发电厂控制与管理系统信息安全

中国自动化学会发电自动化专业委员会　组编
朱松强　主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

发电厂控制与管理系统信息安全

中国自动化学会发电自动化专业委员会　组编
朱松强　主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

随着两化深度融合的不断推进，电厂开始了自身数字化、智能化的发展，电厂控制系统对于信息系统的依赖程度越来越高，信息化技术在电厂广泛应用的同时也带来病毒和黑客侵入的威胁，使发电厂控制与管理系统信息安全面临严峻的挑战，这种形势促使中国自动化学会发电自动化专业委员会组织编写了这本书。

本书介绍了发电厂过程控制的发展过程、控制与管理系统当前的信息安全现状与挑战。重点以发电厂控制与管理系统信息安全应用为导向，结合目前电厂的实际生产环境以及国家部委、能源行业的相关规定，提出了发电厂控制与管理系统信息安全防护体系的规划和建设思路，系统性地阐述了电厂控制与管理信息安全防护相关技术原理和技术体系、管理体系建设方案，介绍了电厂控制与管理系统信息安全风险评估和安全防护人才培养的内容、方法与步骤，最后提供了控制与管理系统信息安全防护方案的设计、实施与平台应用情况测试结果的具体案例，供读者参考，帮读者进一步加深对全书内容的理解和掌握。

本书可作为发电厂热控和控制网络信息安全从业人员进行控制网络与信息安全规划、部署建设和日常管理的重要参考，也可作为从事工业控制系统的网络安全规划、设计、工程实施和管理的技术人员或高等院校、电厂热控、信息专业的学习、培训教材。

图书在版编目（CIP）数据

发电厂控制与管理系统信息安全/朱松强主编；中国自动化学会发电自动化专业委员会组编. —北京：中国电力出版社，2017.12

ISBN 978-7-5198-1494-6

Ⅰ. ①发… Ⅱ. ①朱…②中… Ⅲ. ①发电厂－计算机管理系统－信息安全②发电厂－计算机管理系统－信息安全 Ⅳ. ①TM62

中国版本图书馆 CIP 数据核字（2017）第 301608 号

出版发行：中国电力出版社
地　　址：北京市东城区北京站西街 19 号（邮政编码 100005）
网　　址：http://www.cepp.sgcc.com.cn
责任编辑：郑艳蓉（010-63412379）　柳　璐
责任校对：太兴华
装帧设计：王红柳　张　娟
责任印制：蔺义舟

印　　刷：三河市百盛印装有限公司
版　　次：2017 年 12 月第一版
印　　次：2017 年 12 月北京第一次印刷
开　　本：787 毫米×1092 毫米　16 开本
印　　张：17.5
字　　数：371 千字
印　　数：0001—2000 册
定　　价：70.00 元

朱松强，浙江仙居人，硕士，教授级高级工程师，国家科学技术奖励专家库成员，浙江省电力学会副理事长。长期从事能源生产技术和安全管理工作，多项成果荣获省部级科技进步一等奖。组织团队深入传统煤电生产效率、大气污染物超低排放、设备事故预警诊断、智能电厂建设方面的科研和实践，使浙能集团连续十四年荣获浙江省政府安全生产优秀考评；在全国发电机组可靠性竞赛中荣获金牌机组比例在国内领先。此外，还致力于安全生产工作科学化、规范化、精细化以及安全生产标准化体系建设和风险防控研究与实施，负责《电力企业安全生产管理规范（火力、水利发电厂部分）》（DB33/787—010）的编制工作。

周慎学，浙江台州人，硕士，高级工程师，浙江浙能台州第二发电有限责任公司总经理。长期从事火力发电厂热工自动化及电厂基本建设项目管理工作，具有丰富的基建管理经历和项目管理经验。曾荣获浙江电力行业管理创新优秀成果一等奖及省部级科技进步奖三项，参与审定《创建电力优质工程策划与控制系列丛书》，并在《中国电力》等杂志发表论文五篇，取得实用新型专利一项。

《发电厂控制与管理系统信息安全》

编 审 单 位

组编单位 中国自动化学会发电自动化专业委员会

编写单位 浙江省能源集团有限公司

浙能台州第二发电有限责任公司

华能国际电力股份有限公司长兴电厂

国网浙江省电力公司电力科学研究院

中国电子技术标准化研究院

浙江浙能技术研究院有限公司

杭州安恒信息技术有限公司

浙江省电力学会

北京京能高安电燃气热电有限责任公司

杭州聚盛广科技有限公司

编 审 人 员

主　　编　朱松强

副 主 编　周慎学　范　渊　陈胜军　周自强

参　　编　夏克晁　范科峰　尹　峰　李　辉

董勇卫　周　俊　范海东　王焕明

傅林平　王剑平　陈学奇　陈胡敏

蔡卫国　华国钧　胡伯勇　陈大宇

姚相振　李　琳　柏元华　吴卓群

虞云军　苏　烨　杜永春　孙　迪

吴侃侃　卢　化　徐晶霞　陈　波

丁俊宏　王　蕙　孙长生　史先亚

孙坚栋

主　　审　刘吉臻

序　言

当前火电厂建设与生产面临新的机遇与挑战。一方面，在地方政府关于节能减排政策的要求下和发电集团集约化管理需求的驱动下，发电厂开始了新一轮以智能化为核心的技术发展。另一方面，智能化电厂在发展中将不断与移动互联网、云计算、大数据和物联网等先进技术相互融合，在促进火电厂的进一步转型升级的同时，也会因为互联而诱发一系列网络安全问题，使发电厂既面临着传统网络的安全风险，也面临工业控制系统安全的风险，工业控制系统的网络安全问题日渐受到重视。

近几年来，工业控制系统网络安全事件层出不穷，震网、乌克兰电网等事件后，我国已深刻认识到黑客攻击、网络病毒将给工业控制系统和国家关键基础设施带来严重危害。发电厂的安全稳定运行关系到国计民生，因此在发电厂智能化发展过程中，必须做好控制系统信息安全防护工作，并建立一套行之有效的控制系统信息安全防护体系。

中国自动化学会发电专委会组织专家积极开展智能发电厂体系建设的研究工作，先后出版了指导性文件《智能电厂技术发展纲要》，制定了中国电力企业联合会团体标准《火力发电厂智能化技术导则》，与工业和信息化部电子工业标准化研究院信息安全研究中心一起组织开展《发电厂控制系统与信息安全防护及管理体系建设》研究与应用试点项目工作，并在总结试点工作的基础上编写了《发电厂控制与管理系统信息安全》。在专业技术竞争激烈的今天，他们将自己长期用心血与汗水换来的宝贵经验，无私地奉献给了广大读者，相信丛书一定会给广大电力工作者和读者带来启发和收益。

本书介绍了发电厂过程控制的自动化、信息化和智能化的发展过程，当前面临的控制与管理系统信息安全问题，提出了安全防护体系建设思路和方案、风险评估过程和方法、信息安全专业人才的培养方式与内容，最

后给出了具体电厂的实施案例，基本覆盖了发电厂当前控制与管理系统信息安全防护所要开展的工作内容。

希望本书的出版，能帮助专业人员提高解决工控网络信息安全防护问题的能力，推动我国发电厂控制系统与信息安全防护及管理体系建设的深入开展，为国民经济的增长与繁荣做出贡献。

金耀华

2017 年 11 月 1 日

前　言

随着计算机技术、通信技术和网络技术的发展，工业控制系统正在从数字化、网络化迈向智能化，国内大量发电企业在国家支持和自发驱动下，开始了工业控制系统的升级换代，实现网络化、智能化的生产管理。目前国内绝大多数发电企业的电力调度和生产已完全依赖于计算机监控系统和数据网络，且随着互联网的不断渗透，以及智能设备的使用，电力系统已从原来的相对封闭、稳定的环境变得更加开放和多变，传统工业控制系统的潜在安全性正在遭受严重的挑战。

近些年，工业控制系统网络安全漏洞不断被曝出，网络安全事件层出不穷，震网、乌克兰电网等事件后，世界各国已深刻认识到黑客攻击、网络病毒给工业控制系统、国家关键基础设施可能带来的危害。发电厂作为能源领域的重点行业，其安全稳定运行关系到国计民生，将面临黑客和敌对势力攻击的危险。如何针对发电厂控制网络和信息安全建立一套行之有效的防护体系，已成为我国电力行业的当务之急。

为落实国家主管部门关于加强工业控制系统信息安全（简称工控安全）保障能力建设的相关要求，工信部电子四院积极组织专业技术力量，联合国家信息技术安全研究中心等单位，开展《工业控制系统安全控制应用指南》等国家标准研制工作。为进一步做好工控安全保障工作，树立工控安全标准试点应用项目，形成产业示范效应，工业和信息化部电子四院信息安全研究中心通过中国自动化学会发电自动化专业委员会协调，在浙江能源集团公司、华能国际电力股份有限公司支持下，选择了浙江两家发电厂为试点单位，联合杭州安恒科技有限公司、国网浙江省电力公司电力科学研究院、浙江浙能技术研究院有限公司、杭州聚盛广科技有限公司等单位，在借鉴发电厂两化融合工作中取得的成功经验基础上，共同开展《发电厂控制系统与信息安全防护及管理体系建设》研究与应用试点项目工作，并在试点工作总结的基础上编写了本书。

本书共分为八个章节，第一章简单介绍了发电厂的类型及自动化、数字化、信息化、智能化的发展进程和当前智能化发电厂建设情况；第二章详细阐述了目前发电厂控制与管理系统面临的信息安全威胁及挑战；第三章通过对相关法律法规和标准规范的梳理，结合目前国内外的先进技术理念，提出了发电厂控制与管理系统信息安全保障体系的构建思路和设计方法；第四章给出了适用于发电厂控制与管理系统的信息安全技术方案，并重点介绍了主要采用的安全技术和产品；第五章基于信息安全管理体系（ISO 27001），介绍了电厂如何建立一套全面而有效的信息安全管理体系；第六章重点介绍了电厂开展风险评估的依据、过程和方法，来不断提升电厂控制与管理系统信息安全综合防护能力；第七章阐述了我国信息安全人才的现状，并提出了复合型信息安全人才的新型培养方式和方法；第八章以编写组参与的实际项目为例，阐述了电厂控制与管理系统信息安全防护体系平台的建设方案设计、实施、应用过程情况以及平台的实际测试情况。

本书在编写过程中，除了引用编写组专家多年的工作实践、研究成果和《发电厂控制系统与信息安全防护及管理体系建设》研究与应用试点项目外，还大量参考了一些国内外优秀的论文、书籍，以及在互联网上公布的相关资料，由于互联网上资料数量众多、出处引用不明确，无法将所有文献一一注明出处，对这些资料的作者表示由衷的感谢。

最后，鸣谢参与本书策划和幕后工作人员！存有不足之处，恳请广大读者不吝赐教。

编写组

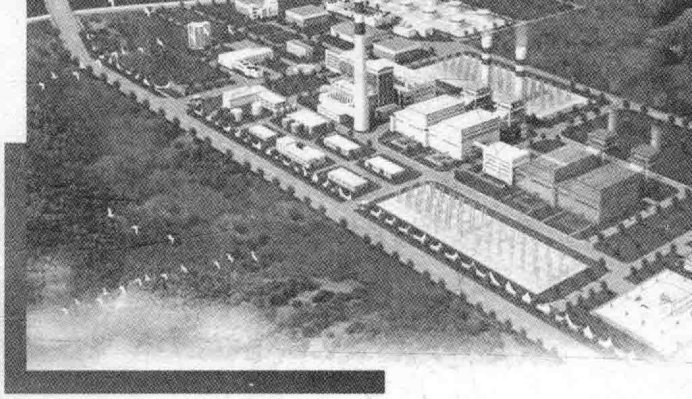
2017 年 11 月 10 日

范渊，美国加州州立大学计算机科学硕士毕业，杭州安恒信息技术有限公司董事长兼CEO，国家“千人计划”特聘专家，兼任中国网络安全空间协会常务理事、国家信息安全标准化委员会委员、中国计算机学会计算机安全专家委员会常委、浙江工业互联网产业联盟理事长等职务。对Web应用安全、数据库安全、工控系统安全等领域有深入研究；登上全球BLACKHAT（黑帽子）大会演讲的第一位中国人；多次承担国家级重大科技专项，拥有数十项国际国内发明专利；带领团队曾承担G20杭州峰会、世界互联网大会、北京奥运会、广州亚运会、上海世博会等重大活动的网络安全保障任务。荣获浙江省杰出青年、第四届杭州市杰出人才、中国通信协会“网络与信息安全杰出人才”、2016中国互联网发展基金会首届“网络安全优秀人才”和2016年度十大风云浙商人物等称号，出版《智慧城市与信息安全》一书。

陈胜军，高级工程师，华能国际长兴发电厂生产副总经理，华能集团优秀节约环保型企业创建工作指导专家库成员，华能集团电力生产技术专家。参加了国内首台超超临界百万机组的建设和生产，历任华能玉环生产部主任、厂长助理，积累了丰富的超超临界百万机组建设和生产管理经验。先后获得省部级科学技术奖三项、国家级二等企业管理现代化创新成果奖一项、地市级科技进步奖两项、华能国际股份公司安全生产合理化建议特等奖等多项奖励，取得实用新型专利一项，在《热力发电》等期刊、全国性技术研讨会发表论文多篇。

周自强，高级工程师，国网浙江省电力公司电力科学研究院副院长。长期从事输变配电设备运维及科技与信息化管理工作，曾参与国家电网公司新农村电气化供电模式研究以及县域电力专用通信网研究和示范工程建设。在国内外知名期刊和学术会议上发表论文十余篇，获得国家电网公司科技进步奖一项、国网浙江省电力公司科学技术进步奖多项。

目　录



第一章

发电厂过程控制的发展

发电厂是电力生产中的重要环节，随着智能电网的启动和建设，传统发电厂已不能很好地适应智能电网的发展需要，电厂的智能化发展势在必行。智能化电厂是数字化电厂的进一步深入和发展，在数字信息处理技术和通信技术的基础上，通过集成智能的传感与执行、控制和管理等技术达到更安全、高效、环保的运行，与智能电网及需求侧相互协调，与社会资源和环境相互融合的发电厂。本章主要介绍发电厂的类型及数字化发展进程，着重介绍发电厂过程控制自动化与信息化的发展过程，并对智能化电厂的概念、结构内容、当前建设情况进行了介绍，对未来发展进行了分析和展望。

第一节 发电厂概述

发电厂（或发电站）是将自然界蕴藏的各种一次能源转换为电能（二次能源）的工厂。根据发电厂使用的能源不同，发电厂主要可划分为火力发电厂、水力发电厂、核能发电厂和风力发电厂，其他还有地热发电厂、潮汐发电厂、太阳能发电厂、生物质发电厂等。

一、火力发电厂

火力发电厂是利用燃烧燃料（煤、油、天然气等）所得到的热能来进行发电。火力发电厂的发电机组有两种主要形式：利用锅炉产生高温高压蒸汽冲动汽轮机旋转带动发电机发电，称为蒸汽轮机发电；燃料进入燃气轮机将热能直接转换为机械能驱动发电机发电，称为燃气轮机发电。

蒸汽轮机发电厂主要系统组成有燃料系统、燃烧系统、汽水系统、电气系统、控制系统等。

在上述系统中，最主要的设备是锅炉、汽轮机和发电机，它们安装在发电厂的主厂房内。主变压器和配电装置一般安装在独立的建筑物内或户外。电厂基本生产过程是，

燃料在锅炉中燃烧，将其热量释放出来，传给锅炉中的水，从而产生高温高压蒸汽；蒸汽通过汽轮机又将热能转化为旋转动力，以驱动发电机输出电能，图 1.1 所示为燃煤发电厂流程。

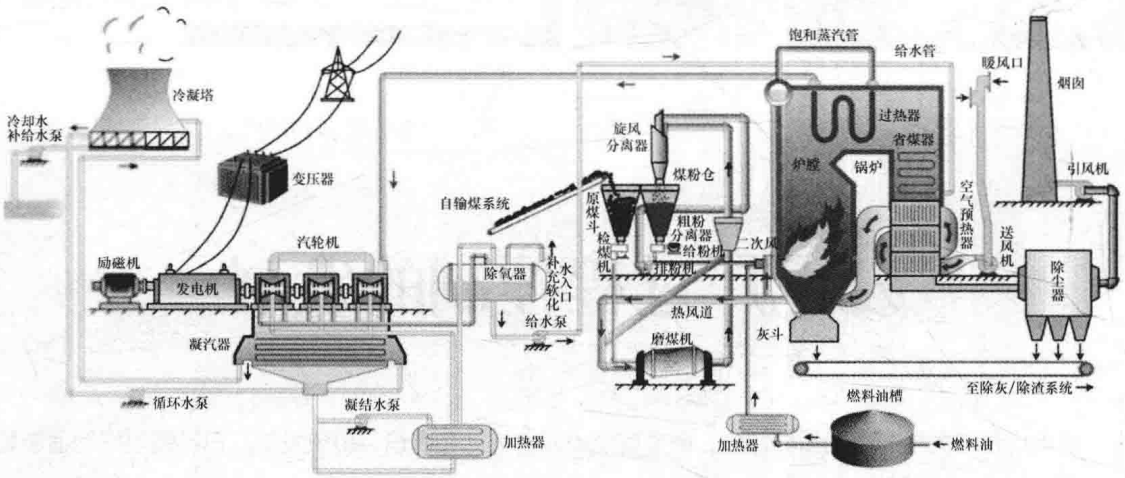


图 1.1　燃煤发电厂流程

燃气轮机发电采用燃气轮机联合余热锅炉发电，这被称作联合循环发电厂。燃气轮机联合循环发电机组是燃气轮机、发电机与余热锅炉、蒸汽轮机（凝汽式）或供热式蒸汽轮机（抽汽式或背压式）共同组成的循环系统，它是将燃气轮机做功后排出的高温乏烟气通过余热锅炉回收转换为蒸汽，送入蒸汽轮机发电，或者将部分发电做功后的乏汽用于供热。常见形式有燃气轮机、蒸汽轮机同轴推动一台发电机的单轴联合循环，也有燃气轮机、蒸汽轮机各分别与发电机组合的多轴联合循环。

二、水力发电厂

水力发电是运用水的势能转换成电能的发电方式，其原理是利用水位的落差（势能）在重力作用下流动（动能），如从河流或水库等高位水源引水流至较低位处，水流推动水轮机使之旋转，带动发电机发电。由于技术成熟，是目前人类社会应用最广泛的可再生能源。以水力发电的电厂称为水力发电厂，简称水电厂或水电站。

水力发电依其开发功能及运转形式，可分为传统水力发电与抽水蓄能水力发电两种。

传统的堤坝式水力发电厂系统如图 1.2 所示，其流程为河川的水经由拦水设施攫取后，经过压力隧道、压力钢管等水路设施送至电厂，通过阀门控制水流量使水冲击水轮机，水轮机转动后带动发电机旋转发电，发电后的水经由尾水路回到河道，供给下游的用水使用。

抽水蓄能式水力发电是一种储能方式，但并不是能量来源。当电力需求低时，多出的电力推动电泵将水泵至高位储存；当电力需求高时，便以高位的水做发电之用。此法可以改善发电机组的使用率，在商业上非常重要。

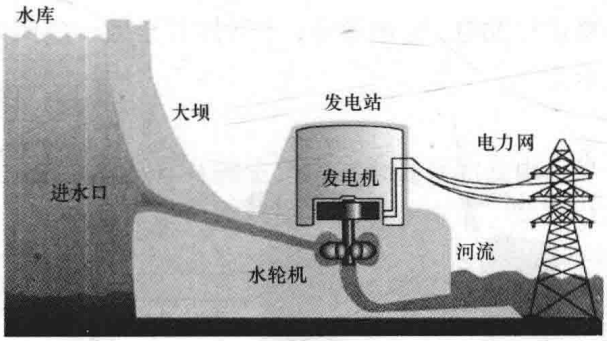


图 1.2　堤坝式水电厂系统

三、核能发电厂

核能发电厂是利用核反应堆中核燃料裂变链式反应所产生的热能，用来加热水，并在蒸汽发生器内产生蒸汽，图 1.3 所示是核能发电厂系统图。蒸汽通过管路进入汽轮机，驱动汽轮机再带动发电机旋转发电。因此核电站主要分为两部分：一部分是利用核能产生蒸汽的核岛，包括反应堆装置和一回路系统；另一部分是利用蒸汽发电的常规岛，包括汽轮发电机系统。

核能发电厂根据核反应堆的类型，可分为轻水堆式、压水堆式、沸水堆式、气冷堆式、重水堆式、快中子增殖堆式发电厂等。核电站使用的核燃料一般是放射性重金属铀-235 或钚。

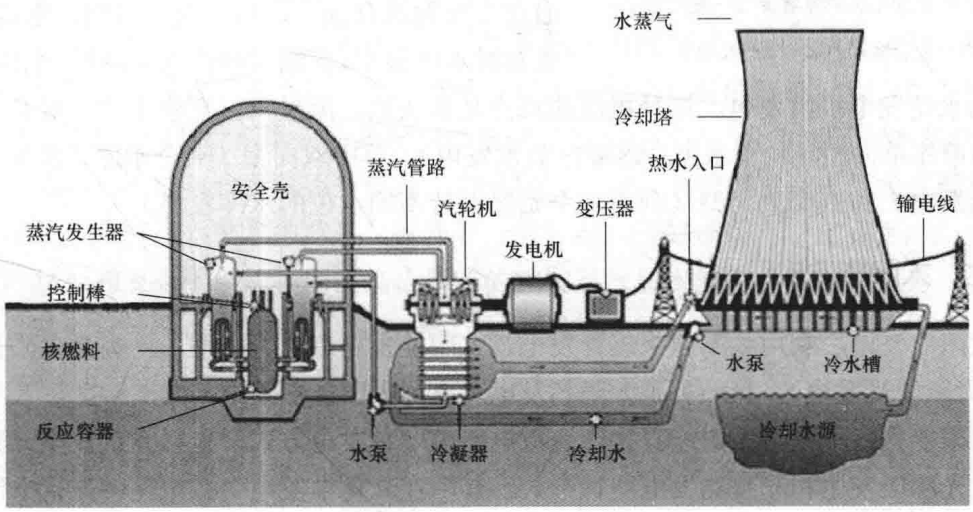


图 1.3　核能发电厂系统图

四、风力发电厂

风力发电厂是利用自然风，利用风力吹动建造在塔顶上几十米长的大型桨叶旋转，

带动风力发电机旋转来进行发电。它由数座、十数座甚至数十座风力发电机组成，图 1.4 所示为风力发电系统示意。

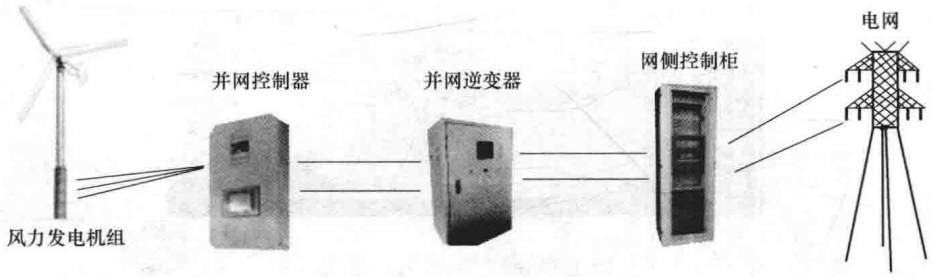


图 1.4　风力发电系统示意

五、地热发电厂

地热发电厂利用地热井，喷出具有一定压力的过热蒸汽，送入汽轮机驱动发电机来进行发电；或者利用地热井涌出的具有一定压力和温度的汽水混合物或热水，通过闪蒸系统来进行发电。图 1.5 所示为闪蒸系统发电原理示意。

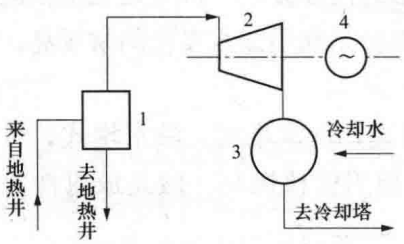


图 1.5　闪蒸系统发电原理示意

1—闪蒸分离器（或扩容器）；2—蒸汽透平；3—混合式凝汽器；4—发电机

六、潮汐发电厂

潮汐发电厂是利用潮汐水流的移动，或是潮汐海面的升降，将海洋潮汐能转换成电能的发电厂。通过在海湾或有潮汐的河口筑起水坝，形成水库。涨潮时水库蓄水，落潮时海洋水位降低，水库放水，以驱动水轮发电机组发电。这种机组的特点是水头低、流量大。潮汐电站一般有 3 种类型，即单库单向型（一个水库，落潮时放水发电）、单库双向型（一个水库，涨潮、落潮时都能发电）和双库单向型（利用两个始终保持不同水位的水库发电）。

七、太阳能发电厂

太阳能发电厂利用太阳能来进行发电，太阳能发电有两大类型，一类是太阳光发电（亦称太阳能光发电），另一类是太阳热发电（亦称太阳能热发电）。

太阳能光发电是将太阳能直接转变成电能的一种发电方式，包括光伏发电、光化学发电、光感应发电和光生物发电四种形式，其中在光化学发电中有电化学光伏电池、光电解电池和光催化电池。

太阳能热发电是先将太阳能转化为热能，再将热能转化成电能，它有两种转化方式，一种是将太阳热能直接转化成电能，如半导体或金属材料的温差发电，真空器件中的热电子和热电离子发电，碱金属热电转换，以及磁流体发电等；另一种方式是将太阳热能通过热机（如汽轮机）带动发电机发电，与常规热力发电类似，只不过是其热能不是来