

国际原子能机构《核安保丛书》第4号

技术导则

防止核电厂遭受破坏的 工程安全问题



IAEA

国际原子能机构

国际原子能机构《核安保丛书》

国际原子能机构《核安保丛书》出版物旨在处理与防止和侦查涉及核材料和其他放射性物质及其有关设施的盗窃、破坏、擅自接触和非法转移或其他恶意行为并做出响应有关的核安保问题。这些出版物符合并补充了国际核安保文书，例如经修订的《核材料实物保护公约》、《放射源安全和安保行为准则》、联合国安理会第 1373 号决议和第 1540 号决议以及《制止核恐怖主义行为国际公约》。

国际原子能机构《核安保丛书》的类别

原子能机构《核安保丛书》出版物按以下类别发行：

- **核安保法则**包含核安保的目标、概念和原则，并提供安保建议的基础。
- **建议**提出成员国在实施核安保法则时应当采用的最佳实践。
- **实施导则**进一步详细阐述这些广泛领域内的建议并提出其执行措施。
- **技术导则**出版物包括：**参考手册** — 在具体领域或活动中就如何适用实施导则提供详细措施和（或）指导；**培训导则** — 包括原子能机构在核安保方面的培训班教学大纲和（或）手册；以及**服务导则** — 在原子能机构核安保咨询工作组的行为和工作范围方面提供指导。

起草和审查

一些国际专家协助原子能机构秘书处起草这些出版物。对于核安保法则、建议和实施导则，原子能机构召开不限人数的技术会议，为感兴趣的成员国和相关国际组织提供适当的机会审查草案文本。此外，为确保高水平的国际审查和达成高度国际共识，秘书处向所有成员国提交草案文本，以供进行 120 天的正式审查。这使得成员国在文本印发以前有机会充分表示他们的意见。

技术导则出版物是与国际专家密切磋商后制订的。技术会议并非必需的，但为了广泛征求意见，也可以在认为必要时召开。

国际原子能机构《核安保丛书》出版物的起草和审查过程考虑到机密性，并且承认核安保与总体乃至具体国家的安全关切有着密不可分的联系。一个基本的考虑是在这些出版物的技术内容上应当虑及相关的原子能机构安全标准和保障活动。

防止核电厂遭受破坏的工程安全问题

下列国家是国际原子能机构的成员国：

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

《国际原子能机构规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的国际原子能机构规约大会核准，1957 年 7 月 29 日生效。国际原子能机构总部设在维也纳，其主要目标是“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《核安保丛书》第 4 号
技术导则

防止核电厂遭受破坏的 工程安全问题

国际原子能机构
2011 年·维也纳

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《世界版权公约》之条款的保护。自那时以来，世界知识产权组织（日内瓦）已将版权的范围扩大到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国际原子能机构印刷形式或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。垂询应按以下地址发至国际原子能机构出版科：

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
传真：+43 1 2600 29302
电话：+43 1 2600 22417
电子信箱：sales.publications@iaea.org
<http://www.iaea.org/books>

© 国际原子能机构·2011 年
国际原子能机构印制
2011 年 11 月·奥地利

防止核电厂遭受破坏的工程安全问题

国际原子能机构 奥地利·2011 年 11 月
STI/PUB/1271
ISBN 978-92-0-523310-9
ISSN 1816-9317

前 言

为响应国际原子能机构（原子能机构）2002 年 9 月大会的一项决议，原子能机构采用了一项旨在防止核恐怖主义的综合方案。该方案对原子能机构有关以下方面的活动进行了协调，即核材料和核设施的实物保护、核材料衡算、侦查和应对核材料和其他放射性物质的贩卖、放射源的安保、核材料和其他放射性物质运输中的安保、成员国和原子能机构的应急响应和应急准备措施，以及促进各成员国遵守相关的国际文书。原子能机构还帮助鉴别与核材料和其他放射性物质安保有关的威胁和薄弱环节。尽管如此，对核材料和其他放射性物质以及有关设备的实物保护作出规定，确保此类物质在运输安保，以及打击放射性物质非法贩卖和意外移动，仍是国家的责任。

自从 2001 年 9 月 11 日袭击以来，对恐怖分子可能威胁核设施的理解发生了明显的变化。在核工业内部，随即的国际响应是通过增加设施警戒武装力量、靠安装附加安保装置增强实物保护、加强保护程序、严格出入控制、增加地面交通工具的隔离距离、审查和更新应急准备，以及一般来说在各级有关报警和响应的政府单位和私人部门之间提高密切合作的必要意识来加强安保。

仍然不太明确的是，可以进行和应该进行什么样的补充分析来确定核电厂安全重要构筑物、系统与部件是否能够针对可能的恐怖分子袭击提供最佳的实物保护，以及确定费用效益好的修补变更。全世界许多核电厂许可证持有者，在某些情况下由其监管机构委托，计算了电厂构筑物当受到飞机撞击同时考虑到动力学效应和产生的火灾效应时的牢固性。这些计算一般来说只限于非能动构筑物和系统的性能。

在任何恐怖分子袭击或破坏行动中，首先关注的是实现和维持安全停堆状态，包括热阱和放射性物质的安全壳继续可供利用，直到事件得到控制。本出版物提供了评定保护核电厂防破坏包括远距离袭击的工程安全方面的指导原则。

本出版物是原子能机构内外安全和安保专家广泛对话的成果。它考虑了来自监管机构和设计机构的反馈意见。它详述了关于核材料和核设施防破坏实物保护的更全面的概念。对草案作出主要贡献的外部人员是 J.J. Johnson 和 G.J.K. Asmis。负责本出版物的国际原子能机构官员是核设施安全处的 A. Gürpınar。

致 谢

国际原子能机构对中国国家原子能机构为本出版物的翻译所作的贡献表示感谢。

编 者 按

本报告无论在法律方面还是在其他方面均不涉及因任何人的作为或不作为而引起的责任问题。

尽管在保持本出版物所载资料的准确性方面十分谨慎，但无论国际原子能机构还是其成员国均不对使用本出版物可能产生的后果承担任何责任。

国家或领土的特定称谓的使用并不意味着作为出版者的国际原子能机构对于该国家或领土、其当局和机构或其边界划定的法律地位做出任何判断。

提及具体公司或产品（不管是否已经载明为注册的公司或产品）名称并不意味着有任何侵犯所有权的意图，也不应当被解释为国际原子能机构方面的核可或推介。

目 录

1. 引言.....	1
1.1. 背景.....	1
1.2. 目的.....	1
1.3. 范围.....	2
2. 背 景.....	3
3. 评价方法学.....	6
3.1. 概述.....	6
3.2. 威胁评价.....	7
3.3. 拟定具体的威胁情景.....	7
3.4. 极端环境载荷评价.....	9
3.5. 实物保护系统设计和评价概述.....	17
3.5.1. 实物保护系统.....	17
3.5.2. 要害区识别.....	19
3.6. 针对 1 型威胁和 2 型威胁事件的设施评定.....	19
3.6.1. 背景.....	19
3.6.2. 破坏裕度评定程序.....	21
3.6.3. 识别成功路径.....	22
3.6.4. 安全停堆设备清单.....	24
3.6.5. 安全停堆设备清单和要害区.....	25
3.6.6. 构筑物、系统与部件的能力评价.....	25
3.6.7. 破坏裕度评定小组的组成.....	28
3.6.8. 电厂现场访查.....	28
4. 决策方法学.....	29
5. 结论意见.....	31
附录一：实物保护流程图描述.....	33

附录二：电厂现场访查37

参考文献49

定义51

参与起草和审定的人员55

1. 引言

1.1. 背景

保护核设施防止恶意行为可以采取若干不同的形式。本出版物只讨论与破坏核设施有关的问题，也就是说，防止或缓解由恶意行为引发也许有放射性后果的事件。

本报告中的导则考虑了构筑物、系统与部件的现有牢固性。重要的是，注意到一般说来核设施，特别是核电厂，可以被认为具有良好的防恐怖袭击能力。它们有良好的实物保护系统和程序，并且被设计成能尽量减少发生事故的可能性，而万一发生事故也不会以非受控方式释放放射性物质。此外，核电厂被专门设计成能处理内外极端载荷，例如振动、热、超压和撞击。核设施抵抗极端事件的能力取决于它们的具体场址和设计特征，例如因极限风、风载飞射物、地震、失水事故引起的内压和火灾造成的载荷——因此也就是所需的抵抗力（能力）。

在本出版物的范围内，自评定（以下简称为“评定”）是由许可证持有者连同有关的地方或国家主管部门进行的对核电厂防破坏包括远距离袭击（即规定的威胁情景）能力的评定。

1.2. 目的

按照当前的威胁环境，本出版物的总体目的是提供评价任何以核电厂为目标、可能通过辐射照射或放射性物质释放危及电厂人员、公众和环境的健康和安全的恶意行为有关的危险的方法，并且必要时推荐旨在降低危险（主要通过升级）的纠正行动。

这些导则阐述了一种评定核电厂安全相关构筑物、系统与部件选定子集系统承受破坏引发事件能力的方法学。所提出的方法学，包括筛选，综合应用了现有的安全裕度评定技术。

具体地说，本出版物的目标是：

- (a) 提供《核材料和核设施的实物保护》(INFCIRC/225/Rev.4) [1]中的信息、关于核材料和核设施防破坏实物保护的全面指导以及防破坏的工程安全问题；
- (b) 提供与关于识别核设施内部要害区和关于制订和维护设计基准威胁全面指导的联系；
- (c) 提供在破坏引发事件方面评定核设施的通用准则；
- (d) 使用从既定的（即达成共识的）定义中提出的通用术语，必要时也定义新术语，来说明安全/安保联合概念；
- (e) 提出一种安全裕度评定方案，即允许使用设计过程中的不同接受标准（例如对照设计允许的最佳估计）；
- (f) 提供一种评定程序使得设施营运者（或监管人员）可以作出决策是否需要加强或升级安全相关构筑物、系统与部件、实物保护措施或场内或场外的应急程序；
- (g) 用作用于未来手册、技术指导、调查工具和服务的一种基础性文件。

1.3. 范围

本出版物涉及所有核设施，包括核电厂、研究用反应堆、燃料制造厂、后处理厂和乏燃料储存设施。然而重点放在核电厂，因为它们涉及最复杂的分析。

在这个范围内考虑的事件包括：

- (a) 涉及暴力入侵场址的保护区（即在电厂管理部门行政控制下的区域）的事件，例如通过“恶意入侵的交通工具”（例如一辆装有爆炸物和武装入侵者的卡车）。
- (b) 由场区外部人员引起的事件。这样一类事件可能涉及导弹、在场区内释放毒气或者操纵飞机袭击设施。
- (c) 由内部人员引起的事件。

(d) 涉及多种袭击方式的事件，例如上述各种事件的结合。

对于反应堆设施来说，恶意行为的目标或者可能是其破坏将引起堆芯损坏导致放射性后果的系统，或者可能是放置或储存核燃料（新的或用过的）或放射性物质的区域。对于非反应堆设施来说，第二类目标是关系最大的。

被认为是这些导则范围以外的事件包括下列袭击：

- (i) 其唯一目的是盗窃核材料或其他放射性物质的；
- (ii) 在核材料运输期间发生的；
- (iii) 只涉及经济损失的。

2. 背 景

本出版物提出的方法学，其设计要使操作人员和安全专家与安保专家、负责应急准备的机构及其他各级政府机构密切合作，以便对破坏引发的事件提供纵深防御。本节概述这种相互关系，并提出政策和准则使得在第 3 节中说明的详细工程评价和在第 4 节中说明的决策过程得以进行。

图 1 中的流程图表明涉及的所有单位在发生恶意行动情况下如何合作保护核电厂。流程图更详细的说明，包括各方框和决策点的解释，在附录一中给出。

威胁分为两种类型：

- (a) 1 型威胁（TT-1）指的是由内部人员或打算侵入设施（有或者没有内部人员帮助）的敌手对核电厂构成的威胁。
- (b) 2 型威胁（TT-2）与此相反，指的是在电厂边界以外发出的威胁，不需要现场有敌手存在。这类威胁的实例包括例如肩上发射的导弹和飞机等远距离袭击。

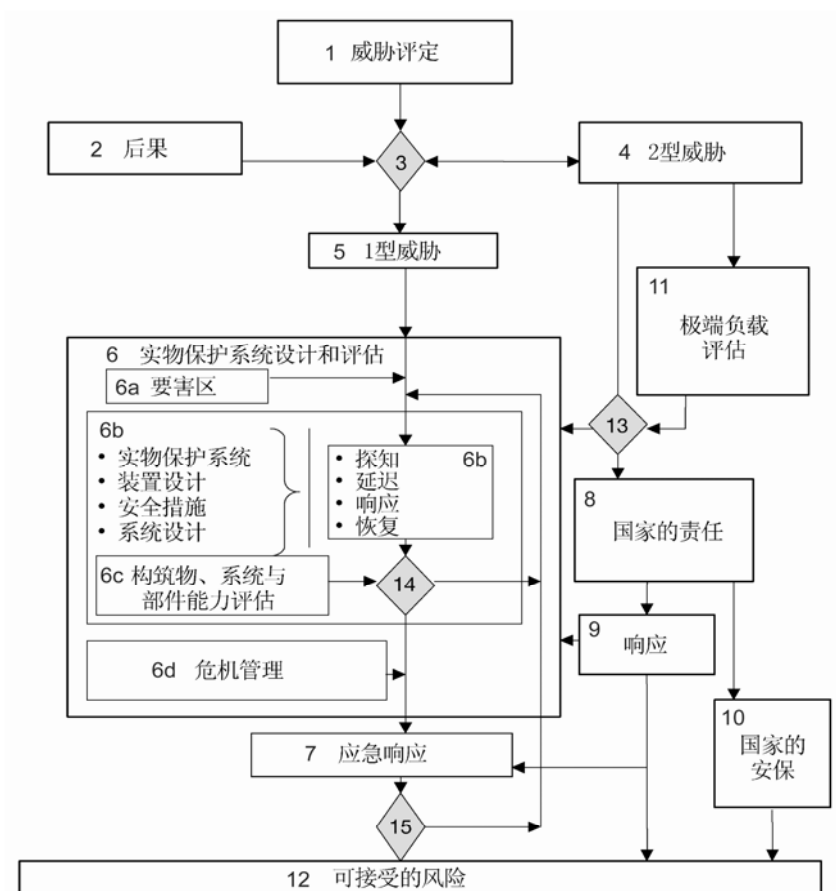


图 1. 核材料和核设施的防破坏实物保护。

作此区分是为了反映用来对付每种威胁的工程措施在方法上的差别。对于 2 型威胁，其措施是提供防破坏保护的主要内容，对于 1 型威胁是提供再加一层的纵深防御，并且它们的使用需要与实物保护措施密切协调。

面对当前威胁环境的挑战出现的一个共识是需要所有国家实体的多方合作。其中包括政府机构，例如情报服务机构、军队、警方、地方政府主管部门、市政当局和民防组织。

进行危险评定需要专门标准。一般来说，这些标准是由核监管者提供的。以下是一套标准样本：

- (a) 万一发生袭击时核电厂的牢固性足以防止大量裂变产物快速非受控释放（即灾祸性失效）吗？
- (b) 重要安全系统是否继续执行它们的功能（例如冷却核燃料和包容放射性物质释放），或者它们能按需要启动和运行吗？
- (c) 在袭击发生后，即使发生相关效应例如火灾、烟雾和结构破坏，重要安全系统能运行到可以进行修理的时候吗？
- (d) 万一发生大规模外部袭击，核电厂的设计和运行以及响应程序和能力能够最大程度减少公众和设施工作人员的照射吗？

安全构筑物、系统与部件的生存能力接受标准、营运者行动以及应急预案和程序作用的发挥可以根据现实的（即不保守的）假设。

一项基本评定标准与成功路径的数目和在这些成功路径上构筑物、系统与部件的行为限值有关。

第 3 节中概述的评价方法学，提供了一种手段来确定当处于给出威胁情景中是否有一种或几种安全停堆路径存在所需的安全功能。在本出版物中，术语“成功路径”指的是监管机构或其他主管机构所要求和定义的对于一个电厂系统的子集其可操作性和生存能力足以确保该厂性能标准得以满足的部件的最小集。一个成功路径可能包括超过电厂安全停堆的功能，如果所关心的尺度是释放到环境中的放射性低于容许限值的话。在这里术语“安全停堆路径”定义为不考虑安全壳或因放射性释放而对公众造成的照射实现和维持安全停堆状态所要求的部件的最小集。当术语“安全停堆路径”和“成功路径”没有必要区分时，它们在本出版物中可互换使用。此外，术语“性能标准”是用来表示与所需的构筑物、系统与部件功能（性能）类型有关的标准。与此相反，术语“接受标准”指的是构筑物、系统与部件在给定功能方面允许的行为限值。两者都由监管机构确定。

该方法学也可以用于多层的接受标准。例如，对于设计基准威胁造成的情景，接受标准可以类似于设计参数，也就是说，保持了全部安全系统冗余性和安全相关系统与构筑物的完整性。对于设计基准威胁外威胁的情景，接受标准可以允许只存留一个成功路径并对所需的构筑物、系统与部件使用现实的行为限值。

评定的结果可以是，对于给定的威胁情景，没有一个安全停堆路径被证明是能满足成员国接受标准的。在这种情况下，成员国可以决定根据进一步的措施例如场外防止和缓解的威胁情景以及适当的响应措施管理这种局面。

由监管主管部门规定的有关所需成功路径数目的标准，决定了评定程序的复杂性。例如，如果设想只有一个成功路径可供利用并允许构筑物、系统与部件用现实的行为限值，那么要评价的构筑物、系统与部件的数目将是比较少的（因为只有一个路径），并且牢固性筛选过程将更加直接了当。在大多数场合下，安全停堆被认为是“成功”的，在这一路径上的构筑物、系统与部件构成一个“安全停堆设备清单”。重要的是注意使评定过程从一开始就集中于“安全停堆设备清单”上。

3. 评价方法学

3.1. 概述

第 3 节安排如下：第 3.2 节列出按照从威胁评定中导出的情景进行评价所需要的投入；为本报告目的，情景被确定为 1 型威胁或 2 型威胁。第 3.3 节阐述对于要评价的具体核电厂筛选 2 型威胁的过程。这一过程产生了一套要评价的威胁情景、对于场址和设施的具体考虑以及这些威胁按察觉的对设施危险水平的顺序。第 3.4 节阐述威胁情景向供详细评价的工程参数的转换。第 3.5 节总结在工程安全评价与电厂实物保护系统和可用措施之间的关系。也包括关于要害区识别及其与成功路径和安全停堆路径概念关系的简短讨论。第 3.6 节详述了用于 1 型威胁和 2 型威胁情景工程安全评价的方法。方法的要素包括：识别成功路径，建立系统安全设备清单（部件及其功能特性要求），构筑物、系统与部件能力评价，建立评定小组，电厂现场访查和文档要求。在第 3.6 节中的评价表明安全停堆设备清单中的部件承受恶意袭击的能力；在第 4 节中从决策方面考虑这些能力。

3.2. 威胁评价

国家规定要评价核威胁的后果。在破坏的情况下，接受标准关系到电厂工作人员和公众的安全，并且按照各项放射性后果阐述危险的接受标准[1]。

设计基准威胁说明“潜在的内部敌手和/或外部敌手的属性和特性，这些人可能试图擅自转移核材料或进行破坏，因此要根据这一背景来设计和评价实物保护系统”[1]。

可能需要由电厂加以考虑而又没有列入设计基准威胁的威胁被称为“设计基准威胁外威胁”。因为用于设计基准威胁外威胁事件的接受标准可能不同于用于设计基准威胁事件的，所以要对两者加以区别。所有威胁也可以用 1 型威胁和 2 型威胁予以说明。

3.3. 拟定具体的威胁情景

评价过程这一步骤的目标是针对具体要评价的设施更好地规定威胁情景。根据以下考虑，这一过程可能导致排除某些情景：

- (a) **场址和设施特征：**周围地形和植被也许足以排除由电厂边界以外发起的某些威胁情景。对于某些类型威胁，厂址的地点和布置可能限制具体场区内区域会受到影响的可能性。例如，电厂地点位于丘陵、山峦或峡谷可能限制大型飞机袭击场址的可行接近角和速度。其他的因素，例如输电线路的位置，可能限制大型飞机袭击的预想通道。对于冲击波载荷状况，由地形效应和毗邻构筑物提供的构筑物屏蔽可能限制其影响区，因此应该加以考虑。同样，可能有利于敌手的潜在场址条件也需要给予谨慎的考虑，例如核设施邻近公共运输基础设施（公路、铁路、机场）或工业区和居民区。研究用反应堆往往位于研究中心内部或大学校园内，可能使得潜在的入侵者或攻击者难以识别。
- (b) **场址上设施的类型和数目：**一座核电厂场区内也许有几台反应堆机组，可能有相互关联的安全或支持系统。多机组场址常常假定当对付非共因事件时其他机组系统可供利用。此外，其他的关键

设施也许位于电厂边界内，例如用于燃料水池乏燃料储存或干式重屏蔽容器储存的设施。研究用反应堆场址也许有相关的实验室、同位素生产设施和热室。当受到 2 型威胁袭击时场址上的所有设施可能需要同时予以实物保护。评价应该考虑到场区内所有设施及其安全系统的所有相互关联。这种考虑包括环境排放的后果评定，这种排放对于场址上的所有设施是累计的。

(c) 设计：核电厂是针对各种极端环境载荷条件设计的。抵御内外设计基准事件 — 例如火灾、管道甩动、失水事故、地震、极限风、爆炸或飞机撞击 — 的措施为核电厂提供了一个保护“外套”。重要的是当评价威胁情景时要考虑这种保护。实际上，某些情景也许会从进一步考虑中排除，因为它们被设计基础条件有效地限制了。根据事件（对于整个设施）、极端载荷（对于每个物项）或从载荷导出的分级要求能够证明受到限制。

(d) 设施场外独立安保措施：电厂边界以外有效的行政措施及其他措施被称作设施场外独立安保措施。这些措施的范围可以从航空方面加强安保到由在场址附近的场外单位实行的监视。如果措施到位并且有效，可能用来从考虑中排除某些威胁情景或更好地规定威胁情景的参数化方法。

在天然来源或意外人为来源的外部事件的筛选过程中，一般来说使用两种方法：由距离与规模筛选和由发生概率筛选。在第一种方法中，对于核电厂厂址假定事件的最短距离和最大范围（即最保守的条件），然后评定对电厂安全的潜在破坏影响。如果发现影响微不足道，则针对所评定的参数筛选出事件。例如，根据对所关心的安全相关系统的有效屏障距离，也许筛选出一个涉及装有爆炸物车辆的袭击情景。由概率筛选一般来说更加复杂和不确定，并且也许应用于不是由距离和规模筛选出的事件。筛选所用的概率水平一般来说比用于设计目的的小一两个数量级；由于概率性筛选程序的估计性质，为维持保守性和不排除任何事件，使用较小的数量级。然而，在意外发生的事件的概率筛选和因破坏引起的事件之间存在着显著差异。对于意外外部事件的筛选标准，一般来说是假定破坏可能性更大的情景发生的频率小 — 也就是说，事件越大，发生的频率越低。对于破坏事件，取决于破坏者的目标和能力，这一假设也许不成立。

破坏事件不支持在绝对概率基础上的概率筛选。然而第 3.6.1 节提出一种利用适合于解决威胁的概率安全评定工具的方法，在这种情况下有条件的终止标准是计算的，并可以提供筛选各种威胁的基础。这一方法假定最上游的事件是确定性的（即 $p=1$ ），但是由这一事件演化的事件序列根据电厂布置、系统设计和结构的牢固性可能表现为概率性的。

在这个阶段为降低针对威胁情景评价设施所需要的工作量可以实施的其他行动包括以下：

- (a) 按照对核设施事实上的相似性可以把威胁情景组合起来。可以选定组合威胁情景的一个情景或一种组合进行详细评价。这样组合的威胁情景把威胁情景降低到一个更加容易管理的数目。可以指定一个威胁论证和核安全专家小组进行这项活动。
- (b) 可以筛选出低能力和低安全重要性的构筑物、系统与部件；例如可以确定某些构筑物为低能力的，因此在成功路径定义的考虑中将其排除。

3.4. 极端环境载荷评价

要进行评价的破坏威胁情景可能有两种类型 — 1 型威胁或 2 型威胁。足够详细地说明了这些情景，从而可以规定与每种情景有关的极端环境。

这里重点是威胁情景和相关极端环境的工程安全问题。潜在威胁清单包括内部和外部以及以及两者结合引发的事件。此外，正如在这里说明的，找出和评价了多模式威胁。预计某些威胁情景将涉及入侵者袭击，或者是单独进行的，或者是多模式袭击的一部分。

极端环境载荷评价的目的是为电厂工程机构提供一个由威胁情景产生的、可以应用于部分或整体设施的环境条件矩阵。其结果是一个规定了电厂工程人员在评价为成功电厂性能所需的构筑物、系统与部件时要考虑的环境载荷和载荷组合的环境载荷表。有了这种资料，电厂工程部门就可以确定设施抵抗威胁的能力。环境载荷评价是威胁情景和评价过程之间的接口；它仅仅包括工程方面，而不是详述威胁情景。

在评价过程中，设施因设计和建造条件产生的固有强度应该得到承认。

在这一过程中，重点放在设施安全停堆以及在整体恢复行动和必要时厂外其他单位给予帮助所需期间保持安全停堆状态所要求的构筑物、系统与部件上。针对以下大量环境条件设计和评价构筑物、系统与部件：

- 构筑物一般来说提供压力保持、屏蔽和约束中的一种或多种功能以及支持系统和部件。构筑物和构造单元是按在整个设施寿命期间的运行工况和事故工况设计的。工作载荷包括静载荷、动载荷、大气温度、热载荷、振动、辐射作用、压力保持和老化效应（辐射、腐蚀及其他材料老化的影响）。构筑物的设计考虑了偶然载荷，例如飞射物撞击（内部或外部产生的）、极限风、洪水、地震、爆炸/冲击波（内部或外部产生的）、极端的热载荷、极端的辐射作用、因管道甩动及其他现象造成的脉冲载荷和重载荷落下。在设计中考虑了某些载荷条件同时发生。
- 一般说来系统是按照构筑物成套的运行工况和事故工况设计的。系统设计也包括了功能的冗余性以及系列和元件的分离、隔离和多样性，以便在正常运行和事故两种工况下提供高度可靠的成功系统性能。
- 部件一般来说是按照构筑物和系统成套的运行工况和事故工况设计的。然而设计、限定和维持部件所考虑的环境一般来说比对于构筑物和系统的更加广泛。正常运行工况包括各种规定的条件（例如温度、湿度、辐射、冷却、振动），部件在这些条件下必须发挥功能（例如泵按照规定流速输送流体）。

因此在这项任务中规定的极端环境条件需要按照设计的正常运行工况和事故工况进行评价。重要的是清楚了解构筑物、系统与部件的设计要求，例如在事件期间仍然完全可以运行、在规定时间内能够恢复运行或即使其他的构筑物、系统与部件功能不能恢复也能保持结构完整性。构筑物、系统与部件具有明显的抵抗与威胁情景有关的极端环境条件的固有能力。

在如下系列表格中说明了规定待评价威胁情景工程问题的过程。在表 1 中把威胁情景与极端环境相联系。对于在第 3.2 和 3.3 节确定的每一个威胁情景，找出了可能影响设施的极端环境。所用的例子纯粹是假想的，现象的范围和规定的参数没有打算保持完整，也不一定精确。

表 1 各列如下：

- 威胁情景编号是数值介于 1 和所考虑威胁情景总数中间的一个数字标识符。

例子：假定为威胁情景 1 号。

- 威胁情景描述是用于识别目的的威胁情景的简短描述。

例子：情景涉及飞入核电厂场址满装燃料的波音 767 飞机的撞击。

- 物理载荷条件是威胁情景施加的载荷条件的类型和特性的数字标识符。标识符直接关联于用于撞击的表 2、用于爆炸/冲击波的表 3、用于受热/火灾的表 4、用于有害物质释放的表 5 和用于其他环境后果的表 6。表 6 提供了关于在评价中所需要的工程学科的指导以及为什么需要考虑某些环境载荷组合的背景。

- 撞击指的是由数字并参考表 2 确定的冲击载荷条件。

例子：假定冲撞击载荷条件 1 和 2。

- 爆炸/冲击波指的是由数字并参考表 3 确定的爆炸/冲击波载荷条件。

例子：没有冲击波或爆炸载荷与 1 号威胁情景相联系，或者被认为是飞机撞击的附属影响。

- 受热/火灾指的是由数字并参考表 4 确定的受热/火灾荷载条件。

例子：假定了受热/火灾环境载荷条件 1。

- 有害物质释放指的是由数字并参考表 5 确定的有害物质释放状态。

例子：没有有害物质释放状态与 1 号威胁情景相联系。

- 在表 1 中确定了窒息、水淹及其他现象供未来考虑。窒息、停风和使构筑物、系统和部件丧失运行必需的空气被作为潜在的关注提出；例如柴油发电机缺乏空气就不能起动和运行。因消防技术（泡沫）造成的窒息可能需要进行评价。由内部或外部来源造成的洪水也可能需要进行评价；例如上游水坝的破坏可能释放的大量水涌进场址。

表 1. 极端环境载荷矩阵的例子

威胁情景 编号	威胁情景 描述	物理载荷条件						
		撞击 (表 2)	爆炸/ 冲击波 (表 3)	受热/ 火灾 (表 4)	有害物 质释放 (表 5)	窒息 (表 6)	洪水 (表 6)	其他 (表 6)
1	飞入核电厂场址满装燃料的波音 767 飞机的撞击	1, 2	无	1	无	无	无	无
2	肩上发射的导弹射入反应堆建筑物							
3	在场址大门处卡车内爆炸							

表 2 确定了电厂工程评价构筑物、系统与部件用的撞击参数。在这里来源于表 1 的威胁情景的例子仍然仅用于说明目的。

表 2 各列如下：

- 飞射物类型/编号是飞射物载荷标识符，数值介于 1 和所考虑的飞射物撞击情景的总数中间。
例子：1 号飞射物是装满燃料的波音 767 机身；2 号飞射物是波音 767 飞机的发动机。
- 描述简要说明了载荷条件的来源。
例子：1 号飞射物是装满燃料的波音 767 飞机的撞击；2 号飞射物是波音 767 飞机发动机的撞击。
- 质量/重量指的是飞射物的质量/重量。
例子：1 号飞射物是 200 000 千克，包括燃料；2 号飞射物是每台发动机 3500 千克。

表 2. 冲击波参数定义矩阵的例子

飞射物 类型/ 编号	描述	质量/ 重量	飞射物撞击				附属影响		
			形状/ 布置	撞击角	撞击 速度	相对 硬度	火灾	爆炸/ 冲击波	其他
1	波 音 767 飞 机 机 身，装满 燃料	200 000 千克	柔性的	小于30°， 由水平 方向	180 米/秒	柔性的	1	无	无
2	波 音 767 飞机发动 机，作为 抛射体	3500 千克	3米直径 /刚性圆 柱	小于30°， 由水平 方向	180 米/秒	刚性的	无	无	无
3									

- 形状/布置提供更加具体的飞射物描述，如果可以获得也给出规定的尺寸。
例子：1 号飞射物被称作柔性的机身，尺寸待定；对于 2 号飞射物发动机假定为刚性的，尺寸如同所示。
- 撞击角指的是潜在撞击角的角度或范围，考虑到物理学和实现该目的所必需的人的能力。
例子：撞击角范围是从水平方向 0 到 30°。
- 撞击速度是飞射物的速度，考虑到物理学和实现该目的所必需的人的能力。
例子：撞击速度是 180 米/秒。
- 在评定飞射物对构筑物、系统与部件影响的时候相对硬度是一个重要的参数；它可以是一种定性或定量的度量。
例子：1 号飞射物机身被认为是柔性的；飞射物 2 号是刚性的。

- 附属影响是随直接影响例如混凝土散裂或碎块发生的影响——对撞击点附近的部件有附属影响。它们可能在技术条件的其他地方规定，例如在这里使用的例子中的火灾。
 - 飞射物撞击引起火灾，或者因为携带着燃料，或者因为撞击易燃物，例如柴油罐。

例子：1 号飞射物与受热/火灾条件 1 相联系，是一种由飞机撞击造成的喷气燃料火灾。飞射物 2 号没有有关的燃烧条件。
 - 飞射物撞击引起爆炸/冲击波，或者因为飞射物携带了爆炸物在撞击时引爆，或者因为飞射物撞击了爆炸物储存设备。

例子：假定没有发生爆炸。
 - 其他危害例如可能包括入侵者与导弹攻击互相配合。

例子：确定没有其他危害。

表 3 确定了一套简化的爆炸/冲击波载荷条件，将由电厂工程用于评价构筑物、系统与部件的能力。在这里所用的例子假定没有爆炸/冲击波条件。表 3 各列如下：

- 爆炸号是爆炸/冲击波条件的标识符，其数值介于 1 和所考虑的冲击波条件的总数中间。
- 表 3 中的参数是爆炸物特征的描述语的例子。对于一般说明，梯恩梯当量和参考距离（从设施基准点起计算）是最普通的信息。有关事件和反射波的具体信息将针对进行评价的各个核电厂制订。细节是大量场址具体特征的函数。

表 3. 爆炸/冲击波参数定义矩阵的例子

爆炸编号	描述	梯恩梯当量	参考距离	压力脉冲	
				入射的	反射的
1					
2					
3					

表 4 确定了电厂工程用于评价构筑物、系统与部件的受热和火灾特征。
表 4 各列如下：

- 火灾编号是受热/火灾条件的标识符，其数值介于 1 和所考虑的火灾条件的总数中间。
例子：假定了 1 号受热/火灾条件。
- 描述简要地说明了火源。
例子：例子中的火源是波音 767 飞机喷气燃料燃烧。
- “设施外部火源”类别中的条目规定了假定火源在设施外面的火灾危险。对于飞机撞击或其他类似的威胁情景，设施边界内外易燃物的分布是重要的。两处明显的分布点是电厂院落和进入建筑物的穿入点。其他的包括设施边界外部可能妨碍应急响应人员及其他人员进入的那些分布点。重要参数的例子是易燃物的数量和类型、热势和温度的估计以及燃烧的持续时间。
例子：波音 767 飞机的喷气燃料溅出并被点燃；没有进入建筑物的穿入点。燃料的数量是 50 000 千克。高温燃烧（1000℃）持续时间是 最长 1 小时，300℃ 余火 5 至 7 小时。
- “设施内部火源或易燃物”类别的条目规定了假定火源在设施之内或火灾是由于外部火源而在内部点燃的火灾危险。重要参数的例子是易燃物的类型和的数量、位置和估计的燃烧持续时间。
例子：假定没有内部火源。

表 5 确定了核电厂有害物质释放条件的重要参数。有害物质释放和其他方式同时攻击似乎是可信的；其他方式可能包括针对化学释放影响加以防范的敌手。在例子中假定没有有害物质释放。

表 5 各列如下：

- 案例编号是有害物质释放号，数值介于 1 和所考虑有害物质释放条件的总数中间。
- 物质描述简要说明有害物质。
- 数量指的是物质释放的数量和释放发生的时间范围。

表 4. 受热/火灾参数定义矩阵的例子

火灾 编号	描述	设施外部火源					设施内部火源或易燃物				
		易燃物/ 点火	数量	热势/温度	燃烧持续 时间	其他	建筑物/ 院落	数量	类型	着火 可能性	燃烧 持续 时间
1	由波音 767 飞机引起的喷气燃 料火灾	是	50 000 千克	1000 °C	1—8 小时						
2											
3											

表 5. 有害物质释放定义矩阵的例子

案例 编号	物质描述	有害物质载荷条件						
		数量	窒息效应（人员）	窒息效应（部件）	致命或致残效应（人员）	持续时间	穿入范围	其他
1								
2								
3								
4								

- 窒息效应(人员)逐项详列对人员(例如电厂操作人员、安保部队)的物理效应, 包括是否需要保护装置的征兆和执行的时间范围。
- 窒息效应(部件)确定窒息或断风对部件的可能影响, 例如应急柴油发电机是否可能受到一种具体化学品大气弥散的不利影响。
- 致命或致残效应(人员)确定对电厂工作人员的潜在影响。
- 持续时间是有害物质存在的时间范围, 注明是否发生散布。
- 穿入范围说明有害物质通过包括供暖、通风和空调系统的流道移动进入建筑物之内或留在电厂院落内的范围。

表 6 和支持资料用作在威胁情景规定和工程安全专家的评价要求之间的接口。它包含环境载荷标识符和要考虑的环境载荷组合。在这里表 6 是为说明目的而简化的。对于安全停堆设备清单中的每个物项, 都有一套要考虑的载荷条件和载荷组合。

3.5. 实物保护系统设计和评价概述

核电厂中的实物保护系统被设计成能保护设施抵御设计基准威胁。在一个设计基准威胁事件期间, 工程安全方面支持实物保护系统, 并构成纵深防御的一个附加层次。这里为完整起见包括了实物保护系统的一个非常简短的描述。这一程序的有效评定和执行, 需要实物保护系统专家和那些负责工程和运行安全的工作人员的综合努力。

3.5.1. 实物保护系统

防破坏实物保护需要结合硬件(安保装置)、程序(包括组织警卫和履行警卫职责)和设施设计(包括布局)。实物保护措施的设计要考虑了到核设施的特征、核材料、国家的设计基准威胁和可能的放射性后果。

一个有效的实物保护系统(见图 1 中的方框 6b)实施如下主要功能:

- (a) 威慑;
- (b) 探知和评定;
- (c) 延迟;
- (d) 响应。

表 6. 极端环境载荷定义矩阵的例子

厂 区	要害区	描述	物理载荷条件						
			撞击	爆炸/冲击波	受热/火灾	有害物质释放	窒息	洪水	其他
建筑物 1									
2									
3									
区 1									
2									
3									
4									
院落 1									
2									
物项 1									
2									
3									

3.5.2. 要害区识别

要害区是一个“保护区内拥有设备、系统或装置或者核材料的区域，它若遭破坏有可能直接或间接导致不可接受的放射学后果”[1]。图 1 中的方框 6a 显示确定设施内要害区的范围。通过评价恶意行为的后果，安全专家和安保专家密切合作确定核设施内可能遭到破坏、需要加以保护防止万一受到袭击造成不可接受的放射性后果的目标[1]。如果全面安全原理要求，最小的整套设备、系统与装置可能包括所有指定的安全系统。另外，最小集可以是所有设备、系统与装置的一个子集，这也取决于国家或其指派者确定的标准。要害区识别过程是复杂的，可能使用多种不同方法。要害区的数目和范围因设施而异。

如上所述，要害区识别过程涉及目标识别，这是实物保护系统设计的基础。目标识别的重点是保护什么，而实物保护系统设计要解决的是如何保护确定的目标。目标识别不考虑实物保护措施是否能够被破解或者提供实物保护是否困难。换句话说，目标识别是找出要保护的区域、部件或功能；对这些项目的威胁和针对一种威胁保护它们的难易是在这些项目确定以后考虑的。

找出安全停堆路径的过程可以与要害区识别过程整合在一起。如果找出要害区的全面安全原理与对于 2 型威胁事件的全面安全原理相容，那么在要害区和安全停堆设备清单设备之间可能存在着——对应的关系。在这一情况下，在安全停堆设备清单物项和要害区之间的密切关系将会保持。然而更可能的是，用于要害区识别和实物保护系统设计的全面安全原理可能不同于用于 2 型威胁事件的。在这种情况下，将找出包含安全停堆设备清单物项的要害区子集。

如同所有与破坏有关的信息一样，要害区识别过程的结果是敏感的，应该按照严格的保密规则加以保护。

3.6. 针对 1 型威胁和 2 型威胁事件的设施评定

3.6.1. 背景

这个程序的重点是针对 1 型威胁和 2 型威胁事件保护的工程安全问题。

对于 1 型威胁事件，考虑由入侵者运送和引爆的炸弹及其他爆炸物对构筑物、系统与部件的影响。在这种情况下，可以假定实物保护系统不是有效的和把工程安全措施用作纵深防御的一个附加层次。尽管以下情况对于 1 型威胁和 2 型威胁两者都同等可用，但是为了详细说明把重点放在后者。

评价程序可以按三个可用方案加以考虑：

- (1) 第一个方案表明 2 型威胁极端环境条件已包括在设计基准载荷条件内。这个方案可适用于核电厂的部分安全系统直到整体电厂。应该用进一步筛选的方法排除威胁情景（见第 3.3 节靠距离和规模或靠概率技术筛选的讨论）。在程序的这个阶段，如果确定情景的后果不会引起堆芯损坏，通过检查来排除威胁情景是可能的。此外，对于所讨论的设施出现的内外事件应用那种借助于概率风险评定的概率筛选技术是可能的。在概率筛选方案中，事件树是针对所关心的威胁情景建造的。在每个事件树的根部是相当于威胁情景的始发事件。应该进行最终状态的条件概率计算，例如条件堆芯损坏概率或条件大规模早期释放概率，而每个最终状态都以威胁情景的发生为条件。如果条件堆芯损坏概率或条件大规模早期释放概率满足保守的接受标准，那么威胁情景可以从进一步考虑中排除。对于威胁情景发生的可能性不进行评价，因为即使概率等于 1，堆芯损坏或安全壳破坏的可能性也低于许可阈值。
- (2) 第二个方案是参考内部和/或外部事件概率风险评定的结果，由此可以进一步了解核电厂的易损程度：
 - (i) 对系统事件树/失效树进行的敏感性研究可以找出特别关心的易损状况，包括非常易损状况和易损状况。一个非常易损状况是，在这种场合概率安全评定的定性结果表明至少有一个最小割集包括在假定威胁情景条件下预期发生将导致堆芯堆芯损坏之类严重后果的事件。一个易损的条件是，在这种场合基于假定不能利用的系统组合进行的敏感性评价，概率安全评定的定量结果显示发生堆芯损坏之类事故的概率明显提高。这两个假想的情况用来加强对易损的电厂运行状态和条件的评价。

(ii) 现有内外事件的概率风险评定，当进行修改以考虑由威胁情景产生的其他基本事件和失效模式时，可以提供对核电厂因构筑物、系统与部件的冗余性、多样性和空间分离而造成的牢固性的深入了解。这一定性或定量评定可以提供由于引起电厂失效需要大量失效同时发生而可以消除一些具体威胁情景的信心。

(3) 第三个方案是进行安全裕度评定，以证实核电厂能够抵御威胁情景、实现安全停堆并维持安全停堆状态。这一确定性方案，在这里相当于破坏裕度评定（SMA），是本出版物其余部分的主题。

当评价所提出的实体改变和运行改变的费用-效益比时，应该根据 (a) 迄今运行对构筑物、系统与部件材料状态的影响（老化效应）和 (b) 预期设施未来寿命考虑核电厂的使用年限。

对于非反应堆设施（或设施的一部分，例如乏燃料水池）所关心的参数是条件大规模早期释放概率。安全停堆标准可以用例如保持冷却剂循环和燃料完整性来代替。

3.6.2. 破坏裕度评定程序

一般来说，评价工程安全设施抵御 2 型威胁事件能力的破坏裕度评定方案包括以下步骤。这些步骤中所用的假设可以不同，取决于 2 型威胁是否被归入设计基准威胁还是设计基准威胁外威胁。

- (a) 把极端环境定义矩阵（表 6 和支持资料）引进评价程序，其中包含用于工程评价的载荷环境和载荷组合的定义。这些极端环境可以包括撞击、爆炸/冲击波、受热/火灾、振动、有害物质释放、洪水及其他因场址而异的状态。
- (b) 规定处于极端载荷环境中的核电厂的综合性能标准。例如，对于一座处于 2 型威胁事件中的核反应堆综合性能标准可以规定为威胁情景开始以后 24 小时的热停堆或冷停堆。另外一个假设是在 24 小时内可以从电厂边界外面有效地动员其他的帮助。在任何场合下都由成员国确定性能标准，包括从电厂边界外面能够有效地动员其他的帮助以前的停堆持续时间。

- (c) 规定将用于工程评价的假设。对于一座核电厂假设的例子是：
 - (i) 场外电源丧失；
 - (ii) 电厂的运行状态（例如满功率、停堆/换料）；
 - (iii) 系统标准（例如安全停堆路径的冗余性）。
- (d) 规定构筑物、系统与部件能力标准。
- (e) 规定一个或多个安全停堆路径或成功路径。
- (f) 证实在要害区识别过程中找出的每个备选要害区集包含用于至少一个成功路径的设备。一种替代方案方法将确定备选要害区集，然后对其中某些或全部备选集进行能力评价。
- (g) 在给定的上述假设下，找出组成安全停堆路径并且要求在威胁情景事件期间和以后发挥功能的构筑物、系统与部件。规定这些构筑物、系统与部件在事件期间和以后必须执行的具体功能。注意某些威胁情景也许有这样一些大的受影响区或足印，其中针对足印内重大损坏可能性进行的全面厂址简单筛选可能限制要评价构筑物、系统与部件的数目。在威胁情景足印内的那些构筑物、系统与部件可以合理假定为失效，而它们的更多细节考虑得不到保证。
- (h) 评价构筑物、系统与部件当处于规定极端环境载荷状态时的能力。
- (i) 规定电厂能力衡量标准，例如当处于找出的威胁情景中时的高置信度低失效概率值。把电厂高置信度低失效概率值与接受标准进行比较。

3.6.3. 识别成功路径

破坏裕度评定的基本目标是规定一个或多个成功路径，可以证明当处于威胁情景中时它们有恰当的裕度执行所要求的功能。在成功路径上的构筑物、系统与部件按设计或经过修改有能力承受要求的环境，具体地说是防止敌手的破坏。一般说来，可能存在几个可能的成功路径。破坏裕度评定方案是要选出当受到极端载荷时最容易证明具有适当裕度或能力的成功路径。此外，成功路径应该考虑到电厂运行人员培训和规定的程序，虽然承认对于某些威胁情景电厂的损坏可以如此广泛以至于现有电厂培训和程序也许不适用或不适当。重要的是成功路径的选择考虑对实物保护系统的

要求。对要害区的现有定义可以给予考虑，也可以重新定义要害区以包括成功路径的构筑物、系统与部件。在这两种情况下，要害区的数目和位置对于保护目的应该是有效的。

所选择的成功路径将取决于“成功”是如何定义的。根据性能标准，“成功”可以仅指安全停堆和余热排除；这通常被称作“安全停堆路径”。性能标准既规定了成功的含义（只有安全停堆或有补充要求），也规定了所需要的成功路径数目。

多层次方案可以用来规定成功路径和构筑物、系统与部件性能的接受标准。例如，第一个层次将适用于非灾难性的威胁情景，在这种场合评价标准可以类似于设计基准考虑——也就是说，设计水平的全部系统冗余性（遵守单一失效标准和冗余路径）和构筑物、系统与部件性能行为限值。两个这种威胁的例子是轻型飞机对场区的撞击和汽车炸弹离电厂一定距离处爆炸。在这些情况中，进行检查后重新启动设施是可行的。根据国家实践，设计基准威胁可能包括也可能不包括此类事件。

第二个层次将适用于可能需要证明只有单一安全停堆路径（即控制反应堆的手段、冷却燃料和包容放射性物质释放）场合下的事件；这一类的例子包括民用飞机和商业飞机的撞击。在这种情况下，考虑到部件的极限能力，构筑物和系统接受标准可以明显放松。

第三个层次将适用于可能是灾难性的非常大的事件，例如场区内受到大型飞机或多个飞射物的撞击。在这些情况中，响应可能包括场内和场外的应急措施。在所有的这类情况中，必须确保停堆，尽管冷却核燃料和包容放射性物质释放的工程手段的重大破坏可能是被允许的。在这些情况中，预期重新启动设施是不可能的。

这些情况中的每一个都导致一个或多个不同的安全停堆路径。对于一个不太严重的事件，安全停堆路径可能包括对于灾难性事件的安全停堆路径的部分或全部。每个安全停堆路径或成功路径包括一个电厂系统的子集，其中有安全系统、支持系统、安全壳及其他构筑物以及营运者行动，这个子集的可操作性和生存能力足以使设施安全停堆并且在规定期间保持它处于安全停堆状态。成功路径是系集，并且一般来说不包括所有安全系统。成功路径应该与电厂运行相容。

正如在第 3.6.2 节中提到的，对于系统和构筑物、系统与部件的接受标准必须由负责任的机构确定。为本出版物的目的，安全停堆路径的数目是非实质性的。讨论的重点是安全停堆设备清单，它是依系统性能标准组合起来的（见第 3.6.4 节）。

对于核电厂来说，构成安全停堆路径的构筑物、系统与部件当处于考虑中的一个或多个威胁情景中时应该执行四项功能，即：

- (a) 反应堆反应性控制；
- (b) 反应堆冷却剂压力控制；
- (c) 反应堆冷却剂存量控制；
- (d) 衰变热排除。

如果在评定过程中这些功能的一项或多项不能表明性能成功，就应该考虑恢复和保持安全壳完整性以及降低放射性释放的手段。

安全停堆路径的文档记录一般来说包括一个系统清单（一线系统和支持系统），并逐项详列它们的功能、设计和依赖关系。经常创建两个依赖性表格，记录一线系统对支持系统的直接依赖性和支持系统之间的依赖性。

安全停堆路径识别过程产生：

- (a) 安全停堆路径的识别及其选择的正当性；
- (b) 组成安全停堆路径的一线系统和支持系统清单及其特征；
- (c) 列出一线系统和支持系统之间直接依赖性以及支持系统之间依赖性的依赖性表格。

3.6.4. 安全停堆设备清单

找出安全停堆路径上的构筑物、系统与部件并列于安全停堆设备清单。安全停堆设备清单数据库应该包括构筑物、系统与部件的名称、部件类型、制造商、设计条件、功能、在要害区内的实际位置、新定义或扩展的威胁要求环境和物理载荷状态（直接或间接的撞击效应；直接或间接的冲击波效应；受热的火灾载荷；振动；窒息对可操作性的影响，包括火灾的烟雾影响；以及内部或外部水源造成的水淹）。这个数据库总结了安全停堆设备

清单中每个物项针对考虑中的要求环境的评价。为安全停堆设备清单中的每一物项确定其表 6 给出的极端环境载荷及其支持资料。预计一座商用核电厂安全停堆设备清单将包含几百个构筑物、系统与部件；其他类型设施安全停堆设备清单中的物项也许会明显减少。

附录二中的表 8 列出了一种可以接受的数据库格式。以表格形式给出的合成安全停堆设备清单提供了用作评价安全停堆设备清单中构筑物、系统与部件的指导、指示、路线图和供小组审查的最初文档。构筑物、系统与部件能力评价既在办公室中一般来说利用分析技术和资料进行，也在电厂现场访查期间在电厂中进行（见附录二关于电厂现场访查的详细说明）。

3.6.5. 安全停堆设备清单和要害区

列于安全停堆设备清单中的设备和构筑物是那些必须发挥核电厂安全停堆并保持安全停堆状态功能的物项。因此，这些物项应该位于要害区，也就是说，设施内由实物保护系统加以保护的区域。如果在一个有有效实物保护系统的运行电厂中进行评价，预计大多数安全停堆设备清单物项将位于以前确定的要害区。然而，安全停堆路径识别过程的一种结果是重新指定要害区。如果评定中考虑设计基准威胁外威胁事件，可能需要增加一些以前没有指定为要害区的区域（即在设计基准威胁假设下没有加以保护）；同样，以前指定为要害区的也可能不再需要定义为要害区。

3.6.6. 构筑物、系统与部件的能力评价

安全停堆路径一旦确定，所需要的构筑物、系统与部件便进入供评价的安全停堆设备清单。对于安全停堆设备清单中的每个构筑物和部件，规定了实现系统性能成功的功能要求。表 6 和支持资料描述了与威胁情景有关的安全停堆设备清单部件的载荷环境或要求环境。这些载荷或要求是实际的，例如撞击力、受热、湿度、冲击波压力、振动和窒息气体。有待确定、评价和证实的失效模式与这些载荷直接有关。构筑物、系统与部件的能力或易损性评价在很大程度上依赖于进行评价的工程安全人员的专门技术和经验的结合。

在评价能力时，可能需要相当大的灵活性。基于经验的工程判断与实验数据和分析结合在一起，以便得到一个给定成功路径上的构筑物、系统与部件的能力。对于“处理 1”类别中的物项（见附录二中的第 II.5.2 节），

现有数据可能需要用实验数据补充。要求有谨慎的文件记录，确保成功路径上的全部物项和营运者行动得到彻底的评价，满足考虑中威胁情景的环境条件。

也可能要进行能力评价，以便确定安全停堆设备清单中的部件处于威胁情景中的高置信度低失效概率状态。对于一个给定成功路径，成功路径的高置信度低失效概率被假定为路径上最低的高置信度低失效概率部件。这是一个适用于评价目的的电厂高置信度低失效概率的保守估计。高置信度低失效概率的概率定义是小于大约 5% 概率的失效而置信度为 95%。拟定代表安全停堆设备清单物项能力的高置信度低失效概率在文献中有充分说明，并且在针对超设计基准地震事件中评价核电厂时得到广泛地使用[2]。

高置信度低失效概率可以利用概率论技术或者确定论技术进行估计。对于概率论方法，极端的环境要求是以威胁情景的发生为条件的。要求可以由分析或实验数据产生。例如，对于一起喷气飞机燃料火灾，环境要求是热载荷掠过受影响厂区在时间和空间上的分布。这些分布包括不确定性估计——或者是独立的偶然和认知不确定性，或者是复合的不确定性。在全概率方法中，易损性功能同样是用概率方法找出和描述的。因此，对于喷气飞机燃料火灾的例子，构筑物或具体构造单元的破坏可以关联到施加的热载荷及其持续时间。这些易损性功能包括不确定性估计。对于概率安全评定方法，易损性功能（用概率方法描述）是在事件树/失效树中为所有基本事件找出的。对于概率论方法，高置信度低失效概率值和极端环境要求功能是通过概率方法与易损功能结合在一起的，而高置信度低失效概率值是以威胁情景的发生为条件的。

另一个更普通的方案是用确定论方法估计高置信度低失效概率值。以威胁情景的发生为条件的环境载荷条件的确定性估计，是以一种具体的非超越概率为目标计算的，例如 84% 或大约为中值加上一个标准偏差。确定了易损性数值的确定性估计，再次以一个具体的非超越概率为目标。然后把这两个标量值进行比较。如果环境要求不超过易损值，那么高置信度低失效概率值至少与环境要求一样高，或者至少与威胁情景参数一样高。对于喷气飞机燃料火灾的例子，如果热载荷小于因所考虑的安全停堆设备清单物项的热载荷造成的失效估计，那么安全停堆设备清单物项就有至少与威胁情景参数一样高的高置信度低失效概率值（例如对于波音 767 飞机对

厂址的撞击，是表 1 和表 4 中定义参数)。对所有安全停堆设备清单物项进行评定，提供了一个由对于给定威胁情景的电厂高置信度低失效概率组成的估计。

优先采用确定性方法，因为就像构筑物、系统与部件的抗震评价一样，规则一旦确定，没有经过概率方法培训的工程师们就可以进行这种评价。以不同的方式处理恐怖袭击的规则需要另外制订，利用超设计基准评价特别是超设计基准地震评价的指导原则可以方便地做到这一点。

关于以不同方式进行的极端事件工程评价的指导原则可以在大量国际原子能机构出版物及其他出版物中找到。特别是参考文献[3]解决了例如飞机撞击、外部火灾、爆炸、危险物品和水淹诸多危害。它也提供了关于技术评价方法的一系列参考文献，并且对于爆炸危险引进高置信度低失效概率概念。国际原子能机构的其他出版物详述一般来说是意外发生的、工程评价方法适用的不同危害。

构筑物、系统与部件能力评价的步骤包括：

- (a) 熟悉电厂，其中许多方面是在决定安全停堆路径、产生安全停堆设备清单和确定安全停堆设备清单部件载荷环境期间完成的。另外熟悉所关心的构筑物、系统与部件因电厂而异的文献也在这一阶段进行。
- (b) 在办公室内和在厂内对安全停堆设备清单物项的评价。厂内评价指的是在第 3.6.8 节和附录二中讨论的现场访查。在办公室内评价指的是综合分析具体安全停堆设备清单物项的设计资料和鉴定资料。应该根据需要进行计算，以确定载荷环境和这些物项的失效或能力。
- (c) 在电厂现场访查期间证实在所有评价阶段所作的假设。
- (d) 文档编制。
- (e) 产生安全停堆设备清单，以及对于在评价中考虑的所有环境载荷条件作出高置信度低失效概率估计。

3.6.7. 破坏裕度评定小组的组成

破坏裕度评定小组包括：

- (a) 对电厂系统、安保、运行和工程非常熟悉的电厂专家，他们负责把威胁情景（2 型威胁事件）转变成电厂不同区域内的具体极端载荷条件（见第 3.3 和 3.4 节）。这项活动应该严守秘密，把产生的极端载荷条件传送给相关的专家进行评价。
- (b) 安保（实物保护系统）专家，再补充以电厂运行和场内应急管理专家。评定小组的这个方面在这里不予讨论，尽管在附录二中有个简短说明。
- (c) 工程安全评定、系统设计、工程（土木工程、结构、火灾、电气、机械、仪器仪表和控制）以及电厂运行方面的专家。评定小组的这个方面是本出版物的重点，有关活动最后考虑有关的极端载荷条件筛选出某些构筑物、系统与部件，而针对这些条件确定构筑物、系统与部件需要作更详细的分析。

其他例如飞射物、飞机或爆破方面的专家在评价中是有帮助的。

需要备好程序以便尽量减少秘密信息的暴露，特别是负责评价构筑物、系统与部件处于具体的环境载荷条件下能力的专家。一个目标是保持威胁信息和电厂状态信息分离，尤其是当把环境载荷条件通知有关专家时——他们不需要知道威胁细节。这是被破坏裕度评定方法接受的。

3.6.8. 电厂现场访查

附录二详细描述了电厂现场访查。电厂现场访查的主要目标是审查已经进行的筛选，确定新的概念和审查已经提出的容易采纳的概念，审查已经找出的成功路径和安全停堆设备清单中的构筑物、系统与部件，用设计资料核查建成状态或现实状态，把类似的构筑物、系统与部件及其要求环境分组，审查要害区定义和边界，以及把现场访查的结果整理成文件（见第 II.2 节）。

4. 决策方法学

第 3 节提出评价核电厂工程方面承受恶意攻击能力的方法。更具体地说，所描述的方法为决策者提供了在成功路径上必须加以保护和对于列入设计基准威胁或设计基准威胁外威胁情景具有定量能力的关键构筑物、系统与部件的清单。这些情景可以是 1 型威胁事件，也可以是 2 型威胁事件。

找出的易损性或具有不能接受的低能力的物项，其处理情况应该通过找出尽可能多的实际方法来成功缓解不利的后果。问题的评定和解决应该考虑纵深防御以及场内所有可得到的安全和安保方案；也应该找出场外的可利用资源，例如那些用于应急准备和消防的资源（例如灭火材料、泵、电缆、电源、重型起重设备及可用于缓解各种威胁损坏结果的其他设备）。此外，在决定适当的行动时应该考虑政府的所有其他安保程序。

决策过程示于图 1，并在附录一中有详细说明。确定危机管理是评价过程中的一项任务；其中包括事故缓解，同时考虑安全壳性能及其他缓解措施。

为了实现可以接受的有关恶意行动的总风险，其路线图中有四个主要决策点（细节见附录一，其中也涉及升级决策）。对于找出的易损性，电厂管理部门有若干方案，例如加强实物保护系统，提升电厂危机管理能力，为改进布局作准备和对构筑物、系统与部件作工程变更。

在决策过程中必须考虑到的一系列因素列于表 7。

有些威胁情景基于电厂资源的保护（例如工程升级和加强实物保护）是有问题的，可能必需与国家主管部门讨论如何应对这些威胁情景。国家主管部门可能决定实施其他的场外预防或响应措施。

表 7. 决策者相关事项

决策步骤	评 价 结 果
是 所 评 定 的 易 损 性 的 严 重 性	破坏奏效，而缓解系统，如果有的话，没有提供所希望的对放射性释放的防护水平。 破坏失败，但是剩余的安全裕度小到不能接受或不确定。 安保系统瓦解，而没有防止破坏行为。
电厂方案	实物保护升级：旨在防止要害区中（或在成功路径上）物项受到挑战的行动和改进。 安全系统升级：包括冗余性、多样性和分隔措施。 结构加强：目标是万一发生因恶意行为造成的极端载荷一个给定物项得以幸存的努力。 营运者行动：如果在恶意行为或破坏事件以前有一些警告时间，停堆或其他的行动可能是适当的；如果没有警告时间，营运者在袭击期间或以后的行动在事件诊断和响应方面可能是重要的，如果这一工作不是自动进行的。
优化	关于分配升级和变更所需要的资源的决策，基于在防止破坏行动或者消除其引发放射性物质释放可能方面估计的能力改进。 具体地说，决策基于： (a) 估计的“性能”改进（例如冗余度改进）； (b) 实行的难易； (c) 完成升级时间（例如停机）； (d) 处于危险之中的时间。
现 有 严 重 事 故 管 理 能 力 的 利 用	设施也许有缓解特性（例如事故管理程序），原来打算用来尽量减少超过适用设计基准的事故后果，因此有可能性缓解得逞破坏的放射性放射性后果。它们可能需要得到加强，以便在可能包括部分或完全丧失主控制室、替代停堆盘、技术支持中心和/或操作人员的条件下更圆满解决指挥与控制问题和应急计划执行。这些能力需要以其他的干预措施（例如响应部队、消防队）加以补充。
场 外 特 性 和 能 力	利用实体屏障、隔离区和由警察监视核设施的出入道路可以降低袭击的可能性和严重性（例如对于车辆炸弹的基准距离）。

5. 结论意见

本出版物中的导则基于这样一个前提，即结合到现有核设施中的设计、布局和安全基础结构可能在相当大程度上有利于缓解恶意行动的影响。然而，这一好处不能一成不变地应用于所有威胁和所有需要的安全功能。

在这些导则中描述的评价过程，连同所提出的核设施运行、核安全工程和实物保护专家的互动模型，为电厂管理部门及其他利益相关方提供了关于升级或实施其他的手段降低公众危险的决策所需要的牢固性和易损性信息。

这些导则被设计成面对 21 世纪破坏行动的新现实，能在管理其核设施的风险和抵御对核设施可能的威胁方面得益于各种国际监管体制。

附录一

实物保护流程图描述

本出版物第 2 节中的图 1 给出了一个流程图，表明所有有关单位在万一发生恶意袭击时如何共同保护核电厂。本附录提供图 1 中各方框和决策点的详细说明。

方框 1

威胁评定在这里定义为一种分析，其中记录了涉及核设施或核材料在其利用、储存或运输期间可能引起不希望后果的潜在敌手的可信动机、意图和能力。威胁评定过程的结果描述了可信的威胁。

方框 2

后果在这里定义为对公众、国家、关键利益集团和国际社会利益的潜在影响水平。后果可以就潜在的放射性物质释放水平和潜在的辐射照射水平加以定义。对这些后果的关注将影响关于制订设计基准威胁的决策过程。

菱形框 3

对于一个给定的威胁环境和核电厂失效的潜在后果，需要考虑不同类型的威胁情景。根据成员国的实践，这些威胁可能属于设计基准威胁，也可被认为是设计基准威胁外威胁。根据这些威胁影响核电厂的方式，它们可以被分为 1 型威胁或 2 型威胁。1 型威胁事件涉及敌手入侵到保护区内，而 2 型威胁类涉及远距离的攻击。在这一点上，必须决定哪种威胁情景应该列入潜在威胁清单和各个威胁情景属于哪一类（1 型威胁或 2 型威胁）。

方框 4

2 型威胁描述远距离的威胁情景。

方框 5

1 型威胁描述涉及敌手入侵或打算入侵保护区的威胁情景。

方框 6

针对破坏的实物保护需要硬件（安保装置）、程序（包括组织警卫和履行他们的职责）和设施设计（包括布局）的结合。在这里，设施设计指的是电厂布置有利于探知过程、延迟、响应、恢复和/或构筑物、系统与部件对极端载荷的牢固性等方面，以及应付严重事故的设计措施。

方框 6a

要害区位于“保护区内拥有设备、系统或装置，或者核材料的区域，如遭破坏可能直接或间接导致不可接受的放射性后果”[1]。在指定这种区域时，应该考虑电厂安全设计、电厂的位置和设计基准威胁。要害区识别所用的方法取决于设施的复杂性、可利用的安全文档（安全分析报告、概率安全评定，等等）和为此目的组织的现场访查。

方框 6b

实物保护系统应该设计成能探知和延迟列入设计基准威胁的恶意行为并给予适当的响应。一般来说，这些主要功能是由实物保护措施例如探知和出入控制系统、屏障和响应部队提供的。一项包括现有安全措施评价和考虑系统空间分离和冗余性的设施设计分析，提供了适当实物保护措施的设计基础。为了设计适当的响应，营运者有关恢复停用系统的即时场内行动需要加以考虑。

方框 6c

如果设计基准威胁包括对电厂构筑物、系统与部件产生极端载荷的恶意行为，需要进行这些构筑物、系统与部件的能力评价。在这一评价中用的接受标准应该由主管部门确定。

方框 6d

堆芯损坏后危机管理涉及电厂缓解后果的行动。这种行动应该考虑敌手继续留在场址阻碍或瓦解缓解行动的可能性。

方框 7

要求应急响应缓解通过失去指定安全系统导致或有可能导致失去核过

程控制的恶意行为的场外放射性后果。它包括由国家机构为了应付这种局面进行的所有行动（与营运组织合作），包括为了对抗旨在中断和瓦解应急响应的恶意行为采取的具体措施。

方框 8

实物保护的责任在于国家，而国家也应该确保实施核材料和设施实物保护的主要责任在于有关许可证的持有者。设计基准威胁被主管部门用于评价实物保护措施，而被营运者用于规划和设计这些措施。

方框 9

国家主管部门或机构的响应可能包括对袭击设施的主动响应。响应也包括国家应急组织的行动。

方框 10

国家安保包括确认一个可信威胁为设计基准威胁外威胁的措施。这些措施应该连同应急响应能力一起考虑以便使其余的风险保持在可接受的程度。措施的范围可能包括情报、空中交通安保和军事防御。

方框 11

当一种不属于设计基准威胁的可信威胁变成实际关注的主题，而国家的实物保护系统在短期内又不能实施时，要进行极端载荷评价。设施能力的重新评价需要利用现实的（即不太保守的）裕度进行。评价可能产生关于继续运行可行性的决策。考虑到事件超过设计基准威胁和极端载荷评价的结果，主管部门可以决定把这些事件包括在实物保护评价过程中（可能使用不同的和不太保守的接受标准）和/或部分承担保护责任。

方框 12

在这里术语风险指的是一种将能造成不希望后果的可能性。风险可以降低，但是不能消除。所有的判断和决策都意味着接受一定程度的风险。没有任何恶意行为数据库可用来进行作为成功袭击的概率（基于统计资料）与造成后果乘积的风险计算。然而，一些国家已经选择估计条件风险，也就是说如果袭击发生造成不希望后果的风险。

菱形框 13

产生了 2 型威胁事件清单和对这些极端载荷进行了某种评价以后，需要针对具体的威胁情景作出关于分担保护核电厂和对这种袭击作出响应责任的决策。特别是，保护措施可以在电厂管理部门与地方和/或国家主管部门之间分担。指向左边的箭头表示那部分责任是指望电厂管理部门承担的。

菱形框 14

在这一点上，需要确定该实物保护系统在与专设安全系统（构筑物、系统与部件）结合的情况下是否有能力保护核电厂抵御 1 型威胁事件和电厂管理部门负有责任的那部分 2 型威胁事件。如果要有能力，就需要考虑其他纵深防御层（特别是危机管理，它主要是电厂管理部门的责任）。另外，在升级实行以后应该重新评价实物保护系统和构筑物、系统与部件的能力。

菱形框 15

在这个最后的决策点，国家必须确定，在实施了所有可用到的纵深防御层以后，具体威胁的风险是否已经降低到可接受的程度。在这一决策中，考虑了由电厂和国家主管部门（包括安保和响应机构）所起的作用。

附录二

电厂现场访查

II.1. 评定导则：概述

本出版物是为了帮助处于设计基准威胁事件和设计基准威胁外威胁事件中的核设施能力评价而编写的。本出版物的重点放在工程安全方面。关于实物保护系统方面，具体地说响应入侵者威胁，在别处解决。然而厂内评价或电厂现场访查的概念包括在这里。

评定过程包括以下步骤：

- (1) 威胁评价：包括威胁评定、后果标准和决策过程。威胁评价是对以前定义的和新定义的威胁的完全认定和评价，然后将其分类以便纳入电厂评价。防范设计基准威胁和设计基准威胁外威胁的工程安全是这些导则的主题。
- (2) 设计基准威胁外威胁的详细说明：这项任务是评价设计基准威胁外威胁对评定中核设施的适用性，产生一个用于评价的威胁情景清单。在这个评定阶段可以进行其他筛选。
- (3) 极端环境载荷评价：这一阶段用作在威胁情景和电厂工程机构为评价给出的载荷环境的定义之间的接口。由威胁情景产生的环境条件矩阵可以被用于部分设施或整个设施。产生的环境荷载矩阵（见表 6）及其支持资料定义了工程安全载荷环境。
- (4) 破坏裕度评定。本报告中提出的方法学被称作破坏裕度评定（SMA）程序。采用适当的假设和接受标准，它同样适用于设计基准威胁和设计基准威胁外威胁的工程安全问题。破坏裕度评定是基于：
 - (i) 在极端环境定义矩阵中的输入资料（表 6 和支持资料）。
 - (ii) 处于极端载荷环境中的核设施的综合性能标准。例如，对于一座处于设计基准威胁外威胁中的核反应堆，综合性能标准可以规定为威胁情景开始以后 24 小时的热停堆或冷停堆。另

外一个假设是在 24 小时内可以从电厂边界外面有效地动员其他的帮助。由成员国确定性能标准，包括从电厂边界外面能够有效地动员其他的帮助以前的停堆持续时间。

- (iii) 据以进行设计基准威胁或设计基准威胁外威胁工程评价的假设，例如丧失场外电源、设施的运行状态（全部或部分运行）、系统标准（冗余性）和构筑物、系统与部件能力标准（法规或放宽）。
- (iv) 一种或多种安全停堆或成功路径的定义。
- (v) 在上述假设下，在安全停堆路径上并要求在威胁情景期间和以后发挥功能的构筑物、系统与部件的确认，以及这些构筑物、系统与部件在事件期间和以后必须执行的特定功能的定义。在安全停堆设备清单中详细列举了这些构筑物、系统与部件（见表 8 一种可以接受的安全停堆设备清单格式）。
- (vi) 构筑物、系统与部件（安全停堆设备清单中的物项）当处于规定的极端环境载荷条件下时能力的评价。对于破坏裕度评定，能力的度量处于确定的威胁情景中的高置信度低失效概率。这一阶段要求进行办公室内和厂内的评价；后者构成电厂现场访查，而这正是本附录的主题。
- (vii) 电厂能力大小的确定，例如处于确定威胁情景中的高置信度低失效概率。电厂高置信度低失效概率可与接受标准相比。

II.2. 电厂现场访查的目的

电厂现场访查的主要目的是：

- (a) 审查过程初期或评价阶段本身进行的筛选以证实其适当性；
- (b) 确定新的概念和审查已提出的易被采纳的概念，确认它们的有效性和证实它们适用的威胁情景（或要求环境）可能被有效地化解；
- (c) 审查确定的成功路径和安全停堆设备清单中的构筑物、系统与部件，确认构筑物、系统与部件在袭击期间和以后所要求的功能，确认对于每个威胁情景构筑物、系统与部件所处的要求环境，确

定或确认所关注的与威胁有关的失效模式，以及确定可以从进一步考虑中排除的牢固的构筑物、系统与部件；

- (d) 以设计资料证实建成状态或当前状态，包括电厂系统、工程和实物保护系统；
- (e) 把类似的构筑物、系统与部件及其要求环境分类供电厂现场访查以后进一步分析；
- (f) 审查要害区定义及其边界以评价它们对安全停堆设备清单的适用性和规定典型布局供进一步评价；
- (g) 把现场访查结果整理成文件。

II.3. 敏感信息安保

含有实物保护信息的所有有关信息和文档，不管是逐条地还是为了评定核设施实物保护的工程安全问题而汇编在一起的，都被认为是安保敏感信息，要加以适当保护。现场访查小组和支持人员（例如行政支持人员）应该由经过适当审查得到信任的专家组成，并且已对这些人进行过背景检查。

II.4. 电厂现场访查小组

电厂现场访查小组由营运者的工作人员、具有特定专门技术的顾问和可能的话还有监管人员组成。其任务和责任如下：

- (a) 组长：组长指导现场活动、工程评价和执行安保要求。因为这件工作的敏感性质，活动需要以一种集中和妥善的方式进行以确保对所有有关信息的控制。组长必须可靠（最好是营运者的一名雇员），具有指导这些活动以及确保过程安全和完整必需的权威、指导技能、适当的工程背景和对密级信息管理的彻底了解。组长根据需要可以与国家主管部门互动，以便规定或阐明待评价威胁情景的要素。
- (b) 工程安全专家：工程安全专家（营运者工作人员中的专家和必要时具有特定专门技术的顾问）组成现场访查小组，重点是工程安

全方面。应该代表的工程学科是系统、土木工程、结构、机械、电气以及仪器仪表和控制。为确保完整性，在每次评价中要考虑到所有的工程学科。所有的工程安全专家必须由营运者或其他相关的机构（例如监管机构）判断是可靠的，并且必须经过正确的审查和培训以保持过程的安全和完整。

- (c) 电厂运行人员：电厂运行人员是小组必不可少的组成人员，在整个电厂现场访查活动中他们的专门技术应该都可利用。

本出版物的重点是工程安全。属于实物保护系统人员责任的设计基准威胁和设计基准威胁外威胁问题，可以单独评价，也可以和工程安全方面一起评价。当和工程安全问题一起评价时，可以组织一个包括实物保护专家在内的综合小组。如果设计基准威胁或设计基准威胁外威胁包括具有综合威胁的多模式袭击，组成这样一个小组尤其可取。

小组成员，包括组长，只要需要就应该指定他们参加现场访查工作，尽量不担任兼职。

II.5. 电厂现场访查程序

电厂现场访查程序包括现场访查准备以及现场访查的初步筛选和详述筛选。电厂现场访查活动和控制受益于独立的安保工作地点，这种工作地点确保了工作和有关文档的安全和完整。

II.5.1. 现场访查准备

- (a) 熟悉电厂：
 - (i) 应该把电厂的全面文档汇编在一起，包括安全分析报告、系统描述、管道和仪器仪表设备图（P&ID）、电气单线图、操作程序、电厂总布置图、电厂机电设备位置图、对内外事件的概率风险评定以及设计基准威胁外威胁评定以外的任何其他评定；
 - (ii) 应该把有限制使用的实物保护系统信息汇编在一起，特别是那些指定要害区中的安全停堆设备清单物项的信息；

- (iii) 电厂出入要求应该得到满足，包括辐射防护、安全实践和安保实践（需要遵守“合理可行尽量低”原则）。
- (b) 应该磋商或建立关于安全停堆路径和安全停堆设备清单中构筑物、系统与部件的电厂文件，并且应该规定对安全停堆设备清单中每个项目的环境要求，包括实体要求和安保要求。
- (c) 应该筹建一个安全停堆设备清单数据库，用以概括每个安全停堆设备清单物项针对要求环境的评价。预计一座商用核电厂的安全停堆设备清单将包括几百个物项。其他设施类型的安全停堆设备清单物项也许数目要少得多。
- (d) 应该编制各个构筑物、系统与部件数据表，其中包含上述某些信息。资料应该用现场和办公室产生的构筑物、系统与部件特定评价结果作补充，包括：现场记录；所进行的安全、安保和工程分析；以及现场修改。
- (e) 应该制订一个厂内现场访查计划，表明小组的数目和每个小组的组成。预计将需用一个以上小组，总数取决于所考虑的问题、需要的专家和保密要求。

表 8 说明一种可以用于安全停堆设备清单数据库的格式。表 8 各列如下：

- 安全停堆设备清单编号是构筑物、系统与部件一个唯一的数字标识符，可能包含位置、系统或其他信息。
- 构筑物、系统与部件名称包含关于构筑物、系统与部件的描述性资料（例如附属建筑，柴油发电机 1A，等等）。
- 构筑物、系统与部件标识编号是电厂特有的标识符。
- 描述是简要地描述构筑物、系统与部件。
- 威胁情景编号是与待评价威胁情景总清单有关系的一个标识符。
- 位置指的是为了帮助安排厂内现场访查和评价威胁后果的一系列位置标识符。它可能包括用于实物保护系统评价的要害区标识符。
- 物理载荷状态是要考虑的载荷状态类型的标识符，它提供了关于所需要的专家和厂内现场访查接触以及关于待评价联合载荷状态（例如撞击加上火灾）的指导。

- 撞击指的是在评价中要考虑的直接和间接撞击效应。直接撞击效应是例如飞射物直接撞击的状况；间接撞击效应是例如混凝土的碎块和振动引发的载荷。
- 要考虑的爆炸/冲击波效应可以是直接的或是间接的。直接效应是冲击波压力；间接冲击波效应是例如振动引发的载荷状态。
- 受热/火灾指的是由火灾受热或火焰对构筑物、系统与部件的直接影响。
- 窒息和相关状况可能起源于烟雾、有毒化学品或消防技术的结果。这种破坏方式可能影响人员或系统；例如柴油发电机的进气系统被淹堵可能发生柴油发电机系统的窒息。控制室的可居住性和场区内安保人员的安全应该加以评价。
- 对来自内部或外部的水淹可能需要进行评价。

表 9 提供了在构筑物、系统与部件评价中针对物理载荷条件的各物项数据表的样本格式。在现场访查前期阶段，将确认考虑中的构筑物、系统与部件的基本信息填入表格内，表格的其余部分在完成现场访查和评价时再填写。这样评价的文档就包括那些摘要和详述的评价。表 9 以构筑物、系统与部件针对抗震及其他外部事件评价所用的数据表为基础。对于抗震评价案例，22 类设备中的每一类使用唯一的数据表。每一类有需要评价的特有的设备性能和状态以证实其抗震性能。这些数据表称作“筛选评价工作单”(SEWS)，用于创制当前评价的类似工作表的基础。要收集和评价的资料可能需要修改以考虑非振动破坏模式，也就是说，例如受热、湿度和直接撞击的环境条件。

II.5.2. 初步筛选现场访查

初步筛选现场访查应该实现以下目标：

- (a) 确定电厂每个安全停堆设备清单物项的位置和可接近性；
- (b) 确认其他任何安全停堆需要的构筑物、系统与部件，将其添加到安全停堆设备清单中；
- (c) 以能力考虑审查和确证构筑物、系统与部件的筛选；

表 9. 用于物理载荷状况的筛选评价工作单例子

构筑物、系统与部件名称： _____ 构筑物、系统与部件标识编号： __

构筑物、系统与部件描述： _____

位置： 建筑物 _____ 标高 _____ 房间/区/排/列 _____

威胁情景编号/描述： _____

要害区确认： _____

性能要求： _____

摘要（能力对要求）

撞击载荷：

 直接： _____

 间接： _____

冲击波载荷：

 直接： _____

 间接： _____

受热/火灾载荷：

 受热： _____

 火灾： _____

表 9. 用于物理载荷状况的筛选评价工作单例子（续）

窒息：

烟雾：

有毒化学品：

其他：

水淹：

内部：

外部：

其他：

说明：

[有关评价的摘要注释]

附件：

现场访查注释

相互影响的危害评价

— 空间的相互影响：落下、接近，等等

— 喷淋/水淹相互影响

构筑物、系统与部件的照片和关键评价要素

计算、支持资料，等等

特别部件评价工作单，当可用和适当时

- (d) 确认可能的便利补救方法；
- (e) 给位于较大设备物项内或较大设备物项上的所有的部件分类；
- (f) 给相同位置内的部件分类，尤其是同一个要害区内的，用于评价空间共同环境；
- (g) 针对规定威胁评价构筑物、系统与部件的能力是否适用；
- (h) 文件结论。

初步筛选现场访查目视检查了那些可接近的构筑物、系统与部件。对于每个安全停堆设备清单物项有三个可供选择的类别处理：

- (i) 处理 1：对于这一类构筑物、系统与部件，能力显然低于要求，需要改进。
- (ii) 处理 2：这一类物项的能力不确定，需要进一步评价确定是否需要改进。
- (iii) 处理 3：对于这一类物项，能力显然高于要求，构筑物、系统与部件适合于规定的威胁。

初步筛选现场访查应该正确地形成文件。初步现场访查的主要结果是确定显然牢固的安全停堆设备清单物项。那些被定为处理 3 类构筑物、系统与部件，因此无需进一步评价。处理 1 类和处理 2 类的物项需要更详细的办公室内和厂内评价。

II.5.3. 详细筛选现场访查

对于所有构筑物、系统与部件，只要它在规定环境载荷情景中的能力没有得到证实，就要进行详细筛选现场访查。其中包括厂内评价，并且许多情况下要进一步分析计算和评价，结果分成了两类构筑物、系统与部件：

- (a) 第一类构筑物、系统与部件是那些在初步现场访查期间从进一步考虑中排除的。在这个阶段，现场访查工程师更详细地评价这些系统和部件，作出部件是否需要进一步分析或修改的判断。
- (b) 第二类构筑物、系统与部件，电厂改进显然是有正当理由的。在这些情况下，现场访查工程师建议要实行的改进。

详细筛选现场访查应该正确地形成文件。最好用摄影和/或视频记录补充文档。表 8 是整个安全停堆设备清单摘要文档的验收表格。利用表 9 给出的表格，加上随附的支持资料，可以把构筑物、系统与部件的评价形成文件。

文档应该严格地保密，只分发到有必要知道的人。

II.6. 特殊课题

场址上并存设施的类型和数目

一座核电厂场址内也许有几台反应堆机组，可能有相互关联的安全或支持系统；多机组场址常常假定当对付非共因事件时其他机组系统可供利用。此外，其他的关键设施也许位于电厂边界内，例如燃料水池乏燃料储存或干式重屏蔽容器储存。研究用反应堆场址也许有相关的实验室、同位素生产设施和热室。当遭遇到设计基准威胁外威胁时所有并存设施可能需要同时进行实物保护。评价应该考虑到场区内所有设施，以及其安全系统的任何相互关联。这种考虑包括环境排放的后果评定，这种排放对于场址上的所有设施是累计的。

相互影响

电厂现场访查是一种确定在特定威胁中可能影响安全停堆设备清单物项性能并使这一种设备不能运行的空间相互影响的关键手段。在这些区域中的主要关注是“清理家务”。潜在相互影响的识别和评定需要现场访查小组的准确判断。

落物

落物是非安全相关物项或安全相关物项的结构完整性失效，它可能击中破坏一个安全相关项目。对于这种会威胁到安全停堆设备清单物项的相互影响，撞击必须包含相当大的能量和目标必须是易损的。

例如，一个照明灯具落到 10 厘米直径的管道上可能不是对管道的一种

可信的破坏威胁。然而，相同的照明灯具落到开式继电盘上就是可能造成破坏性的相互影响，因而应该加以解决。因飞射物撞击建筑构件（墙壁、隔板或屋顶）造成的混凝土碎块在落下范围内对于精细设备可能是一种可信的破坏方式。未加固的砌筑墙是落物相互影响的一个常见来源。一般来说砌筑墙的位置很接近安全相关设备，则它们的毁坏可能导致设备损坏。

邻近

邻近相互影响定义为两个或更多物项足够靠近，即一个物项的行为对其他物项会产生后果的状态。邻近相互影响最常见的例子是火灾或爆炸；在参考文献[4]中讨论这些相互影响。

喷淋和水淹

喷淋和水淹可能是没有合适支撑或锚固的管道、系统或容器的损坏造成的结果。意外喷淋对安全停堆设备清单物项的危害经常与消防水管系统有关。最常见的喷淋水源是由撞击所引起的喷淋器高位水箱的损坏。因为火灾和受热是遍及工场厂址尤其是在建筑物和各区内的潜在威胁，现场访查应该评价所有安全停堆设备清单部件对喷淋的易损性。一般来说，火灾和灭火装置的设计评价肯定考虑了喷淋易损性。如果喷淋水源可能达到对喷水敏感的设备，那么该水源应该改装，通常通过增加支撑以降低偏转和撞击或应力。一个替代方案是保护目标 — 在这种情况下是构筑物、系统与部件。

大型罐可能是潜在的水淹源。现场访查小组应该在电厂人员的帮助下评定水淹源损坏的潜在后果和地面排水系统缓解水淹源损坏后果的能力。

参 考 文 献

- [1] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev. 4 (corr.), IAEA, Vienna (1999).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Evaluation of Existing Nuclear Power Plants, Safety Reports Series No. 28, IAEA, Vienna(2003).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).

定 义

下列定义专门应用于本报告中出现的术语，有许多不一定符合国际上在别处采用的定义。

评定 见“自评定”。

能力 构筑物、系统与部件受到可能包括实体性质、操作性质和行政性质的具体威胁时的牢固性的“绝对”量度。能力是相对于某一具体度量标准规定的。法规能力是装置设计特征符合法规的程度。抗失效能力是构筑物、系统与部件受到某种具体威胁时的牢固性的程度。

能力评价 确定构筑物、系统与部件、操作程序、实物保护系统等当受到具体威胁时的能力的过程。一个实例是确定构筑物和部件对撞击、冲击、爆炸、振动、蒸汽和/或负荷条件的抗失效能力、强度或牢固性。能力评价可以发现易损环节和系统相互作用；通常认为被评价的物项远比设计限值牢固。

设计基准威胁（DBT） 潜在的内部敌手和/或外部敌手的属性和特性，这些人可能试图擅自转移核材料或进行破坏，因此要根据这一背景来设计和评价实物保护系统（定义摘自参考文献[1]）。

高置信度低失效概率（HCLPF） 高置信度低失效概率的概率定义是小于大约 5%失效概率而置信度为 95%。高置信度低失效概率值可以用概率论技术或确定论技术估计。优先采用确定论方法，因为决定要求和能力定义的规则一经确定，即使没有经过概率论方法培训的工程技术人员也可进行评价。

裕度 预期性能对于规定标准或尺度的相对量度。它可以用确定论方法或概率论方法度量和表示。裕度的一种量度是能力和负荷条件之间的关系。例如对于一个结构元件来说，爆炸压力要求和抗失效压力能力之比（ D/C ）小于 1 就表示对失效存在着裕度。

安全裕度 机组作为一个系统当以一种安全尺度为标准进行评价和受到某种具体威胁时的预期性能的量度。中间结果包括构筑物、系统与部件当受到某种具体威胁时的预期性能，并可以定义为构筑物、系统与部件在成功路径上能力对要求的最小比值。

情景 一套设想的或假定的状态和/或事件。通常在分析或评定中用来表示要进行模化的潜在未来状态和/或事件，例如在核设施中可能的事故。一种情景可以表示在单一时间点或单一事件中的状态，也可以表示状态和/或事件（包括过程）随时间的变化。安全分析人员可使用事故情景对电厂可能事故的响应进行描述和模化。一种事故情景，通常对拟议的电厂布置设定一个始发事件，可用来模化系统响应并酌情包括不同运营者的行动。

筛选 一种旨在不再考虑对保护或安全不太重要的因素，以便集中于更重要因素的分析。一般来说，这是通过考虑非常不利的假想情景实现的。筛选是按照不同学科用各种工具进行的：

- (a) 在威胁评定中，筛选用来排除恐怖分子的某些可能行为，因为例如存在国家的其他保护策略、认识到敌手的能力水平不高、强大的保卫部队和/或发生这种事件的概率低。
- (b) 针对场址和电厂的筛选可以排除某些威胁情景，例如因为现场地点或设计的固有牢固性。

自评定 在本报告中即指“评定”，自评定是由营运组织根据需要在外部机构和顾问的帮助下进行的评价过程，以便找出和纠正那些妨碍该组织实现其安全和安保目标的安全和安保问题。自评定活动的最终结果可能包括核设施改造升级在内的风险降低策略。这被认为是外部组织进行更正式审查（例如监管审查）的第一步。

成功路径 对于一个包括安全系统、支持系统、安全壳结构和营运者行动的电厂系统子集，其可操作性和生存能力足以确保核电厂安全停堆、排除余热、根据需要包容和对于考虑中的威胁情景必要的继续控制行动的部件的最小集。

威胁评定 系统地分析与一个国家内或边境以外设施、活动或来源有关的危险的过程，其目的是找出：

- (a) 在这个国家可能需要采取保护行动的事件和相关区域；
- (b) 将有效缓解这种事件后果的行动。

术语威胁评定并不意味着任何威胁在引起损害的意图和能力意义上已经与这种设施、活动或来源联系起来。

设计基准威胁外威胁 在评定中找出的一种虽然未包括在设计基准威胁中但仍然可信的威胁。需要考虑设计基准威胁之外的威胁以确保核设施的实物保护。

威胁情景 其始发事件是一次破坏行动的情景。

1 型威胁 (TT-1) 由内部人员或由打算入侵设施实施其行动的敌手（有或者没有内部人员帮助）对核设施造成的威胁。一般说来，设施的实物保护系统被设计成能对付这类威胁。设计基准威胁考虑了多种这类威胁。

2 型威胁 (TT-2) 敌手无需出现现场而由电厂边界外部发动的攻击对核设施造成的威胁。这类威胁敌手的实例包括远距离袭击，例如肩上发射的导弹和飞机恶意撞击。设施的实物保护系统通常难以对付这类袭击，因为它不是为此目的设计的。对于很多但非全部核设施来说，2 型威胁被认为是设计基准威胁外威胁。

要害区 保护区内拥有设备、系统或装置，或核材料的区域，它若遭破坏有可能直接或间接导致不可接受的放射学后果。保护区是由实体屏障围绕的包含 I 类或 II 类核材料和/或要害区的处于监视下的一种区域。

现场访查 能使有经验的工程人员、操作人员、安保与安全人员和技术人员的小组根据彻底的现场检查和对现有文件，例如设计图、操作程序、安全分析报告和概率安全评定报告（例如 1 级、2 级、3 级、火灾概率安全评定、地震概率安全评定、停堆概率安全评定），进行审查以迅速了解设备布置和程序的技术。

参与起草和审定的人员

Asmis, G.J.K.	Consultant, Canada
Beck, D.	Sandia National Laboratories, United States of America
Contri, P.	International Atomic Energy Agency
Asmis, G.J.K.	Consultant, Canada
Ek, D.	Sandia National Laboratories, United States of America
Godoy, A.	International Atomic Energy Agency
Gürpınar, A.	International Atomic Energy Agency
Gutschmidt, W.D.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Hagemann, A.	International Atomic Energy Agency
Jalouneix, J.	Institut de radioprotection et de sûreté nucléaire, France
Johnson, J.J.	Consultant, United States of America
Kim, S.C.	International Atomic Energy Agency
Lambright, J.	Lambright Technical Associates, Inc., United States of America
Kluegel, J.U.	Kernkraftwerk Gösgen-Däniken AG, Switzerland
Kovalev, K.	MINATOM, Russian Federation
Kostarev, V.	CKTI-Vibroseism Co., Ltd, Russian Federation
Krutzik, N.	Consultant, Germany
Kwak, S.M.	Compuserve, Republic of Korea
Lojk, R.	Canadian Nuclear Safety Commission, Canada
Moses, C.	Canadian Nuclear Safety Commission,

	Canada
Murray, A.	Australian Nuclear Science and Technology Organisation, Australia
Nishida, S.	Japan Nuclear Energy Safety Organization, Japan,
Ostropikov, V.	Federal Atomic Energy Agency, Russian Federation
Park, C.K.	Korea Atomic Energy Research Institute, Republic of Korea
Skelton, S.	Office for Civil Nuclear Security, United Kingdom
Tang, W.	Beijing Institute of Nuclear Engineering, China
Tardiff, A.	Nuclear Regulatory Commission, United States of America
Yagi, T.	Nuclear Material Control Center, Japan
Wieland, B.	Consultant, Switzerland

顾问会议

奥地利，维也纳：2002 年 11 月，2003 年 9 月，
2003 年 12 月，2004 年 4 月

咨询组会议

奥地利，维也纳：2004 年 4 月，2004 年 10 月

核安保咨询组的审查

奥地利，维也纳：2004 年 4 月，2004 年 10 月

作为安全和安保专家广泛对话的成果，本出版物为评价核电厂防破坏包括远距离攻击的工程安全问题提供了指导。该指导考虑了现有构筑物、系统与部件的牢固性，并且强调防破坏的那些与防极端外部事件例如地震与龙卷风和外部事故发挥协同作用的方面。本出版物引入了防破坏纵深防御方法，以及包括一些安全和安保相关系统和活动的若干层次，并且促进许可证持有者与主管部门合作开展自评定。

国际原子能机构
维也纳

ISBN 978-92-0-523310-9
ISSN 1816-9317