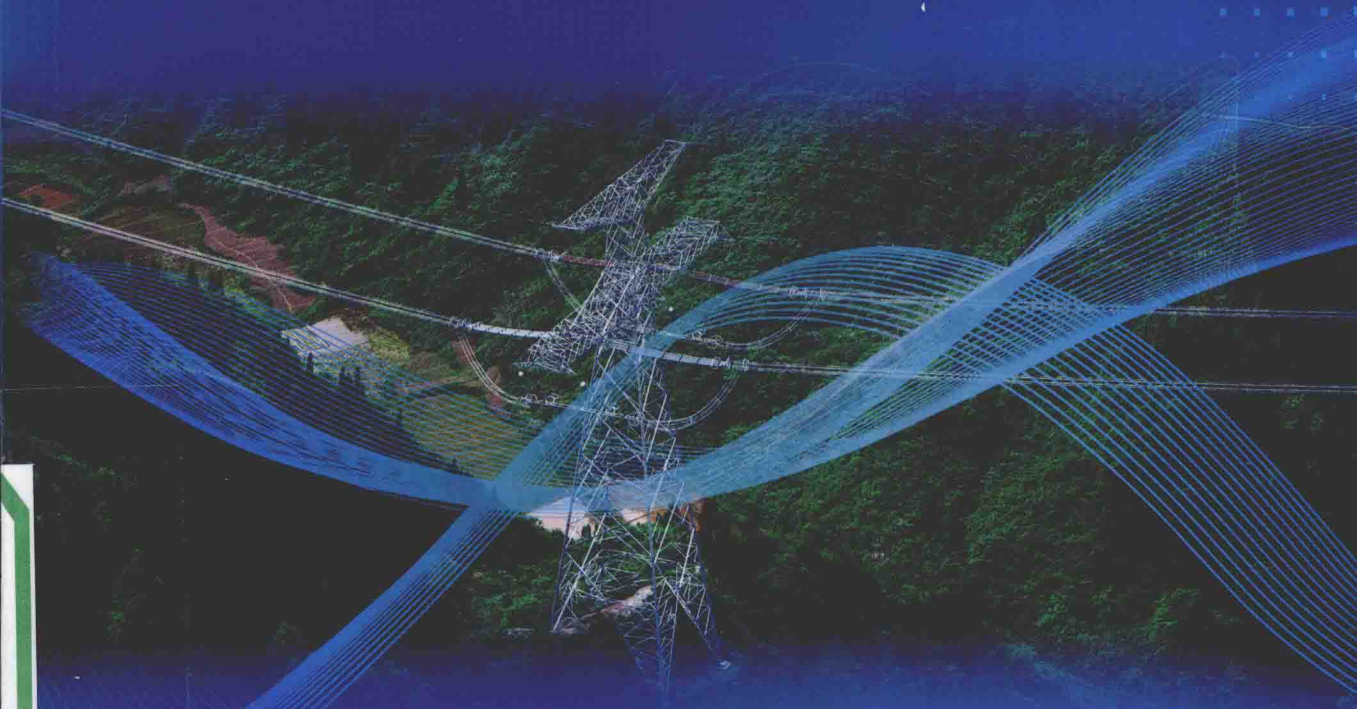
电力信息系统测评技术与应用

林为民　余　勇　蒋诚智　石聪聪　等编著



中国电力出版社
CHINA ELECTRIC POWER PRESS

电力信息系统测评技术与应用

林为民　余　勇　蒋诚智　石聪聪　等编著

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书详细介绍了信息系统测评技术及其在电力信息系统中的应用。全书分为六章，包括概述、信息系统测评技术、电力信息系统测评标准与规范、电力信息系统测评的生态环境、电力信息系统测评过程和电力信息系统测评案例。

本书可供从事信息系统测评技术研究与应用工作的人员阅读使用。

图书在版编目（CIP）数据

电力信息系统测评技术与应用 / 林为民等编著. —北京：中国电力出版社，2015.10

ISBN 978-7-5123-8167-4

Ⅰ. ①电… Ⅱ. ①林… Ⅲ. ①电力系统－信息系统－系统测试 Ⅳ. ①TM7

中国版本图书馆 CIP 数据核字（2015）第 197753 号

中国电力出版社出版、发行

（北京市东城区北京站西街 19 号 100005 http://www.cepp.sgcc.com.cn）

汇鑫印务有限公司印刷

各地新华书店经售

*

2015 年 10 月第一版 2015 年 10 月北京第一次印刷

787 毫米×1092 毫米 16 开本 15.25 印张 364 千字

印数 0001—2000 册 定价 **65.00** 元

编著人员名单

主　编　林为民

副主编　余　勇　蒋诚智　石聪聪

参　编　李尼格　曹宛恬　郭　骞　俞庚申

范　杰　高　鹏　叶　云　冯　谷

车建华

前　言

随着信息系统规模的不断扩大和复杂性的日益增加，信息系统质量成为信息系统生命周期过程中越来越重要的问题。信息系统测评是保证信息系统质量的主要手段，是信息系统开发过程中必不可少的环节，近年来受到人们越来越多的重视。信息系统测评是应用测评工具和方法按照测评方案和流程对所开发的信息系统产品进行功能、性能和安全性测试，以确保所开发的信息系统产品满足用户的需求。

信息系统测评的目的包括：①确认信息系统的质量，即确认信息系统是否能做用户所期望的事情（do the right thing）和是否以正确的方式来做用户所期望的事情（do it right）；②提供有关信息系统的信息，比如为项目经理或开发人员提供反馈信息，为风险评估准备所需信息；③帮助改进信息系统研发的方法和过程。信息系统测评是一项专业性较强的工作，要求测评人员具备许多理论知识和较为丰富的工程实践经验。缺少这些知识和经验，测评的深度和广度就不够，信息系统的质量也就难以保证。因此，软件测试人员需要接受专门的培训并在实践中不断积累经验。

随着建设坚强智能电网发展战略目标的提出，电力行业对信息系统的质量要求也越来越高。电力工业作为一种涉及国计民生的基础能源产业，对社会的正常生产和民众的日常生活起着极为重要的作用。信息技术的发展正在对电力的安全生产和系统的平稳运行产生着前所未有的影响，并不断深入到电力各个领域中，逐步提高了电力行业的信息化水平。但是，电力系统规模的扩大化和结构的复杂化趋势，要求电力行业正在使用或即将上线的信息系统具备完善的功能、优越的性能和可靠的安全性，否则将有可能对电力的生产和运行造成不可估量的危害。电力信息系统测评作为保障电力信息系统质量的重要手段，同

样受到了电力企业管理人员的高度重视。对于正在使用的电力信息系统，要求定期开展有针对性的功能、性能和安全性测评，以尽早发现并解决运行中的电力信息系统可能出现的问题；对于即将上线的电力信息系统，更是要求开展全面详尽的功能、性能和安全性测评，不达要求不准上线运行。由于电力信息系统的业务功能和部署方式具有行业独特的特点，需要结合通用的信息系统测评方法，进行电力信息系统测评的技术积累和实践应用，为全面保障电力信息系统的质量和实现电力的安全生产奠定基础。

本书首先系统地介绍了信息系统尤其是电力信息系统测评的基本概念和关键技术；其次，介绍了电力信息系统测评所遵循的国内外和电力行业标准规范、电力信息系统测评的生态环境及电力信息系统测评的主要流程；最后，介绍了电力领域开展的一些信息系统测评实践，为信息系统测评技术在电力领域的应用提供了一些借鉴与参考。

本书由林为民、余勇、蒋诚智、石聪聪等编著。编者均为从事电力信息系统测评、电力行业信息化及电力信息安全等领域的科研人员、开发人员或管理人员，具有丰富的电力信息化从业经验。本书在编写过程中，参阅并引用了大量国内外研究人员的相关科技文献和研究资料，在此谨致诚挚的谢意。

由于时间仓促，书中难免有疏漏和不足之处，真诚希望读者和同仁批评指正。

编　者

目　录

第一章

概　　述

当今社会，信息系统已经成为人们生活不可或缺的一部分。随着对信息化依赖性不断增强，人们对信息系统的质量也提出了更高的要求。用户不仅对信息系统的功能期望值越来越高，而且对信息系统的性能和安全性要求越来越高。在这种情况下，信息系统测评作为控制信息系统质量的重要手段应运而生。本章主要介绍信息系统测评的主要概念及电力信息系统测评的基本情况。

第一节　信息系统测评概述

一、信息系统测评的概念

信息系统是由计算机硬件设备、网络装置、软件程序、数据信息和文档资料等构成的以收集和处理信息为核心的集合。随着信息系统的应用日益普及，其建设规模越来越大。信息系统生命周期的各个阶段都离不开人的参与，由于人的工作难免出现错误，因此人为因素是信息系统质量问题的主要原因之一。与此同时，随着信息系统实现功能的不断强大，其复杂程度越来越高。例如，Windows NT 操作系统的代码大约有 3 200 万行，使得出现的缺陷概率增加。复杂性是引起信息系统质量问题的另一个重要原因。

对信息系统整个生命周期进行全方位的测评，是保证信息系统质量的有效手段。通过测评能够发现信息系统的许多质量问题。例如，在英国约克大学为英国海军开发的 SHOLIS 项目中，虽然利用程序正确性证明方法已经排除了开发前期的许多错误，但是信息系统测评仍然发现整个开发过程中 15.75%的错误。信息系统测评是对信息系统中的每个组件及系统整体的功能、性能和安全进行测试，并依据测试结果给出相应的评价。信息系统测评通过测试发现信息系统存在的问题，通过评价说明信息系统的质量水平。

信息系统测评主要用于检验信息系统与需求目标是否吻合，相关功能、性能和安全指标是否达到预期要求。测评人员基于需求分析报告中提出的功能、性能和安全需求，按照设计的测评用例进行测评，以期发现对需求的理解差异、系统错误、功能缺陷、性能瓶颈和安全隐患等各个方面的问题，从而保证信息系统符合业务运营的要求。通过测评，可以确保信息系统符合质量标准，使其在交付后能够正确、可靠、平稳和安全地运行，有效地支持业务运营。与此同时，测评作为设计和开发的补充，为设计人员和开发人员提供修改意见，帮助改进信息系统。

在开始信息系统测评之前，需要做好以下准备工作：①制订测评计划，详细说明测评的内容与步骤，并以此作为风险管理的手段；②根据需求设计测评案例，保证测评与需求的一致性；③建立参与测评各方的组织架构和管理流程，保证测评过程的有序和效率；④建立独立的测评团队，执行并记录测评结果，保证信息系统质量。建立独立测评团队的

目的是保证测评的客观性、专业性和资源效率。信息系统测评对象主要包括硬件环境和应用软件两个部分。硬件环境测评主要确认所安装和配置的物理主机、网络设备和存储设备等在内的硬件环境能够正常工作，应尽早将所有硬件设备安装到位并进行联调测试。应用软件测评主要测评所开发软件程序的功能、性能和安全的正确性，信息系统的质量与所开发的软件程序密切相关，并对测评的结果产生明显影响，应该对单个软件和软件之间的集成情况进行详细测试。

二、信息系统测评的发展历程

早期的信息系统开发人员并没有意识到信息系统开发需要测评这个重要的环节。20世纪60年代，几乎没有通用硬件，程序员只是根据具体应用，在大型机、小型机或专用计算机上编写程序代码，主要强调编程技巧，对信息系统的开发没有系统化措施。信息系统测评只是程序员在代码编写结束后进行的一种正确性验证活动，当时没有专门的测评理论和技术，更没有专职测评人员，往往将调试与测试混为一谈，程序员根据经验猜测开发错误。20世纪60年代中期至70年代中期，计算机在许多领域得到了应用，信息系统也从单用户模式发展成为多用户模式，并且出现了实时系统和数据库管理系统。这个阶段开发的信息系统仍然不太复杂，但是人们已经开始思考开发流程问题，并提出了“软件工程”的概念。

随着信息系统开发技术的不断提高，人们逐渐认识到测评对保证信息系统质量是一个至关重要的环节。20世纪70年代，测评理论和技术开始进入探索、创立和发展阶段。1972年，软件测试领域的先驱者Bill Hetzel博士在North Carolina大学首次举行了以信息系统测评为主题的正式学术会议，这标志着信息系统测评理论和技术开始成为业界的研究对象。此后，各种信息系统测评理论和技术如雨后春笋般出现，各种相关的学术会议不断举行。1979年，Glenford Myers在*The art of software testing*这本书总结了众多测评方法，并第一次提出信息系统测评的目的在于证伪，而非证真，即测评是为了发现错误，这是测评理念的一次突破。

20世纪80年代，随着PC和Windows操作系统的诞生，计算机开始进入PC时代。与此相应的是，以微软公司为代表的新一代软件公司开发了大量基于PC的信息系统，其规模成指数级增长，超过几百万行甚至几千万行代码的信息系统开始出现，这对测评工作提出了更加严格的要求。为了适应这一要求，开发厂商开始成立质量保证（quality assurance，QA）部门保证信息系统的质量。后来，质量保证部门的职能转变为流程监控，而信息系统测评则从中分离出来成为独立的岗位，在信息系统开发项目中设置测评专职人员成为一种共识。这个时期，测评理论和技术也有了质的飞跃，业界开始形成一些公认的测评经典理论，构成了现有测评理论的基本框架。

20世纪90年代中期，随着互联网的普及，人类社会进入网络时代，全球数以万计的计算机用户通过网络连接在一起，相应的信息系统也迅速从单机或局域网模式向互联网模式迁移。基于互联网的分布式计算技术被广泛应用于各种类型的信息系统中，使信息系统比以往任何时代都要复杂。在网络时代，信息系统测评需要解决更多的理论和技术难题，必须深入研究分布式远程测评、负载平衡测评、安全性测评等以往很少关注的领域。信息系统测评开始从单纯的技术环节演变成一个需要完整理论体系的系统工程，进而成为一门专业的学科。

作为保证信息系统质量的重要手段，信息系统测评的受重视程度也不断提高。但是，国内信息系统测评的总体情况与国外相比还存在一定的差距，主要表现在以下四个方面：

（一）对信息系统测评的重要性认识不足

长期以来，国内很多IT公司存在“重开发、轻测评”的观念，认为信息系统能够运行即可，不必为测评支付额外的成本。这些IT公司对信息系统测评的重要作用认识不足，没有专职的测评部门和测评人员，大部分选择信息系统开发人员和集成人员做兼职测评。而在国外，如微软公司，信息系统测评占据项目周期多半的时间，以IE 4.0为例，其代码开发时间为六个月，而测评及稳定程序时间为八个月。从投入的资金、人力和物力来看，以美国信息系统开发和生产的平均资金投入为例，通常“需求分析”和“规划确定”各占3%，“系统设计”占5%，“编程”占7%，“测评”占15%，“投产和维护”占67%。由此可见，测评在信息系统开发中的地位非常重要。值得庆幸的是，国内用户对信息系统质量的要求越来越高，测评的地位正在逐渐提高。一些大中型信息技术公司加强了测评意识，在公司内部设立了专职的测评部门，配备了专业的测评人员，并在信息系统开发过程中不断强调测评环节，以求提交给用户高质量的产品。

（二）信息系统测评还未形成产业

在某些发达国家和地区，信息系统测评已经发展成为一个产业。在美国硅谷，信息系统开发公司必须有专门的测评部门，其中信息系统测评人员的数量相当于信息系统开发人员数量的3/4，负责信息系统测评的质量保证部门经理与信息系统开发的主管在职位上是平行的。在信息系统开发产业发展较快的印度，信息系统测评在信息系统开发公司中同样拥有举足轻重的地位。而国内的信息系统测评还没有形成真正的产业，正处于快速发展阶段。为了适应信息系统测评的需求，各地成立了一些专业测评机构，如信息系统测评中心、信息安全测评中心、网络测评实验室等。这些机构正在逐渐形成测评服务体系，对信息系统开展独立的第三方测评，以公正、公平、权威的测评结果，为信息系统质量鉴定提供重要的依据。

（三）缺乏信息系统测评专业人员

由于长期对信息系统测评重视不够，具备相应技术技能的高素质专业测评人才非常缺乏。目前，我国测评人才的培养主要通过社会化的培训机构及行业认证来完成，而大多数高等院校没有设置相关的专业和课程，所以专业人才的培养远远不能缓解人才市场的紧缺状况。专业人员的缺乏从某种程度上影响了信息系统测评领域的发展。

（四）信息系统单项测评发展不均衡，综合测评比较薄弱

信息系统是一个多层次、跨领域的集合体，其测评涉及多个方面的专业知识。就目前形势来看，信息系统测评多数是针对某个方面的单项测评，如硬件产品测评、软件程序测评、网络安全测评等，而且这些单项测评的发展不均衡。例如，硬件产品测评经过多年的积累，测评理论研究比较深入，测评技术和工具比较成熟，相对属于发展较快的领域；而软件程序测评和网络安全测评两个领域虽然近年来得到国家和厂商的高度重视，相继发布了一些测评标准，测评人员队伍也逐渐壮大，但仍然不能满足实际需求，不能有效地保证信息系统的质量完全符合用户的要求。此外，信息系统的综合测评发展相对落后，相关参考标准规范还不够完善，相关测评技术研究还比较薄弱。

总体而言，信息系统测评日益受到重视，正在向着规范化、综合化和以业务应用为核

心的方向发展。信息系统并非可以直接使用的静态产品，而是一种需要与运行环境相互协调、具有动态特征的特殊产品，其质量不仅依赖于软件程序的质量，还依赖于运行环境的质量。因此，应从系统工程的高度对信息系统进行全方位的测评，这样才能从根本上发现各种功能缺陷、性能瓶颈和安全隐患，以完善信息系统的功能状况，提高信息系统的性能表现和加强信息系统的安全水平。这就需要测评人员具备综合素质，不仅要懂功能测评，而更要懂性能测评和安全测评及整体测评。只有融会贯通众多领域的知识，才能做好信息系统测评工作。

三、信息系统测评的目的

低成本、高质量的信息系统是信息产业的服务目标之一。由于信息系统产品的独特性，其质量问题难以避免，因此积极有效地开展信息系统测评变得十分重要。信息系统的开发与部署过程存在多种实现风险，如输出结果错误、系统不够可靠、处理过程不符合组织原则或政府规定、安全水平达不到标准、系统易用性差和所提供服务令人不满意等，这些潜在风险都会影响信息系统的质量，并给用户带来损失。

随着信息系统实现过程的推进，排除质量问题的成本越来越高，越是在实现过程后期发现的质量问题，其修复成本越高。此处的修复成本包括四个方面：①造成质量问题的费用；②发现质量问题的费用；③解决质量问题并添加正确规格说明、代码和文档的费用；④重新检测以确认修改后信息系统正确性的费用。正确的应对策略是将测评融入信息系统实现过程的每个阶段，而不是将其作为一个单独环节执行。遵循“尽早测评”的原则能够在信息系统交付之前解决大量的质量问题，研究表明近 2/3 的信息系统质量问题出现于设计和开发阶段，说明如果不能在设计和开发阶段进行测评，将有近 2/3 的质量问题隐藏于交付的信息系统中。因此，测评活动需要覆盖信息系统生命周期的各个阶段。在需求分析阶段，重点是确认需求定义是否符合用户的要求；在设计和编码阶段，重点是确定设计和编码是否符合需求定义；在测试和安装阶段，重点是审查信息系统的运行是否符合需求规格说明；在运营维护阶段，重点是做好需求、代码和系统版本的变更控制，针对实施的变更行为重新测评信息系统，以确定更改和未更改的部分都能正常工作。

信息系统测评是信息系统质量保证过程的重要组成部分，一个完备的测评方案能够为信息系统的正常上线提供有效的保障。重视信息系统测评，是信息系统开发者和使用者都不能忽视的工作。为了确保信息系统能够满足用户的需求，必须选择合适的测评策略，对用户需求进行全面的分析和正确的理解，对信息系统开展适度的测评。研究测评策略的目的是找到一种费用效益比率合理的测评方法，指导测评过程的执行，在可以接受的成本范围内达到信息系统的质量要求。

信息系统的质量问题无法彻底消除，信息系统测评也不可能永远进行。由于信息系统内部结构的复杂性，只有进行枚举测评，才能发现信息系统的全部质量问题。从经济学角度而言，信息系统测评的目的是以最少的人力、物力和时间找出信息系统潜在的质量问题，通过修正质量问题将实现过程中可能引起损失的风险减小到可以接受的程度，从而回避信息系统发布后由质量问题而带来的商业隐患和风险。风险的概念确定了信息系统存在的质量问题是否可以接受，经济学的考量决定了需要完成的测评类型和测评次数。确定测评的好坏不是由系统分析员或程序员决定，而是由商业的经济利益决定。

从功用角度而言，信息系统测评的目的是检验信息系统的功能、性能和安全性与用户

需求的符合程度，以便向用户提交一个高质量的信息系统。通过运用各种测评方法和技术，信息系统测评检验信息系统是否满足其研制任务书、需求规格说明或设计等文档中规定的接口、功能、性能及安全性等要求，以发现信息系统存在的问题。

因此，如何在有限的条件（如人力成本、时间资源、经费支撑等）下开展信息系统测评以发现潜在的问题，最大限度地保证信息系统的质量，成为信息系统测评方法和技术不断发展的源动力。在测评过程中，综合考虑开发情况、运行环境等诸多因素，有针对性地选择合适的测评工具开展自动化或半自动化测评，可以进一步提升信息系统测评的效率和质量。研发信息系统测评的程序与工具、建立信息系统测评的规范与标准、形成信息系统测评的理念与方法既是信息系统测评的主要任务，也是信息系统测评的目的之一。

第二节　电力信息系统测评概述

电力信息系统是专门用于电力企业各级部门之间，实现业务运维信息收集与处理、办公管理信息流动与共享、电力生产与运维科学决策的信息系统。电力企业引入了大量的电力信息系统。这些电力信息系统部署于电力企业不同安全级别的部门，涉及电力工业控制、电网信息通信、企业资源管理等众多业务领域。对这些电力信息系统开展全方位的测评，是确保电力安全稳定和高效运行不可或缺的一项工作。

一、电力行业信息化发展现状

我国电力行业的信息化可以追溯到20世纪60年代。最初的电力行业信息化也是电子计算机应用的起步阶段，当时的计算机体积大、价格昂贵，主要用于电力工程设计与验证、科研实验与计算等方面。20世纪80年代后期，计算机和信息系统在各行各业的推广应用，其在电力行业得到了快速发展，典型的领域有电力负荷预测、计算机辅助设计、计算机仿真实验、电力系统调度自动化、电力系统数据采集与监控等。近年来，随着互联网的快速发展和电力改革的逐步深入，电力企业将信息化由操作层向管理层扩展，特点是从单机、单项目逐步向网络化、综合应用发展。在“十一五”规划期间，信息化建设被纳入电力行业总体发展战略，进一步与电力企业的生产、经营和管理相融合。电力行业信息化的应用条件逐步完善，主要表现在以下方面：①电力行业信息化的基础设施日渐完善；②电力企业管理的方式逐步现代化；③电力系统信息化的趋势初步显现；④电力规划与设计数字化的趋势已经呈现；⑤发电效率不断提高。

（一）国外电力行业信息化的发展现状

随着电力行业信息化的不断发展，电力信息资源开发利用取得了很大进展，数字化和网络化的信息资源总量有了明显提高。国外许多大型电力企业在开展信息系统建设的同时，建立了设备管理和综合查询等业务基础数据库，实现了业务数据的统计报表和挖掘分析功能，电力生产与经营的历史数据得到了统一管理和有效利用。一些发达国家（如美国、德国、英国和法国等）的电力行业信息化水平代表着世界电力行业的发展状况。美国电力行业的基础网络、自动化系统、管理信息系统和信息系统测评处于世界领先水平，绝大多数电力企业已采用信息系统，并且实现了电网分析系统和信息系统的完全集成。德国通过改变不适应电力市场竞争的传统经营模式，全面升级改造电力企业的信息系统，部署能够提高管理效率的电力自动化系统，其电力信息系统建设也走在了世界前列。

（二）国内电力行业信息化的发展现状

我国的电力信息化虽然起步较晚，但是发展很快，尤其在电力行业改制后，借助我国信息化和互联网的发展潮流，迅速开启电力行业信息化的建设工作，成为电力行业发展的重要推动力量。我国电力行业信息化的发展主要体现在以下两个方面：

（1）信息通信技术不断完善。信息与通信技术是信息化的关键，通信方式在一定程度上决定着信息化的程度。我国的电力通信传输，在20世纪70年代采用电力线载波，当时仅应用于继电保护等少数领域；在20世纪80年代采用模拟微波；在20世纪90年代采用数字微波，逐渐应用到调度通信、通话、数据传输等方面。近年来，以光纤为代表的数字传输方式得到了快速推广应用，形成了以光纤和数字微波传输为主，卫星、电缆、无线电等多种通信方式并存的通信系统，覆盖了全国多数省市，电力专用通信网已经建成并初具规模。

（2）信息化应用程度不断提高。电力行业信息化主要分为两类应用：电力生产控制和电力企业管理。电力生产控制主要是指实现电力企业生产调度的自动化。电力企业管理主要是指实现管理信息系统、企业资源规划、企业资产管理、自动作图、设备管理、地理信息系统、电能计量、电力营销系统等电力业务系统的数字化管理。两个领域的信息化普及程度越来越高，在很大程度上提高了电力企业的生产效率。例如，国家电网公司实施的“SG186”工程，是电力行业信息化建设新时期的重要事件，充分体现了我国电力行业信息化建设取得的巨大进步。

目前，我国电力行业信息化建设已经具备一定的规模，并取得了一定的经济效益和社会效益。但是，与上述国家相比，我国还需要在提高管理效率、降低成本和适应市场变化等方面进一步提升电力行业信息化的发展水平。随着经济市场化和全球化的深入，电力企业面临着更多的机遇和挑战，这就要求电力企业通过信息系统整合企业业务、强化企业管理来提高自身竞争力，以更好地适应电力未来发展潮流。

（三）我国电力行业信息化的不足

我国电力行业投入运行的众多信息系统虽然发挥了巨大作用，但是仍然存在许多不足，主要表现在以下四个方面：

（1）标准制定相对落后。我国有关电力信息化的标准还比较少，极大制约了电力信息与电力设备的优化发展，导致信息系统质量下降。

（2）信息录入效率低下。许多电力企业的信息录入仍然依靠人工方式，录入时间长、及时性差。

（3）信息格式不够规范。电力信息系统的数据格式不统一，电力数据的完备性差，造成很多电力数据缺失、无效。

（4）信息不唯一。不同信息系统之间缺乏联系，没有形成电力信息系统的闭环系统，造成电力信息的不唯一。

为了解决上述问题，促进我国电力行业信息化的健康发展，可以采取以下措施：

（1）制定统一的电力行业信息化标准。参照当前国际成熟的信息技术标准，建立符合我国电力企业实际情况的信息化标准，包含统一的数据编码格式、软件标准体系架构、电力业务标准和信息网络测评标准等，既能规范我国电力企业信息化的建设，又能通过测评保障我国电力信息基础设施的质量。

（2）建立统一的电力信息系统平台。建立统一的平台是解决信息孤岛、软件兼容和业务沟通等问题的有效方法，应以 SG-ERP 系统建设为契机，整合现有电力信息系统，尽早实现电力企业的数据集中管理、业务操作规范和电力服务一体化。

（3）形成健全的电力信息测评服务体系。通过深入研究电力信息网络的功能、性能和安全测评关键技术，全面掌握电力相关标准规范的内涵，在进一步提高电力企业测评人员专业素质的同时，形成完善的电力信息网络测评服务体系，为电力安全生产和稳定运营提供全方位的支撑。

二、电力信息系统的部署架构

比较重要的电力信息系统包括监控与数据采集/能量管理系统（supervisory control and data acquisition/energy management system，SCADA/EMS）、配电自动化系统（distribution automation system，DAS）、配电管理系统（distribution management system，DMS）、调度管理信息系统（dispatch management information system，DMIS）、管理信息系统（management information system，MIS）和办公自动化系统（office automation system，OAS）等。SCADA/EMS 主要负责对发电厂、变电站及输配电线路的电力生产和运行情况进行实时监控、分析与处理，为电网调度提供决策依据；DMIS 主要负责对电网的调度运行、继电保护、电网通信、运行记录等进行半实时化管理，为调度和管理提供及时、准确的决策信息；MIS 主要负责电力企业的信息管理和决策支持等；OAS 主要负责电力企业的网上办公自动化。电力系统的特点决定了 SCADA/EMS 的安全等级最高，其次是 DMIS、MIS 和 OAS。为此，必须针对各自特点采取相应的安全技术，通过综合设计解决其信息网络安全。

（一）电力信息系统的体系架构

目前，我国多数电力企业已经建立能够实现生产设备管理、电网实时监控、安全监察管理、营销业务管理、计划统计管理、人事劳资管理、办公自动化、综合指标查询、科技教育管理和电子邮件服务等功能的信息系统。这些信息系统需要遵循如图 1-1 所示体系架构。

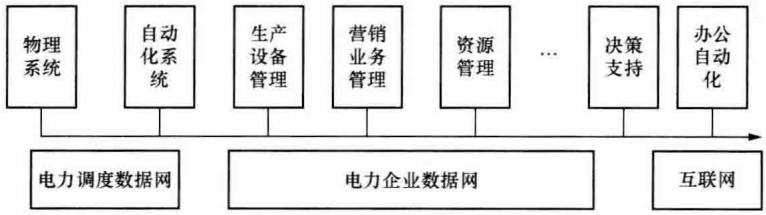


图 1-1　电力信息系统的体系架构

目前，我国电力系统采用专用网络和公共网络相结合的体系构架。其中，电力调度数据网（SPDnet）和电力企业数据网（SPnet）是电力专用网络，在保证信息网络安全的前提下与互联网连接。为了保障电力系统的安全，根据电力系统各个部分对安全的要求程度不同，将电力系统划分为三层四区。按照所实现的功能，电力信息系统可以划分为三层：第一层是自动化系统，第二层是生产管理系统，第三层是管理信息系统和办公自动化系统。将三层功能与电力系统体系架构对应起来，产生四个安全工作区域：安全区Ⅰ——SPDnet 支撑的自动化系统，凡是具有实时监控功能的系统或其中的监控功能部分均属于该区，如调度自动化系统、相量同步测量系统、配电自动化系统、变电站自动化系统、发电厂自动

监控系统等，是电力系统安全防护的重点；安全区Ⅱ——SPDnet 支撑的生产管理系统，原则上不具备控制功能的生产业务系统和批发交易业务系统属于该区，如水调自动化系统、电能量计量系统、发电侧电力市场交易系统等；安全区Ⅲ——SPnet 支撑的生产管理系统，如调度生产管理系统、雷电检测系统、气象信息接入和客户服务等；安全区Ⅳ——SPnet 支撑的电力信息管理系统，如 MIS 和 OAS 等。电力信息网络的体系结构体现了以下安全策略：

（1）分区防护。根据系统中业务的重要性和对一次系统的影响程度，将电力系统划分为四个安全工作区，重点保护位于安全区Ⅰ中的实时监控系统和安全区Ⅱ中的电力交易系统。

（2）网络专用。SPDnet 与 SPnet 通过正向型和反向型专用安全隔离装置实现（接近于）物理隔离，SPDnet 提供两个相互逻辑隔离的 MPLS-VPN 分别与安全区Ⅰ和安全区Ⅱ进行通信。

（3）横向隔离。安全区Ⅰ和安全区Ⅱ之间采用逻辑隔离，隔离设备为防火墙；安全区Ⅰ、安全区Ⅱ与安全区Ⅲ、安全区Ⅳ之间实现（接近于）物理隔离，隔离设备为正向型和反向型专用安全隔离装置。

（4）纵向认证。安全区Ⅰ和安全区Ⅱ的纵向边界部署具有认证、加密功能的安全网关（IP 认证加密装置）；安全区Ⅲ和安全区Ⅳ的纵向边界部署硬件防火墙。

（二）电力安全隔离技术

电力系统的信息网络相对互联网而言是一个内部网络。内部网络的安全防护措施主要为防火墙、入侵检测系统等被动防护方式，而主动防护主要是采用安全隔离等方式。实现安全隔离的技术主要有物理隔离技术、协议隔离技术和防火墙技术等。图 1-2 所示为一种安全隔离装置的示意图。该隔离设备含有两个接口计算机，且均采用经过安全加固的操作系统，剔除了所有常规的网络功能。接口计算机 A、B 分别负责与实时系统和非实时系统连接，其中接口计算机 A 是实时网络中的一个节点，接口计算机 B 是非实时网络中的一个节点，接口机 A、B 之间不采用标准网络物理连接，而是采用高速数据总线（如并行端口、USB 端口、SCSI 端口或双端口 RAM 等）互连，从而保证了物理层的网络安全。

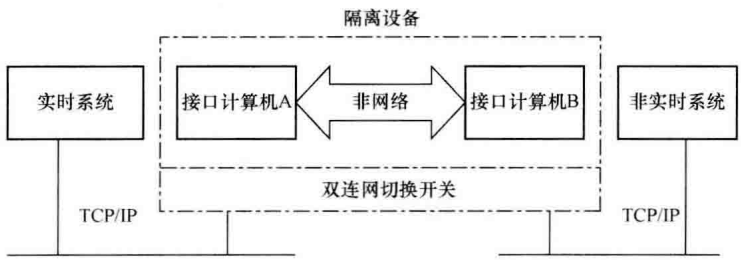


图 1-2　安全隔离装置及网络连接

1. 物理隔离技术

物理隔离是指在物理意义上将内部网与外部网分离，使两者之间无法通过直接或间接（包括防火墙或代理服务器等）的方式连接，是防范计算机病毒、黑客入侵和拒绝服务攻击等安全威胁的有效手段。电力系统的安全区Ⅰ、安全区Ⅱ与安全区Ⅲ、安全区Ⅳ之间采用物理隔离以保证安全性。物理隔离为内部网划定了明确的安全边界，使网络的可控性增强。

物理隔离可以有效地保障外部网不能通过网络连接侵入内部网，同时防止内部网信息通过网络连接泄露至外部网。

物理隔离技术可以分为两类：时间隔离系统和安装于联网机器上的网络安全隔离卡。时间隔离系统通过转换器在内部网和外部网之间频繁切换，实现内部网和外部网之间的通信要求。时间隔离系统主要包括专用物理隔离切换装置、数据暂存区等，采用防火墙、基于内核的入侵检测、安全操作系统、离线邮件转发、智能离线浏览及病毒扫描与清除等技术，组成内部网与外部网之间的数据交换安全通道。网络安全隔离卡的功能是以物理方式将一台机器虚拟为两台机器，并实现公共与安全两种完全隔离的状态，从而使一台机器可以在安全的情况下连接内部网与外部网。对应于两种状态，硬盘从物理上划分为安全和公共区两个分区。在网络安全隔离卡的控制下，安全状态时，机器只能使用安全区与内部网连接，此时外部网连接是断开的，且硬盘公共区的通道是封闭的；公共状态时，机器只能使用硬盘的公共区与外部网连接，而此时与内部网是断开的，且硬盘安全区也是封闭的。通过这种方式，网络安全隔离卡实现了内部网与外部网的物理隔离。

2. 协议隔离技术

协议隔离技术是指在内部网与外部网的连接端点处，配置协议隔离器来隔离内部网与外部网。协议隔离器使用两台不同设备上的通用网络接口分别连接内部网与外部网，而设备之间通过使用专用密码通信协议的接口卡进行互连。通常情况下，内部网与外部网是断开的，只有当交换信息时，内部网与外部网才会通过协议隔离器连通。

3. 防火墙技术

防火墙是设置于被保护网络和外部网之间的一道屏障，以防止发生不可预测的破坏性侵入。防火墙通过检测、限制或者修改穿越防火墙的数据流，尽可能地对外部网屏蔽内部网的信息、结构和运行状况，以实现网络的安全保护。防火墙技术在电力信息系统安全设计中，主要起逻辑隔离的作用。通过设置防火墙相关参数，可以实现数据包过滤、应用级网关和代理服务等安全功能。数据包过滤是指在网络层对数据包进行选择，选择的依据是在其内设置过滤逻辑，通过检查数据流中每个数据包的源地址、目的地址、所用端口号、协议状态等属性确定是否允许该数据包通过。应用级网关是在应用层上建立协议过滤和转发功能。它针对网络应用服务协议，使用指定的过滤逻辑对数据包进行分析、登记和过滤并形成报告。代理服务是将所有穿越防火墙的网络通信链路分成两段。防火墙内部网与外部网之间的应用层“链接”由两个代理服务器的“链接”实现，外部网的链路只能到达代理服务器，从而起到隔离内部网和外部网的作用。

4. 虚拟专用网和虚拟局域网技术

为了实现不同应用系统之间信息的隔离，在电力信息安全体系结构中可以采用虚拟专用网（virtual private network，VPN）或虚拟局域网（virtual local area network，VLAN）技术。虚拟专用网的核心是采用隧道、信息加密、用户认证和访问控制等技术，通过 L2TP、IPSec 等协议和密码技术的处理，将各个子网的数据加密封装后，通过虚拟的网络隧道进行传输，从而防止敏感数据的泄密，也可以通过在同一设备上采用多个虚拟路由器实现虚拟专用网。

虚拟局域网是按照网络用户的性质和需求而非所在物理位置，将其划分成若干个“逻辑工作组”，每个“逻辑工作组”称为一个虚拟局域网。同一虚拟局域网中的所有用户共享