文章编号：0258-0926(2020)06-0001-07; doi:10.13832/j.jnpe.2020.06.0001

概率安全评价在核能安全分析领域的应用和发展

余红星，武铃珺，邓纯锐，邓 坚，卢毅力，
张 航，彭欢欢，王小吉

中国核动力研究设计院核反应堆系统设计技术重点实验室，成都，610213

摘要：概率安全评价（PSA）是核能安全分析领域的两大分析方法之一。本文从 PSA 概念入手，首先从理论基础、分析视角等多个方面比较了确定论和概率论 2 种分析方法的差异；其次，梳理 PSA 在核能安全分析领域的历史进程，通过回顾 PSA 在技术和法规上的变化，展示了 PSA 与核能安全在提升过程中相互促进的关系；再次，阐释 PSA 技术在风险量化预测、平衡安全设计、安全决策、安全监管方面的应用，并通过华龙一号（HPR1000）的实例展示了 PSA 在核能安全分析中的具体应用方式。最后，对 PSA 技术未来的发展方向进行了预测，指出确定论和概率论 2 种分析方法将深入融合，PSA 分析从安全目标向任务目标转移、从静态向动态转换、从认知向感知转换的发展方向。

关键词：概率安全评价（PSA）；核能安全；堆芯损伤频率（CDF）；大量放射性释放频率（LRF）；放射性风险

中图分类号：TL364^{+}.5 文献标志码：A

Evalution and Application of Probabilistic Safety Assessment in Nuclear Energy Safety Analysis

Yu Hongxing, Wu Lingjun, Deng Chunrui, Deng Jian, Lu Yili,
Zhang Hang, Peng Huanhuan, Wang Xiaoji

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu, 610213, China

Abstract: Probabilistic safety assessment (PSA) is one of the two major safety analysis methods in the field of nuclear energy safety analysis. Starting from the concept of PSA, this paper firstly compares the difference between deterministic safety assessment and probabilistic safety assessment from the theoretical basis and analytical perspective. Secondly, it combs the historical process of PSA in the field of nuclear energy safety analysis, and through reviewing the changes in technology and regulations of PSA, it shows the mutual promotion relationship between PSA and nuclear energy safety in the process of upgrading. Thirdly, the application of the PSA method in risk quantitative prediction, balance safety design, risk safety-making, and risk safety supervision is expounded, and the application of PSA in nuclear energy safety assessment is illustrated by HPR1000. Finally, the future development direction of PSA technology is predicted. It points out that the deterministic safety assessment and probabilistic safety assessment will deeply integrate, and the PSA analysis will shifts from security target to task target, from static to dynamic, and from cognitive to perceptual direction.

Key words: Probabilistic risk assessment (PSA), Nuclear energy safety, Core damage frequency (CDF), Large release frequency (LRF), Radiological risk

1 PSA 的基本涵义

针对核反应堆系统进行的概率安全分析、概率安全评价（PSA）、概率风险评价（PRA）或定量风险评价（QRA）具有相近的涵义，是指美

收稿日期：2020-03-13；修回日期：2020-08-14

作者简介：余红星（1969—），男，研究员级高级工程师，博士研究生导师，现从事先进压水反应堆研发工作，E-mail：yuhong_xing@126.com

国原子能委员会 1975 年发表的《核电站风险报告》（WASH-1400）研究形成的基于概率论分析得到对核反应堆风险认识的分析方法[1]。

PSA 以可靠性理论和系统工程学方法为主要基础，针对核反应堆系统，主要采用“故障树+事件树”的分析模式，按照层层退防的理念研究事故的演变进程，分析所有可能的初因事件下设备/系统/人因的响应，得到核反应堆整体风险水平的认识，获得设备/系统/人因对风险的重要度贡献，用于指导核反应堆系统的设计/运行/维修/退役全过程的风险控制。

PSA 分为 3 个层次[1]，某种意义上分别与纵深防御原则的第三、四、五层防御目标相对应。

（1）一级 PSA 分析，分析范围限定于安全相关系统（包括安全级和非安全级），针对事故后的系统响应，关注放射性源堆芯（包括乏燃料）的安全，获得放射性包容风险的认识。一级 PSA 关注的是安全壳的安全，风险源是堆芯放射性物质释放。

（2）二级 PSA 分析，分析范围限定于安全壳内，针对严重事故下响应，关注安全壳对放射性物质的包容，获得放射性释放风险的认识。二级 PSA 关注的是厂区的安全，风险源是安全壳放射性物质释放。

（3）三级 PSA 分析，分析范围限定于安全壳外环境，针对厂外应急区域的气候、地理位置、环境条件等，关注放射性在环境中的迁移，获得放射性扩散风险的认识。三级 PSA 关注的是厂区以外环境的安全，风险源是厂区放射性物质释放。

2 确定论与概率论的对比

确定论和概率论是安全分析的主要方法[1]。确定论和概率论分析既各有侧重，又相辅相成、互为补充。2 者的侧重点和优势如图 1 所示。

确定论以纵深防御原则为基础，以安全相关系统能够实现其预设功能为假设，论证系统在设定功能充分发挥作用的情景下后续事故的发展，给出系统安全的结论，论证设备、人因设计功能的充分性；概率论以系统固有可靠性为基础，以安全相关系统可能丧失其预设功能为假设，论证系统在丧失其原有设计功能的情景下后续事故的发展，给出发生放射性风险概率的结论，评价设备失效、人误对风险的贡献程度。

确定论分析以概率论为指导，概率论分析以确定论为基础，例如：确定论中设计基准事故（DBA）分类以事故可能的发生概率为划分依据，概率论中事故系统响应的成功准则以确定论分析为依据。当前核反应堆安全设计是以确定论为主、概率论为辅的模式开展安全分析，2 者结合运用使得当今核反应堆的安全得到较好保障。

3 PSA 技术发展历程

20 世纪 40 年代，概率安全的理念首先在航空工业领域被提出，后被引入核能安全分析领域。PSA 的历史进程主要可以归纳为（图 2[2]、图 3[3]）：①美国 1957 年发布的 WASH-740 中对核事故导致的放射性物质释放的概率做了模糊描述，促使安全工作者开始思考事故的发生概率问题；②概率风险理念起源于 1967 年法默曲线的发布，开辟了概率及可靠性理念在核能安全领域的应用；③PSA 诞生于 1975 年 WASH-1400 报告，首次提出从时间进程上进行事故推演追踪的“事件树”方法，具有里程碑意义；④PSA 分析意义被肯定于 1979 年，美国三哩岛严重事故（TMI-2）印证了 WASH-1400 的一个重要结论。TMI-2 后，核安全工作者开始对 PSA 产生兴趣；⑤PSA 体系成熟于美国 1990 年发布的《严重事故风险：五座核电厂的评价》（NUREG-1150）报告，总结 PSA 已有研究成果并且对 PSA 的应用提出了独到的见解，具有里程碑意义；⑥PSA 的使用在法规中被确立于 1995 年《概率安全评价方法在核活动中的应用：最终政策声明》，标志着“涵盖风险信息的安全管理或称为风险指引型的安全管理理念”的形成；⑦PSA 方法大发展，20 世纪末 PSA 已成为核反应堆安全评价的一种标准化方法，是进行安全评价和安全决策的重要工具，被核安全监管当局和核能行业从业者所广泛使用。

4 PSA 技术的应用

PSA技术已在核电厂设计、审批、监督、评价、定期安全审评、运行、维修、试验、退役各方面被广泛地采用。PSA在核能安全分析领域的应用主要体现在以下几方面。

4.1 科学认知核反应堆的风险

PSA 能给出的是某种后果和后果可能发生的概率值。PSA 通过确定核反应堆系统、设备、人

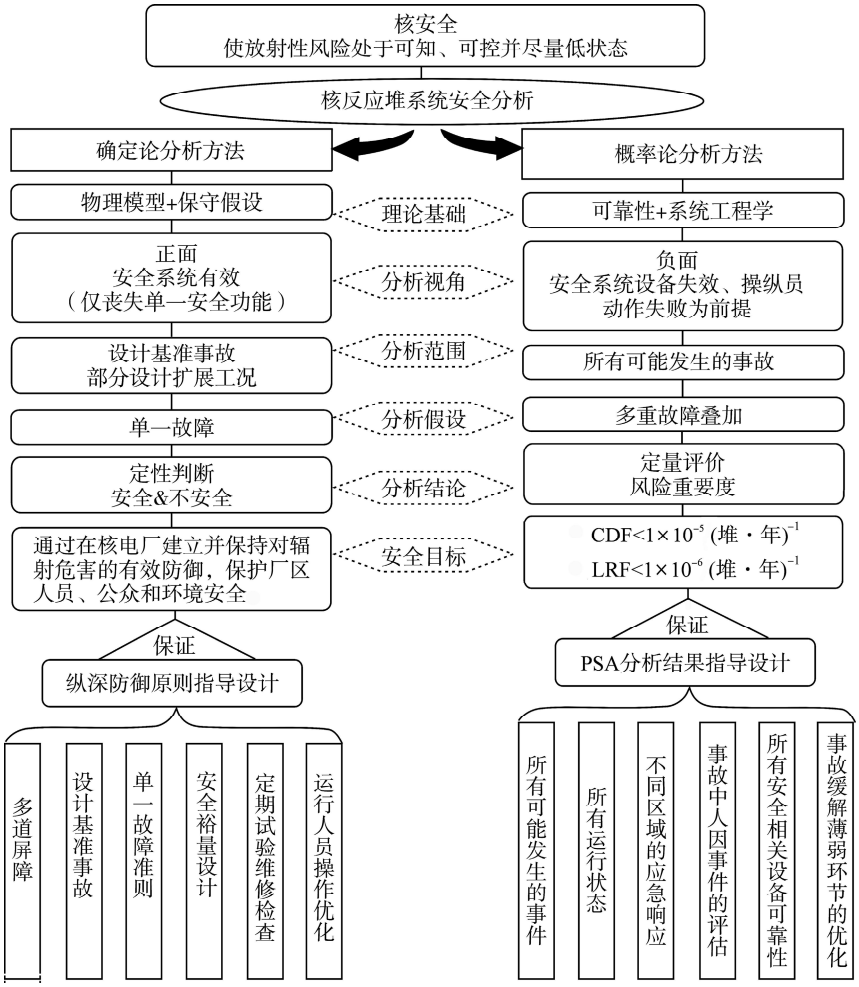

图 1　两大核能安全分析方法的对比

Fig. 1　Two Major Safety Analysis Methods for Nuclear Power Reactor

CDF——堆芯损伤频率；LRF——大量放射性释放频率

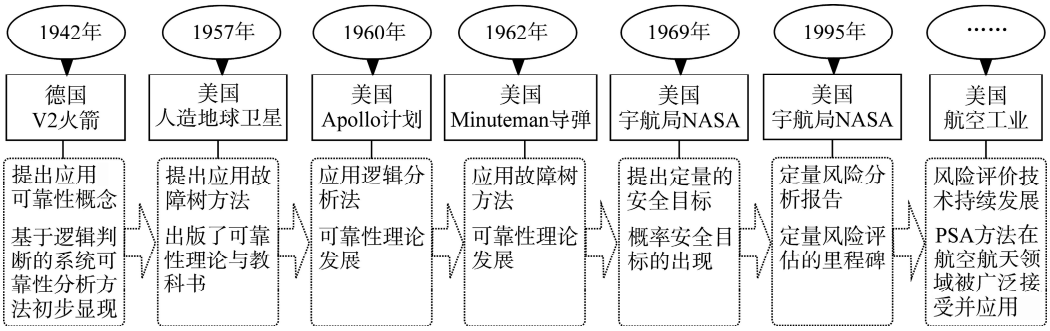

图 2　概率安全分析方法的诞生和发展

Fig. 2　Emerge and Development of Probabilistic Safety Assessment Method

因、信号之间的逻辑关系，合理的推演可能的事故发展进程，通过各要素的固有可靠性，科学地认知核反应堆的放射性风险。

PSA 分析时能够涵盖风险要素间的交互，包括：人-机交互、设备之间的交互、系统之间的交互、人和规章之间的交互。PSA 通过对各风险要素的共因性、相关性、不确定性和重要度等多方面的分析，认知各风险要素间的交互影响关系，给出各要素对风险的贡献程度的排序。通过 PSA 对风险的推测和各要素对风险的贡献程度的认

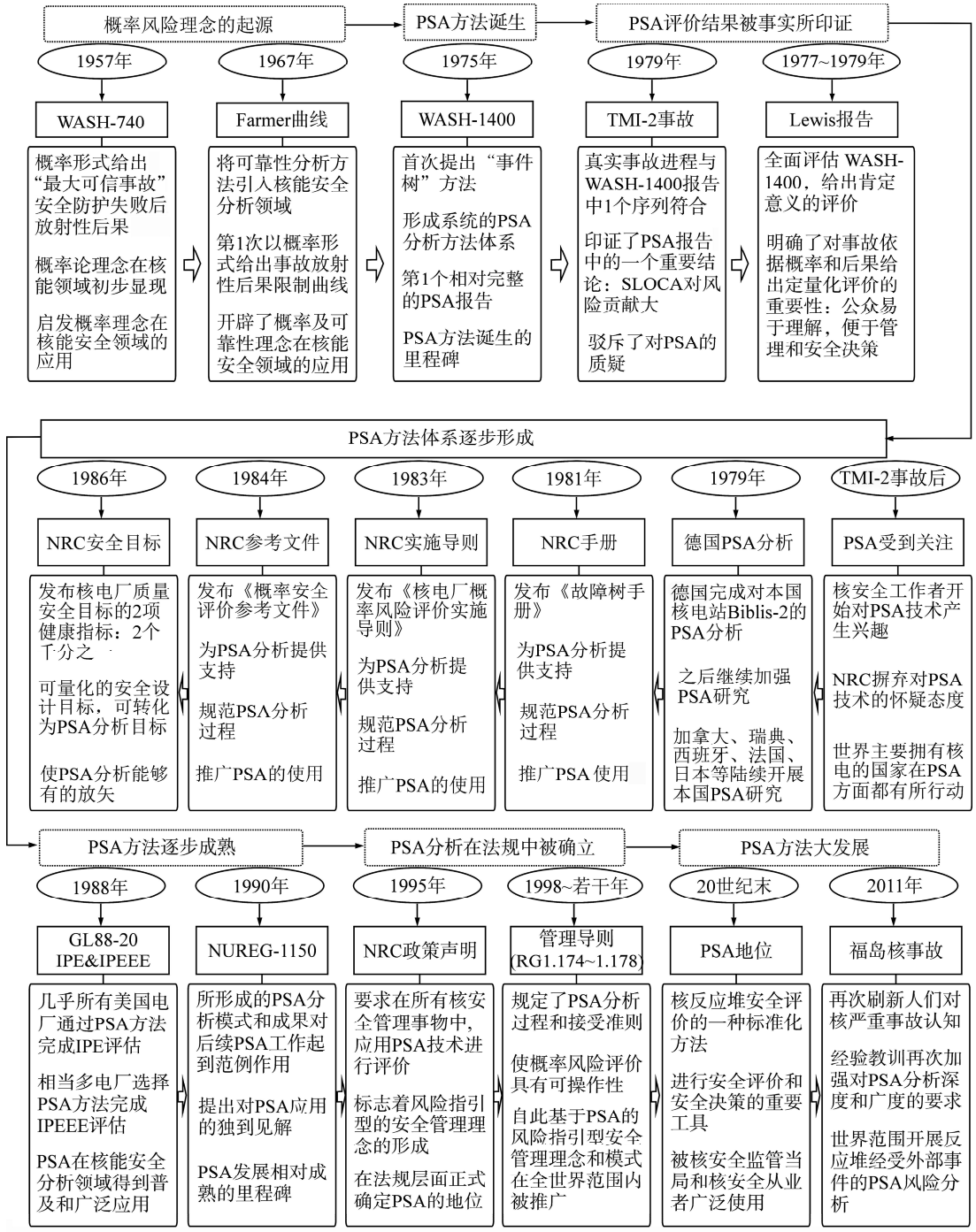

图 3 PSA 技术发在核能安全分析领域的发展历程

Fig. 3 PSA Application in Nuclear Power Safety Analysis

知，对风险重要贡献项进行控制、优化、更改，从而使得核反应堆放射性风险得以降低。

4.2 指导安全平衡设计

PSA 可以从安全的角度平衡设计，以对风险贡献的程度为标尺进行设计优化，主要措施为：

（1）潜在事故的平衡，依据始发事件发生概率的大小，调整优化设计，降低突出贡献的潜在事故的发生概率。

（2）单个系统内设备的平衡，依据对风险的推测，对系统内设备配置进行优化调整，避免出现某个设备成为风险贡献的突出项。

（3）系统间的平衡，依据对风险的推测，对

安全系统配置中是否增设、取消或变更相关系统做出决策，避免出现某个系统成为风险贡献的突出项。

（4）人因因素的平衡，依据对风险的推测，修改操作方式、优化操作流程、优化操作面板警示符号、加强特定事故操作员培训等，避免某一人因成为风险贡献的突出项。

（5）经济性和安全性的平衡，依据对风险的推测，有针对性地设计调整和优化，从经济和安全两方面进行衡量，避免出现高经济投入但安全收效甚微的投入。

4.3 风险管理

风险管理主要为通过PSA分析对各项核活动进行风险评估[4]，用量化的方法判断安全相关的活动或变更是否会导致系统风险产生大的变化；量化评估在运行、检测、维修和试验中可能出现的高风险状态或配置、行为，对反应堆系统进行风险管理。风险管理着重于风险的控制，着眼于实时或定期地跟踪并及时发现风险突变点、评判风险变化程度并加修正。

4.4 风险指引型决策

风险指引型决策是安全监管的重要模式[5]，以风险预测为导向和切入点，在原有确定论分析和工程判断的基础上考虑PSA分析的辅助作用，得到包含风险信息的分析、决策和管理方法。风险指引型安全策略使得监管部门和核电厂能够获知在设计和运行中哪些问题对公众健康与安全有重要意义，并予以重点关注。此理念影响核电安全从设计到运行到延寿（退役）的各个方面。通过PSA分析得到的风险认识，在不降低核电厂安全水平的基础上，通过风险分析改变对风险贡献小事项的关注度，增加对风险贡献大事项的关注度，减少现行法规、导则和管理中不必要的保守程度，减轻核电厂不必要的负担和成本。

中核集团自主研制的百万千瓦级先进三代核反应堆“华龙一号”（HPR1000），安全设计中进行了较为全面地PSA分析，并采纳了众多PSA安全见解进行设计优化。比如，功率运行工况下丧失外电源事件、停堆成功后应急柴油发电机组自动启动失败事件演变为全厂断电（SBO）事故，此种情况下堆芯余热只能通过“气动辅助给水泵+大气释放阀”的形式带出，如图4中事件序列8所示。该事故序列造成的CDF为1.26×10^{-7}(堆·年)$^{-1}$，占丧失外电事故导致CDF的45%，而丧失外源始发事件组导致的CDF约占总CDF的8%，风险贡献是非常显著的。通过设计优化，针对这一问题增设二次侧非能动余热排出系统（PRS），在上述序列中气动辅助给水泵无法启用的情况下，PRS自动投入运行带走堆芯余热，PRS失效的序列才会导致堆芯损坏，如图5中事故序列10所示。该事故工况中二次侧事故冷却失败分支下的CDF降低到了1.05×10^{-9}(堆·年)$^{-1}$。由于PRS的存在，使得二次侧排热手段在辅助给水泵丧失后有了多一重的安全保障。增设的PRS系统可在很多事故的缓解中使用，提高了事故后二次侧带热的可靠性，有效降低了总体堆芯损伤风险。根据HPR1000的全范围PSA分析，增设PRS系统使得CDF降低约60%，风险收益十分显著。

5 PSA技术未来的发展方向

5.1 确定论和概率论分析方法合二为一

在核能的和平利用中，安全相关的所有事物都具有确定性和概率性的双重属性。

（1）确定性：系统、设备、人因都是应安全需要而存在的，在设定的安全功能要求下实现响应。

（2）概率性：系统设备由于材料、工艺等具有固有的可靠性，人因由于规程设置、控制面板、报警提醒等具有的固有可靠性。

这2种属性在某些影响因素发生变化时，其对于安全的影响需要另一个属性来评判。

确定性在其安全要求的基础上会考虑一定裕量以保证功能的实现，但其自身是无法评判裕量的大小、变化对安全的贡献程度，这一方面需要概率性进行评判。概率性在其使用环境的变化下会发生变化，比如长时间处于某种环境条件下设备的可靠性变化，但自身无法判断可靠性变化是否对安全产生实质影响，这一方面需要进行确定性研究。因此，只有在将核反应堆确定性和概率性二者结合的情况下，才能获得对安全较为全面的评判。

在“实际消除大量放射性释放”的安全要求下，确定论和概率论的结合必将是越来越紧密，界限逐渐模糊直至合二为一，成为核能安全最为精准的分析手段和工具。

5.2 PSA分析从安全目标向任务目标转移

当前核反应堆PSA分析注重于事故缓解，指导设计往往趋向于多重手段的设置，而如何避免事故的发生是PSA分析没有关注到的领域，这应该也必须成为PSA未来发展的方向。

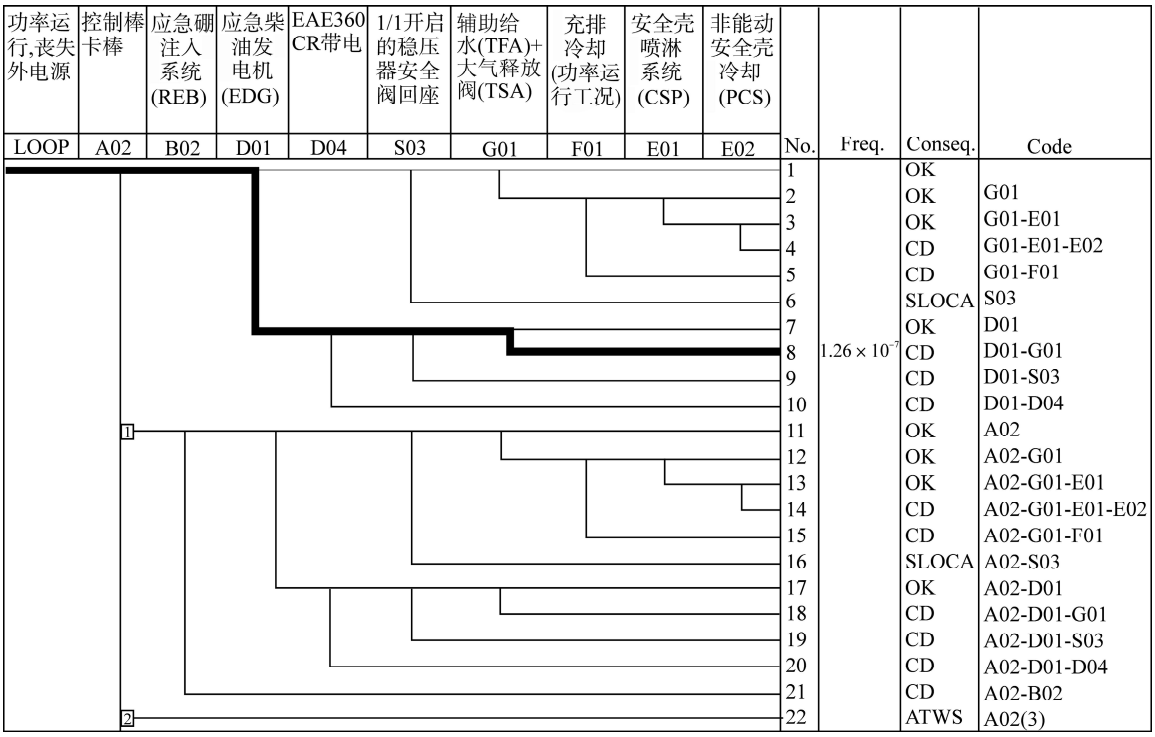

图 4 华龙一号丧失外电源事件树（不含 PRS）

Fig. 4 Loss of Offsite Power Accident in HPR1000（PRS Excluded）

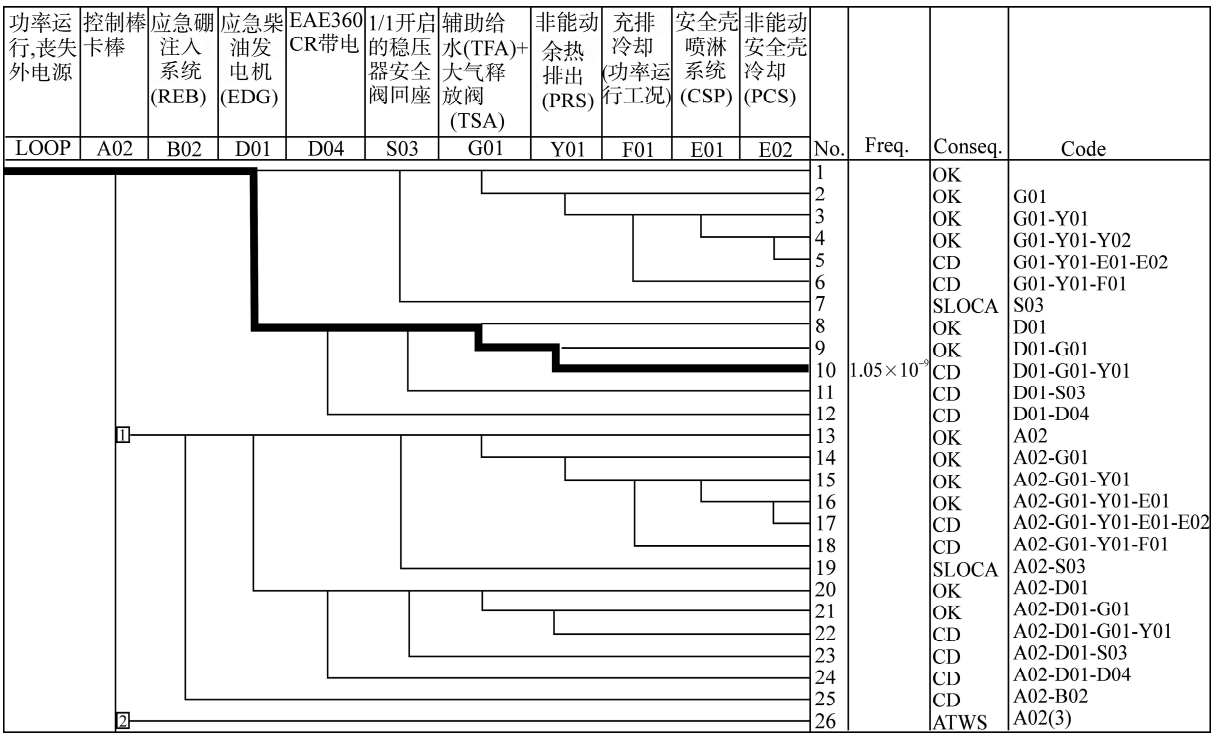

图 5 华龙一号丧失外电源事件树（含 PRS）

Fig. 5 Loss of Offsite Power Accident in HPR1000（PRS Included）

PSA 分析应从安全目标向任务目标转移，其分析的风险后果可以定义为是否停堆、是否后撤、是否导致维修、维修时间是否足够等在事故发生前或发生后一定时间段内的具体对象。通过这种任务目标的设定，以 PSA 的视角审视和查找可能引发任务目标失败的因素，深入剖析影响任务目标完成的重要贡献项，以期通过优化设计，降低任务目标失败的频率，提升任务可靠度，全面降低核反应堆事故发生的概率，提高其固有安全性。

5.3 PSA 分析从静态向动态转移

现有 PSA 是一种静态的分析模式，由设计人员主导建立固定的分析模型进行核反应堆风险的预测/评估。实际上核反应堆的任何一个微小波动，都将导致风险的变化，为了获得实时风险的认识，需要一种动态的 PSA。

实现动态 PSA，就需要急速提高建模的效率，急速缩短采集数据、分析数据的时间，当今社会，人工智能的大发展和社会大数据的建立让动态 PSA 成为可能。通过人工智能技术，让机器自主学习 PSA 的分析模式，快速解析核反应堆安全相关信息，形成批量的标准化 PSA 模型。通过大数据分析技术，及时采集、分析核反应堆运行、维修、退役等过程的安全相关数据。应用工业界的大数据，对于设备可靠性的影响、人因可靠性数据的影响等，在社会数据的类比下进行分析，获得反映社会实践反馈的可靠性数据变化趋势，解决核反应堆数据少导致可靠性分析不准确的问题。

通过人工智能和大数据的结合，在获得实时风险预测的同时，还能够结合机器分析和工业界数据类比，给出最优化的降低风险的方式方法。

5.4 PSA 分析从认知向感知转换

PSA 分析过程中存在的不确定性造成对其分析结果的不信任。不确定性来源于认知，科学工作者通过统计学原理对事物发展的规律进行推测演算，不确定性的程度取决于认知的程度，这是当前科学中无法规避的。

PSA 本身是对风险的预测，其预测的准确性是无法得到证实的，因此是否能够突破认知的不确定性和局限性，从感知的角度去看待风险。感知是人类在认识事物中的第一反映，比如说人被蛇咬了，会感知到蛇是危险的，那么下次再碰到蛇，则不会先去判断这条蛇是否有毒，而是选择绕行，避开这个风险。PSA 分析对风险的判断也可以采用这一理念，从感知的角度去分析从而对风险进行规避。采用归纳法，对已有过的风险经验进行总结，举一反三，以彼之错误看我之安全，将感知事物的过程引入到 PSA 分析中来，对风险进行全新的认识和预测。

从认知向感知的转变并不是一种倒退，而是对现有 PSA 分析的重要补充，是现有 PSA 分析的查缺补漏。将感知引入 PSA，是变相的接受确定的风险，是确定论和概率论融合的又一种模式，是对安全判断的经验反馈，也是消除陡边效应、完善 PSA 分析成果的手段。

6 总 结

概率安全评价作为核能安全分析领域的两大分析方法之一，其分析过程相较于确定论的定性安全判断，更偏重于定量的分析不安全的程度。PSA 方法能够对核电厂的潜在风险进行预测和管理，可获得建设性，甚至革新性的对核电厂设计与安全运行的有效指导。

PSA 技术的发展和应用，推动了核反应堆风险量化安全的提高，PSA 技术的逐步完善，能够推动提升核安全以最小的代价获得最大的降风险收益。

PSA 技术应用向着更深、更广的方向发展是大势所趋。确定论和概率论两大分析方法将深入融合，PSA 分析必将从安全目标向任务目标转移、从静态向动态转换、从认知向感知转换。PSA 技术的未来将从全新视角提升核安全。

参考文献：

[1] 朱继洲，奚树人，单建强，等. 核反应堆安全分析[M]. 西安：西安交通大学出版社；北京：原子能出版社，2004: 144-154.

[2] PATE-COMELL E, DILLON R. Probabilistic risk analysis for the NASA space shuttle：A brief history and current work [J]. Reliability Engineering and System Safety，2011(74): 345-352.

[3] 李春，张和林. 概率安全分析的发展与应用展望[J]. 核安全，2007(01): 58-63.

[4] 顾晔艺. 浅谈风险指引型核安全法规体系[J]. 核安全，2008 (01): 26-36.

[5] U. S. NUCLEAR AND REGULATORY COMMISSION. An Approach for Using Probabilistic Risk Assessment in Risk- Informed Decisions on Plant- Specific Changes to the Licensing Basis: Regulatory Guide 1.174（rev2）[S]. USA: Office of Nuclear Regulatory Research, 2011.

（责任编辑：刘 君）