

提高核电站安全可靠性的平行系统方法

熊 刚¹, 王飞跃¹, 侯家琛¹, 董西松¹, 张家麟², 付满昌³

(1. 中国科学院 自动化研究所 复杂系统管理与控制国家重点实验室 北京市智能化技术与系统工程技术研究中心, 北京 100190; 2. 核工业第二研究设计院, 北京 100840; 3. 国核自仪系统工程有限公司, 上海 200233)

摘要 安全可靠性是核电站存在和发展的生命线, 目前它还主要是通过人的经验和严格管理等来保证, 但其智能性和科学性还不够。核电站是一个涉及多方面的动态变化要素的复杂系统, 现有控制、仿真和管理技术还不能为其生产运行和管理提供安全可靠的充分保证。本文以 ACP 方法为基础, 基于信息技术最新发展成果, 提出了采用自上而下的规划和自下而上的设计相结合的方法, 来开发“核电站可靠性规划和设计软件包”, 使得核电站在建造前就有了安全可靠方面的科学依据。进而提出平行系统方法, 分析其基本原理和成功应用实例, 并介绍其在核电站中应用的人工系统、计算试验和平行执行的具体内容, 给出了 PTS、PES 和 PMS 等具体应用。

关键词 核电站; 安全可靠; ACP 方法; 人工系统; 计算实验; 平行系统

To improve safety and reliability of nuclear power plant with parallel system method

XIONG Gang¹, WANG Fei-yue¹, HOU Jia-chen¹, DONG Xi-song¹, ZHANG Jia-lin², FU Man-chang³

(1. State Key Laboratory of Management and Control for Complex Systems, Beijing Engineering Research Center of Intelligent Systems and Technology, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China;
2. Beijing Institute of Nuclear Engineering, Beijing 100840, China;
3. State Nuclear Power Automation System Engineering Company (SNPAS), Shanghai 200233, China)

Abstract The safety and reliability is the soul of nuclear power plant. Until now, it is still not smart and reasonable enough because it is assured by strict management and human experience and knowledge. Nuclear power system is a typical complex system consisting of many dynamic factors, and the conventional control, simulation and management technology can't assure its operation and management. Based on ACP approach, using the latest IT technology, “soft package of reliability planning and design of nuclear power plants” is proposed where “top-down” plan method is combined with “bottom-up” design method to assure the safety and reliability. Then, parallel system method is proposed. The main content includes: The basic principal and successful application; artificial systems, computing experiments, and parallel execution methods used in nuclear power system; PTS, PES and PMS.

Keywords nuclear power plant; safety and reliability; ACP approach; artificial systems; computing experiments; parallel system

1 引言

在 2009 年哥本哈根气候变化会议上, 减少碳排放已成为世界绝大多数国家的共识。核电, 作为节能减排与可持续发展能源的最佳选择之一, 未来必将得到更大的发展。核电站只需消耗很少的核燃料, 就可以产生大量的电能。例如, 一座 100 万千瓦的火电站每年耗煤三四百万吨, 而相同功率的核电站每年仅需铀燃料三四十吨。发展核电是加快经济发展方式转变的重要举措。核电站的建设和运营, 涉及材料、冶金、化工、机械、建筑、电子、仪器制造、信息技术等众多行业, 发展核电, 可以有效地带动基础研究、系统集成、装备制造、工程管理等能力的提升, 有利于战略性新兴产业的蓬勃发展, 进而推动国民经济各行业的发展方式向依靠科

收稿日期: 2011-09-26

资助项目: 国家自然科学基金 (61174172, 70890084, 60921061, 90920305)

作者简介: 熊刚 (1969-), 男, 博士, 研究员, 北京市智能化技术与系统工程技术研究中心副主任, 研究方向: 复杂系统的智能控制、流程工业综合自动化、平行系统、企业信息化与智能化等。

技进步、劳动者素质提高和管理创新的方向转变。据国际原子能机构 (IAEA) 统计, 截至 2010 年初, 世界运行中的核电机组共计 437 台, 装机总容量约为 371 GW(e); 在建 56 台, 装机约为 52GW(e); 2030 年, 装机将达 807GW(e)。目前, 美国、印度等国均提出了中长期核电发展目标和计划。中国有 6 个核电站的 13 台在役核电机组, 核电装机容量达到 11 GW(e)(见图 1), 与相同规模的火电相比, 相当于每年少排放二氧化碳 6700 万吨、二氧化硫 25 万吨、氮氧化物 15 万吨。“十二五”期间, 我国面临的改善能源结构和应对气候变化的任务更为艰巨, 发展核电将成为促进节能减排和推进生态文明建设的重要力量。中国已经成为世界上在役核电机组最多的国家。国家能源局的数据显示: 我国核电在建 23 台, 占世界在建 57 台机组的 40%, 国内核电已经步入建设发展的加速期。因此, 我国核电技术的自主研发已变得越来越重要, 如何保证核电站的安全、可靠是核电可持续化存在与发展的重中之重。



图 1 中国核电站分布图 (来自于互联网)

从 1954 年前苏联建成世界上第一座试验核电站、1957 年美国建成世界上第一座商用核电站开始, 核电产业已经过了几十年的发展, 核电技术到现在也已经发展到了第三代。一般来讲, 第一代核电是指从当年的军用堆转为和平利用原子能; 第二代核电是指专门针对民用核发电而设计的核电站, 现在世界上多数的核电站都可以说是第二代; 第三代核电技术如美国西屋的 AP1000 或者法国阿海珐的 EPR, 他们可以大大提高核电站的安全性, 能够做到非能动的安全保障等等; 2000 年开始研发的第四代核电站, 其高温气冷堆、钠冷却堆的安全性和经济性更优越, 废物量极少, 无需厂外应急, 并具备固有的防止核扩散能力, 给核电自动化提出了新挑战。

我国在核能技术研发和核电的利用方面已经积累了几十年的经验。目前, 我国正在引进以西屋公司 AP1000 和法国 EPR 为代表的第三代核电技术, 其中包括仪控系统和保护系统等。中国的核电事业正处在一个即将腾飞的时期, 从 1984 年秦山一期 30 万千瓦核电站的开工建设到如今第三代全数字化百万千瓦级大型压水堆核电站的引进, 中国的核电事业迎来了一个崭新的时期^[1]。在《国务院关于加快培育和发展战略性新兴产业的决定》中, 把发展核电放到了新能源产业的首要位置。《国家“十二五”规划纲要》也明确提出, “在确保安全的基础上高效发展核电”。政府相关部门在 2010 年已经着手对《国家核电中长期发展规划》进行调整。未来 5~10 年, 我国新建核电机组将以每年 5~8 台的速度递增, 成为世界核电发展的火车头。2015 年, 我国核电装机容量将达 40 GW(e), 到 2020 年, 则可能达到 100 GW(e), 占全国电力装机容量的 5%, 发电量的 8%。

安全是核电站最重要的问题, 核泄漏事故是核电站的噩梦。广岛和长崎首先让世人见识到核弹的巨大威

力, 而切尔诺贝利的核灾难, 又让更多人的眉头紧锁, 核泄漏事故后产生的放射污染相当于日本广岛原子弹爆炸产生的放射污染的 100 倍, 8 吨多强辐射物质泄露, 辐射危害严重, 导致事故后前 3 个月内有 31 人死亡, 850 万受到或多或少的辐射, 之后 15 年内有 6~8 万人死亡, 13.4 万人遭受各种程度的辐射疾病折磨, 有 15.5 万平方公里的土地面积遭受放射污染, 40.4 万人被迫迁居, 放射危险将持续 10 万年, 经济损失近 2000 亿美元。近的有 2010 年的广东大亚湾核电站发生核泄漏事故和 2011 年日本福岛核电站因地震引起的泄露事故。尤其是日本福岛核电站的泄露事故引起了全球的反核浪潮, 多国计划停建或缓建核电站, 德国等一些国家甚至计划关闭所有核电站。作为世界上核电建设发展最为迅速的中国, 对核电站的安全问题更值得关注与深入研究。

但核电站的安全问题不仅设计到核电站的规划、设计、选址、建设等工程方面的问题, 更涉及到管理、人为、恐怖活动等社会因素, 以及地震、火灾等自然因素, 传统的理论建模方法难以对其进行研究; 而因道德、经济或安全方面的因素, 传统的实验手段也很难进行(如切尔诺贝利核电站爆炸的直接原因就是因为进行极限实验)。研究核电站安全需要新的系统理论和新的方法。

平行系统(ACP 方法)采用整体论的观点考虑复杂系统的问题, 在传统控制系统基础上, 充分考虑了对社会性和人为要素的控制功能, 提高了认识复杂系统要素相互作用的动态演化规律的能力, 提高了控制复杂系统对象应对变化和非正常状态的能力。本文以 ACP 方法为基础, 基于信息技术最新发展成果, 提出开发“核电站可靠性规划和设计软件包”, 以核电站仪控系统和保护系统为主要对象, 为核电站安全可靠的设计和生产提供先进的方法, 为核电技术国产化提供新的思路。

本文剩余部分主要内容如下, 第 2 节介绍核电站安全的现状分析及应对策略; 第 3 节从系统预选、详细设计、方案评估等几方面介绍核电站可靠性规划和设计; 第 4 节对平行系统(ACP)方法的原理、特性、应用进行分析; 第 5 节以 ACP 理论为基础分析了提高核电站安全可靠性的平行系统方法, PTS、PES、PMS 三个组成部分及具体功能; 最后对全文进行了总结。

2 核电站安全的现状分析及应对策略

安全可靠是核电站绝对的第一目标。目前, 核电领域制定了数百个国家级和国际性法规和标准^[2]。核电站设计也要遵循不少原则, 比如单一事故准则、多重性(冗余性)准则、多样性准则、独立性准则、事故安全设计准则、避免共因事故准则、可试验性和可维修性准则、设备停役准则等。但对于第三代核电站的典型代表 AP1000^[3] 和 EPR 来讲, 它们的设计、建造和运行管理并不是尽善尽美的, 比如: 它们确保安全可靠的手段主要还要依靠经验制定更严格的管理、标准、法规、设计方法等来保证, 因此其智能性和科学严谨性还不够。很多安全、可靠性参数是人为估计出来的, 并不严密。此外, 严格的管理和数百个相关标准和法规, 也都是靠人来制定和实施, 难以定量的论证其科学性。核电站的国产化设计和运行控制需要创新的思想。

“理论研究”和“科学实验”是传统科学研究的两种手段, 随着计算机和信息技术的发展, “计算技术”正在成为第三种手段, 相关建模和仿真技术正在被越来越广泛地接受并应用。本文提出的核电站创新设计和运行控制的核心思想, 主要就是将上述三种手段综合利用。

随着科技进步, 系统设备(硬件和软件)可靠性的不断提高, 核电站运行环境得以逐步改善。但作为核电站人—机系统极其重要的“人”的因素, 仍然是导致事故发生的主要根源。一方面, 由于其生理、心理、社会、精神等特性, 存在一些内在弱点, 使其行为具有多样性和可塑性以及难以控制性; 另一方面, 尽管系统的自动化程度提高了, 但归根结底还要由人来控制操作, 要由人来设计、制造、组织、管理、维修、训练, 要由人来决策, 因而人在系统中的作用不是削弱了, 而是更加重要和突出了。人贯穿于核电站整个寿命周期, 它影响着核电站安全的各个方面, 正如 IAEA 在《安全文化》中所指出的: “除了人们往往称之为‘上帝的旨意’以外, 核电站发生的任何问题在某种程度上都来源于人因失误(human error)”。导致人因事件的原因有几种: 一是工作条件设计不当引起的; 二是由于人的不安全行为造成的; 三是恐怖活动等故意破坏行为。

针对核电站内外部要素间错综复杂关系及必须实现的安全可靠目标, 本文提出的应对策略包括: 1) 在核电站设计阶段, 采用自上而下的规划和自下而上的设计相结合的方法, 开发出包括跨时间和空间的数据、模型和经验的“核电站可靠性规划和设计软件包”, 使得核电站在建造前就有了安全可靠性计算结果作为科学依据; 2) 在核电站运行阶段, 在现有仪控系统和保护系统基础上, 采用 ACP 方法开发相关的平行系统, 来促使核电站更智能化地适应内外部各种变化, 更准确地预测和预防各种危险, 从而进一步提高和保证核电站的

安全可靠性; 3) 在工程因素之外, 充分考虑人为等社会因素对核电安全的影响.

3 核电站可靠性规划和设计

以核电站仪控系统为例, 其设计、研制的许多方面, 都已经运用到高可靠、高利用率、高抗干涉和高抗破坏等方面的经验. 各种特定类型核电站中所使用的仪表、仪器、控制和保护系统间, 共性多于差异.

我国著名科学家钱学森说过, “产品的可靠性是设计出来的, 生产出来的, 管理出来的”, 这一思想, 越来越为人们所理解. 世界各国开展的可靠性工作经验证明, 可靠性设计对产品可靠性有重要影响. 据日本电子行业的统计, 产品不可靠的原因中, 设计占 80%, 元器件占 15%, 制造工艺占 5%^[4]. 又据美国海军电子实验室统计, 产品不可靠的原因中, 设计占 40%, 元器件占 30%, 使用和维护占 20%, 制造占 10%^[5].

过去, 在设计人员中曾流行的思想和看法是: “产品性能好则说明其质量好”、“生产出符合规定性能要求的产品就说明产品符合质量要求”. 现在, 单纯追求性能的观点已经越来越不适合, 而对产品的可靠性、维修性以及寿命周期费用的关注程度必将会越来越高.

对于决定核电站存亡的安全可靠性来讲, 在设计阶段就必须科学规划和设计. 实现可靠性设计与分析的目的和任务, 就是使性能设计和可靠性设计能有机地结合, 在设计思想上应有一个转变, 要从单一追求性能, 到抓综合效能的变革. 这里给出可靠性规划和设计中的“系统效能”的概念, 它就是系统在规定的条件下满足给定定量特征和服务要求的能力. 它是系统可用性、可信性及固有能力的综合反映, 一般可用如下公式表示:

$$E = A * D * C$$

式中: E- 系统效能; A- 可用性; D- 可信性; C- 固有能力; 这里所说的“可用性 (A)” 表示战备完好, 也就是系统在任一随机时刻需要开始执行任务时, 处于工作或可使用状态的程度, 即某系统“开则能动”的程度.“可信性 (D)” 表示任务成功, 是指系统在任务开始时可用性给定的情况下, 在规定的任务剖面中的任一随机时刻, 能够使用且能完成规定功能的能力, 即某系统“动则成功”的程度. 固有能力指的是不考虑可靠性和可用性的情况下, 特定系统所能完成特定的任务的能力. “效能 (E)” 和“可靠性 (R)”、“维修性 (M)”之间的关系可用图 2 表示. 可见, “可用性 (A)” 和“可信性 (D)” 均为“可靠性 (R)” 和“维修性 (M)” 的函数, 因此, “效能 (E)” 为 R、M、C 的函数即: E: f(R, M, C)^[6].

核电站可靠性规划和设计方法, 简单论述如下:

3.1 系统结构预选

在初步设计阶段, 主要确定核电站的结构时, 是进行可靠性设计工作最有效的时间节点. 在此期间, 可靠性的考虑会影响到设计的决策, 并且可以保证所选定的结构一定能发展成满足可靠性要求的核电站结构. 这是一个递进的过程, 通过不断地寻找和尝试不同的系统结构, 直到所有的约束都满足为止. 可靠性的考虑并不是设计中所要求的唯一约束. 其它的约束, 包括容量、尺寸、形状、重量、价格和进度等, 全部必须充分地满足. 可靠性分析提供一个有纪律的框架, 在这个框架下就能够更好的研究满足其他各种制约因素. 这样做的结果是, 不仅得到了一个更可靠的系统, 而且从所有其它适用的准则看来也是一个比较好的系统.

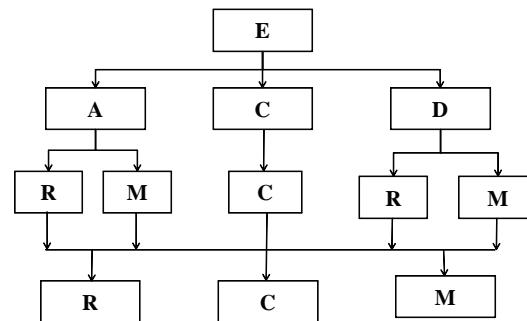


图 2 系统效能与可靠性、维修性的关系

3.2 可靠性方面的详细系统设计

从可靠性潜力评价中选出的或推荐的核电站设计方案，须进一步详细设计。要选用质量已知的部件，这些部件能在预定环境下及在其额定阈值内很好地工作。尽量用各种可能的方法去模拟模型，并确信满足相关性质的假定。如果模型能够假设，一个或一组部件元件的故障与其它元件的故障统计无关，那么设计者应该设法使其实现。例如假定两个检测仪表通道互相独立，那么它们应该这样定值，使得只是在极不可能的场地下两套才可能都失败。

简单而直接的系统是容易理解的，容易模拟，并且具有高的可靠性。如果没有取得最优的模型，就冒险去研制系统，那么系统可能变得如此复杂且杂乱无章，以致难以仿此制造。并且，从直观上看来，整个系统也是值得怀疑的。安全准则也决不会允许设计这种系统，因为这种系统不能简单化为易处理的可靠性模型。

简单地说，就是在普通的核电系统详细设计程序中要加上可靠性分析与设计的科目，其中可靠性系统设计的概念和相应的数学关系都不难理解。

3.3 设计方案评价

进行核电系统可靠性分析的主要价值，是确信某些普通部件是不会对不可靠性做出意外的和毫无根据的贡献。如果发现了这种问题，就可通过选用更好的部件，更纷繁和更全面的测试或合理的使用有冗余度的部件或模块来弥补这个缺陷。

基于上述核电站可靠性规划和设计思想和方法，就可以研发出“核电站可靠性规划和设计软件包”，它相当于计算机辅助设计 (CAD)、产品数据管理 (PDM) 和产品生命周期管理 (PLM) 之类的软件产品。同时，在经改造之后，它可成为之后平行系统中的人工系统部分。

4 平行系统方法介绍

平行系统，是指由某一个自然的实际系统和对应的一个或多个虚拟或理想的人工系统所组成的共同系统。实际上，经典的传递函数方法、状态空间方法，从最优控制理论，到参数识别和变结构自适应控制，特别是基于参考模型的自适应控制都可以看作是平行控制理论的早期的发展形式。现代控制理论是成功应用平行系统理念的典范，它首先建立实际系统足够精确的模型，然后分析其特性、预测其行为、控制其发展，然而，由各种数学模型形成的人工系统往往以离线、静态、辅助的形式应用于实际系统的控制。在 Fel'dbaum 提出对偶控制概念，参数或结构的自适应变化等控制思想后，人工系统的地位和作用有所突破，但在理念和规模上都未能改变人工系统的非主导地位。为此，国内学者几年前提出的平行系统框架（如图 3），为复杂系统的控制研究提供了一个全新的思路和视角^[7]。其最大特点就是要改变人工系统的非主导地位，使其角色从被动到主动、静态到动态、离线到在线，以至最后由从属地位提高到相等的地位，使人工系统在实际复杂系统的控制中充分地发挥作用^[7]。应用闭环控制原理，平行系统可以描述为如图 4 所示的双闭环控制系统。

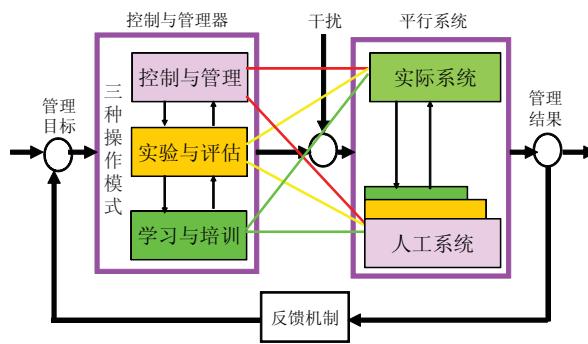


图 3 平行系统理框架

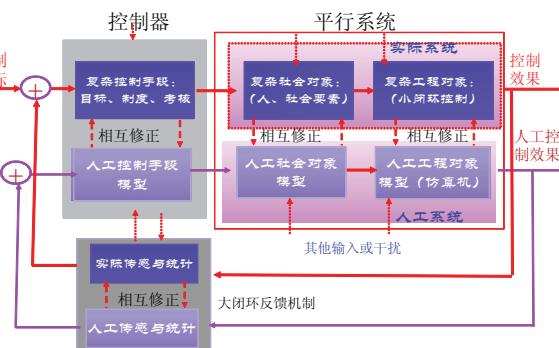


图 4 平行系统的双闭环控制原理图

平行系统理论框架下的 ACP 方法体系包括人工系统 (artificial systems)、计算实验 (computing experiments) 和平行执行 (parallel execution)，其基本原理和方法可以描述为：综合考虑多方面因素，采用智能体建模方法建立与实际系统“等价”的人工系统，解决实际系统难以建模的难题；在人工系统上通过计算实验或“试验”来认识实际系统各要素间正常和非正常状态下的演化规律和相互作用关系；通过二者的相互连接，对二者之间的行为进行对比和分析，研究对各自未来的状况的“借鉴”和“预估”，相应地调节各自的控制与

管理方式; 最后利用计算实验所认识的规律实现双闭环的并行执行: 正常情况下, 利用人工系统认识复杂系统千变万化规律, 帮助实际系统不断适应变化, 不断优化实际系统的控制和管理, 预测和预防非正常情况发生; 非正常情况下, 利用人工系统找到让实际系统迅速、最优化地恢复正常应急管理方法, 帮助正确地处理问题, 快速低成本地恢复正常, 减少损失。

平行系统的优势在于它符合了解决复杂问题必须遵循的思路:

1) 必须采用整体论的观点考虑复杂系统的问题。此类系统结构不明确, 边界不确定, 以往的系统分析方法往往难以刻画要素之间的相互关系。必须探索研究复杂系统的新途径, 比如基于人工系统的方法。

2) 复杂系统问题不存在“一劳永逸”的解决方案。此类系统涉及人与社会的动态变化, 问题本身也在不断变化和发展之中, 不可避免地需要一个不断深化的认识过程, 也导致了对这类系统不存在精确完备的整体解析模型。因此, 无法“一劳永逸”地解决系统的问题。需要基于“不断探索和改善”的原则, 建立有效可行的计算实验方法体系, 为不断地完善系统解决方案提供科学依据。

3) 复杂系统问题不存在一般意义上的最优解, 更不存在唯一的最优解。首先, 基于解析模型的最优解与假设条件直接相关, 往往具有较强的条件敏感性, 假设与实际状况的“失之毫厘”, 导致最终结果的“差之千里”。其次, 复杂系统问题一般不存在单一的优化指标, 而多层次、多目标的优化指标往往造成多个甚至无数个解决方案, 谁是最优解决方案难以判断。基于这种认识, 可以利用人工系统与实际系统并举的平行系统和方法, 追求具有动态适应能力的有效解决方案。按照“摸着石头过河”的方式, 一步步对复杂系统进行管理^[8]。

平行系统在传统控制系统基础上, 充分考虑了对社会性和人为要素的控制功能, 增加了人工系统和计算实验平台、平行执行平台等功能, 提高了认识复杂系统要素相互作用的动态演化规律的能力, 提高了控制复杂系统对象应对变化和非正常状态的能力, 对复杂科学和智能科学的理论创新具有重大科学意义, 对包括核电的各个领域的复杂系统应用实践具有非常重大的指导意义, 已经引起国内外的关注: 相关研究在 2007 年到 2012 年期间连续 6 年获得自然科学基金创新团队项目支持。相关研究成果“智能控制理论与方法的研究”, 于 2007 年度获得国家自然科学二等奖。2008 年的“控制科学与工程学科发展报告”对其进行了完整介绍。科技出版社 2009 出版的“创新 2050: 科学技术与中国的未来”系列丛书中, 多处论述到。2010 年 11 月份, 中国自动化学会平行控制与管理专业委员会正式成立。2009 年 12 月和 2010 年 12 月, 第一、第二届全国平行控制(管理)会议成功在北京举行^[9-14]。2011 年 8 月将举办第三届, 并计划以后每年举办一届。在具体应用方面: 2009 年 6 月, 平行系统成功在茂名乙烯上线使用, 科技时报做了相关报道, 到 2010 年 8 月, 累计产生效益超 1 亿元; 专家组鉴定认为“……整体技术达到国际先进水平”; 在 973 等项目资助下研发的平行交通控制与管理系统(PtMS), 成功应用到苏州公路的优化控制与管理, 专家组鉴定认为“具有原始创新性; 整体设计与部分技术达到国际领先水平; 具有重大应用价值”, 该成果先后获得 2009 IEEE Outstanding ITS Application Award 和 2010 IEEE ITS Institutional Lead Award; 2010 年, 针对上海世博会安全和广州亚运会公共交通研发了相关的平行系统。2011 年, 科技部和国家自然科学基金委在社会安全和复杂生产领域设立有 ACP 方法相关的项目。参照平行系统思想, 国内越来越多的单位和学者开始在社会演化和军事等领域的研究^[15-19]。总体来讲, 平行系统的研究与实践正处于从起步到快速发展阶段^[20]。

5 提高核电站安全可靠性的平行系统方法

基于上述理论和实践成果, 以提高核电站安全可靠性的平行控制与管理系统(PMS: parallel management system)为例(如图 5), 来介绍平行系统方法的具体应用。PMS 包括实际系统和人工系统两大部分。其中的实际系统主要是指目前核电站的仪控系统和保护系统等, 人工系统部分又包括人工系统 A、计算实验 C 和平行执行 P 三个子部分, 下面将逐一介绍。

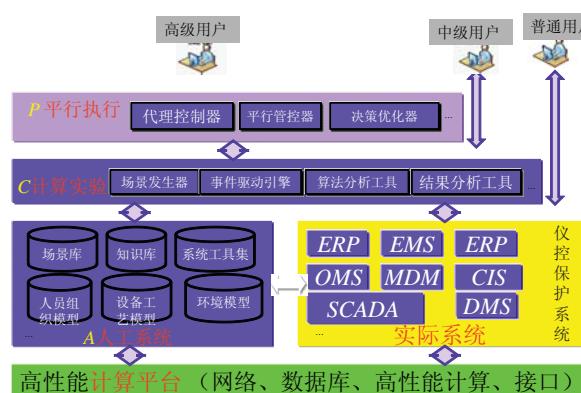


图 5 核电站的平行控制与管理系统 PMS

5.1 实际系统部分

以 AP1000 核电站的仪控系统和保护系统为例, 如图 5 右下部所示, 实际系统是指核电站现有系统, 主要包括运行与控制中心系统 (OCS)、数据显示和处理系统 (DDS)、保护和安全监测系统 (PMS)、反应堆紧急停堆系统 (RTS)、电厂控制系统 (PCS)、多样驱动系统 (DAS)、专用监测系统 (SMS)、堆芯设备系统 (IIS) 等, 仪控系统的软件平台是 Common Q, 保护系统的软件平台是 Ovation.

核电站的控制是通过仪控系统、保护系统等形成的“小闭环”来完成, 其安全可靠性可以得到较好的保证。核电站的管理应该是在“小闭环”之外, 再加入核电站管理和人员等形成的“大闭环”来完成, 以适应不断变化的社会环境和物理环境, 实现诸如安全、平稳、环保等多个目标。但是目前的核电站管理是靠人的经验制定严格标准和管理制度, 之后通过人去执行“大闭环”管理, 存在很多不足。比如:

- 1) 没有将人、管理和环境等各类复杂社会因素, 通过信息化手段去实现精确和实时的“大闭环”管理, 因此容易发生人员的误操作等;
- 2) 现有系统条件无法对各类可能发生的问题进行实验, 如许多正常环境下无法做的实验、潜在的问题、各类不可预测事件等;
- 3) 现有核电系统对各类控制方法及应急保护预案也缺乏科学的分析研究^[21].

事实上, 核电站的安全可靠运行控制和管理是一个难以解决的复杂系统多约束、多目标的动态优化问题。需要引入平行系统方法辅助实际系统并对其做出拓展, 以提高和确保核电站的安全可靠运行。

5.2 人工系统 (A)

人工系统构建是平行系统实现的基础。可以根据“简单的一致”原理, 从对简单核电站对象及其相互作用基本一致的认识出发, 充分考虑简单对象的主动性和随机性, 通过综合集成, 从行为生成的角度出发, 自下而上地对核电站涉及的各类要素进行建模。如对仪控系统及保护系统进行建模, 对操作人员及组织进行建模, 对各类场景进行建模等。建模方法包括代理 (agent)、复杂网络、语言动力学等。

之后, 就可以实现实际系统与人工系统的虚实交互。第一步的建模重点是核电系统结构的建模, 在结构合理前提下, 具体参数可以有一定偏差。通过对实际系统的学习, 可以渐进地减少这些差异。第二步主要就是人工系统对实际系统的学习, 既包括对原始数据离线的学习, 也包括对实时数据的在线学习。此时, 实际系统地位高于人工系统, 对人工系统具有指导作用, 实际系统对人工系统进行“生长”和“培育”; 人工系统则通过对实际系统的不断学习, 不断调整内部结构和参数, 递归地完善建模的精度及其效果。进而, 人工系统和实际系统通过接口协议进行连接, 实现虚实交互, 初步构建平行系统。必须说明的是, 人工系统对实际系统的学习并不追求对实际系统的重现, 而只是追求结构和功能的“等价”或“同构”。换句话说, 我们建立的并不是“一个”实际系统的仿真模型, 而是“一簇”可以成为现实的人工模型, 自然这“一簇”模型中应该包含实际系统模型。

人工系统最大的特点是充分考虑了人为的因素。从美国的“三里岛事故”到“切尔诺贝利事故”直至现在的福岛核泄漏事故, 其原因都不能排除“人为”因素。日本福岛核电站事故原因除“天灾”外, 其事故的主要原因出在运营管理上。核能技术的安全性虽然无懈可击, 但如果疏于管理, 同样会造成灾难。所以, 人工系统同时考虑工程复杂性和社会复杂性两个方面。

5.3 计算实验 (C)

在确信平行系统中人工系统能等价于实际系统之后, 就是从计算仿真到计算实验来验证各种可能和假设, 从而帮助我们分析人工系统的特征和行为。我们视人工系统为一个可控可重复的“实验室”, 可以系统地设计各种各样的试验, 引入各种不确定甚至传统上难以量化的因素和事件, 多次重复并以统计的方法对结果进行分析, 从而使传统的仿真变成系统性的实验, 进而实现对复杂过程系统的定量分析。值得注意的是, 在计算实验方法中, 传统的计算模拟变成了“计算实验室”的“试验”过程, 成为“生长培育”各类突发事件的手段, 而实际事件只是这个“计算实验”的一种可能结果而已。根据这一理解, 自然就可以利用计算模拟进行“计算实验”了。利用计算实验方法对人工核电系统进行各种“试验”, 对此复杂过程系统的行为进行预测和分析。如试验生产方案或制度、操作人员的典型行为对生产系统故障的影响、分析大幅度改变操作方案对操作人员和核电运维的影响、预测突发性或周期性的社会变化对系统的干扰、研究在“极限”、“失效”或“突变”条件下生产系统的行为、界定重大生产事故对企业和社会的冲击、以及对应的方案措施进行评估等。

在人工系统基础上, 通过计算模拟和涌现方法可以方便地“生长”各种核电站复杂现象, 产生和分析复

杂系统的行为, 进而建立计算实验的理论和方法, 以此克服难以对核电复杂系统进行实验的困难, 为深入分析复杂核电系统的行为和有效评估决策的效果奠定基础。通过各类事件驱动系统及场景发生器对各类场景及存在的问题进行计算实验, 如气候、地震等对核电站的影响, 仪控系统和保护系统的各类错误所能引发的潜在问题, 保护系统的实际执行, 人工操控所带来的问题等; 同时对各种方案进行评估分析, 从而找出最好的安全保护预案。

5.4 平行执行 (P)

利用计算实验结果, 就可以实现实际系统和人工系统的平行执行。一方面, 通过采用计算实验的各类结果, 对实际系统进行指导, 以达到优化的目的。另一方面, 将实际系统的结果再次反馈到人工系统当中进行修正, 以达到虚实共两部分同进步的目的。可以开发不同的平行执行系统以实现不同目的, 比如: 培训 (training)、评估 (evaluation)、控制 (control)、管理 (management) 或优化 (optimization) 等。平行系统常用的方式:

1) 用于人员学习和培训的 PTS (parallel training system)。在这一领域中, 人工系统主要是被用作核电站人员的学习和培训。通过实际系统与人工系统的适当连接组合, 可以使有关人员迅速地掌握核电站的各种状况以及对应的行动, 相关的理论和技术知识, 特别是岗位行为进行情景式的虚拟环境、全方位的学习和培训, 提高整体效果和质量。

2) 用于实验和评估的 PES (parallel evaluation system)。主要是将复杂核电站的社会要素 (环境、管理、人员等) 和工程要素 (物理设备、仪控系统、保护系统等) 作为一个有机整体, 依据总体和分级目标进行各个方面的实验和评估。在这一过程中, 人工系统主要被用来进行计算实验, 分析了解各种不同情况下, 复杂系统的行为和反应, 并对不同相关环境要素、管理制度、人员行为和生产方案等的解决方案的效果进行验证与评估, 作为选择和支持管理与控制决策的依据。

3) 用于控制与管理的 PMS (parallel management system)。在这一领域中, 人工系统试图尽可能地模拟实际系统, 对其行为进行预估, 从而为寻找对实际系统有效的解决方案或对当前方案进行改进提供依据。进一步, 通过观察实际系统与人工系统评估的状态之间的不同, 产生误差反馈信号, 对人工系统的评估方式或参数进行修正, 减少二者的差距, 并开始分析新一轮的优化和评估。针对核电站安全可靠性等的需求, PMS 可以优化控制、管理和保护功能, 同时增强核电站的应急处置能力^[22]。

开发各类平行系统的先后决定于实际需求, 以及人工系统的开发进展。对于核电站来讲, 可以首先针对其仪控和保护部分的功能需求, 递归式地开发该部分以可靠性为中心的 PTS、PES 和 PMS。之后, 再将范围扩展到核电站的其它部分, 比如: 电气、核岛等。这应该是比较实际的安排。

5.5 平行系统实现

以 PMS 为例, PMS 硬件方面可以借助高可靠性设计的嵌入式系统, 这样便于简化系统设计, 同时提高可靠性。PMS 软件方面以可靠性为目标, 采用基于 ACP 方法的智能化整体解决方案, 保证系统各单元的互用互补。PMS 设计目标是, 在只剩下一个测量单元、一个网络单元、一个控制单元和一个执行单元时, PMS 系统仍然能完成核心的保护和控制任务。

6 结论

本文以 ACP 方法为基础, 提出了核电站设计阶段采用自上而下的规划和自下而上的设计相结合的平行系统, 使得核电站在建造前就有了安全可靠性方面的科学依据。一旦得到验证, 就能推广应用到三代核电站的自动化和信息化系统的国产化之中, 将可实现积木式的系统构建和在线组态。长远发展下去, 可最终形成高可靠性的各类平行系统。平行系统方法在石化领域已经有成功应用实践的验证, 推广应用到三代核电站的自动化和信息系统国产化后, 可以进一步提高其智能化和科学化水平。文中所描述的预期效果是美好的, 但是要成功实现任重道远。

参考文献

- [1] 段志勇, 赵凤娟, 黄海涛, 等. 国际核电发展动态及我国核电发展的思考 [J]. 黑龙江电力, 2009, 31(3): 234–236.
Duan Z Y, Zhao F J, Huang H T, et al. Developing dynamic of nuclear power international and consideration of developing nuclear power in China[J]. Heilongjiang Electric Power, 2009, 31(3): 234–236.
- [2] 核电站安全系统可靠性分析一般原则 [S]. GB/T9225–1999, 1999.

- The general principles of reliability analysis of safety system of nuclear power plants[S]. GB/T9225-1999, 1999.
- [3] 林诚格. 非能动先进核电站 AP1000[M]. 北京: 原子能出版社, 2008.
- Lin C G. Advanced Passive Nuclear Power Plants[M]. Beijing: Atomic Energy Press, 2008.
- [4] 商建东, 陈康宁. 质量驱动产品开发方法及其应用研究 [J]. 自动化仪表, 2000, 21(1): 43-48.
- Shang J D, Chen K N. The quality-driven method of product development and the applied research[J]. Process Automation Instrumentation, 2000, 21(1): 43-48.
- [5] 夏贵斌, 黄政, 陈立强, 等. 多种负荷下的电子元器件突然失效率估算方法 [J]. 中国设备工程, 2009, 7: 47-49, 57.
- Xia G B, Huang Z, Chen L Q, et al. Estimation method of sudden failure rate of electronic components under the effect of multi-load[J]. China Plant Engineering, 2009, 7: 47-49, 57.
- [6] 格拉祖诺夫 [克]. 自动控制系统可靠性理论基础 [M]. 北京: 水利电力出版社, 2009.
- Glazunov. Automatic Control System Reliability Theory[M]. Beijing: China Water Power Press, 2009.
- [7] 王飞跃. 平行系统方法与复杂系统的管理和控制 [J]. 控制与决策, 2004, 19(5): 485-489.
- Wang F Y. Parallel system methods for management and control of complex systems[J]. Control and Decision, 2004, 19(5): 485-489.
- [8] 王飞跃. 关于复杂系统研究的计算理论与方法 [J]. 中国基础科学, 2004, 41(6): 3-10.
- Wang F Y. Computational theory and method on complex system[J]. Chinese Basic Science, 2004, 41(6): 3-10.
- [9] 中科院平行管理系统在茂名石化成功上线 [N]. 科学时报, 2009-07-01.
- Parallel Management Starts its On-Line Pilot in Maoming Petrochemical Successfully[N]. Science Times, 2009-07-01.
- [10] 中国科学技术协会. 控制科学与工程学科发展报告 (2010-2011)[R]. 中国科学技术出版社, 2008.
- China Association for Science and Technology. Report on Advanced in Control Science and Engineering (2010-2011)[R]. Chinese Press of Science and Technology, 2008.
- [11] 中国科学院. 创新 2050: 科学技术与中国的未来 [R]. 北京: 科学出版社, 2009.
- Chinese Academy of Sciences. Innovation 2050: Science and Technology and China's future[R]. Beijing: Science Press, 2009.
- [12] 中国科学院. 平行管理技术. 中国至 2050 先进制造科技发展路线图 [R]. 北京: 科学出版社, 2009.
- Chinese Academy of Sciences. Parallel Management Technology, Chinese Advanced Manufacturing Technology Development Roadmap to 2050[R]. Beijing: Science Press, 2009.
- [13] 钱晓峰, 张鹏翥. 社会金融仿真系统框架设计 [C]// 第一届全国社会计算会议, 2009.
- Qian X F, Zhang P X. Framework design of social financial simulation system[C]// 1st Chinese Conference on Social Computation, 2009
- [14] Wang Y Z, Zeng D J, Zheng X L. Epidemic spreading on scale-free networks with heterogeneous links weights[R]. University of Arizona, 2009, 12.
- Zhang W, Liu W C, Wang Q W, et al. The modeling for the complexity of capital market: Agent-based computational experiment finance[J]. Modern Finance and Economics, 2003, 155(23): 3-7, 16.
- [15] 张维, 刘文财, 王启文, 等. 面向资本市场复杂性建模: 基于 Agent 计算实验金融学 [J]. 现代财经, 2003, 155(23): 3-7, 16.
- Zhang W, Liu W C, Wang Q W, et al. The modeling for the complexity of capital market: Agent-based computational experiment finance[J]. Modern Finance and Economics, 2003, 155(23): 3-7, 16.
- [16] 张军. 研究社会系统演化的计算实验方法 [J]. 实验室研究与探索, 2008, 27(10): 40-44.
- Zhang J. Computational experiment for social evolution[J]. Research and Exploration in Laboratory, 2008, 27(10): 40-44.
- [17] 顾佳, 贺仲雄. 人工生命、人工社会、人工涌现的和谐仿真 [C]// 2006 系统仿真及其应用学术交流会, 2006, 8: 335-338.
- Gu J, He Z X. Harmony simulation of artificial life, artificial society, and artificial emergence[C]// 2006 System Simulation and Application Symposium, 2006, 8: 335-338.
- [18] 柴象海, 金先龙. 基于 Agent 的公共场所突发事件三维仿真建模与应用 [J]. 上海交通大学学报, 2008, 42(10): 1669-1673.
- Chai X H, Jin X L. The 3D simulation modeling and application of paroxysmal calamity in public places based on agent[J]. Journal of Shanghai Jiaotong University, 2008, 42(10): 1669-1673.
- [19] 臧垒, 蒋晓原, 王钰, 等. 基于计算实验的探索性分析框架研究 [J]. 系统仿真学报, 2008, 20(12): 3077-3081.
- Zang L, Jiang X Y, Wang Y, et al. Research on framework of exploratory analysis based on computational experiments[J]. Journal of System Simulation, 2008, 20(12): 3077-3081.
- [20] 熊刚, 王飞跃. 平行管理理论与方法 [C]// 第一届平行管理会议, 2009.
- Xiong G, Wang F Y. Theory and methods of parallel management[C]// 1st Chinese Conference on Parallel Management, 2009.
- [21] 王飞跃. 从一无所有到万象所归: 人工社会与复杂系统研究 [N]. 科学时报, 2004.
- Wang F Y. From nothing to Vientiane: Research on artificial social and complex system[N]. Science Times, 2004.
- [22] 王飞跃. 关于复杂系统的建模、分析、控制和管理 [J]. 复杂系统与复杂性科学, 2006, 3(2): 27-34.
- Wang F Y. The modeling, analysis, control and management of complex systems[J]. Complex Systems and Complexity Science, 2006, 3(2): 27-34.