共服务机构进行市场运营等数据交流，与设计单位、建设单位、调试单位、监理单位等进行建设过程中的数据移交，与国际互联网等公共网络进行接口等。
- × 只要这些联系的方式是通过电子介质传输，就会存在信息安全威胁。建设好电厂信息系统与所有外部系统的信息安全屏障，是电厂设计和运行时首当其冲需要考虑的问题。

谢谢

中国能源建设集团工程研究院