

IAEA

国际原子能机构

安全标准

丛书

核电厂的安全评价与验证

安全导则

No. NS-G-1.2



IAEA

国际原子能机构

国际原子能机构安全相关出版物

国际原子能机构（原子能机构）安全标准

根据原子能机构《规约》第三条的规定，原子能机构授权制定或采取旨在保护健康及尽量减少对生命与财产的危险的安全标准，并规定适用这些标准。

原子能机构借以制定标准的出版物以国际原子能机构安全标准丛书的形式印发。该丛书涵盖核安全、辐射安全、运输安全和废物安全以及一般安全（即涉及上述所有安全领域）。该丛书出版物的分类是安全基本法则、安全要求和安全导则。

安全标准按照其涵盖范围编码：核安全（NS）、辐射安全（RS）、运输安全（TS）、废物安全（WS）和一般安全（GS）。

有关原子能机构安全标准计划的信息可访问以下原子能机构因特网网址：

<http://www-ns.iaea.org/standards/>

该网址提供已出版安全标准和安全标准草案的英文文本。也提供以阿拉伯文、中文、法文、俄文和西班牙文印发的安全标准文本、原子能机构安全术语表以及正在制订中的安全标准状况报告。欲求详细信息，请与原子能机构联系（P.O. Box 100, A-1400 Vienna, Austria）。

敬请原子能机构安全标准的所有用户将其使用方面的经验（例如作为国家监管、安全评审和培训班课程的基础）通知原子能机构，以确保原子能机构安全标准继续满足用户需求。资料可以通过原子能机构因特网网址提供或按上述地址邮寄或通过电子邮件发至 Official.Mail@iaea.org。

其他安全相关出版物

原子能机构规定适用这些标准，并按照原子能机构《规约》第三条和第八条 C 款之规定，提供和促进有关和平核活动的信息交流并为此目的充任各成员国的居间人。

核活动的安全和防护报告以其他出版物丛书的形式特别是以**安全报告丛书**的形式印发。安全报告提供能够用以支持安全标准的实例和详细方法。原子能机构其他安全相关出版物丛书是**安全标准丛书适用规定**、**放射学评定报告丛书**和**国际核安全咨询组丛书**。原子能机构还印发放射性事故报告和其他特别出版物。

安全相关出版物还以**技术报告丛书**、**国际原子能机构技术文件丛书**、**培训班丛书**、**国际原子能机构服务丛书**的形式以及作为**实用辐射安全手册**和**实用辐射技术手册**印发。保安相关出版物则以**国际原子能机构核保安丛书**的形式印发。

核电厂的安全评价与验证

安全标准调查

国际原子能机构欢迎您回复。请访问网址：

<http://www-ns.iaea.org/standards/feedback.htm>

下述国家是国际原子能机构的成员国：

阿富汗	希腊	尼日利亚
阿尔巴尼亚	危地马拉	挪威
阿尔及利亚	海地	巴基斯坦
安哥拉	教廷	巴拿马
阿根廷	洪都拉斯	巴拉圭
亚美尼亚	匈牙利	秘鲁
澳大利亚	冰岛	菲律宾
奥地利	印度	波兰
阿塞拜疆	印度尼西亚	葡萄牙
孟加拉国	伊朗伊斯兰共和国	卡塔尔
白俄罗斯	伊拉克	摩尔多瓦共和国
比利时	爱尔兰	罗马尼亚
贝宁	以色列	俄罗斯联邦
玻利维亚	意大利	沙特阿拉伯
波斯尼亚和黑塞哥维那	牙买加	塞内加尔
博茨瓦纳	日本	塞尔维亚和黑山
巴西	约旦	塞舌尔
保加利亚	哈萨克斯坦	塞拉利昂
布基纳法索	肯尼亚	新加坡
喀麦隆	大韩民国	斯洛伐克
加拿大	科威特	斯洛文尼亚
中非共和国	吉尔吉斯斯坦	南非
智利	拉脱维亚	西班牙
中国	黎巴嫩	斯里兰卡
哥伦比亚	利比里亚	苏丹
哥斯达黎加	阿拉伯利比亚民众国	瑞典
科特迪瓦	列支敦士登	瑞士
克罗地亚	立陶宛	阿拉伯叙利亚共和国
古巴	卢森堡	塔吉克斯坦
塞浦路斯	马达加斯加	泰国
捷克共和国	马来西亚	前南斯拉夫马其顿共和国
刚果民主共和国	马里	突尼斯
丹麦	马耳他	土耳其
多米尼加共和国	马绍尔群岛	乌干达
厄瓜多尔	毛里塔尼亚	乌克兰
埃及	毛里求斯	阿拉伯联合酋长国
萨尔瓦多	墨西哥	大不列颠及北爱尔兰联合王国
厄立特里亚	摩纳哥	坦桑尼亚联合共和国
爱沙尼亚	蒙古	美利坚合众国
埃塞俄比亚	摩洛哥	乌拉圭
芬兰	缅甸	乌兹别克斯坦
法国	纳米比亚	委内瑞拉
加蓬	荷兰	越南
格鲁吉亚	新西兰	也门
德国	尼加拉瓜	赞比亚
加纳	尼日尔	津巴布韦

原子能机构《规约》于 1956 年 10 月 23 日在纽约联合国总部召开的国际原子能机构规约会议上通过，于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳。原子能机构的主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构安全标准丛书第 NS-G-1.2 号

核电厂的安全评价与验证

安全导则

国际原子能机构
维也纳，2005 年

版 权 说 明

国际原子能机构的所有科学和技术出版物均受1952年（伯尔尼）通过并于1972年（巴黎）修订的《万国版权公约》之条款的保护。自那时以来，世界知识产权组织（日内瓦）已经扩大了这一版权，以包括电子形式和虚拟形式的知识产权。必须获得许可而且通常需要签订版税协议方能使用原子能机构印刷形式和电子形式出版物中所载全部或部分内容。欢迎有关非商业性翻印和翻译的建议并将在个案基础上予以考虑。询问事宜应通过电子邮件地址 sales.publications@iaea.org 发至原子能机构出版科或按以下地址邮寄：

Sales and Promotion Unit, Publishing Section

International Atomic Energy Agency

Wagramer Strasse 5

P.O. Box 100

A-1400 Vienna

Austria

传真：+43 1 2600 29302

电话：+43 1 2600 22417

网址： <http://www.iaea.org/books>

© 国际原子能机构 • 2005 年

国际原子能机构印制

2005 年 8 月 • 奥地利

核电厂的安全评价与验证

国际原子能机构，奥地利，2005 年 8 月

STI/PUB/1112

ISBN 92-0-513805-3

ISSN 1020-5853

序

总 干 事

穆罕默德·埃尔巴拉迪

国际原子能机构《规约》授权原子能机构制定旨在保护健康及尽量减少对生命与财产的危险的的安全标准。原子能机构必须使这些标准适用于其本身的工作，而且各国通过其对核安全和辐射安全的监管规定能够适用这些标准。原子能机构对这样的一整套安全标准定期进行审查并协助实施这些安全标准已经成为全球安全体制的一个关键要素。

在 20 世纪 90 年代中期，原子能机构开始对其安全标准计划进行大检查，包括修改监督委员会的结构和确定旨在更新整套标准的系统方案。已经形成的新标准具有高水准并且反映成员国的最佳实践。在安全标准委员会的协助下，原子能机构正在努力促进全球对其安全标准的认可和使用。

诚然，只有对这些安全标准在实践中加以适当应用，它们才会是有效的。原子能机构的安全服务——其范围包括工程安全、运行安全、辐射安全、运输安全和废物安全，直至监管事项和组织中的安全文化——协助成员国适用安全标准和评价其有效性。这些安全服务能够有助于共享真知灼见，因此，我继续促请所有成员国都能利用这些服务。

监管核安全和辐射安全是一项国家责任。目前，许多成员国已经决定采用原子能机构的安全标准，以便在其国家条例中使用。对于各种国际安全公约缔约国而言，原子能机构的安全标准提供了确保有效履行这些公约所规定之义务的一致和可靠的手段。世界各地的设计者、制造者和营运者也适用这些标准，以加强电力生产、医学、工业、农业、研究和教育领域的核安全和辐射安全。

原子能机构认真看待世界各地用户和监管者正在面临的挑战，这就是确保世界范围内的核材料和辐射源在使用中的高水平安全。必须以安全的方式管理核材料和辐射源的持续利用以造福于全人类，原子能机构安全标准的目的正是要促进实现这一目标。

编 者 按

如果列入附录，该附录可被视为标准的一个不可分割的组成部分并具有与主文本相同的地位。如果列入附件、脚注和文献目录，它们可被用来为用户提供可能是有用的补充信息或实例。

英文文本系权威性文本。

援引其他组织的标准不应被解释为国际原子能机构认可这些标准。

目 录

1. 引言	1
背景 (1.1—1.2)	1
目的 (1.3—1.5)	1
范围 (1.6—1.8)	1
结构 (1.9)	2
2. 安全评价、安全分析和独立验证	2
安全评价和安全分析 (2.1—2.7)	2
独立验证 (2.8—2.12)	3
设计、安全评价和独立验证之间的关系 (2.13—2.19)	4
3. 安全重要的工程问题	6
概述 (3.1)	6
成熟的工程实践和运行经验 (3.2—3.6)	6
创新设计的特点 (3.7—3.9)	7
纵深防御的实施 (3.10—3.16)	7
辐射防护 (3.17—3.25)	9
构筑物、系统和部件的安全分级 (3.26—3.31)	10
抵御外部事件的措施 (3.32—3.49)	11
抵御内部危害的措施 (3.50—3.56)	14
与可适用的规范、标准和导则的一致性 (3.57—3.58)	15
载荷和载荷组合 (3.59—3.62)	15
材料的选择 (3.63—3.72)	16
单一故障评价和冗余度/独立性 (3.73—3.80)	17
多样性 (3.81—3.85)	19
安全重要物项的在役测试、维护、修理、检查和监测 (3.86—3.90)	20
设备鉴定 (3.91—3.96)	20
老化和已磨损机械 (3.97—3.101)	21
人-机接口和人因工程的适用 (3.102—3.116)	22
系统的相互作用 (3.117—3.121)	24
在设计过程中使用计算工具 (3.122—3.123)	25

4. 安全分析 25

 通用的指导意见 (4.1—4.32) 25

 假想始发事件 (4.33—4.49) 29

 确定论安全分析 (4.50—4.122) 32

 概率论安全分析 (4.123—4.231) 45

 敏感性研究和不确定性分析 (4.232—4.235)..... 61

 所用的计算机程序的评价 (4.236—4.244)..... 62

5. 独立验证 (5.1—5.10)..... 64

参考文献 66

参与起草和审订的人员 69

认可安全标准的机构 71

1. 引言

背景

- 1.1. 本出版物支持题为《核动力厂安全：设计》[1]的安全要求出版物。
- 1.2. 本安全导则是在对以下所有有关出版物进行系统审查后编写的：《安全基本原则》[2]、《核动力厂安全：设计》[1]、现行的和正在修订的其他安全导则的修订本、INSAG报告[3, 4]，以及论述核电机组安全的其他出版物。本安全导则还给《核安全公约》的缔约方提供如何履行该公约第14条规定的“安全性评价和验证”义务方面的指导。

目的

- 1.3. 题为《核动力厂安全：设计》[1]的这份“安全要求”出版物说，应该在将设计提交给监管机构之前进行全面安全评价，并对这种安全评价进行独立验证（参看第3.10—3.13节）。本出版物提供应该如何满足该要求的指导性意见。
- 1.4. 本安全导则既给设计者提供如何在初步设计过程和设计修改期间进行安全评价的建议，又给营运单位提供如何以新的或已有设计为基础对新核电机组的安全评价进行独立验证的建议。将这些有关安全评价的建议用作对已有机组进行安全审查的指导性意见也是合适的。根据现行标准和惯例对已有机组进行审查是为了判断是否存在可能影响机组安全的任何偏差。本安全导则介绍的方法和建议也可被监管机构用于进行监管审查和评价。虽然本安全导则的大多数建议是通用的，适用于各种类型的核反应堆，但某些具体的建议和例子主要适用于水冷反应堆。
- 1.5. “安全评价”、“安全分析”和“独立验证”等术语在不同国家中的用法不尽相同。这些术语在本安全导则中的使用方式将在第2节中加以解释。这里所用的“设计”一词，包括机组的安全运行和管理用的规范。

范围

- 1.6. 本安全导则提出了进行安全评价和独立验证用的关键建议。它提供支持参考文献[1]的详细指导，特别是在安全分析领域。然而，本安全导则不包括可

在涉及具体设计问题和安全分析方法的其他IAEA出版物中找到的所有技术细节。

1.7. 在不同国家中，具体的确定论或概率论安全目标或放射学限值可以是不同的。确定这些目标或限值的工作是各国监管机构的责任。本安全导则提供一些由国际组织制定的目标和限值，以供参考。营运者（有时是设计者）也可以设定他们自己的安全目标，它们可以比监管者设定的安全目标更严格，或者可以涉及不同的安全问题。在某些国家，预计营运者会把这件事看作它们的整个安全项目的“所有权”的一部分。

1.8. 对已有专用安全导则的机组系统，本安全导则不提供有关其安全评价的具体建议。

结 构

1.9. 第2节给出术语“安全评价”、“安全分析”和“独立验证”的定义，并概述它们之间的关系。第3节给出供对重要要求和机组设计要求进行安全评价用的关键建议。第4节给出供安全分析用的关键建议。它描述如何识别假想始发事件（PIE），此类事件是在包括安全分析、确定论瞬态分析和严重事故分析、以及概率论安全分析在内的整个安全评价过程中要用到的。第5节给出对机组安全性进行独立验证用的关键建议。

2. 安全评价、安全分析和独立验证

安全评价和安全分析

2.1. 就本文而言，安全评价是贯穿整个设计过程的一个系统过程，目的是确保拟议中的（或实际的）机组设计满足所有相关安全要求，其中也包括营运单位和监管者设定的要求。安全评价包括，但不局限于正式的安全分析（参看第4节）。设计和安全评价是由机组设计者进行的同一迭代过程的组成部分，这一过程要一直持续到获得能够满足所有安全要求（其中或许还包括在设计期间新提出的安全要求）的设计方案为止。

2.2. 安全评价的范围是核对设计是否已满足《核动力厂安全：设计》[1]第3—6节给出的安全管理要求、主要的技术要求、以及机组设计要求和机组系统设计的要求，并核对是否已进行过全面安全分析。

2.3. 安全管理要求（参考文献[1]第3节）涉及与成熟的工程实践、运行经验和安全研究有关的课题。

2.4. 主要的技术要求（参考文献[1]第4节）包括确保已提供了足够纵深防御的技术要求，以及确保事故预防和辐射防护已得到了最优先考虑的技术要求。

2.5. 机组设计要求（参考文献[1]第5节）涉及诸如设备鉴定、老化，以及通过提供冗余度、多样性和实体分隔确保安全系统可靠性等问题，。

2.6. 机组系统设计要求（参考文献[1]第6节）涉及与反应堆堆芯、反应堆冷却系统以及诸如安全壳与应急堆芯冷却系统之类的安全系统的设计有关的问题。

2.7. 关于安全分析，参考文献[1]第5.69段说，“对机组设计进行安全分析时，既要使用确定论分析方法，又要使用概率论分析方法。然后以这种分析为基础，制定和验证安全重要物项的设计依据。还应该证明已设计好的机组有能力满足针对每一类机组状况规定的放射性释放量限值和潜在辐射剂量的可接受限值，并证明纵深防御原则已得到贯彻。”确定论和概率论安全分析工作的范围和对象将在下面的第4.17—4.22段叙述。

独立验证

2.8. 参考文献[1]第3.13段说，“营运单位应确保在将设计提交监管机构之前，由与设计人员无关的个人或小组对安全评价进行独立验证。”

2.9. 独立验证应当由营运单位负责，并尽可能由与设计者和进行安全评价的人员无关的专家组进行。所谓无关人员，是指没有参与设计和安全评价中任何工作的人员。此种独立验证与设计单位内部进行的质量保证（QA）审查完全是两码事。

2.10. 安全评价是设计者为处理一切相关安全要求而进行的综合研究工作，该项工作贯穿整个设计过程，而独立验证是由营运单位或代表营运单位进行的，而且可能只与已交给监管机构请求批准的设计有关。

2.11. 由于需要由独立验证处理的设计和安全评价方面的问题比较复杂，因而独立验证通常与设计过程同步进行，而不是等到设计结束时再进行。

2.12. 单独进行的独立审查应当由监管者进行，目的是核对设计是否满足监管部门的要求。

设计、安全评价和独立验证之间的关系

2.13. 图1不仅示出了安全评价、独立验证、安全分析和核电机组设计期间进行的其他活动之间的关系，还示出了目前的这份安全导则和与设计过程有关的其他IAEA出版物之间的关系。

2.14. 在将设计从初步概念逐步发展完善的过程中，设计者有必要考虑机组营运者和监管者两者明确规定的一切安全要求及其他要求。就发展中的核计划和引入新设计而言，这些设计要求或许会在设计过程中进行修正或变得更加明确。就新颖设计而言，或许会在设计过程中逐步形成详细要求。

2.15. 在整个设计过程中，安全评价和独立验证是由不同的小组或单位进行的。然而，这些安全评价和独立验证是迭代设计过程中不可缺少的组成部分，而且两者的主要目的都是确保机组满足安全要求。有鉴于此，这两个专题是在同一份安全导则中论述的。在某些情况下，监管机构在设计阶段就已介入。

2.16. 在设计过程的不同阶段（例如在开始建造或开始功率运行之前），将会暂停设计过程，并编制安全分析报告，以描述到那一时刻为止已进行过的设计和评价。这种报告能给监管机构的审查和评价提供输入。

2.17. 如果独立验证与设计和安全评价同步进行，则这样的独立验证会更有效，因为及早讨论和澄清一些安全问题能加速并有助于问题的解决。当设计工作仍然在进行时，很容易采纳试图改进设计或安全评价的任何建议。另一方面，人员的关系过于密切会使人质疑验证的独立性，因而应该在有效性和独立性之间搞好平衡。

2.18. 在设计过程中拟采取的重大设计决定，或许需要由营运单位进行专门的独立设计审查，这种审查仅限于拟采取的决定所涉及的范围，并可以判断可适用于拟决定事件的安全要求是否得到满足。

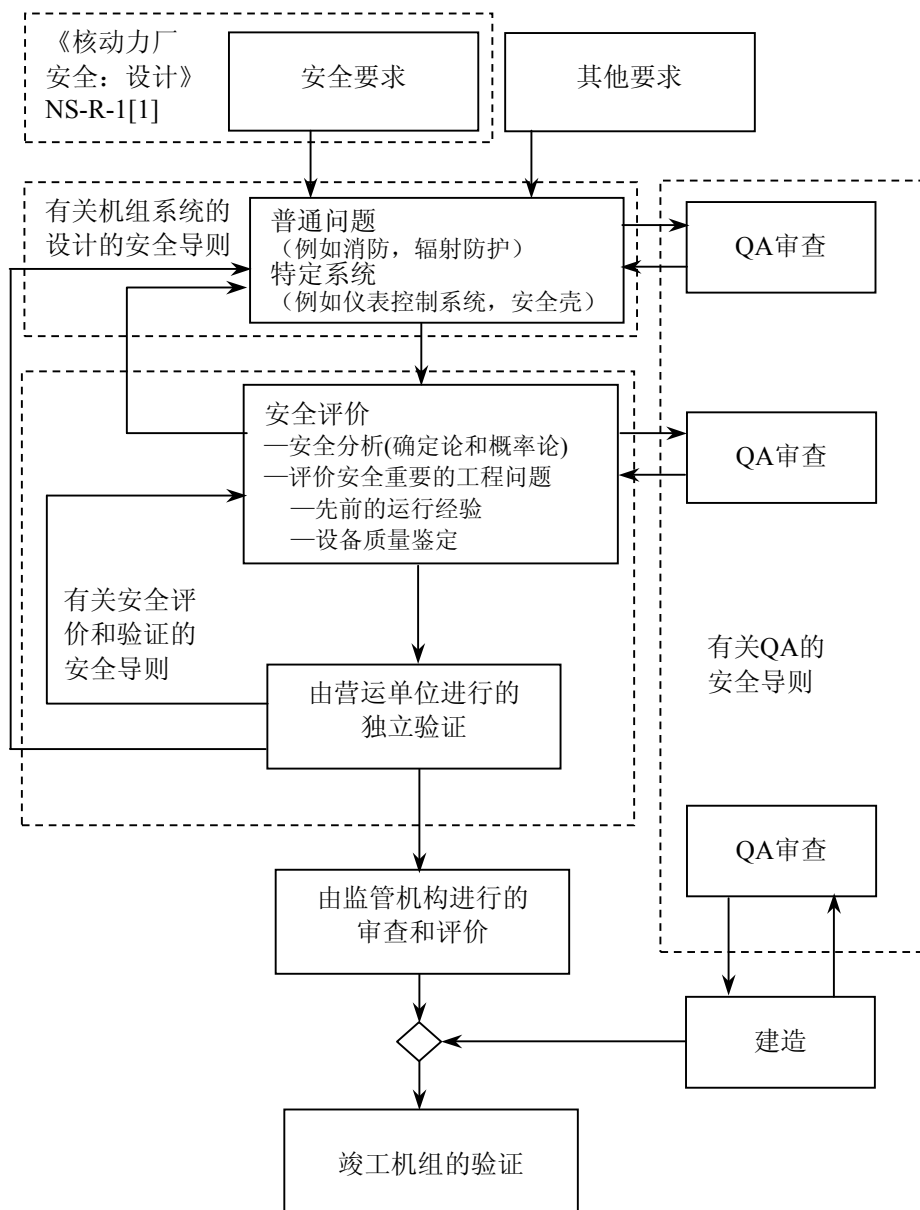


图1. 与核电机组设计有关的IAEA安全标准[1]涵盖的领域。

2.19. 设计工作应该依照QA大纲进行，包括对全部设计文件进行独立审查。常规的QA程序在安全导则SG-Q-10 [5]中论述。

3. 安全重要的工程问题

概 述

3.1. 本节包括供评价设计是否满足参考文献[1]第3—5节的要求用的建议和重要考虑事项。这些要求涵盖安全重要的普通工程问题，并适用于核电机组的一切系统。尽管安全分析可能未明确涉及到评价是否正确地执行了对此类问题的要求，但这种评价是安全评价工作的重要组成部分。对其中的某些问题没有明确定义的验收准则可供使用，因而评价是否满足安全要求的工作主要以良好的工程判断为基础。

成熟的工程实践和运行经验

3.2. 对于改进型反应堆，只要可能，此种设计应使用早先已在运行机组中获得成功应用的构筑物、系统和部件（SSC），或者至少要对其他机组已获得的相应运行经验给予应有的考虑。

3.3. 在进行安全评价时应该考虑已有的运行经验，目的在于确保安全领域内的一切相应经验教训已在该设计中得到充分考虑。运行经验应该成为改善机组纵深防御的基本信息来源。

3.4. 设计和安全评价方面的运行经验反馈应充分利用大量的运行资料，其中的大部分可对感兴趣的单位和个人公开。关于运行经验的数据应该从以下几方面获取：(i)国家数据库；(ii)世界核营运者联合会（WANO）和IAEA-OECD核能机构（OECD NEA）的事故报告系统；以及(iii) IAEA安全重要事件评价组（ASSET）的出访报告。

3.5. 从某个真实事件序列进行外推的分析方法已证明是一种有用的设计方法。具体做法是设想如果再发生其他故障（与真实场合中发生的故障相比），机组中最终会发生些什么。

3.6. 通用安全研究计划的成果也可能给从事评价任务的设计者和审查者提供有用支持。安全研究成果通常可从公开会议、书刊和计算机数据库中找到。IAEA

的安全问题通用数据库和IAEA技术文件（IAEA—TECDOC）就是在安全研究领域获得的国际成果。

创新设计的特点

3.7. 根据从运行经验、安全分析和安全研究中吸取的经验教训，有必要考虑是否需要采取超越既定做法的设计改进，并考虑此类设计改进的价值。当引入创新或不成熟的设计或设计特点时，安全要求是否得到满足应该通过相应的支持性示范计划加以证明，且此类设施应该在交付使用之前得到充分测试。

3.8. 例如，非能动安全系统与外部支持系统（如电力）无关，并且可能比能动系统更简单更可靠。当然，应该采用适当而周密的开发、测试和分析计划，以令人信服的方式证明非能动系统的实际性能和可靠性。

3.9. 另一个应用现代技术的实例是使用基于计算机的安全系统和控制系统。与传统的硬连线系统相比，计算机化的系统具有潜在优点，包括硬件的功能更强、测试能力更好和可靠性更高。然而，在某些具体装置中，这些优点的获得可能是以牺牲简单性和透明度为代价的，因此应该在尽可能接近实际运行工况的情况下进行范围更广的评估和测试，以证明计算机化系统（包括软件）的性能和总的可靠性。这方面的进一步指导可以在参考文献[6]中找到。

纵深防御的实施

3.10. 正如参考文献[1]第2.10段中指出的，纵深防御战略的目的有两个：第一，预防事故；第二，倘若预防失效，那就探测和限制事故的潜在后果并阻止其演变成更严重的工况。

3.11. 纵深防御通常按5个层次构筑。如果某一层失效，后面的一层就可以加以补偿或纠正。这些层次防御的实施与更高和更低层次的防御有效性无关。每一层保护的目的是实现这些目的的基本手段见表1。应该把头3层防御措施作为设计基准，目的是确保堆芯的结构完整性得到保持和限制公众可能受到的辐射危害。与此相反，应该把第4层防御措施看作超设计基准，目的是在考虑经济与社会因素条件下，使发生严重机组工况的可能性和放射性释放量保持在合理可行尽量低（ALARA）的水平。

3.12. 应该把最高级别的优先权给予以下几方面：防止对实体屏障完整性的不适当挑战；防止屏障受到挑战时失效或旁路；防止屏障因另一屏障的失效而失效；以及防止放射性物质的大量释放。

表1. 每一层保护的目和实现这些目的的基本手段

层别	目 的	基本手段
第1层	预防异常运行和失效	保守的设计和高质量的建造与运行
第2层	控制异常运行和探测失效	控制、限制和保护系统，以及其他的监视设备
第3层	将事故控制在设计基准以内	专设安全设施和应急规程
第4层	控制严重的机组工况，包括阻止事故发展和减轻严重事故后果	补充措施和事故管理
第5层	减轻放射性物质大量释放的放射学后果	厂外应急响应

3.13. 应该对设计进行评价，以便验证确保第1—4层防御有效性的具体措施是否已得到实施。

3.14. 对纵深防御实施情况的评价，应该在完整的安全分析支持下通过证明大量要求已得到满足来实现。这种评价应该确认，通过确保基本的安全功能可得到履行和放射性物质的释放可受到控制，使可能的始发事件均能按照各自的纵深防御层次得到充分处理。

3.15. 评价过程应该特别注意可能同时对一个以上的屏障产生不利影响，或引起安全系统的冗余设备同时失效的内部和外部危害。

3.16. 只要适用，设计应该有探测每一层的防御失效或旁路的措施。应该给每一种运行模式具体规定需要的防御层次（例如，在某些停堆模式中，安全壳是可以打开的，并且处于此种模式时指定的这些防御层次应该始终是可利用的）。

辐射防护

3.17. 有关辐射防护设计方面的详细建议请参看IAEA专门的安全导则¹。设计者应该考虑与机组设计有关的这些建议。评价的主题是证明“安全基本原则”中所说的“辐射防护目标”已得到实现。下面讨论某些重要的辐射防护设计问题。

3.18. 就正常运行和预期运行事件而言，应该考虑以下两项设计目标：(1) 保持辐射剂量低于规定限值，以及 (2) 保持辐射剂量合理可行尽量低。应该通过将计算的当量剂量与本国法律法规规定的限值相比较，证明第一个目标已得到实现。相关的设计计算应该由设计者进行评价，以确保输入数据的正确性和所用成套方法的有效性（参看第4节）。

3.19. 第二个设计目标（满足ALARA原则）意味着所有的剂量应该在考虑了经济和社会的因素后保持合理可行尽量低。辐射防护的优化过程应该涉及到使危害（费用）和收益（安全收益增加）保持一定程度的平衡。在这一优化过程中，辐射受照量的倾向值和有关的设计措施可能来自拥有良好运行记录的同类已有机组。安全评价应该考虑运行经验并酌情考虑附加的设计措施或改进措施，以便进一步减少工作人员和公众的辐射受照量。此类措施可能是直接的（增加屏蔽），也可能是间接的（减少设备的维护时间）。

3.20. 应该借助以下习惯做法降低辐射受照量，诸如将燃料包壳缺陷减到最少、使用耐腐蚀材料、减少长寿命腐蚀和活化同位素的形成、使一回路冷却剂泄漏量很低、使高辐射区内的维护量减到最小，以及使用遥控工具和机器人。

3.21. 应该在设计期间对各项预防措施，诸如足够的检查与维护空间、充分的辐射防护屏蔽以及正确安装机组设备，进行系统评价。

3.22. 机组设计者和安全评价者还应该考虑最后退役期间的操作剂量。当遭受高辐射剂量的构筑物中使用“牺牲层”（如压力容器周围使高放废物尽量减少和有利于压力容器拆除的混凝土屏蔽层）时，材料的选择和拆解设备和工具所需空间也是值得注意的事项。

3.23. 乏燃料贮存和装卸设施之类的舱室和设备以及放射性废物贮存库的设计，应该说明尽量减少因失效而可能导致的释放量的措施。

3.24. 设计者应该表明已经采取了足够的设计措施，以便依照参考文献[1]对辐射防护进行监测。

¹ “安全丛书” No.50-SG-D9，核动力厂的辐射防护设计问题（1985）。

3.25. 应该对用于预防事故工况的设计措施的充分性进行评价，办法是将安全分析中计算出的释放量和剂量与监管机构规定或接受的限值进行比较。减轻超设计基准事故的放射性后果，或许需要在厂区及其周围地区采取特殊行动（事故管理和制订应急计划）。在进行安全评价时，设计者应该确保事故管理和制订应急计划用的相关参数已经被充分纳入机组的设计中。

构筑物、系统和部件的安全分级

3.26. 应该规定一切SSC的安全重要性，并建立参考文献[1]中详细规定的安全分级方法，以便就每一安全级别标出以下内容：

- 相应的法规和标准，以及由此而来的有待设计、制造、建造和检查部件时应用的相应措施；
- 系统有关的特性冗余度之类，如是否需要应急电源和环境条件鉴定；
- 准备在确定论安全分析中采用的PIE系统的可利用率或不可利用率；
- 质量保证措施。

3.27. 一般说来，应该规定以下一些分级方法并验证其充分性与一致性：

- 按受影响安全功能的重要性对系统进行分级；
- 按失效后果的严重程度、机械方面的复杂程度和额定压力，对承压部件进行分级；
- 按被研究的构筑物或部件需要在地震期间和地震之后保持其完整性和履行其功能的必要性，并考虑余震及逐渐加大的损伤，对抗震能力进行分级；
- 按它们的安全功能或安全支持功能，对电气系统、仪器仪表和控制系统进行分类。由于存在着应用广范、因现场而异的分类表，因而此种分级也许不同于机组其他系统的分级；
- 按质量保证措施分类。

3.28. 划定SSC的安全级别应该基于本国的处理方案，除依赖工程判断外，应该对确定论和概率论研究给予适当信任。

3.29. 就确定论安全分析而言，用于判断是否符合验收标准的那些安全功能只能依靠已分级的SSC来履行。

3.30. 在设计阶段可以使用概率论安全分析方法（PSA）确认构筑物、系统和部件的分级。

3.31. 某个安全级别中的系统和/或部件的失效，不应该引起更高安全级别的其他系统和/或部件的失效。应该对被定为不同安全级别、可能会互相影响的不同系统的隔离和隔断是否充分进行评价。

抵御外部事件的措施

3.32. IAEA几种专门的“安全丛书”出版物²对外部事件进行了大量论述，并提供了一些供安全评价用的指导性意见。尽管如此，我们仍将某些关键问题简述如下。

3.33. 应该在安全评价中加以处理的事件与被选作机组厂址的地点有关。这些事件一般包括：

外部自然事件，诸如：

- 极端恶劣的气候条件；
- 地震；
- 外部水淹；

人因事件，诸如：

- 飞机坠毁；
- 由运输和工业活动引起的危害（火灾，爆炸，飞射物，释放有毒气体）。

² “安全丛书” Nos 50-SG-D5, External Man-induced Events in Relation to Nuclear Power Plant Design (1996); 50-SG-D15, Seismic Design and Qualification for Nuclear Power Plants (1992); 50-C-S (Rev.1), Code on the Safety of Nuclear Power Plants: Siting (1988); 50-SG-S1 (Rev.1), Earthquakes and Associated Topics in Relation to Nuclear Power Plant Siting (1991); 50-SG-S5, External Man-induced Events in Relation to Nuclear Power Plant Siting (1981); 50-SG-S7, Nuclear Power Plant Siting: Hydrogeologic Aspects (1984); 50-SG-S10A, Design Basis Flood for Nuclear Power Plants on River Sites (1983); 50-SG-S10B, Design Basis Flood for Nuclear Power Plants on Coastal Sites (1983); 50-SG-S11A, Extreme Meteorological Events in Nuclear Power Plant Siting, Excluding Tropical Cyclones (1981); 50-SG-S11B, Design Basis Tropical Cyclone for Nuclear Power Plants (1984).

3.34. 设计基准应该与选定的厂址相适应，以历史和实际数据为基础，并用按照规定阈值选择的有关每起事件的一般概率分布的一组值表示³。

3.35. 当由于对数据质量缺乏信心而不可能进行此类概率论评价时，可以使用确定论解决方案，并依赖包络性的准则和工程判断。

3.36. 要求其履行基本安全功能的SSC，应该设计得能经得起由设计基准事件引起的载荷，并能在此种事件发生期间和发生之后履行其功能。这应该通过合适的结构设计、冗余度和隔离来实现。

3.37. 与外部事件相关的放射学风险不宜超过与起源于内部的事故相关的放射学风险的范围。应当核实比设计基准以外的外部事件稍微严重一点的外部事件不会导致其后果不成比例的增加。

3.38. 极端恶劣的气候条件:应该针对每一种极端的恶劣气候条件规定设计基准事件。此类气候条件包括：

- 极端的风负荷，
- 极端的气温，
- 降水和降雪量的极值，
- 极端的冷却水温度和结冰，
- 极端的海洋植物量。

3.39. 设计基准应该考虑可以合理假设可能会同时发生的极端恶劣气候条件的组合。

3.40. 应该通过测试、实验或工程分析证明，核电机组中的构筑物一定能经得起由外部事件施加的载荷，且不会诱发使机组回到并维持某种状态（所有的基本安全功能都能够长期得到保证的那种状态）所需的物项发生任何失效。

3.41. 应该通过测试、实验或工程分析证明，安全系统能够在设计基准规定条件（例如气温、海水温度和水位）范围内履行其安全功能。

³ 在某些成员国中，预计设计会针对发生频率大于 $10^{-4}/a$ 的自然事件提供保护措施。亦见No.50-SG-S1 (Rev.1), Earthquakes and Associated Topics in Relation to Nuclear Power Plant Siting (1991)。

3.42. 正如IAEA“安全丛书”No.50-SG-S1 (Rev.1)⁴中指出的,应该使用厂区周围地区的地质调查成果、有关该地区的地震历史资料以及古地震数据,导出该厂址的SL-2地震。然后使用这个SL-2地震建立该核机组的设计基准地震(DBE)。

3.43. 拥有使机组停止运行并使机组长期保持安全稳定状态这种功能的系统、构筑物和部件应该设计得经得起设计基准地震而不会丧失功能。

3.44. 如情况合适,抗震鉴定应该包括结构分析、振动台试验和与运行经验的比较。

3.45. 外部水淹:应该对厂区周围地区进行评价,以便判断外部发生可能危及核机组的洪水的可能性。评价应包括由于降水过大、潮位过高、河流泛滥、水坝溃决和它们的可能组合引起水淹的可能性。

3.46. 应提供保护措施,以便阻止外部洪水导致安全系统设备的失效。⁵

3.47. 飞机坠毁到机组上的估算概率应该来源于相关的飞机坠毁统计数字,并考虑核机组离机场的距离和在特定厂址附近活动的各种飞行器的飞行路径和活动次数。飞机坠毁统计数字应该在机组的整个寿期内不断更新。

3.48. 如果飞机坠毁的估算概率大于可接受值,则保护措施应包括加固其中有安全重要系统和部件的构筑物,并将冗余的设备队列按如下方式隔断和分离,即它们不会因一次飞机坠毁或随后的燃料着火的打击而全都受到损伤。抵御飞机坠毁的措施应该集中在使机组回到安全状态并让机组维持在所有安全功能可以得到保证的那种状态所需的物项上。⁶

⁴ “安全丛书”No.50-SG-S1 (Rev.1) Earthquakes and Associated Topics in Relation to Nuclear Power Siting (1991)。此安全导则还详细规定了相当于经常标为可操作的基准地震(OBE)的第二个震级(SL-1),OBE是指在机组使用寿期内可以合理预期在厂区发生的地震,它还可能相当于发生该级别地震之后重新评估该机组的安全性以便继续运行的“检查震级”。

⁵ 有关外部洪水的更详细资料请参看“安全丛书”Nos 50-SG-S10A, Design Basis Flood for Nuclear Power Plants on River Sites (1983); 50-SG-S10B, Design Basis Flood for Nuclear Power Plants on Coastal Sites (1983)。

⁶ 有关如何考虑飞机坠毁的更详细资料请参看“安全丛书”No.50-SG-S5, External Man-induced Events in Relation to Nuclear Power Plant Siting (1981); 该安全导则将被题为“External Human Induced Events in Site Evaluation for Nuclear Power Plants”的另一份安全导则(尚未出版)所取代。

3.49. 就由运输和工业活动引起的危害而言，应该明确列出在厂区附近运输危险货物⁷和能引起火灾、爆炸、飞射物和释放有毒气体和影响核电机组安全的工业活动，并规定设计基准事件。

抵御内部危害的措施

3.50. 几种专门的IAEA“安全丛书”出版物⁸对内部危害进行了大量论述，并提供了一些供安全评价用的指导性意见。本节简述一些关键问题。

3.51. 设计应考虑诸如以下的内部事件施加于构筑物或部件上的具体负荷和环境条件（温度、压力、湿度、辐射）：

- 管道抖动；
- 冲击力；
- 由管道、泵、阀门的泄漏或破裂引起的内部水淹和喷射；
- 内部飞射物；
- 载荷跌落；
- 内部爆炸；
- 火灾。

3.52. 应该用事实证明，对于管道故障（诸如，喷射冲击力、管道抖动、反作用力、压力波力、压力增大、湿度、温度和辐射）对部件、建筑物、电气设备和仪器仪表与控制系统（I&C）设备的影响已得到充分考虑。具体地说，应该表明以下几点：

- 在设计安全级设备、此类设备的支撑物及相关建筑物时已经考虑了反作用力；
- 安全重要部件及其内部构件已经设计成能抵御可信的压力波力和流动力；
- 安全壳之类安全重要建筑物的压力增大问题已得到考虑；

⁷ 有关如何考虑工业活动危害的更详细资料，请参看“安全丛书”No.50-SG-S5（将被取代；参看脚注6）。

⁸ “安全标准丛书” No.NS-R-1, Safety of Nuclear Power Plants: Design (2000); “安全丛书” No.50-SG-D2, Fire Protection in Nuclear Power Plants (1992); 50-SG-D4, Protection Against Internally Generated Missiles and their Secondary Effects in Nuclear Power Plants (1980)。

- 安全重要的电气设备和I&C设备已设计得可经得起发生假想泄漏和破裂时的温度、湿度和辐射的极大值。

3.53. 关于内部水淹，应该对该机组的相关建筑物进行水淹分析，且应该考虑以下一些可能引发水淹的因素：承压部件泄漏和破裂、由来自相邻建筑物的水造成的水淹、消防系统的误动作、水槽溢出和隔离器件失效。

3.54. 安全重要SSC的高程应该比预期的最高洪水位更高或应该受到充分保护。

3.55. 内部飞射物可能是由于汽轮机之类的旋转部件失效产生的，或者是由承压部件失效产生的。应该考虑可能产生的汽轮机飞射物的优先飞行路径。除非能证明可能的飞射物不会使安全重要SSC受到明显的损坏，否则应在汽轮机与有安全级别的建筑物的相对取向中反映出该优先飞行路径。同样，应对有安全级别建筑物中的高能部件的位置尽可能地加以限制。

3.56. 当相关的载荷跌落可能导致机组内部或机组外部产生辐射受照量时，或当它能引起安全重要系统损坏时，设计时应考虑起重装置的失效。

与可适用的规范、标准和导则的一致性

3.57. 为了确保核机组的安全性，SSC的设计应考虑它们与安全有关的意义。安全重要SSC的设计应该依照与有待履行的安全功能的重要性相应的设计要求进行。划定的SSC的级别给确定该SSC的设计要适用什么样的法规和标准提供了依据。

3.58. 一般说来，供设计使用的法规和标准清单由营运单位以电力公司要求的形式提供或直接由监管机构提供。当然，应该对这些规范和标准进行审查和分析，以便依照现行的知识和工艺技术评价它们对于安全重要SSC的设计的适用性、充分性和充足性。如果某些法规和标准不足以确保该SSC具有与有待履行的安全功能的重要性相当的质量，则应该根据需要对这些规范和标准进行补充或修订，以便确保相应的SSC质量。

载荷和载荷组合

3.59. 应该将有安全级别的相关构筑物 and 部件设计得能经得起由各种运行状态和设计基准事故引起的一切相关载荷，包括由内部和外部危害引起的那些载荷。

3.60. 因此，安全评价的一个重要组成部分是：

- 确定每一有安全级别的构筑物或部件的相关载荷和载荷组合；
- 确定每一载荷和载荷组合的预计发生频度；
- 针对已确定的载荷和载荷组合估算在有安全级别的构筑物和部件中的应力和张力；
- 估算构筑物或部件中发生的单次损伤和累积损伤，估算时要考虑一切相关的劣化（例如蠕变、疲劳、老化）和它们之间可能发生的相互作用。

3.61. 这组载荷和载荷组合应该是完整的，并与安全分析用的假设保持一致。应该以历史记录、运行经验、电力公司的要求或厂址特性（视情况而定）为基础，酌情对预计的发生频度以及在机组寿期内预期的瞬态事件总数进行评价。

3.62. 估算应力和张力时除考虑一切有关的物理量之外，还应考虑由每一载荷、每一载荷组合和相应边界条件引起的环境条件。验收准则应充分反映出防止构筑物或部件随之发生失效的措施，这是减轻与假定载荷相应的危害的后果所需要的。

材料的选择

3.63. 材料应满足与其设计和制造有关的标准和要求。确定材料的设计寿命时应考虑到运行条件（例如，放射学和化学环境、一次性和周期性载荷）的影响。此外，应考虑设计基准事故对它们的特性和行为的影响。

3.64. 对于恰当性是建立在测试基础上的那些材料来说，所有的测试结果都应形成文件。

3.65. 接触放射性流出物的材料应具有抵御相关腐蚀机理的防腐蚀特性，并具有抵抗在运行工况下发生的化学反应的能力。应该尽可能避免碳钢与放射性产物接触。如果在包含放射性排出物的系统中使用高分子材料，则这种材料应该是耐辐射的。

3.66. 接触反应堆冷却剂的不锈钢或镍合金、蒸汽发生器使用的管材、较大的管道和燃料元件包壳，应具有充分的耐腐蚀性。反应堆一回路冷却剂系统的部件或用不锈钢或镍合金制造的二回路系统不应该含有低熔点元素（诸如铅、铋、镉、铟、汞、锌、铈、锡）及其合金。应该防止包含低熔点元素的轴承合金污染给水系统。为了减少操作剂量，应尽可能限制与反应堆冷却剂接触的材料中的钴含量，当个别情况下使用钴合金时应证明其正当性。应该估计从与冷却剂接触的材料中释入反应堆冷却剂中的镍量。

3.67. 设计时应确保对与不锈钢部件接触的材料（例如管道保温层）中的卤族元素进行控制，以免产生晶间应力腐蚀裂纹（IGSCC）。

3.68. 就反应堆冷却剂压力边界的铁素体材料而言，应该证明它能在高温高压下抵抗快速扩张的裂纹并具有抗疲劳性。所有的不锈钢焊接件应具有抵抗晶界腐蚀的能力，并应该控制 δ 铁的含量，以便尽量减少在焊接奥氏体不锈钢期间形成微裂纹。

3.69. 应该特别注意所用材料在水化学方面的相容性，以便阻止腐蚀现象的发生。对于暴露于湿蒸汽或能引起严重侵蚀的液体之下的所有设备，应该使用耐腐蚀和耐侵蚀的材料。可以使用含铬（Cr >0.5%）低合金钢。

3.70. 选择保温材料时应注意将它们应用所产生的副作用（例如停运期间维修人员受到的剂量、发生事故时阻塞地坑）降至最小。就事故期间保温材料因喷射力产生的碎屑能否引起地坑阻塞这个问题，应该对选定的保温材料进行试验。

3.71. 选择在辐射环境中使用的材料时，应该考虑辐射对材料性质的影响。例如，光纤暴露于中子场时会受到损伤。这会对采用了此种电缆的所有系统（通常是基于计算机的控制和保护系统）的安全功能产生不利的影响。

3.72. 因为辐射的活化，选择在辐射环境中使用哪些材料的决定有可能对退役产生明显的影响。应在设计阶段对这方面问题进行评价。

单一故障评价和冗余度/独立性

3.73. 正如参考文献[1]中所表达的和IAEA“安全丛书”No.50-P-1,《Application of the Single Failure Criterion》[7]中所解释的那样，适用单一故障准则是要确保，假定安全组⁹的任一部件发生单一故障时，发生设计基准范围内研究过的PIE¹⁰之后所需的安全功能仍能得到履行，以及设计基准中针对该事件规定的限值不会被超过。

3.74. 在适用单一故障准则时，应该列出可能因PIE引发的任何故障，并将该故障包括在进行单一故障分析用的起点内。

9 “安全组”的定义是：“指定用于履行特定假想始发事件所需的所有行动的设备集合，其功能是确保设计基准中针对预期运行事件和设计基准事故规定的限值不被超过。”

¹⁰ 关于PIE的定义和更详细的说明，请参看IAEA“安全标准丛书”No.NS-R-1,《核动力厂安全：设计》中的附件。

3.75. 应该针对给机组确定的每一个PIE列出能实现所需要的一组安全功能的安全组。单一故障分析应该列出安全组（包括必需的所有支持系统）内部件的所有故障模式。此外，应该识别可能因单一故障引发的所有故障，并在分析中纳入这些故障与单一故障，其中应该包括可能是由支持系统（诸如电力或冷却水系统）的故障引发的部件故障。然而，在单一故障分析期间的任何时候都不应该假定会发生一次以上的随机故障。

3.76. 在安全组可能出现的最坏配置期间应该适用单一故障准则。特别是，对于机组的运行允许某些设备停止使用相当长的一段时间以便在需要安全组处于备用状态之时进行维修、测试、检查或修理的情况，此时应该假定单一故障发生在由机组的操作规程或技术规格书所允许的设备停运得最多的那种情况实际已经发生之时。尽管如此，正如参考文献[1]第5.38段所说，对于规定的持续时间有限的停运，不遵守单一故障准则的情况可以认为是合理的。对于所有此类情况，连同推导出的允许停运时间，应该解释其合理性（参看参考文献[1]第5.42段）。

3.77. 在单一故障分析中应该考虑的故障一般包括能动部件的故障（诸如按需要打开或关闭的阀门发生故障以及启动与运行用的泵发生故障）和非能动部件的故障（诸如安全系统管道系统的故障），这些故障的发生概率各不相同，分布很广。在单一故障分析中，可以假定非能动部件不发生故障，因为它们的设计、制造、检查和在役期间的维护都会达到极高的质量水平，并假定它们不会受到PIE的影响。不过，应该证明在单一故障分析中省略的每一种部件失效模式的合理性。对非能动部件而言，应该考虑PIE发生后预计该部件还要运行的总时间。在实践中，非能动部件的单一故障常常只是在发生PIE之后的较长一段时间（例如24小时）后考虑，这与所适用的质量标准有关。

3.78. 单一故障分析可以不必处理发生频度很低的PIE，或不必考虑极不可能发生的那类PIE的后果。

3.79. 题为《核动力厂安全：设计》[1]的安全要求出版物规定，假设发生单一故障，机组的相关系统仍应能履行以下安全功能：

- 反应堆快速停堆，
- 从堆芯排出余热，
- 堆芯应急冷却，
- 安全壳隔离，
- 安全壳热量的排出，
- 安全壳大气的控制和净化。

3.80. 在实践中，也许会提供比由单一故障准则导出的冗余度更高的冗余度，以便获得足够高的可靠性或出于运行方面的考虑；例如(i)允许设备停役，以便在需要该安全组处于备用状态之时进行维护或修理；(ii)给监视性测试留有余地；或(iii)减少机组布局方面的困难。这意味着PIE的本身并不是事故。它只是导致运行事件、设计基准事故或严重事故（取决于当时发生的其他故障）的一系列事件中起始事件。典型的例子是：设备故障（包括管道破裂）、人因差错、人类活动诱发事件和自然事件。设备队列之间的连接应该以这种方式来设计，单一故障无法导致一队列以上设备的丧失。冗余队列应该靠屏障或距离分开，以便确保内部危害无法导致一队列以上的设备丧失。

多样性

3.81. 通过使用类似部件来加入冗余的安全系统，其可靠性肯定会受到能导致许多冗余部件同时失效的共因故障的限制。为了消除这种限制，可以通过加入多样性来增加可靠性（参看参考文献[1]附录II）。

3.82. 多样性的程度可以是不同的，取决于所实施的设计方案。如果使用不同类型的设备以物理上不同的方式来履行相同的安全功能，则其多样性程度就高。例如，采用让固体中子吸收剂落入反应堆堆芯和将中子吸收剂溶液注入一回路冷却剂这两种不同系统的停堆系统。当然，如果使用不同类型部件以相同的方式来履行安全功能，则其多样性程度就低。例如，该系统不同部分中的泵和阀门属于不同类型或是由不同制造商提供的应急给水系统。

3.83. 在可靠性要求很高的地方，应该加入多样化的履行安全功能手段。多样性程度应该与履行安全功能的手段所要求的可靠性相称。

3.84. 在安全系统内加入了多样性的地方，应该证明它符合所要求的系统可靠性。就这一点而言，应该对可能存在的共因故障之类的共同弱点进行充分讨论。例如，共同弱点可以是设计缺陷、加工缺陷、运行或维修的差错、自然现象、人因事件，或来自机组内部的其他操作或失效的无意识级联效应。

3.85. 应该认识到，提供多样性会增加机组的复杂性和费用，并给机组的运行和维护增加困难和费用。这应该在设计过程中加以处理，并应该在安全系统可靠性的增加量和附加的复杂性之间取得平衡。

安全重要物项的在役测试、维护、修理、检查和监测

3.86. 除了下文将要介绍的外，安全重要的SSC应该设计得能够在核电机组的整个寿期内定期地就其完整性和履行功能的能力进行测试、维护、修理、检查或监测，根据物项性质的不同，周期可以从几天到几年不等。显然，机组进行不停堆维护的频率越高，则需要在机组停运期间进行的维护就会越少。设计时应该注意这些活动能够按与有待履行的安全功能的重要性相称的标准实施，不会使厂区人员受到过量辐射照射。

3.87. 如果安全重要的SSC无法设计得能使测试、检查或监视达到令人满意的程度，则应该采取充分的安全防范措施以补偿潜在的隐藏故障。

3.88. 设计者应该编写具体的设计导则，以便保证检查和测试的可达性。就此而论，应该评价的关键问题包括：部件周围有足够的空间可供利用；通过减少放射性物质在一回路压力边界内部的沉积或增加屏蔽，减少部件周围的辐射场；减少一回路的泄漏量；准备永久或可拆卸的出入通道，并在构筑物上安装供移动部件用的挂钩；以及将部件安装在便于检查和测试的合适位置。

3.89. 凡是无法达到的地方，可以在设计时准备一些永久性的导轨以及留有足够的空间，允许将被检查设备移到适当的位置并借助遥控器具进行操作。安全评价应该查明此种可能性已经考虑过。

3.90. 虽然实施诸如上文所述的措施在大多数场合下有助于解决保持操作剂量较小的必要性和定期测试与检查的必要性的矛盾，但在某些复杂的场合下，应该在设计层面上通过安全分析精确地研究这两个必要性之间的正确折衷方案。

设备鉴定

3.91. 设备鉴定主要适用于需要在事故工况下履行安全功能的安全系统。

3.92. 期望设备届时能履行安全功能的工况或许与平常的工况不同。随着机组的运行，设备性能也许会受老化或使用条件等因素的影响。期望设备届时能履行安全功能的环境条件，应该作为设计过程的一部分加以明确。预期会在各种事故中出现的此类环境条件包括温度、压力、辐射、振动与湿度的极值，以及喷射冲击。

3.93. 功能方面所要求的能力应该在机组的整个寿期内得到保持。在设计期间，应该注意老化这个共因故障效应。在设计时，应该通过适当地规定环境条件、

工艺条件、负载周期、维护计划、服务年限、典型测试计划、更换零件以及更换间隔等来考虑老化问题。

3.94. 鉴定程序应该确认，在其整个使用寿期内，设备能够在需要时履行其安全功能，并承受相应的环境条件（动力学效应、温度、压力、喷射冲击、辐射、湿度）。这些环境条件包括在正常运行、预期运行事件和事故工况期间预期会出现的偏差。对于设备经历外部自然事件并期望它在此类事件期间或之后能履行安全功能的情况，鉴定工作应该重现这种自然现象施加于该设备上的状态。

3.95. 此外，能够由特定运行工况（诸如在安全壳漏泄率定期测试期间）合理预期以及可能引起的任何异常环境条件，应该包括在鉴定工作内。预期在严重事故期间要运行的设备，应该尽可能地通过测试、实验或工程分析表明它拥有能够在严重事故工况下实现设计意图的合理可信度。

3.96. 通过对原型设备的测试（典型测试）进行鉴定的做法是更可取的。但是，对于大部件的振动或设备的老化来说，这并不总是完全可行的。在这种情况下，应该依靠在相似条件下的设备性能的外推、分析或测试加分析。

老化和已磨损机械

3.97. 安全评价应该考虑机组的系统和部件是按不同尺度受到老化效应的影响。其中的某些效应是大家所熟知的，也能够采取相应措施。但经验表明，一些其他效应是不可预见的，因而应该采用合适的测试、检查和监视计划，以便探测这些效应是否可能发生。应该拟定准备在该机组使用寿期内实施的完整行动计划，并在设计阶段确定实施这一计划的技术前提。定期的安全审查是判断老化和已磨损机械是否已经得到了正确考虑的好方法，也是探测预料之外的问题的好方法。

3.98. 设计压力容器时应该考虑在机组的整个寿期内由来自堆芯的快中子通量的作用引起的脆裂。由良好的设计提供的保护措施能防止脆裂过量、便于探测脆裂和有可能采取补救措施。由于尺寸和/或中子学效应方面的差别，这个问题对压水反应堆（PWR）的影响比对沸水反应堆（BWR）的影响更严重。焊接区更容易受脆裂的影响，因为焊接过程引入的杂质可以致使焊接区对 neutron 辐射特别敏感。焊缝周围的焊接热影响区（HAZ）常常是微裂纹和残余应力积聚的地区，使得该地区对脆裂的效应愈加敏感。

3.99. 只要切实可行，应该避免在活性燃料区段的范围内存在焊缝。

3.100. 对于限制和监测压力容器的脆裂这个问题，应该进行相应的研究。为此，应该在考虑了不确定度的情况下，将中子注量（中子通量在该机组使用寿期内的积分）保持在能确保足够的机械性能得到保持的水平以下。应该确保备有相应的监测计划，具体做法是使压力容器焊缝样品和中子注量测量器具暴露于有代表性的中子通量之下。另一个较大的老化过程影响着PWR的蒸汽发生器传热管系统。传热管的质量会因多种原因而劣化，应该对此进行监测，以便允许采取预防性的和补救性措施，诸如改变水化学和在泄漏或失效之前修理或堵塞管道。机组的设计应该通过留出充足的间隔、铺设导轨和固定点，以便于蒸汽发生器的监视、修理和更换。

3.101. 过去的运行经验表明可能发生的其他老化效应见下文。机组的设计应该将这些问题在设计阶段排除掉，或引入能在其发生的初始阶段就可及时探测的手段以及和实施相应纠正行动的手段：

- 在压力管式反应堆中，压力管的氢化和脆裂可能导致更换压力管；
- 振动和失效，压力容器内部构件的腐蚀，这些现象应该是可以用合适的监视手段检测到的；
- 堆芯管嘴和反应堆内部构件产生裂缝；
- 管嘴和导管中发生的热瞬变和压力瞬变；
- 发生在管接头处的热混合；
- 导管中的温度分层及部件中的其他管道侵蚀，这些现象应该是可以靠定期检查检测到的，并应借助合适的设计措施使检查比较容易；
- 电缆绝缘层有机材料或通风系统密封材料的老化，应该在设计中加以考虑，以便允许探测和可能时更换。

人-机接口和人因工程的适用

3.102. 关于在设计中如何适用人因工程原则的详细建议，见IAEA专门的安全导则¹¹。本节将简述某些关键问题。

¹¹ “安全丛书”Nos 50-SG-D3, Protection System and Related Features in Nuclear Power Plants (1986); 50-SG-D8, Safety-related Instrumentation and Control Systems for Nuclear Power Plants (1984); 以及“安全标准丛书”No.NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants (2000) .

3.103. 机组设计应该使操纵员的工作比较方便，以发挥人在运行状态和事故期间的最佳表现。这应该通过在机组设计、运行规程编制和所有操作人员的培训中给予特别关注来完成。

3.104. 应该在设计开发阶段初期就系统地考虑将人因工程和人-机接口包括在设计过程内，并应该持续贯穿于整个设计过程。

3.105. 应该明确列出哪些安全动作是指定要操作人员完成的，其中应包括由负责监测和控制机组、负责对故障作出反应的操纵员执行的安全行动，以及负责维护、测试和标定活动的操纵人员执行的安全行动。

3.106. 应该针对安全行动进行任务分析，以便从决策和执行的角​​度评估可能会施加在操纵员身上的要求。此种任务分析的结果应该决定人-机接口的设计规范、有必要提供的信息和控制措施、运行规程的编写和培训计划。

3.107. 所提供的信息和控制措施应该足以允许操纵员：

- 执行改变反应堆功率水平之类的正常运行；
- 容易地评估机组正常运行、预期运行事件和事故工况时的总体状况；
- 监测反应堆的状况和所有机组设备的状况；
- 识别安全重要机组状况的变化；
- 证实预定的自动安全行动正在执行；
- 识别任何规定动作并执行。

3.108. 应该向操纵员提供有关单个机组系统和设备各种参数的足够信息，以便证实所要求的安全行动已经完成和提供这些行动已经取得预期效果的反馈。

3.109. 厂区运行人员的工作场所和工作环境应该按照人机工程学的原则进行设计，以便使任务能够可靠而高效地完成，其中应包括中央控制室、应急控制室、电厂内的任何就地控制站和可能会执行维护与测试任务的任何场所的设计。应该特别注意显示系统、仪表板布局和工作场所内供维修和测试用的出入口。

3.110. 应该将人-机接口设计得能给操纵员提供包罗万象但易于处理的信息，供他作出正确判断并采取正确动作。

3.111. 应该将需要操纵员在较短时间内进行干预的必要性保持在最低限度内。应该给所有需要在较短时间内采取的动作提供自动化设备。应该根据可证明的最佳估计基础来评价时间裕量。

3.112. 就所有的操纵员动作而言，任务分析应该证明操纵员有充足的时间做出决定和采取行动，证明供做出决定用的信息是简单的并以毫不含糊的方式提供，

并证明控制室或辅助控制点与该控制点的出入口内发生事件后的物理环境是可接受的。

3.113. 机组的设计应该对人的差错比较宽容。只要切实可行，应该使任何不恰当的人的动作不起作用。就此而论，应该在操纵员动作和安全系统启动之间小心地选择优先权。一方面，只要干预的初始准则适用，就不应该允许操纵员超越反应堆保护系统动作。另一方面，在有些场合下，操纵员干预保护系统是必要的。例如为了进行测试或为了修改运行状态采用干预准则进行手动旁路。此外，一旦反应堆保护系统内部发生较大故障，则操纵员应该在严格的行政控制下，出于处理超设计基准事故的考虑而拥有最终干预保护系统的可能性。

3.114. 应该给由操作人员执行的所有活动编写书面规程，包括机组的正常运行和从异常事件与事故（包括严重事故）中恢复。响应异常事件和事故的规程最好是征兆导向的。如情况合适，此类规程应该通过简单的演习和使用原尺寸的实物模型与模拟器进行验证。

3.115. 应该提供充足而可靠的通信手段，使信息与指令能够在各个位置之间顺利传输，以便在正常运行和事故后的恢复期间支持操纵员的行动，其中应包括在主控制室或应急控制室与身在远处的也许必须采取影响机组状况的行的操作人员之间的通信，以及发生事故时与厂区外有关单位之间的通信。通信工具应该在所有相关事故工况下都是可利用的，并应该不与电厂的保护系统相干涉。

3.116. 设计位于远处的控制器件的布局和标识时应该牢记人为因素，以降低操作者在选择位于远处的控制器件时出错的偶然性。

系统的相互作用

3.117. 应该仔细地评估同一机组的各个系统之间、机组和厂外公用事业之间，以及同一厂址上的不同机组之间可能发生的相互作用。应该针对包括外部危害和严重事故在内的所有机组运行状况研究系统的相互作用问题。

3.118. 这种分析不仅应该考虑它们在物理上的互连，而且还应该考虑系统的运行、维护、失灵或失效对其他安全重要系统的物理环境的影响。环境方面的变化会影响系统按预定设置履行功能的可靠性。能够对其他系统的表现产生不利影响的失效例子是，电子设备用的通风的失效，或者流体系统的失效导致装有安全系统设备的区域水淹或湿度过大。

3.119. 正如在特定IAEA“安全导则”¹²中详细讨论过的那样，在对设计进行安全评价时，应该对电网-机组的相互作用进行研究，因为给机组的安全重要系统供电的电源需要有较高的可靠性。

3.120. 安全重要的构筑物、系统和部件，最好不要由两座以上的核动力反应堆共用。不过，如果真的要这样做，则应该通过测试、实验或工程分析证明，在一切状态下对所有反应堆的所有安全要求都能够得到满足。万一发生涉及其中一座反应堆的事故工况，则其它反应堆的正常停堆和排除衰变热应该是可以完成的。对于有可能引起一台以上的机组发生事故的外部事件，应该进行专门研究。公用支持系统应该有能力应付所有受到影响的反应堆。

3.121. 在安全评价时应该核对的其他设计和运行接口，包括规范和运行规程。

在设计过程中使用计算工具

3.122. 工程设计要用到大量软件工具，诸如图表、字母图案、公式、算法和计算机程序（中子物理学、流体动力学、结构分析等等）。这些工具中，包括所用的数学模型，都应该按合适的质量保证程序，包括按照第4节（第4.236—4.244段）中描述的适用于计算机程序的方法对它们进行验证和确认。

3.123. 所有的数学模型应该通过比较、独立的分析和验证表明它们的可靠性，目的是确保它们所固有的不确定度达到整个设计项目所要求的可靠性。

4. 安全分析

通用的指导意见

4.1. 安全分析的目标应该是借助合适的分析工具建立和确认有关安全重要物项的设计基准，并确保整个机组设计能够满足针对每一种机组条件规定的和可接受的辐射剂量和释放量的限值。设计、制造、建造和调试应该与安全分析结合起来进行，以确保设计意图已在竣工机组中得到体现。

¹² “安全丛书” No.50-SG-D7, Emergency Electrical Power Systems at Nuclear Power Plants (1991)。

4.2. 安全分析作为设计过程的一部分,应该由负责安全供应核电的两个单位进行。这两个单位是:

- 设计者,它把安全分析当作设计过程不可缺少的重要部分,且一直要延续到机组的制造和建造中。
- 营运单位,它使用安全分析确保竣工设计在运行时能像所期望的那样履行其功能,并证明该设计在机组的设计寿命中的任一点都满足安全要求。

4.3. 安全分析是申请机组许可证时实施的安全评价的一部分,它应该与设计过程齐头并进,而且应该在这两种活动之间进行迭代。安全分析的范围和详尽程度应该随着设计工作的进展而增加,以便最终的安全分析能反映机组建成时的最终设计。

4.4. 供设计过程中进行安全分析用的建议,也可用作对正在运行机组进行定期安全分析或判断建议的设计修改的安全合理性的指导性意见。有关定期评价的要求见有关运行安全要求的IAEA“安全导则”和支持性“安全导则”。

4.5. 机组设计的模型和数据(这些是进行安全分析必不可少的基础),应该在设计阶段和机组的整个使用寿命(包括退役)内及时进行更新。在设计阶段,更新工作应该由设计者负责;在机组的整个寿命期内,则由营运单位负责。

4.6. 更新过程应该加入一切可获得的新信息、论述新出现的问题、当可以取得更加精益求精的工具和方法时使用此类工具和方法,以及评价设计和运行规程的修改后果(此事在机组的整个寿命期内也许都要考虑)。

4.7. 第3节中叙述过的对安全重要工程问题的评价以及本节叙述的安全分析,应该同步进行。

安全分析的任务

4.8. 安全分析应该针对大量运行工况、假想始发事件(PIE)及其他环境条件(其中的许多条件在机组实际运行时或许是从来不会观察到的)评价机组的行为,以便获得机组在这些场合会有什么表现的全面了解。安全分析还应该证明机组是能够保持在由设计者制定的安全运行范围之内的。

4.9. 安全分析应该根据由营运单位、监管机构或本国或国际其他主管部门可能制定的适用于机组的有关安全和放射性释放量的目标或准则,对机组在各种运行工况和事故工况之下的行为进行正式评价。

4.10. 安全分析应该找出设计中潜在的薄弱环节，评价建议的设计改进，以及提供安全要求已得到满足和机组产生的风险是低得可以接受的证明。如果已经详细规定了风险标准，则安全分析应该包括与此种风险标准进行的比较。

4.11. 安全分析应该充当提出和确认机组保护与控制系统的整定值和控制参数的重要工具，以此来支持机组的安全运行。它还应该被用于制定和验证机组的运行技术规格书与限值、正常和异常情况下的运行规程、维护和检查要求，以及正常和应急的程序。

4.12. 当机组在寿期内出现新问题时，安全分析还应给机组的管理机构和监管机构的决策过程提供支持。在机组的整个寿期内，应该保留机组最初的安全分析，并保持为了解决新的技术问题而再次进行全部或部分此种分析的能力。这意味着应该把机组实际的最新设计资料和运行实绩数据列入机组模型内，以便为实施这种分析提供支持。

4.13. 安全分析应该有助于发现在设计的最初阶段中没有充分考虑到问题、机组工况和始发事件。同样地，安全分析能够找出一些没有必要的PIE或既定的验收标准之类的问题（也就是说，根据更深入的考察，由于此类问题的发生频率极低、无关紧要的条件性概率或潜在后果的影响极小，它们不影响机组的安全性或无助于机组的安全性）。

4.14. 安全分析应该评价：

- 是否已经提供了足够的纵深防御，防御的水平是否保持在使潜在的事故序列能被尽早切断的水平上。
- 机组能否经得起它可能会经历的物理条件和环境条件，其中包括环境条件及其他条件的极值。
- 人因工程和人的行为问题是否已得到充分的论述。
- 有可能在机组寿期内降低机组可靠性的长期老化机制是否已经找到、受到监测及处理（即通过设备升级、整修或更换），以便不影响安全性和不增加风险。

4.15. 安全分析应该通过测试、评估、计算或工程分析证明，为防止预期运行事件或设计基准事故逐步升级为严重事故并减轻其影响而采用的设备，以及应急运行规程和事故管理措施，在将风险减少至可接受的水平方面是有效的。

4.16. 安全分析过程应该是非常可信的，且其范围、质量、完整性和准确度足以使设计者、监管者、营运单位和公众相信机组的设计是安全的。安全分析的结果必然会以较高的置信度使人确信机组将会按设计运行，并确保它在调试期间和机组整个寿期内能满足一切设计验收准则。

确定论和概率论评价工作

4.17. 应该主要采用确定论方法来证明是否已达到较高的安全水平。不过，安全分析应该同时采用确定论和概率论两种方法。事实表明，这两类解决方法是相辅相成的，在有关待批准机组的安全性和能力的决策过程中，这两类方法都应该使用。概率论方法能够提供不靠确定论方法获得的有关对机组性能、纵深防御和风险的见解。

4.18. 确定论方法的目标是处理机组在特定的预定运行状态和事故工况下的行为，并在判断设计的适当性时使用一组特定的规则。

4.19. 一般说来，供设计用的确定论分析应该是保守的。与设计基准事故分析相比，超设计基准事故分析的保守程度通常要小一些。

4.20. 概率论安全分析（PSA）应该着手确定有关机组风险的一切重要影响因素，并评价整个系统配置的设计究竟均衡到什么程度、是否存在风险异常值，以及设计是否满足基本的概率论目标。PSA最好使用最佳估算法。

4.21. 从确定论分析和PSA法得到的见解都应该在决策过程中得到应用。总的说来，这些见解通常是一致的。特别是，凡是在机组的设计或运行中发现有薄弱环节的地方，通常与用于执行一项或多项安全功能的安全系统的冗余度或多样性水平较低有关。

4.22. 在某些场合，确定论分析和PSA得到的见解并不一致。对于这些场合，应该进行个案研究。

基本信息

4.23. 安全分析过程应该以完整而正确的机组设计信息为基础。这些信息应该涵盖机组的一切SSC、厂区外接口和因厂址而异的种种特性。

4.24. 机组设计应该形成文件，并且随着机组设计的得到核准、机组竣工和修改完成而及时更新。

4.25. 对于正在运行的机组，安全分析（例如针对设计修改进行的安全分析）应该使用因机组而异的运行数据，其中包括有关操作人员在正常运行期间受到的放射性剂量的信息，以及厂区例行排出的放射性物质数量的信息。就机组的各系统而言，收集的数据应该包括正常运行时的温度、压力、液位和流量、以及任何运行事件的瞬变响应特性和时间。

4.26. 运行数据还应该包括有关部件和系统的行为的信息、始发事件的发生频率、部件失效率数据、失效模式、维护或测试期间的系统不可利用率，以及部件与系统的修理时间。

4.27. 就处于设计阶段的机组而言，所用的数据应该由来自具有类似设计的正在运行机组的通用数据导出，或由来自研究或测试结果的数据导出。就正在运行的机组而言，这种通用数据库的某些部分可能会随着时间的推移而不断增加，这是由于从该机组本身运行史和维护数据、经验以及检查结果导出的因机组而异的数据在不断增加。

4.28. 安全分析应该涵盖机组内的一切放射性物质源。除反应堆堆芯外，还包括运输途中的辐照燃料、库房中辐照过的燃料和贮存的放射性废物。

安全分析的验收准则

4.29. 应该规定确定论评价和PSA用的验收准则。这些验收准则通常是设计者或营运者所用准则的翻版，并且与监管机构的要求是一致的。

4.30. 这些准则应该足以满足IAEA的安全基本原则[2]和《核动力厂的安全：设计》[1]中给出的“核安全的总目标”、“辐射防护目标”和“技术安全目标”。

4.31. 此外，应该制定详细的准则，用于帮助确保这些较高层次的目标得到满足（参看下面的第4.98段和第4.103段）。这些详细的准则通常会使分析工作简单化。

4.32. 关于概率论的安全准则，若法律或监管部门的要求中有明确的规定则应该引用，或在情况合适时应该重新制定。这些应该与发生具有明显放射性后果的事故（诸如，堆芯损坏、较大的厂区外释放量以及工作人员和公众成员受到的辐射剂量）的可能性有关。

假想始发事件

确定PIE

4.33. 安全分析的起点是需要处理的一组PIE。在参考文献[1]中，PIE的定义是“能导致预期运行事件或事故工况的已确定事件”。PIE包括设备失效、人的错

误和人诱发的或自然发生的事件之类的事件。确定论安全分析和PSA通常应该共用一组PIE。

4.34. 为了进行安全分析而拟定的一组PIE应该是包罗万象的，而且定义时应该涵盖机组的系统和部件的一切可信失效以及在机组的任何运行方式(诸如启动、停堆和换料)期间可能产生的人的错误，应该既包括内部始发事件，又包括外部始发事件。

4.35. 应该以系统的方式确定这组PIE，其中应该包括采用结构化方法来确定PIE，此类方法可能包括：

- 使用危害与可操作性分析法 (HAZOP)¹³、失效模式与效应分析法 (FMEA)¹⁴，以及主逻辑图之类的分析方法；
- 与为类似机组的安全分析编制的PIE清单相比较（虽然这种方法不宜单独使用，因为先前的错误可能会因此而扩散）；
- 分析类似机组的运行历史数据。

4.37. 一组PIE应该随着设计与安全评价工作的向前推进而不断进行复查，而且应该是在这两种活动之间进行迭代。

4.38. 一组PIE还应该包括发生频率很低或后果很轻微的事件，至少在这一过程开始时如此。删去某些PIE也许是可能的。然而，应该证明删去任何PIE是有充分理由的，而且应该把这些理由形成文件。许多PIE将伴随这项分析直到最后，而且只有到这一过程完结时才能断定它是不是无关紧要的。

4.39. 所有的PIE都应该用其发生频率做定量的定义。虽然对各种PSA应用的发生频率应该进行定量定义，但在确定论分析中它是被定性使用的。

内部PIE

4.40. 应该编制内部PIE（起源于机组内部的PIE），以便识别可能存在的对基本安全功能的挑战。虽然履行安全功能的方式与反应堆的详细设计有关，但确定的始发事件类别一般包括：

¹³ HAZOP是一种系统方法，它使用一组关键字来确定可能发生的与可能导致PIE的失效。

¹⁴ FMEA是一种系统方法，它研究每一种部件失效模式，然后确定它们会不会导致PIE（参看参考文献[10]附录V）。

- 从反应堆冷却系统排出的热量增加或减少，
- 反应堆冷却系统的流量增加或减少，
- 反应性分布和功率分布异常，
- 反应堆冷却剂存量增加或减少，
- 从子系统或部件中释出放射性物质。

4.41. 确定一组内部PIE的工作还应该研究安全系统和部件的各种失效方式，以及有可能影响基本安全功能或安全系统的非安全系统和部件的失效方式。其中的大部分失效可以归入上述的若干种类别之一。然而，其中基于PIE的某些失效不属于上述的任何类别，因而被单独归为一类。到目前为止，由PSA判断过的这些其他失效的例子包括：(a) 失去设备冷却水或失去服务水之类的辅助系统失效；(b) 由循环水、服务水、消防或高位辅助水箱的失效引起的内部水淹；(c) 导致一回路系统泵失冷的假的安全壳隔离信号；以及 (d) 泄压阀意外开启。

4.42. 确定一组内部PIE的过程还应该考虑处理反应堆压力边界的各种失效模式，其中包括发生在一切可能发生之处的管道破裂，包括有可能发生在安全壳之外的管道破裂。

4.43. 内部PIE应该包括所有机组运转模式期间可能发生各种失效模式（例如，在最初的堆芯达到临界期间的反应性瞬变以及在安全壳处于开放状态下的换料模式期间冷却剂存量损失），持续时间可忽略不计的失效模式除外。持续时间可忽略不计的模式应当经过细心研究及保守分析，只有在证明它们与计算出的由其他PIE引起的堆芯损坏频率相比是不重要的以后才能排除。

4.44. 一组PIE应该包括由于人的错误而可能发生的PIE。此类PIE的范围可以从维修作业有过失或不安全，到控制设备限值的整定值不正确或操纵员动作有误。这些PIE未必与由设备失效引起的PIE相类似，因为它们中除了始发事件之外，还可能包括共因故障。

4.45. 一组内部PIE应该包括火灾、爆炸、汽机飞射物碰撞和内部原因引起的水灾之类的事件，它们可能会影响反应堆安全并引起给始发事件提供保护的一些安全系统设备失效。这些PIE早已第3节中讨论过。

外部PIE

4.46. 已确定的一组PIE应该包括可能由机组外部引起并可能威胁核安全的所有事件，包括自然发生和人诱发的事件。这些外部始发事件可能导致内部始发

事件和某些安全系统设备的失效，因而需要提供保护以避免发生此类事件。举例来说，地震除了可能导致丧失厂外电源之外，还可能导致机组设备失效。

4.47. 应该将肯定会在指定厂区发生的自然事件纳入到供安全分析用的一组PIE内，其中应该包括地震、厂区外发生的火灾和水灾（包括由水坝、河堤或海堤的崩塌引起的水灾）、极端恶劣的气候条件（温度、降水、降雪，强风）和火山喷发之类的事件。

4.48. 应该将肯定会在指定厂区发生的人诱发事件纳入到供安全分析用的一组PIE内，其中应该包括飞机坠毁、附近的工厂和运输系统的爆炸效应。

4.49. 有关外部事件的详细建议，可以在IAEA有关选址的安全要求¹⁵和支持性的安全导则中找到。

确定论安全分析¹⁶

正常运行

4.50. 有关正常运行的安全分析的目标是评价以下内容：

- 机组的正常运行能否安全地进行，

因此要证实：

- 工作人员和公众成员受到的放射性剂量在可接受限值的范围之内，
- 机组计划释放的放射性物质量在可接受限值范围之内。

4.51. 有关正常运行的安全分析涉及系统和设备按照预期运行所处的、没有内部或外部挑战的所有机组工况。这包括机组预定在其整个寿期内的正常运行和维护期间的所有运行阶段，既包括功率运行，又包括停堆状态。

4.52. 核发电机组的正常运行一般包括：

- 反应堆初次接近临界；
- 反应堆从停堆状态通过临界到达功率运行的正常启动；
- 功率运行，包括满功率和低功率；

¹⁵ “安全丛书” No.50-C-S (Rev.1), 《核动力厂安全规范：选址》(1988)。

¹⁶ 更详细的资料可以在题为《核动力厂的事故分析》(正在编写)的IAEA安全报告系列出版物中找到。

- 反应堆功率水平变化，包括负荷跟踪模式（如果采用的话）；
- 反应堆从功率运行停堆；
- 热备用模式的停堆状态；
- 冷停堆模式的停堆状态；
- 换料模式或等效维护模式的停堆状态，此时反应堆冷却剂压力边界中的较大密闭件打开；
- 其他模式或具有独特的温度、压力或冷却剂存量条件的机组配置条件下的停堆状态；
- 新的和辐照过的燃料的装卸和贮存。

4.53. 安全分析应该评价机组的正常运行能否以机组的参数值不超过运行限值的方式安全进行。

4.54. 安全分析应该制定供安全运行用的工况和限值。这些工况和限值当然会包括若干项，诸如：

- 反应堆保护和控制系统及其他专设安全系统的安全限值，
- 控制系统的运行限值和参考性整定值，
- 工艺运行管理程序性约束条件，
- 允许的运行配置。

更详细的资料见参考文献[8]。

4.55. 对在正常运行时的设计进行的安全评价应该证实，反应堆事故保护停堆或安全系统只有在需要时才会启动。错误的事故保护停堆或安全系统的错误启动对安全来说通常是有害的。

工作人员和公众成员受到的来自正常运行的放射性剂量

4.56. 对正常运行进行的安全分析应该包括对机组总体的设计与运行情况进行分析，以便：预测工作人员和公众成员可能受到的辐射剂量；评价这些剂量值是否在可接受限值范围以内；以及保证这些剂量应该是合理可行尽量低（ALARA）这一原则已得到满足。

4.57. 对于厂区内工作人员来说，剂量预测值应该以机组的运行和维修时涉及的特定作业为基准。剂量预测值应该包括来自直接的辐射照射和摄入的放射性物质的作用。分析应该考虑每项活动的持续时间、频率和人数。估计值应该包括个人的最高剂量和人群的年平均剂量两类。

4.58. 对于公众成员来说，剂量预测值应该包括来自直接的辐射照射、摄入的放射性物质和通过食物链受到的剂量的贡献，且这些都是由机组排出的放射性物质引起的。这些剂量应该是针对关键人群估算出的。

4.59. 当计算出的剂量预测值有不确定度时，应该采用保守假设。

4.60. 当剂量预测值与由放射性物质存量的累积而引起的剂量率，或与由污染水平引起的剂量率有关时，预测值应该以机组使用寿期内可能出现的最大值为基础。

4.61. 剂量预测值应该考虑相关的任何运行经验数据。此类数据可能从实际机组或类似机组的运行导出。

4.62. 这些剂量估计值应该与专门为机组拟定的放射性判据相比较。此类判据应该包括法律要求或监管者要求的剂量限值，并应该考虑国际辐射防护委员会（ICRP）现行的建议。

4.63. 应该对这些剂量估计值的结果进行评价，以便找出机组的设计或系统中的任何薄弱环节；当合理可行时应该进行改进。

来自该机组的放射性物质计划释放量

4.64. 对正常运行的安全分析应该包括估算机组的放射性物质计划释放量。

4.65. 放射性物质计划释放量的估算值应该与为机组拟定的放射性判据（包括任何法律要求或监管机构要求）相比较，并对照ALARA原则进行审查。应该对机组的设计和运行进行评价，而且当合理可行时进行改进，以便减少计划的释放量。

预期运行事件和设计基准事故

4.66. 在设计基准分析中研究过的机组工况包括预期运行事件和设计基准事故（DBA）。这种划分基于事件的频率。

4.67. 预期运行事件是指比正常运行期间进行的操作更复杂，并且可能挑战反应堆安全的那些事件。也许可以预计，在机组的使用寿期内这些事件至少发生一次。通常它们的发生频率大于 10^{-2} 每堆·年。

4.68. 设计基准事故的发生频率低于预期运行事件的发生频率。预计在该机组的使用寿期内它们不会发生，但依照纵深防御原则，在设计核电机组时已经考

虑过这类事故。DBA的发生频率在 10^{-2} — 10^{-5} 每堆·年的范围内，虽然传统上包括在设计基准分析内的几组PIE的发生频率或许更低。

4.69. 设计基准分析的目标应该是给工程设计的容忍错误能力和安全系统的有效性提供强有力的证明。这种分析是通过实施应该考虑模型中的不确定度的保守分析进行的。

导致预期运行事件的假想始发事件

4.70. 对于许多PIE来说，控制系统肯定能补偿事件的效应而不会引起反应堆事故保护停堆或给安全系统施加其他要求（第2层纵深防御）。然而，属于预期运行事件的这一类事件应该预期把在机组的使用寿命内可能会发生的、而且在故障排除后能重新开始运行的所有PIE都包括在内。

4.71. 导致预期运行事件的PIE的典型例子可能包括下文列出的情况。这份清单显然只是象征性的。实际的清单与反应堆的类型和实际的机组各系统的实际设计有关：

- 反应堆排出的热量增加：蒸汽泄压阀意外开启；二回路压力控制失灵导致蒸汽流量增加；给水系统失灵导致热量排出率增加。
- 反应堆排出的热量减少：给水泵跳闸；由于种种原因（控制失灵、主汽阀关闭、汽轮机脱扣、失去外部载荷、失电、失去冷凝器真空度）导致蒸汽流量减少。
- 反应堆冷却系统流量减少：一台主冷却剂泵脱扣；一个主冷却剂系统环路意外地被隔离（如果可适用的话）。
- 反应性分布和功率分布异常：控制棒意外地抽出；由于体积控制系统失灵使硼稀释（对PWR而言）；燃料组件放错位置。
- 反应堆冷却剂存量增加：化学和体积控制系统失灵。
- 反应堆冷却剂存量减少：仪器管线失效引起的很小的失冷事故（LOCA）。
- 从子系统或部件中释出放射性物质：放射性废物系统发生少量泄漏。

导致DBA的假想始发事件

4.72. 应该确定被认为能导致DBA的PIE子集。还应该将被确定为预期运行事件引发因素的所有PIE看作是DBA的潜在引发因素。虽然通常不把发生频率很低的PIE包括在内，但制定任何阈限的工作应该考虑为特定反应堆制定的安全目标。

4.73. 导致DBA的PIE的典型例子可能包括下类列出的情况。这份清单显然只是象征性的。实际的清单必然与反应堆的类型和实际的设计有关：

- 反应堆排出的热量增加：蒸汽管道破裂。
- 反应堆排出的热量减少：给水管道破裂。
- 反应堆冷却系统流量减少：所有的主冷却剂泵脱扣；主冷却剂泵卡死或轴断裂。
- 反应性分布和功率分布异常：控制棒不受控制地提起；控制棒弹出；由于被动环路启动而硼稀释（对PWR而言）。
- 反应堆冷却剂存量增加：应急堆芯冷却意外运行。
- 反应堆冷却剂存量减少：可能的LOCA谱；意外打开一回路系统泄压阀；一回路的冷却剂漏入二回路系统。
- 从子系统或部件中释出放射性物质：使用过的燃料在运输途中或贮存时过热或损坏；气体或液体的废物处理系统破裂。

4.74. 应该指出，历史上已被作为DBA处理过的一些事故的引发因素的发生频率也许低于 $10^{-5}/a$ 。对于已设计和按现代标准建造的机组来说，大破口LOCA之类的PIE就是这样的情况。然而，监管部门的法规或许仍然要求将这种PIE放在DBA这一类加以考虑。

分组

4.75. 根据上文提供的指导性意见，将会确定大量的PIE。没有必要对所有这些PIE都进行分析。正常的做法是将它们分组，并从每组中选出一些包络性限定的事例进行分析。

4.76. 这些包络性的事例应该能识别对已确定的每一项主要安全功能构成最严重挑战的事故。在有些情况下，从某个安全参数（例如，反应堆冷却系统峰值压力）角度看，某一起事故可能是非常严重的，而从另一个安全参数（例如，燃料峰值温度）角度看，就可能是另一起事故才是非常严重的。在这些情况下，所有这些事故序列都要在设计过程中被处理成包络性的事例。

4.77. 安全分析应该证实将这种始发事件的分组和包络性的做法是可接受的。

分析预期运行事件和DBA的目的

4.78. 预期运行事件和DBA的安全分析应该证明安全系统能够履行在以下诸方面的安全要求：

- 能在DBA工况期间和之后使反应堆停堆并保持安全停堆状态。
- 能在从所有运行状态和所有DBA工况停堆以后从堆芯排除余热。
- 能减少释放放射性物质的可能性,并确保任何释放在运行状态期间低于规定限值和在DBA工况期间低于可接受限值。

4.79. 安全分析应该表明机组限值和放射学限值都没有被超出。特别应该证明,防止放射性物质从机组向外释放的某些或所有屏障的完整性都能保持在所要求的范围内。

4.80. 安全分析应该给设计的各种能力和保护系统规定各种整定值,用于确保基本安全功能一直能得到保持。设计基准事件是反应性控制系统、反应堆冷却系统、专设安全设施(例如堆芯应急冷却系统、安全壳系统和安全壳保护系统)、电力系统以及各种安全重要的辅助系统的设计基础。

4.81. 用于评价事件的时限应该长得足以确定设计基准事件的所有后果。这意味有关机组过渡过程的计算工作要扩展到机组已停堆和安全冷却系统已启动(即直至已到达长期的稳定状态)之后。

4.82. 对于新机组和正在进行定期安全评价的机组,应该对所有设计基准事件进行确认和评价。对于已有机组的改进来说,评价应集中在会受到改进影响的设计基准事件上。

4.83. 对于已有机组的改进或再评价来说,在原设计中使用的成套方法和假设由于以下几方面原因可能需要作些改变:

- 原先的设计依据或验收准则或许已不再适用。
- 使用的安全分析工具也许已经被更完善的方法所取代。
- 原先的设计依据或许已不再能得到满足。

4.84. 针对预期运行事件进行的安全分析,本质上与针对事故进行的安全分析是相同的。然而,对于前者来说,这种分析不必像针对DBA的分析那样保守。举例来说,预期运行事件的分析不必假定所有非安全系统和设备都不可利用。

4.85. 此外,预期运行事件应该不会导致对主要用于发生DBA时起保护作用的安全设备的任何不必要挑战。

预期运行事件和DBA的分析方法和假设

方法

4.86. 预期运行事件和DBA的安全分析应该使用合适的中子物理学、热工-水力学、结构与放射学的计算机程序，来确定反应堆对这些运行事件和事故的响应。

4.87. 被用来进行预期运行事件和DBA分析的计算机程序应该得到充分的证实和验证。这包括用于预测反应堆堆芯行为的程序、热工-水力学程序，以及放射性释放量及其后果程序。此外，程序分析人员和用户应该具有相应的资格和经验，并受过培训。

4.88. 对DBA /预期运行事件进行安全分析的计算机编码，应该利用能从类似核电机组和相关的试验数据导出的运行经验。因为预计在机组的使用寿命内会发生一次或一次以上的预期运行事件，因而已经积累了有关此类过渡过程的一些运行经验和数据。

4.89. 构成使用其基础的计算机程序模型参数、初始条件和设备可利用率假设传统上是非常保守的，所有分析参数具有包络性和比较保守。然而，在过去，这些值有时会得出把人引入歧途的事件序列、预测出不切实际的时间尺度，并遗漏一些物理现象。在铭记这些缺点和当前最佳估算程序的成熟程度的同时，在进行安全分析时，应该将其与适当保守地选择输入数据和对结果的不确定度进行充分评价结合起来使用。

4.90. 将最佳的计算机估算程序和比较现实的初始条件假设与边界条件假设结合起来使用，或许也是可接受的。此种解决办法应该以用统计学方法组合起来的有关机组工况和机组程序模型的不确定度为基础，以便在规定的较高概率条件下确定计算结果不会超过验收准则。

4.91. 安全分析应该有合适的质量保证大纲。特别是，一切数据来源应该是有根有据的并形成文件，整个过程应该记录在案并归档，以便允许独立的核对。

假设

4.92. 供设计基准分析用的保守假设一般包括：

- 有关反应堆初始状态（包括功率水平、余热水平、反应性状况、反应堆冷却系统的温度、压力和存量）的始发事件是在不利的时刻发生的。
- 应该假定任何控制系统只有当其履行功能将会加重始发事件的效应时才运行。不相信控制系统的运行可以为减轻始发事件的效应发挥作用。

- 对没有被指定为安全级（全面质量保证、抗震的和设备的合格鉴定）和不按安全级进行维护的一切机组系统和设备，应该假定其失效能使正在分析的PIE产生最严重后果。
- 应该假定最坏的单一故障发生在始发事件所需的安全组正在运行时。对于冗余系统来说，常常假定启动和运行的队列数目最小。
- 应该假定安全系统是在其性能指标最差的状态下运行的。对于反应堆事故停堆和安全系统的触发系统来说，应该假定它们的动作发生在可能的变化范围内的最坏端。
- 事故期间不能被认为是完全可运行的或会达到限值的任何构筑物、系统或部件、且设计者未曾证明它们在事故期间是完全可运行的，则应该假定它们在事故期间是不能利用的。
- 只有可以表明机组工作人员有足够的时间进行所要求的动作、有充足的信息可用于事件诊断（考虑始发事件效应和单一故障准则）、备有合适的书面规程，以及已受过足够的培训后，才可以对他们的防止事故或减轻事故后果的动作进行模拟。一般假定机组工作人员的行动发生在事件开始后的10分钟。

4.93. 所作出的保守假设应该考虑反应堆初始条件的不确定度，包括安全系统触发整定点。

4.94. 设计基准分析应该包括由于始发事件（因此它也是PIE的一部分）而可能发生的任何失效。此事包括以下几项：

- 如果始发事件是部分配电系统失效、则DBA分析应该假定一切由这部分配电系统供电的设备是不可利用的。
- 如果始发事件是高能的事件，诸如导致释放热水的承压系统失效或管道甩动，则DBA的定义应该包括可能受到影响的设备的失效。
- 对于火灾或水灾之类的内部事件或地震之类的外部事件，设计基准事件的定义应该既包括设计用于承受此类事件效应的一切设备失效，也包括起保护作用的一切设备失效。

4.95. 鉴于假设是非常保守的，因而设计基准分析常常能提供强有力的证明，即在超出安全限值之前存在着较大裕量。然而，在使用分析结果时必须小心，因为结果并不总是这样。

4.96. 预期运行事件的安全分析还应该包括确定论DBA分析中使用的许多保守假设，尤其是与过渡期间用来保持关键安全功能的系统有关的假设。然而，没

有必要假定一切非安全系统和设备都已不能利用，并假定不能相信控制系统在减轻始发事件效应方面的作用，除非PIE使得这些系统成为不能利用的。

4.97. 评估的结果应该加以整理，并以合适的格式呈现出来，以便使人们能较好地理解事件的进程，并允许方便地与验收准则进行逐条核对。

验收准则

4.98. 正如参考文献[1]中所陈述的，应该为设计基准范围内的事件和工况制定验收准则。这些准则应该确保能通过下面两个渠道使纵深防御保持合适的水平，即防止对阻止放射性物质释放的屏障的破坏和防止放射性释放量达到不可接受的程度。

4.99. 验收准则应该按以下两个层次制定：

- 总体/高水平的标准，与公众的受照剂量或事故中防止继发性压力边界失效有关。这些准则常常是在法律中规定的，或由监管机构规定。
- 设计者或分析人员规定的详细准则。对于满足总体的验收准则来说，选用这些准则是充分的但并非必需的。此外，分析人员可以在更细小的层次上（验收准则更严格）设定目标值，以便简化分析工作（举例来说，避免不得不做非常复杂的计算）。每一条具体准则的可适用范围和适用条件应该清楚地作出规定。

4.100. 验收准则应该和与事故有联系的状况——例如，始发事件的频率、或反应堆设计与机组工况——有关。为了判断各道屏障的易损性和考虑事故的各个方面，通常需要不同的标准。对于发生频率较高的事件，常常要适用更严格的标准。

4.101. 有关预期运行事件的放射性验收准则一般限制性更大，因为它们的频率更高。总的来说，实物屏障（燃料基体、燃料包壳、反应堆冷却剂压力边界或安全壳）中的任何一道屏障都不应该失效，燃料也不应有任何损伤（或者是，若在运行限值范围以内的较小燃料泄漏早已存在，则没有附加的燃料损伤）。

4.102. 有关DBA的总体验收准则应该是或者没有厂外的放射性影响，或者在禁区外只有较小的放射性影响。较小放射性影响的定义应该由监管机构设定，但一般说来与之对应的是非常严格的剂量限值，目的是排除采取厂外应急行动的必要性。

4.103. 详细的验收准则可能包括以下几方面内容：

- 事件不应该产生后续更严重的机组工况，且不发生其他的独立失效。因此，预期的运行事件本身不会产生DBA，且此类事故本身也不会产生超设计基准事故。
- 减轻事故后果所需的安全系统功能不应该有间接损失。
- 应该将用于减轻事故后果的系统设计得能经得起对于所分析的事故来说最大的载荷、应力和环境条件。这些应该由单独的分析来加以评估，分析内容涉及环境条件（即温度、湿度或化学环境）和加在机组构筑物和部件上的热载荷和机械载荷。
- 一回路和二回路系统中的压力不应该超过针对已有机组工况规定的相关设计限值。为了研究各种失效对安全阀和泄压阀的影响，也许需要进行附加的超压分析。
- 应该针对每一种PIE规定燃料包壳可能发生的失效数目，以便允许总体的放射性准则得到满足。
- 在能使燃料暴露和加热的LOCA中，应该使燃料棒的可冷却的几何形状和结构的完整性得到保持。
- 任何事件都不应该使安全壳内的温度、压力或压差超过已被用作安全壳设计基准的相应数值。

有关超设计基准事故和严重事故的考虑

4.104. 比DBA还严重的事故称作超设计基准事故。此类事故能够产生如下的各种后果：

- 它们处于DBA的保守验收准则范畴内，虽然也许需要用最佳的估计分析来证明这一点。
- 它们超出DBA的保守验收准则，但不会导致明显的燃料损伤或超出基于最佳估计分析的一回路失效限值。
- 由于多重故障和/或操纵员错误，使安全系统没能履行其一项或多项安全功能，导致堆芯明显损坏，以致威胁到阻止从机组释放放射性物质的剩余屏障的完整性。此种情况被称作严重事故。严重事故可能进一步升级为：
 - 堆芯损坏加上一回路失效，但安全壳未失效
 - 堆芯损坏加上一回路和安全壳失效，从而导致放射性物质大量释入环境和要求采取厂外应急措施。

4.105. 安全分析的目标应该是量化机组的安全裕量并证明为这一级事故提供的纵深防御的程度。只要合理可行，这将包括以下一些合理可行的措施：

- 通过提供附加的设备和事故管理规程，阻止各种事件进一步升级为严重事故，控制严重事故的进程和限制放射性物质的释放。
- 通过启动厂内和厂外应急计划，减轻可能会发生的放射学后果。

对于能够导致安全壳过早失效的假想严重事故序列（例如，PWR的高压堆芯融化）而言，应该证明它们是能够以很高的置信度被排除在外的。

选择安全分析用的严重事故

4.106. 严重事故分析应该处理一组有代表性的序列，其中包括安全系统已经失灵和阻止放射性物质释放的某些屏障已失效或已被旁路。应该通过增加附加失效或增加操纵员对DBA序列（包括对安全系统失效）和对来自PSA的占支配地位的事故序列的不正确响应来选择这些序列。

4.107. 应该使用概率论方法与确定论方法以及合理的工程判断的组合来确定可能导致严重事故的重要事件序列。

4.108. 确定严重事故序列的最严格办法是使用一级PSA（参看第4.124段）的结果。当然，根据对涉及严重事故序列的物理现象、设计中存在的裕量及DBA中剩余的系统冗余度的了解，确定具有代表性或包容性的序列或许也是可能的。

4.109. 严重事故的引发因素包括：

- 完全失去从反应堆堆芯排除余热的能力，
- 完全失去堆芯应急冷却能力的LOCA，
- 在一段较长的时间内完全失去电力供应。

4.110. 需要进行分析的各种严重事故序列的细节必然是不同的，这取决于反应堆安全系统的设计。

4.111. 对严重事故的评价应该充分说明机组的设计能力，包括以超过其原先预定功能的方式使用某些安全和非安全系统，来使潜在的严重事故回到受控状态和/或减轻其后果。若相信对系统进行超常使用是有益的，那就应该能合理地假定它们能够且将以分析确定的方式得到运用。

严重事故分析用的方法和假设

4.112. 关于处理严重事故分析和验收准则的最佳方案，目前还没有达成广泛的一致意见。不过，目前存在的明显趋向是，对新的先进反应堆设计适用以下或类似的准则。通常应该使用最佳估计假设、数据、方法和决策判据进行严重事故分析。如果不可能这样做，就应该做出合理的保守假设，并考虑对正在模拟的物理过程的了解的不确定度。

4.113. 严重事故分析应该模拟堆芯损坏后可能发生的和可能导致放射性物质释放到环境的多种物理过程。其中应该酌情包括：

- 堆芯损伤过程和燃料熔化；
- 燃料—冷却剂相互作用（包括蒸汽爆炸）；
- 熔融物滞留在压力容器内；
- 压力容器融穿；
- 一回路内的热量分布；
- 高压熔融物喷出/直接使安全壳加热；
- 氢的产生和燃烧；
- 安全壳失效或旁路；
- 堆芯—混凝土相互作用；
- 裂变产物释放和迁移；
- 冷却压力容器内、外堆芯熔融物的能力。

4.114. 分析一般涉及使用不同程序（包括详细的系统和安全壳分析程序）的多层次的处理办法、比较简单的风险评估与“单项效应”程序，以及源项和放射学影响研究。使用完整的一组程序必然能确保预期的一切现象都得到充分的分析。

4.115. 评价工作应该确保反应堆堆芯、一回路和安全壳模型都得到了准确的模拟。这些模型对分析特别重要，而且可对确定事故的进程有影响。

验收准则

4.116. 有关严重事故的验收准则通常是用风险准则（概率论安全准则）表示的。这些将在第4.219—4.231段讨论。然而，关于这些准则应该是什么这个问题只有有限的一致。

在许多国家中也规定了确定论验收准则，典型的内容如下：

- 在严重事故之后的短期内不应该发生安全壳失效，

- 严重事故之后不应该有短期健康影响，
- 严重事故之后，长期健康影响/¹³⁷Cs释放量应该低于规定限值。

设计时严重事故的考虑因素

4.117. 严重事故分析的目标应该是：

- 评价设计承受严重事故的能力并确定特定的薄弱环节，其中包括评价事故管理中可能使用的设备和可能用于监测事故进程的仪器仪表。
- 评价是否需要在机组设计¹⁷中加入一些给严重事故提供纵深防御的设施。
- 确定能够用来减轻事故后果的事故管理措施。
- 拟定在超设计基准事故和严重事故工况时需要遵循的事故管理大纲。
- 给制订厂外应急计划提供输入数据。

4.118. 对新机组而言，对严重事故的研究应该在设计阶段进行。当然，对当前正在运行的机组而言，应该拟订严重事故管理大纲，以便充分使用一切可利用的设备和规程来减轻此类事故的后果。此类措施可能包括使用备用或多样的系统、使用非安全级设备的规程和方法，以及临时采用外部设备来更换标准部件。有关拟定和实施事故管理大纲的细节在单独的IAEA出版物[9]中讨论。

4.119. 应该利用PSA对上述设计特点和事故管理措施在减少风险方面的有效性进行评价。

应急计划

4.120. 严重事故分析还应该给民政当局提供制定厂外应急计划和应急响应的输入数据。

4.121. 应该使用严重事故分析结果确定能被用作制定厂外应急计划依据的源项。

¹⁷ 这些设计设施或许包括：

- 熔化堆芯搜集器或堆芯展开区和耐堆芯熔融损坏的基座混凝土。
- 放置足以应付发生严重事故后可能出现的氢气产生速度的氢气复合器。
- 能够较长时间运行的带过滤器的安全壳通风系统，以防止安全壳在严重事故之后因超压而失效。

4.122. 源项还可以被用于证明掩蔽、食入碘化钾药片、食物禁令和撤离等措施的有效性。

概率论安全分析

概述

4.123. 概率论安全分析（PSA）提供一种包罗万象的结构化方法，用于确定事故情景和导出风险的数值估计。供核电机组用的PSA通常在以下三个层次上进行：

4.124. **一级PSA**，确定能导致堆芯损坏的事件序列、估计堆芯损坏频率，以及提供对用于防止堆芯损坏的安全系统和安全规程的优缺点的了解。

4.125. **二级PSA**，确定放射性物质能够从机组中释放出来的途径，并估计其大小和频率。分析还增加对事故的预防和减轻措施（诸如使用反应堆安全壳）的相对重要性的了解。

4.126. **三级PSA**，估计公众健康及土地或食物污染之类的其他社会风险。

4.127. 就全世界的大多数核电机组而言，一级PSA现在一直在进行。然而，近年来，不断出现一些供许多类型核电机组进行二级PSA用的标准。到目前为止，已经进行的三级PSA相对较少。

将PSA作为决策过程的一部分

4.128. PSA结果应该作为设计过程的一部分，以评估机组安全水平。由PSA得到的见解，应该与从确定论分析得到的见解一起考虑，以便作出机组是否安全的决定。这应该是一个迭代过程，目的是确保国家要求和准则得到满足，确保设计（如第4.139段所定义的）是均衡的，并确保风险的水平是合理可行尽量低的。

4.129. PSA结果应该被用于识别机组的设计或运行弱点。可以通过考虑始发事件组对风险的贡献和测量安全系统的重要性对风险贡献，以及人的错误对总风险的贡献来识别此类弱点。凡是PSA结果表明只要对机组的设计或运行做些变更就可能减少风险的地方，在考虑了修改的相对费用与效益之后，就应该酌情采纳这些变更。

4.130. 此外，当已经给该机组定义了概率论安全准则时，应该将PSA结果与这些准则相比较。对于给机组定义的一切概率论判据，都应该进行此类比较，包括处理系统可靠性、堆芯损坏、放射性物质释放量、工作人员的健康影响、公众的健康影响，以及土地污染与食物禁令之类厂外后果的概率论准则。

4.131. PSA结果应该被用于拟定与事故有关的运行规程，并提供可转变成机组的技术规格书的输入数据。特别是，PSA结果应该被用于研究为了进行测试或维护而将某些设备停运所引起的风险，并研究监督/测试频率的恰当性。应该利用PSA证实允许的计划停堆次数不会不适当地增加风险，并表明应该避免哪些设备组合的停运。

4.132. 应该使用二级PSA结果判断，一旦发生堆芯损坏，所做的准备是否足以减轻其影响。二级PSA应当论述安全壳是否足够坚固，氢混合/复合系统、安全壳喷淋和安全壳通风系统之类的保护系统提供的保护水平是否足以阻止放射性物质大量释放到环境。此外，应该使用二级PSA来确定哪些事故管理措施能被用来减轻融熔堆芯的影响，或许包括确定可能采取的将水引入反应堆安全壳的附加措施。

4.133. 如果有二和三级PSA结果，应该将这些结果提供给民政当局，作为制定厂外应急计划的技术输入。

对PSA的要求

4.134. PSA的应用应该贯穿机组的整个设计和运行过程，以便为有关机组安全性的决策过程提供帮助。

4.135. 对于新机组来说，理想情况是应该在概念设计期间就启动PSA，用于核对安全系统中提供的冗余度水平和多样性水平是否足够，然后延续到较详细的设计阶段，以评价较细化的设计课题，最后用于支持机组的运行。在设计阶段，这应该是一个迭代过程，确保从PSA得到的见解能反馈到设计过程中。

4.136. 对于已有机组，PSA应该或者作为定期安全评价的一部分，或者用于支持有关拟议改进的安全案例。虽然这两种应用对PSA的要求是一样的，但数据库可能不同。况且，在确定实施什么样的变更来减少风险才合适时，肯定会有差异，这取决于设施的老化、剩余的运行寿命，拟议的修改费用及其他相关因素。

4.137. PSA应该涉及机组的实际或预定的设计或运行，而且应该明确地将其作为分析的起点。机组的状况可以是固定的，如某个特定日期或商定的修改将要完成的某个日期的状况。

4.138. PSA应该开始：识别一切对风险有贡献的故障序列；判断机组的设计或运行有无弱点；以及评价有没有必要作出变更以降低此种弱点的安全重要性。如果分析未确定所有对风险有作用的因素（举例来说，如果它遗漏了某些外部事件或某些停堆状态），则作出的有关下述问题的结论也许是不正确的：有关机组风险水平、所提供的安全系统的均衡情况以及将要做出的用以减少此种风险的设计或操作变更的必要性。

4.139. PSA应该判断安全系统是否有足够的冗余度和多样性，有无足够的纵深防御和总体设计是否均衡。在均衡设计中，PSA应该表明：

- 设计中没有任何特别的设施对风险的作用大得不成比例；
- 没有任何始发事件组对风险的贡献大得不成比例；
- 总的风险水平较低的实现所依靠的贡献因素不具有明显的不确定度；
- 前两道防线承担主要的安全责任；
- 在每一道防线中，没有一个安全系统不成比例地比其它安全系统更重要。

缺乏均衡性通常表示存在着合理可行地降低风险的机会。

PSA范围

4.140. PSA应该处理由机组的所有运行模式对风险贡献。当然，也许比较方便的做法是单独地分析功率运行模式和停堆模式（两者不是同一个层次的问题）。

4.141. 如果PSA只进行到一级，则根据定义，反应堆堆芯就是分析的焦点。如果PSA要进行到二级和三级，则PSA的范围或许要包括由厂区内的其它放射性物质源（诸如用过的燃料和放射性废物）对风险的贡献。只要目的是处理由机组引起的对厂区附近的个人的总风险，就应该把堆芯以外的源包括进来。

4.142. PSA应该将整套PIE（包括内部PIE和外部PIE）作为分析的起点。接着分析应该确定对风险有作用的完整故障序列。这些故障序列应该涉及部件失效、部件在维护或测试期间的不可利用性、人的错误、共因故障，以及如有可能还应该考虑部件的老化。

PSA方法

4.143. 到目前为止，已经针对各种核电机组设计进行过大量PSA。因此，PSA所用的方法已经非常成熟，特别是一级PSA所用的方法。人们认识到，PSA的流程存在着固有的不确定度。不确定度并不是PSA所特有的，确定论安全分析中也存在着不确定度。然而，PSA的成套方法有能力识别其中的大部分不确定度并将其量化。对于正在进行的任何新的PSA来说，所用的方法应该与国际上现行的最佳做法相一致。

4.144. PSA最好自始至终使用最佳估算值法。这当然包括为支持安全系统的成功准则、模拟堆芯损坏以后安全壳内可能发生的现象以及释放到环境的放射性物质的迁移而进行的分析。当不能用PSA进行分析时，应该使用合理的保守假设。

一级PSA：分析堆芯损坏频率

4.145. 一级分析的目标应该是确定堆芯损坏的总频率。这要求定义什么是堆芯损坏，并把这个定义转变成安全系统失效判据。有关进行一级PSA步骤的更详细资料见参考文献[10]。分析应该确定对于堆芯损坏频率的贡献最大的故障序列，确定对于防止堆芯损坏是最重要的安全系统，并判断能否对机组的设计或操作做些变更以减少这种风险。

假想始发事件

4.146. PSA的起点应该是能直接导致或与其他失效结合起来导致向核安全挑战的全部PIE一览表。在PSA中，分析事件序列和进行系统分析时应考虑被包括在确定论分析中的继发性失效。

4.147. 被处理的一组PIE应该包括一切内部和外部事件，包括可能发生但在机组设计期间未考虑过的低频率事件。

4.148. 分析应该包括在机组的一切运行模式期间可能发生的和可能导致从厂区内任何一种源中释放放射性物质的PIE。

有关安全系统要求的规范

4.149. 对于已确定的每一个PIE，应该确定为防止堆芯损坏而需要履行的安全功能。这些安全功能与设计基准分析中处理的那些安全功能是相同的——即探知

始发事件、停堆、余热排出保护安全壳。然而，超过它安全功能就会被认为已经失效的那些限值，可能是比较实际的值，而不是为设计基准分析定义的保守值。

4.150. 应该具体说明履行安全功能所需的安全系统。这应该以最佳估计的瞬态分析为基础，而不是以为设计基准分析进行的保守分析为基础。应该具体说明有多少冗余和多样的系列需要运行。

4.151. 能够识别需要相同的或非常类似的安全系统介入的PIE。为了减少分析数量，标准做法是将PIE分组并在PSA中一起分析。（该方法与第4.75—4.77段中叙述过的供确定论分析用的分组办法类似但并不相同。）然后用使安全系统响应任务最艰巨的始发事件代表始发事件组，所取的频率则是该组中的各个始发事件的发生频率之和。凡是将PIE分组的地方，则分组工作应该以这样一种方式去做，即不应使分析结果变得过分悲观。举例来说，当所选取的代表事件的频率较低，而该组中其他所有事件具有显著较低的安全系统要求，但其频率总和却很大时，就可能发生这种情况。

分析事件序列

4.152. 在分析事件序列时，要给始发事件组构造逻辑模型，以便确定可能发生的导致堆芯损坏的故障序列。这些逻辑模型以基本安全功能为起点，并考虑始发事件组、安全系统和安全系统中的各个部件所要求的安全功能。此类逻辑模型确定部件失效如何能共同导致安全功能失效和堆芯损坏。

4.153. 针对一组始发事件进行的事件序列分析，应该旨在确定导致无法让机组保持在安全限值之内以致发生堆芯损坏的安全系统设备的成功或失效的一切组合。

4.154. 在大多数现行PSA中，对事件序列的分析是借助事件树分析和故障树分析的组合作进行的，因为经验已经证明这是时效率最高的大型逻辑模型处理办法，而大型逻辑模型是核电机组所必需的。当然，单独使用故障树或事件树进行分析也是可能的，而且就特定的事件分析而言，还可以使用动态时变分析技术。

4.155. 应该进行系统的评价，以确定可能由始发事件引发的安全系统设备的失效（以及安全相关或非安全相关设备的失效，如果这些失效可能影响事件序列的话）；应该将失效包括在代表可能发生的事件序列的逻辑模型中。

4.156. 对事件序列的分析应该涵盖能够用于履行所需安全功能的安全系统设备的一切组合。

4.157. 因为核电机组中的某些安全系统共用共同的启动系统或共同的支持系统（诸如电力系统、控制测量设备和冷却系统），因而产生了安全系统之间的功能相关性。应该对机组的设计和运行进行系统评估，以确保已确定的所有这类互相依赖性，并在事件序列分析或系统分析中明确地加以模拟。

安全系统失效分析

4.158. 事件序列分析应该向下延伸至单个基本事件这一层。基本事件一般包括部件失效、部件在维护或测试期间不可利用性、冗余设备的共因故障以及操纵员的错误。

4.159. 系统失效分析应该涉及安全系统设备单个物项的一切相关失效模式。失效模式通常已经由作为设计的一部分进行的失效模式和效应分析确定。PIE的任何继发性失效也应该被归入系统模型中（如果在事件序列模型中并未完全得到说明的话）。

4.160. 应该确定一切必要的支持系统并将其包括在系统失效分析中，应该明确地在逻辑模型中表示出由共同的支持系统引起的互相依赖性。

4.161. 在机组使用寿期内，个别设备物项或设备队列也许会由于需要测试、维护或修理而停役，这必然会减少安全系统履行安全功能的可利用率。在PSA中应该明确地考虑此类设备的停运。这既可以靠将表示设备停运的基本事件引入逻辑模型中来解决，也可以通过进行多次PSA来解决。

数据

4.162. 为了使分析量化，需要下列各项的数据：

- 始发事件频率，
- 设备失效概率，
- 设备停运频率与持续时间，
- 共因故障概率，
- 人的错误概率。

4.163. 所用的始发事件频率和设备失效概率应该与机组的设计或运行相对应。如果可能，应该使用机组特有的数据。当不可能这样做时，应该使用类似机组的运行数据。如果这也不可能，则应该使用通用数据，但要能表明这些数据是相关的。对于低频率的始发事件，应该进行判断。

4.164. 在具体说明设备的故障率时，应该具体说明设备的边界，并应该包括相关的一切失效模式。就泵而言，这包括启动失效、在特定使命时间内运转失效和泵密封处泄漏。

4.165. 所用的统计数据应该涵盖始发事件的一切相关原因以及一切相关的设备失效模式。

4.166. 就PSA中处理的某些物项而言，特别是压力容器失效或强烈地震之类罕见的始发事件的频率，根本没有相关的运行经验。如果认为这些不会对风险作出重要贡献，则可以把它们删除掉，但要证明这样做是合理的。否则，应该对它们的频率进行判断，并给出判断依据。特别是，进行概率论地震灾害评价方法已非常成熟，而且能够适应任何厂址。

共因故障分析

4.167. 安全系统内的冗余设备物项可能由于共同的原因而失效，从而限制系统的可靠性。在共因故障分析中，此类共因故障（CCF）能够在安全系统这一层或在单个部件这一层进行模拟，其中的一种做法是将基本事件引入代表安全系统CCF的逻辑模型，在安全系统这一层模拟CCF。能够被用来估计CCF概率的方案有许多种，包括使用运行经验数据和 β 因子与多个希腊字母方法之类的理论模拟。

4.168. 在共因故障分析中，应该模拟冗余安全系统内可能发生的共因故障。应该证明PSA中所用的CCF模型和数据是正确的。只要可能，应该考虑类似系统的运行经验。

4.169. 先前的分析和运行经验已经表明，非多样的安全系统的失效概率有一个限值，其可能的范围为约 10^{-3} — 10^{-5} 失效/要求，具体数值取决于提供的冗余度水平及其他的设计与运行因素。这应该在分析中得到反映。

人的可靠性分析

4.170. 人的错误能够对事件序列的进程和频率产生影响。人的错误可能发生在事件序列起动之前、期间或之后，能够减轻或加剧事故。应该在PSA中对其进行模拟。应该从事件报告、维修报告、PSA报告和模拟器观测值之类的来源中导出有关人的可靠性的数据。

4.171. 应该确定能导致始发事件的人的错误，并将其作为始发事件频率的一部分加以涵盖。

4.172. 能导致安全系统失效和失去关键安全功能的人的错误，应该在事件序列和安全系统失效分析中明确地加以模拟。

4.173. 所用的人的错误概率应该反映能够影响操纵员表现的各种因素，包括紧张程度、可用于执行该任务的时间、运行规程的可获得性、训练水平和环境条件。这些应该通过作为设计评价组成部分进行的任务分析加以确定。

分析的量化

4.174. 编制出的逻辑模型应该用数据加以量化，以便确定总的堆芯损坏频率和始发事件组的贡献。现有的许多计算机程序都可用来进行这种分析。

4.175. 在将分析量化的过程中，应该导出始发事件组、部件失效、安全系统失效和操纵员错误的重要性，以便确定对风险的贡献来自何方以及安全系统的设计或操作中何处可能有弱点。如果适用，可能对重要性进行定量测量（诸如 Birnbaum和Fussell-Vesely——参看参考文献[10]）。只要模型和数据方面有不肯定度，就应该依靠敏感性研究的支持。

堆芯损坏频率的分析结果

4.176. 应该对分析结果进行评价，以便使人相信它们提供的来自机组的风险是合适的。如果发现有些地方的风险估计值被认为过于保守或过于乐观，则应该对分析进行修正，使之更加接近实际。如果安全系统的成功准则是以保守的设计基准瞬态分析和保守的关键安全功能成功准则为基础的，而不是以推荐给 PSA使用的最佳估计值为基础，则可能出现过分保守的情况。如果潜在的始发事件被不适当地删除，则可能出现过分乐观的情况。

4.177. 应当将分析结果与针对机组建议的有关堆芯损坏频率的安全准则（如果已经规定了此类值的话）相比较。如果针对机组估计出的堆芯损坏频率高得不可接受，则应该对该机组的设计或运行做些变更以降低此种风险。

4.178. 即使堆芯损坏频率低得可以接受，也应该系统地审查 PSA结果，以便确定机组的设计或运行中的相对弱点，并确定为降低堆芯损坏频率可能做出的改进。只要合理可行，就应该做出相应改进。关于合理可行的判断，必然取决于反应堆是处在设计阶段还是运行阶段，以及这些改进所需费用。为了试图将堆芯损坏频率减小或低于设计目标（如果已经定义的话）和产生均衡的设计，这一过程要反复进行。

二级PSA：分析从堆芯损坏到释放放射性物质的事故进程

4.179. 这部分分析以堆芯开始损坏为起点研究事故的进程，并研究将会导致安全壳失效和向环境释放放射性物质的可能现象。有关进行二级PSA的步骤的详细资料见参考文献[11]。

4.180. 分析对设计的有效性和减轻堆芯损坏后果的事故管理措施的有效性进行研究，并提供能够与概率论准则（如果已经定义的话）相比较的、向环境大量释放放射性物质的频率估计值。

机组损坏状态的定义

4.181. 应该把在一级PSA中确定的可能导致堆芯损坏的故障序列组合成几种机组损坏状态（PDS），这些状态要用影响安全壳响应的因子或向环境释放的放射性物质质量来定义。这些因子一般包括已经发生的始发事件的类型、反应堆冷却系统的压力、应急堆芯冷却和安全壳保护系统的状况，以及安全壳的完整性。

堆芯损坏进程的模拟

4.182. 对从堆芯损坏到放射性物质释放这一事故进程的分析，应该模拟挑战安全壳完整性或影响放射性物质释放的重要现象。这些现象列于第4.113段中，相关文献中（例如，可分别参看有更加充分描述的IAEA和OECD/NEA关于二级PSA的报告[11、12]）。

4.183. 分析应该使用逻辑方法来模拟事件序列是如何从堆芯损坏发展到放射性释放的。这通常是借助事件树分析完成的，后者模拟许多时间范畴中的事故序列，并使用一组节点问题模拟事件的发生顺序。建立事件树，需要进行热工—水力计算、模拟裂变产物在安全壳内的释放及迁移。

4.184. 事件树分析应该有足够多的时间范畴与节点，以便允许安全壳内可能发生的重要现象得到处理。即将出台的标准将规定20—30个左右的节点，尽管某些分析实际使用的节点数要比这多得多（例如，NUREG-1150 [13]）。这些节点问题肯定与针对每一PDS画出的事件树中的问题是一样的。然而，由于PDS所表征的初始条件不同，所定义的每种状态的实际事件树的细节肯定有差异。

4.185. 事件树的端点确定了已经发生事件的先后次序和安全壳的状态。可能的结果是安全壳完好无损，或者已经失效。可能的失效模式是：旁路、无法隔离（这两种失效模式在PDS的定义中模拟）、泄漏、破裂或底板融穿。由此产生

的放射性物质释放必然还取决于安全壳的失效是发生在事件序列中的早期还是晚期。

数据

4.186. 与事件树分析的量化相关的数据是与分支点有关的条件概率。可能会发生的现象有相当大的不确定度，因此所用的概率常常以专家的判断为基础。

4.187. 应通过评估证实获得专家判断的框架是健全的，并尽可能陈述和证明供判断用的依据是能成立的。应该考虑已经进行过的热工水力分析、针对其他类似机组进行的分析和可适用的研究数据。安全壳事件树的量化应该考虑正在模拟的各种现象之间的相互依赖性。

安全壳行为分析

4.188. 必需处理的重要议题之一是，安全壳在因堆芯损坏使其载荷增加后的行为及其发生失效的方式。

4.189. 分析时应该论述安全壳的直接旁路（例如，由蒸汽发生器传热管破裂引起的旁路，或由于能向安全壳外排放的接口系统LOCA引起的旁路）和安全壳隔离系统的失效。PDS的定义中通常会包括这部分内容。

4.190. 应该进行结构分析，以便确定当安全壳遇到可能由蒸汽爆炸、不可凝结的气体或氢气燃烧而引起的压力和温度状况时的行为。分析应该以安全壳的实际设计为基础，并把门、贯穿件、密封件及可能存在的其他薄弱区域纳入考虑范围。应该确定安全壳的可能失效模式，还应该估计安全壳发生失效的条件概率值与压力和温度的函数关系。然后利用这些资料估算可用于使事件树量化的条件失效概率。

4.191. 还应该进行一项分析，以确定安全壳底板怎样因熔融堆芯与混凝土的相互作用而失效，这种相互作用是压力容器失效后可能会发生的。应该估算出底板失效条件的概率与余热水平和熔融物冷却条件的函数关系。当安全壳的底板上面有附加的间隔以致底板的穿透能导致放射性通过无过滤设备的通道释出时，应该特别小心。

源项分析

4.192. 在事件树分析中通常有大量的端点，这些端点一般划分成释放和/或源项两类，两者具有类似的放射学特性和厂外后果。

4.193. 释放类别的定义应该包括若干因子，诸如被包括在内的每种同位素的数量、释放的时间、持续时间、部位、能量值和粒度分布。

4.194. 应该确定所定义的每种释放类别的全部源项。应该考虑对源项有影响的一些因子，包括放射性核素的挥发性、从燃料中释出的量、裂变产物在反应堆冷却系统内的滞留，以及裂变产物在安全壳内的滞留。

4.195. 应该计算出每一种释放类别的频率，办法是将分配给释放类别的事件树上的每个端点的频率求和。当PSA的分析范围包括来自厂址中的一切放射性物质源的释放量时，此时应该考虑堆芯外部源的释放量。这也许会涉及定义附加的释放类别，此类释放的厂外影响一般比已损坏堆芯的低，但频率比已损坏堆芯的高。

二级PSA的结果

4.196. 二级PSA的结果通常用列有源项类别或释放类别及其发生频率的表格形式表示。源项和/或释放类别是用它们的放射性核素组成（按照共同的化学和物理性质划分成几个裂变产物组）以及释放特点（事故开始后发生释放的时间、持续时间、高度和能量值）来定义的。由这部分信息能导出大规模释放或大规模早期释放的频率，可供与概率准则（如果已定义的话）相比较。“大规模”被定义成比通常用堆芯放射性存量的份额来定义的那个规定的放射性物质数量大。

4.197. 与PSA其他部分一样，二级分析的结果应该被用于确定风险的主要影响因素和能够降低风险的机组设计变更或运行变更。应该考虑二级PSA所固有的现象学方面的明显不确定度。此类措施可能包括氢气控制系统（有足够的容量可以应付堆芯损坏后的氢气产生速率）、安全壳过滤排气系统以便较长期防止安全壳过压，或专供冷却熔融堆芯用的系统。当考虑到费用和效益后认为这样做合理可行时，应该将这些纳入该设计中。

厂区内的事故管理

4.198. 在事故期间，操纵员可以采取行动防止事故的进一步发展或减缓其后果。分析中常常涵盖的此类事故管理措施是打开泄压阀，以便降低一回路压力和避

免熔融物从处于高压下的反应堆压力容器内喷出，以及在熔融堆芯已经从一回路上流出后给安全壳加水，以提供冷却介质。

4.199. 二级PSA应该被用于确定可以减轻熔融堆芯影响事故管理措施，其中应该包括能够用来支持安全壳功能或限制可能发生的放射性物质释放的行动。应该将这些事故管理措施纳入供机组紧急情况时使用的操作指令中，并应该对负责实施这些事故管理措施的机组操纵员进行培训。严重事故的管理措施应该与机组操纵员在此种场合下可能合理使用的设备、仪器仪表和诊断器件相称。

三级PSA：分析厂外后果

4.200. 厂外后果的分析模拟从核电机组释放出放射性核素、核素在环境中的迁移，及其对公众健康的影响和造成的经济后果。有关三级PSA的实施步骤的更详细资料见参考文献[14]。此种分析应该：(a) 提供厂址附近居民的个人死亡风险估算值，(b) 处理许多厂外后果（包括对公众成员的早期和晚期的健康影响），以及 (c) 研究其他的经济后果。

源项分组

4.201. 正如在第4.192—4.196段中讨论过那样，根据其对大气弥散和厂外后果的挑战，二级PSA确定的故障序列通常就其所具有的类似特性被分成若干释放类别。所定义的一组释放类别应该代表可能从机组释放的放射性物质数量的变动范围。通常采用所释放放射性核素的组成（按它们的挥发性分级）来对类别进行定义。此外，释放类别当然还定义始发事件发生与开始释放之间的时间以及释放的持续时间，因为这些都与制定厂外的应急计划有关。释放类别的频率应该根据释放类别内包括的全部安全壳事件树端点频率之和计算。

大气弥散的模拟

4.202. 现在有许多计算机程序可供进行厂外后果分析使用。需要输入因机组和厂址而异的数据，包括与该机组有关的释放类别和频率，以及与厂址及其周围地区有关的气象学、人口、农业和经济方面的数据。这些程序模拟放射性核素在此种环境中的迁移，包括大气弥散、沉降、再悬浮、食物链通道和典型的照射通道（烟云照射、吸入、污染、地面沉降、重悬浮和食入），以确定对公众的健康影响和厂外的经济后果。（IAEA已经对进行厂外后果分析用的现有计算机程序进行过审查[14]。）

气象数据

4.203. 应该具体列出与该厂址有关的气象数据。应该以在厂址附近收集到的若干年内的数据为基础，而通常包括风向、风速、稳定性类别、降水和混合层厚度。（所需数据的精确度取决于所用的计算机程序。）

人口、农业和经济数据

4.204. 应该具体列出与厂址有关的人口、农业和经济数据。这些数据通常以本国的信息为基础，辅以在厂址附近地区进行的调查。究竟需要哪些数据取决于分析中将包括的健康影响和经济因素类别。汇集信息以供处理所采用的方式将取决于所用计算机程序的具体需要。

社会风险的估算结果

4.205. 如果已经给机组定义了风险判据，则应该将社会风险的估算结果与风险准则相比较。

4.206. 应该将社会风险的估算结果提供给民政当局，作为有关厂外应急计划条款的决策过程的技术输入。

厂外应急计划

4.207. 应急计划和应急准备涉及可以在核电机组厂区内进行的、用于保护工作人员和公众成员免受该机组释放的放射性物质的影响的活动。如果有条件，应该使用三级PSA研究防范措施战略。分析应该包括研究掩蔽、撤离和服用碘化钾药片之类近期措施的好处；并研究食物禁令、移民和土地去污之类长期防范措施的必要性。分析还应该研究启动这些防范措施的方式，是自动启动（取决于机组状态），还是根据剂量决定。

4.208. 三级PSA的结果应该被用于制定应急计划提供输入，并用于评价应急计划各项内容的相对有效性。

PSA的验证

4.209. 分析需要用到许多计算方法，涉及从事件序列分析中使用的逻辑事件模型和故障树模型，到有关堆芯损坏后安全壳内部可能发生的现象的模型，以及用

于模拟放射性核素在环境中的迁移以确定其健康和经济影响的模型。应对计算方法加以验证，以证明用其能恰当地表述所发生的过程。这一点将在下面的题为“所用计算机程序的评定”这一节中论述。

4.210. 由营运单位委托外部团体（常常来自不同的国家）对PSA进行独立的同行审查，这正在变成标准的做法，其目的是就PSA的范围、建模和数据是否合适提供某种程度的担保，并确保它们符合世界上PSA领域现行的最佳做法。

PSA的使用

PSA结果的表述

4.211. 应该对PSA的结果进行考查，以便确定对风险的贡献最大的故障序列。在有些情况下，PSA可以指出起支配作用的贡献因子，但进一步的考查或许会指出这种支配作用是由于PSA中的部分假设过于保守引起的，而不是反应堆设计的真实反映。在这种情况下，应该考虑修正这部分分析，以提供更好的风险估算值。

实时PSA

4.212. 在机组寿期期间应该使用PSA给决策过程提供输入。在核电机组的运行寿期内，常常会对安全系统的设计或机组的运行方式做些修改，例如在维护与试验期间改变机组的配置。这些修改可能对机组的风险水平产生影响。在机组运行期间，必然可以获得有关始发事件频率和部件失效概率的许多统计数据。同样地，或许还能获得新的信息和更完善的方法与工具，这可能会改变早先分析时提出的某些假设，因而改变由PSA给出的风险估算值。

4.213. 因此，在机组寿期期间，应该对PSA进行及时更新，使之反映机组最新状况，随时可供决策过程使用。及时更新应该考虑机组的设计和运行方面的变化、新的技术资料、可以获得的更加完善的方法与工具，以及从机组运行中获得的新数据。应该定期地审查PSA的状况，以确保其一直代表机组的模型。

4.214. 机组的营运者应该在机组的整个使用寿期内收集数据，以核对或更新分析。收集的数据应该包括有关始发事件频率、部件失效率以及机组在试验、维护或修理期间的不可利用率等统计数据。应该根据新的数据对分析加以评价。

4.215. 应该鼓励发展“实时PSA”，以便为机组正常运行期间的决策过程提供帮助，其中包括使用PSA肯定有助于确保其引起的风险充分低的活动，例如规

划检修停机。经验已经表明，这样的实时PSA能够给营运单位带来相当大的好处，而且它的使用普遍地受到监管人员的欢迎。

PSA的局限性

4.216. PSA是设计评价和安全分析过程的关键部分，因为它提供的是针对整个机组的综合风险模型，并允许对潜在事故情景的频率和后果进行一致估计。但是，PSA也有局限性，这是需要大家了解的。

4.217. 特别是，不应该把PSA看成是工程设计评价或确定论设计方法的替代物。相反，应该把PSA看成是提供与机组风险水平有关的见解的工具。应该在决策过程中使用有关风险的见解对确定论分析进行补充。

4.218. PSA中所用的模型和数据都有不确定度。对于由大型数据库或相关的运行经验导出的部件失效概率而言，不确定度相对较小。然而，在其他的许多方面，不确定度要大得多，甚至难以估量。此种情况包括：

- 没有运行经验数据的情况下的初始事件频率与部件失效率，
- 大地震的发生频率及其地面运动情况，
- 对共因故障的模拟，
- 对人的错误的模拟，
- 对严重事故时可能发生的现象的模拟，
- 机组释放的放射性物质造成的厂外后果的估计。

在决策过程中使用PSA的结果时，应认识到这种不确定度。PSA的结果应该得到不确定性分析，或者至少得到敏感性研究的支持。

概率论的安全准则

建立准则

4.219. 在使用PSA结果为决策过程提供支持时，应该建立实施这项工作的正式框架。这一过程的细节当然取决于PSA的特定应用目的、决定的性质和使用的PSA结果。在使用PSA的数值结果时，应该建立某些参考值，以便这些结果能与之进行比较。

4.220. 当PSA的目标是确定起支配作用的风险贡献因子，或在各种设计方案和机组配置之间作出抉择时，可以不要参考值。

4.221. 然而，当PSA的目标是帮助做出有关以下三方面的判断时，则应该拟定概率论安全准则，以便给设计者、营运者和监管者提供有关机组期望安全水平的指导性意见：(i) 计算出的风险是不是可接受的；(ii)建议的机组的设计或运行的变更是不是可接受的；或(iii)需不需要进行变更以降低风险水平。这些准则当然还用来定义设计者、营运者和监管者在履行安全供应核电方面的各自职责时必须实现的目标。

4.222. PSA当然会根据计算出的后果的大小产生各个层次风险的数值量度。可以针对以下量度中的任何一个或所有量度设定概率论的安全准则：

- 安全功能或安全系统（第0层）的失效概率；
- 堆芯损坏频率（一级）；
- 机组放射性物质的特异性释放（例如数量、同位素）的频率或频率与大小的函数关系（二级）；
- 给公众成员造成的特定健康影响或特定环境后果的频率（三级）。

4.223. 供定义概率论安全准则用的一种可能框架见参考文献[15]，其中定义了一个“可容忍性阈值”（风险水平超过此值就是无法忍受的）以及一个“设计目标”（风险水平低于此值时肯定是完全可接受的）。在这两个风险水平之间，存在着这样的—个区域，在这个区域中，只有当降低风险的所有合理可行措施全都已经采取时，风险才是可接受的。虽然有些国家已经采用此法，但国际上尚未就其应用达成共识，更常见的做法是找出被确定为目标、目的、细则或倾向性参考值的概率论安全准则。此外，关于与可容忍性阈值和设计目标相对应的风险水平的数值，国际上也尚未达成共识。

数值

4.224. 以现有核电机组设计和运行经验为基础，INSAG已经建议了能够由现有和拟议的核电机组设计达到的数值。

4.225. 安全功能或安全系统的失效概率：在安全功能或安全系统这一层能够设立概率论目标。可使用这些目标核对所提供的冗余度和多样性的水平是不是充分。此类目标必然是因机组设计而异的，所以这里无法提供指导性意见。安全评价应该证明这些目标已经达到。即使没有达到，设计可能仍然是可以接受的，条件是更高一层的准则已经满足；当然，此时应该对受到质疑的安全系统给予特别关注，看看是否能采取一些合理可行的改进措施。

4.226. 堆芯损坏频率：关于这个问题，INSAG（参考文献[4]）提出了以下目标：

- 对于已有核电机组为 10^{-4} /堆·年，
- 对于未来核电机组为 10^{-5} /堆·年。

4.227. 堆芯损坏频率是最常见的风险量度，因为大多数核电机组至少已经进行过一级PSA而且方法已经非常成熟。在许多国家中，这些数值一直在正式地或非正式地被用作概率论安全准则。

4.228. 向厂外释放大量放射性物质：带有严重社会影响因而要求实施厂外应急安排的放射性物质大量释放，可以用多种方式加以规定，具体的有以下是一些：

- 所释放的最重要核素的绝对数量（以Bq计），
- 堆芯放射性物质存量的份额，
- 厂外受照射最多的人受到的具体剂量，
- 产生“不可接受后果”的释放。

4.229. 关于放射性物质的大量释放，INSAG也提出了概率论安全准则[4]。给出的目标如下：

- 对于已有核电机组 10^{-5} /堆·年，
- 对于未来核电机组 10^{-6} /堆·年。¹⁸

4.230. 虽然尚未就什么情况构成大规模厂外释放这个问题达成共识，但许多国家已经规定了类似的数字准则。

4.231. 对公众成员的健康影响：关于对公众成员的健康影响的目标，INSAG未给出任何指导性意见。在某些国家中，有关公众成员死亡风险的目标是 10^{-6} /堆·年。

敏感性研究和不确定性分析

4.232. 使用最佳估算程序（如推荐给确定论和概率论安全分析用的程序）时，还应该辅以敏感性研究和/或不确定性分析。

¹⁸ INSAG-3 Rev.1[4]除了概率论安全准则，对于未来机组还规定了下列目标：“未来机组的另一个目标是，真正消除可能导致放射性大量早期释放的事故序列，尽管在设计过程中要考虑可能导致安全壳较晚失效的严重事故，并使用较现实的假设和最佳估算值分析，以致其后果是仅需要在区域和时间方面有限的保护措施。”

4.233. 敏感性研究包括程序输入变量和模拟参数的系统变差。应该使用敏感性研究确定分析所必需的的重要参数，并表明在实际输入变差的分析结果中没有突变（“峭壁边缘”效应）。

4.234. 确定论安全分析框架内的不确定度研究，是指机组工况、程序模型和相关现象对各种结果的影响的统计学组合。应该使用这些研究去证实机组的实际参数肯定是以计算结果加不确定度为界，并拥有规定的高置信度。通常使用敏感性研究、程序与程序比较、程序与数据比较以及专家判断的组合来估算不确定度。

4.235. 还应该准备对PSA进行不确定度分析，因为它是关键组成部分。确定和分析不确定度是PSA的基本优势。不确定度也出现在确定论分析中，但其通常得不到承认或分析。相反，在试图说明不确定度时特意使用保守原则。然而，确定论分析中的不确定程度并不是整齐划一的，它能够导致不均匀分析。PSA方法的优势是它能对确定论方法进行补充，并允许对不确定度进行充分表达。对于此种情况，不确定度还应该反映始发事件概率和部件失效概率的变动范围。

所用的计算机程序的评价

4.236. 安全分析要使用大量计算机程序。计算机程序一般包括：

- 估算工作人员所受剂量的放射学分析程序，
- 模拟反应堆堆芯行为的中子物理学程序，
- 模拟燃料元件在正常运行期间和事故后行为的燃料行为程序，
- 模拟反应堆堆芯和相关冷却系统在正常运行期间和事故后行为的热工-水力学程序，
- 模拟LOCA或二回路管线破裂后安全壳压力和温度的行为的热工-水力学程序，
- 模拟部件和构筑物在载荷和载荷组合下的应力-应变行为的结构程序，
- 模拟从堆芯损坏直到安全壳失效这一事故序列进程的严重事故分析程序，
- 模拟放射性物质在机组内部迁移和从机组释放出来后的迁移以确定其对工作人员和公众成员的影响的放射学分析程序，
- 开发用于确定PIE后可能发生的事故序列并估算其频率的逻辑模型的概率论程序。

4.237. 现在正在开发的许多计算机程序试图把上述的部分模型组合成一个程序。

4.238. 安全分析中所用的所有计算机程序应该得到验证和核实。在计算用的计算机程序中所用的方法应当适于既定用途，应该将起控制作用的物理和逻辑方程正确地转变成计算机程序。

4.239. 关于计算机程序，应该证实：

- 用于这些过程的物理模型及其相关简化假设都是正确的。
- 用于表示物理过程的关系式是正确的，其适用界限是明确的。
- 程序的适用界限已经明确。当计算方法仅设计用于模拟规定范围内的物理过程且不应该用于这一范围以外时，这一点很重要。
- 所用的数值方法能提供足够精确的解。
- 计算机程序的设计、编码、测试和文件编制所用的是系统化方法。
- 与程序规格书相关的源程序都已得到评价。（人们认识到对于非常大的程序这未必是可行的。）

4.240. 关于计算机程序的输出，应该证实程序的预测值已经与以下内容比较过：

- 与被模拟的重要现象有关的实验数据。一般包括与“单独效应”和较大的“整体”实验进行比较。
- 机组数据，包括调试或启动期间进行的测试以及运行中发生的事件或事故。
- 已经独立开发出来的使用了不同方法的其他程序。这在模拟严重事故现象时尤其重要。
- 标准问题和/或正在获得足够精确结果的数值基准。

4.241. 应该对每个程序在安全分析中的每次应用进行验证。

4.242. 人们注意到，对于已经开发出的某些程序来说，验证包早已存在。然而，对于正在开发的程序和对于模拟某些尚未被透彻了解的严重事故现象的程序来说，验证程序包可能并不完善。

4.243. 关于计算机程序的用户，应该确保：

- 用户已受过充分的培训并且了解程序，
- 用户在使用程序方面有足够的经验并且充分了解程序的用途和局限性，
- 用户在使用程序时能获得充足的指导性意见，
- 只要可能，用户在开始安全分析之前，已经使用该程序和标准题目做过练习。

4.244. 关于计算机程序的使用，应该证实：

- 节点划分和机组模型能很好地代表机组的行为，
- 输入数据正确，
- 程序的输出能被正确理解和使用。

5. 独立验证

5.1. 独立的安全性验证的目的是确定安全评价满足适用的安全要求。尽管可以方便地将这种验证细分为可以在设计的各个重要阶段进行的若干个阶段，但安全评价的最终独立验证总是应该在设计全部完成后才能进行。

5.2. 进行独立验证的方法基本上可以仿效本“安全导则”第2—4节中讨论的安全评价方法。当然，独立验证的范围可能要比安全评价的小，因为它会把精力集中在最重要的安全问题和安全要求上，而不是扩散到所有的安全问题和安全要求上。

5.3. 独立验证由机组业主—经营者和监管机构两者分别进行，前者一般都对设计单位进行独立审查。

5.4. 业主对其独立验证负完全的责任，即使部分核实工作是委托给独立单位进行的。

5.5. 独立的设计评价活动是全面的QA大纲的一部分，是核电机组设计期间最受关注的一个方面。不过，正如图1中描绘的，独立验证被认为是一种单独进行的附加校核，目的是确保设计的安全性和恰当性。进行独立验证的团体在决定其验证的程度和范围时，可以考虑先前已经进行过的QA审查。

5.6. 正如先前提到过的，本安全导则主要论述在机组开始建造前进行的设计验证活动，并集中论述由设计单位或其代理进行的活动。当然，可以通过类推将其适用于随后的其他验证活动。

5.7. 对安全评价的验证应该由熟悉反应堆工艺技术和安全分析方面的最新发展的专家执行。审查者应该是与机组设计者无关的人员。

5.8. 进行独立验证的审查者应该验证安全评价的过程是否充分。应该给审查者提供与设计相关的所有文件，包括各种计算模拟、数据和假说。此外，应该给审查者提供进入厂址的充分权力，使他们能亲眼看一看关键区域的情况，以证实安全评价充分考虑了设施的实情。

5.9. 必须进行审查的项目清单如下（只是举例，并非全部）：

- PIE的选取,
- 适用的工业标准,
- 与安全和辐射防护评价相关的问题,
- 给划定所有类似案例范围的始发事件假定的最坏机组初始条件,
- 单个事件的组合及其失效后的效应,
- 继发性失效的识别,
- 安全和非安全的系统和部件在各种事件期间的假定运转情况,
- 假定的操纵员动作,
- 可适用于特定分析的已验证计算机程序的选取,
- 可靠性数据及其对特定分析的适用性,
- PSA中的事件树和故障树的建立,
- 共因故障,
- 每种特定放射性释放方式的大气弥散模型的使用,
- 不确定度分析,
- 针对超设计基准事件的分析过程的充分性。

5.10. 应该对挑选出的计算机计算进行独立校核, 以确保分析是正确的。如果未对原始程序进行过足够的检验和验证, 则应该使用替代程序核实其准确性。

参考文献

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).
- [3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).
- [4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion, Safety Series No. 50-P-1, IAEA, Vienna (1990).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Standard Series No. NS-G-2.2, IAEA, Vienna (2000).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes in Nuclear Power Plants: A Guidebook, Technical Reports Series No. 368, IAEA, Vienna (1994).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA, Vienna (1992).
- [11] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety Series No. 50-P-8, IAEA, Vienna (1995).
- [12] OECD NUCLEAR ENERGY AGENCY, Level 2 PSA Methodology and Severe Accident Management, OECD/GD(97)198, OECD, Paris (1997).

- [13] UNITED STATES NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Rep. NUREG-1150, Division of Systems Research, USNRC, Washington, DC (1990).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No.50-P-12, IAEA, Vienna (1996).
- [15] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety Series No. 106, IAEA, Vienna (1992).

参与起草和审订的人员

Couch, D.P.	美国太平洋西北国立实验室
Del Nero, G.	意大利国家环境保护机构
De Munk, P.	荷兰国家核安全部
Fil, N.	俄罗斯液压机试验设计局
Federation Foskolos, K.	瑞士保罗·谢勒研究所
Gasparini, M.	国际原子能机构
Misak, J.	国际原子能机构
Kabanov, L.	俄罗斯国家核安全中心
Federation Krishnan, V.S.	加拿大原子能有限公司
Krugmann, U.	德国西门子AG/KWU电力公司
Lee, J.H.	韩国核安全协会
Omoto, A.	日本东京电力公司
Petrangeli, G.	意大利国家环境保护机构
Rohar, S.	斯洛伐克核管理委员会
Shepherd, C.H.	英国皇家核设施检查机构
Simon, M.	德国反应堆安全与制造公司
Vidard, M.	法国电力公司
Vine, G.	美国电力研究所
Wilson, J.N.	美国核管理委员会

认可安全标准的机构

核安全标准委员会

阿根廷:Sajaroﬀ, P.; 比利时: Govaerts, P. (主席); 巴西: Salati de Almeida, I.P.; 加拿大: Malek, I.; 中国: Zhao, Y.; 芬兰: Reiman, L.; 法国: Saint Raymond, P.; 德国:Wendling, R.D.; 印度: Venkat Raj, V.; 意大利:Del Nero, G.; 日本:Hirano, M.; 大韩民国: Lee, J.-I.; 墨西哥: Delgado Guardado, J.L.; 荷兰: de Munk, P.; 巴基斯坦: Hashimi, J.A.; 俄罗斯联邦:Baklushin, R.P.; 西班牙: Lequerica, I.; 瑞典:Jende, E.; 瑞士: Aberli, W.; 乌克兰:Mikolaichuk, O.; 英国:Hall, A.; 美利坚合众国:Murphy, J.; 欧洲委员会: Gómez-Gómez, J.A.; 国际原子能机构: Hughes, P. (协调员); 国际标准化组织:d'Ardenne, W.; 经济合作与发展组织核能机构: Royen, J.

安全标准委员会

阿根廷: D'Amato, E.; 巴西: Caubit da Silva, A.; 加拿大: Bishop, A., Duncan, R.M.; 中国: Zhao, C.; 法国: Lacoste, A.-C., Gauvain, J.; 德国: Renneberg, W., Wendling, R.D.; 印度: Sukhatme, S.P.; 日本: Suda, N.; 大韩民国: Kim, S.-J.; 俄罗斯联邦: Vishnevskiy, Y.G.; 西班牙: Martin Marquínez, A.; 瑞典: Holm, L.-E.; 瑞士: Jeschki, W.; 乌克兰: Smyshlayaev, O.Y.; 英国: Williams, L.G. (主席), Pape, R.; 美利坚合众国: Travers, W.D.; 国际原子能机构: Karbassioun, A. (协调员); 国际辐射防护委员会: Clarke, R.H.; 经济合作与发展组织核能机构: Shimomura, K.

通过国际标准实现安全

“国际原子能机构的标准已经成为促进有益利用核和辐射相关技术全球安全机制中的一项重要内容。

“国际原子能机构安全标准正在适用于核电生产以及医学、工业、农业、研究和教育，以确保对人类和环境的适当保护。”

国际原子能机构
总干事
穆罕默德·埃尔巴拉迪

国际原子能机构
维也纳
ISBN 92-0-513805-3
ISSN 1020-5853