2018年核设施经验反馈专项培训班

培 训 教 材

环境保护部核与辐射安全中心

2018 年 3 月

国际核与辐射事件分级
（INES）方法

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

国际核与辐射事件分级（INES）方法

赵 力
环境保护部核与辐射安全中心

主 要 内 容

一、概述

二、对人和环境影响的评定

三、对设施的放射性屏障和控制影响的评定

四、对纵深防御影响的评定

- 运输和辐射源事件
- 动力堆功率运行中的事件
- 特定设施中的事件

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

一、概述

1. INES的历史
2. 使用INES的目的
3. INES的适用范围
4. INES的分级
5. 评级原则

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

1. INES的历史

INES最早是“International Nuclear Event Scale”——国际核事件分级的简称。INES手册最早于1992年由IAEA和OECD/NEA联合发布。

后续经过1996年、2001年、2004年、2006年、2008年的多次升版，增加了适用放射源及运输的事件评级；对评级分类上做了修改，新增了很多实例。

国家核安全局参照IAEA 1992版INES手册，在1994年发布了核安全法规技术文件《核事件分级手册》（HAF J0043）。2013年国家核安全局决定对其进行升版，以IAEA 2008版为蓝本进行编译。本课件是以新版本为基础的。

2008版与1992版的主要差异

序号	差异	《核事件分级手册》1992版	《核与辐射事件分级手册》2008版
1	适用范围	动力反应堆；研究堆；采矿和选矿设施；铀浓缩设施；燃料制造设施；乏燃料贮存和后处理设施；废物的预处理、贮存和处置设施等。 不适用于与民用核工业无关的放射性装置或一般的放射性材料运输。	扩大 涵盖了射线照相等工业应用、辐射源在医院中的应用、核设施的活动以及放射性物品的运输等领域。
2	事件分级的基本结构	（1）厂外影响准则 （2）厂内影响准则 （3）纵深防御准则	（1）对人和环境的影响； （2）对设施放射性屏障和控制； （3）纵深防御

2. 使用INES的目的

- 使用统一的标准和用语向公众通报核事件的重要度，便于理解和接受。
- 促进我国对民用核事件的评级工作与国际接轨，满足国际交流的需要。

3. 适用范围

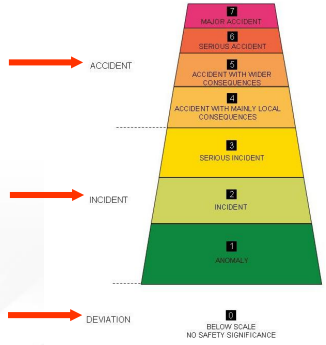
- INES分级准则适用范围广泛，涵盖了包括核电厂、其他核设施、放射性物质和辐射源有关的事件，以及放射性物品运输相关的事件等；
- 只可用于民事（非军事）应用；只与事件的核或辐射安全方面有关，不用于安保相关事件或故意使人受到辐射照射的恶意行为的定级；
- 不涉及：医学治疗中的患者；仅与工业安全有关的事件；其他与核或辐射安全无关的安全事件等。

4. INES的级别

4－7级　“事故”

1－3级　“事件”

0　级　“异常”
（安全上无重要意义）



5. INES分级的原则

每起事件需要从三个方面进行考虑，即：人和环境；放射性屏障和控制；纵深防御。事件定级就是从这三个方面考虑后得出的最高级。

描述和INES级别	人和环境	设施的放射性屏障和控制	纵深防御
特大事故 7级	•放射性物质大量释放，具有大范围健康和环境影响，要求实施所计划的和扩展的应对措施。		
重大事故 6级	•放射性物质明显释放，可能要求实施计划的应对措施		
影响范围较大的事故 5级	•放射性物质有限释放，可能要求实施部分所计划的应对措施。 •辐射造成多人死亡。	•反应堆堆芯受到严重损坏。 •放射性物质在设施范围内大量释放，公众受到明显照射的概率高。其发生原因可能是重大临界事故或火灾。	
影响范围有限的事故 4级	•放射性物质少量释放，除需要局部采取食物控制外，不太可能要求实施所计划的应对措施。 •至少有1人死于辐射。	•燃料熔化或损坏造成堆芯放射性总量释放超过0.1%。 •放射性物质在设施范围内明显释放，公众受到明显照射的概率高。	
重大事件 3级	•受照剂量超过工作人员法定年限值的10倍。 •辐射造成非致命确定性健康效应（例如烧伤）。	•工作区中的照射剂量率超过1Sv/小时。 •在设施内，设计预期之外的区域造成了明显的污染，公众受到明显照射的概率低。	•核电厂接近发生事故，安全措施全部失效。 •高活度密封源丢失或被盗。 •高活度密封源错误交付，并且没有准备好适当的辐射程序来进行处理。
一般事件 2级	•一名公众成员的受照剂量超过10mSv。 •一名工作人员的受照剂量超过法定年限值。	•工作区中的辐射水平超过50mSv/小时。 •设计中预期之外的区域内设施受到明显污染。	•安全措施明显失效，但无实际后果。 发现高活度密封无监管源、器件或运输货包，但安全措施保持完好。
异常 1级			•一名公众成员受到过量照射，超过法定限值。 •安全部件发生少量问题，但纵深防御仍然有效。 •低放放射源、装置或运输货包丢失或被盗。
无安全意义（分级表以下/0级）			

二、对人和环境影响的评定

1. 放射性释放量准则
2. 个人剂量准则
3. 案例

2. 对人和环境影响的评定

人 → 工作人员 / 公众成员 → 个人剂量 / 受照人员数量

环境 → 放射性物质大量释放的情况

2。对人和环境影响的评定

1 放射性释放量准则

➢适用于放射性大量释放到环境中的情况

（INES 4-7级事故）

- 大型核设施发生的释放事故
- 重大的运输和辐射源事故

对不会造成大气释放（例如由放射性物质泄漏引起的水体释放或地面污染）事件，应使用根据剂量进行定级的准则。

2。对人和环境影响的评定

1 放射性释放量准则

➢如何估算放射性释放量？

- **I-131放射性当量：**

I-131“放射性当量”，即假定产生相同的有效剂量，利用转换因子将其他放射性核素的活度转化为相当于多少TBq的I-131的活度。

适用于**核设施**发生放射性**大气**释放的情况。

- **D_2值：** 放射性物品**运输或辐射源**使用期间。

通常，运输和辐射源事故不会高于**5**级

1 放射性释放量准则

核设施的大气环境释放事件

7	向环境释放超过几万 TBq I-131放射性当量 (> 50,000 TBq≈5×10^{16}Bq的I-131）
6	向环境释放几千到几万TBq I-131放射性当量 (> 5,000 TBq≈5×10^{15}Bq I-131）
5	向环境释放几百到几千TBq I-131放射性当量 (> 500 TBq ≈5×10^{14}Bq I-131
4	向环境释放几十到几百 TBq I-131放射性当量 (> 50 TBq≈5×10^{13}Bq I-131)

放射性当量的计算

放射性核素大气释放：

$$D_{总}=Q\ X\ (D_{吸入}\cdot 呼吸率+Vg\cdot D_{地面})$$

不考虑食入剂量——食品的干预水平会防止事故导致人员受到显著照射；

表2-1 核素的^{131}I放射性当量转换因子

放射性核素	转换因子	放射性核素	转换因子
Am-241	8000	Ru-106	6
Co-60	50	Sr-90	20
Cs-134	3	Te-132	0.3
Cs-137	40	U-235(S)[a]	1000
H-3	0.02	U-235(M)[a]	600
I-131	1	U-235(F)[a]	500
Ir-192	2	U-238(S)[a]	900
Mn-54	4	U-238(M)[a]	600
Mo-99	0.08	U-238(F)[a]	400
P-32	0.2	天然铀	1000
Pu-239	10000	惰性气体	可忽略不计（实际为零）

基于I-131放射性当量的事件定级

假定事件导致向环境释放30 TBq 的^{137}Cs

1. 查找放射性当量转换因子:
   - 上表： 40

Cs-134	3
Cs-137	40

2. 释放量乘以相应的转换因子
   - 30*40 TBq = 1200 TBq
3. 与定级准则相比较，给事件定级
   - 5级

6	向环境释放几千到几万TBq I-131放射性当量 (> 5,000 TBq≈5×10^{15}Bq I-131)
5	向环境释放几百到几千TBq I-131放射性当量 (> 500 TBq ≈5×10^{14}Bq I-131

1 放射性释放量准则

➢ 如何估算放射性释放量？

□放射性释放当量：

□ D_2值 ： 放射性物品运输或辐射源使用期间。

D值是一种活度水平，高于该水平的源被认为是“危险源”，如果得不到安全而可靠的管理，极可能造成严重的确定性效应。

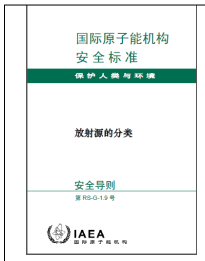
D_1值：失控 √ 扩散 ×

D_2值：失控 √ 扩散 √

D值=D_1和D_2中的最大限制值

常用实践举例

类别	活度（大小）	常用实践
1	＞1000 D	辐照装置；远距离治疗仪
2	＞10 D	工业γ照相机
3	＞1 D	固定式工业测量仪：测井仪



IAEA出版物《放射源的分类》，定义了各种同位素的D_2值。

表2-2　各种同位素的D_2值

放射性核素	D_2（TBq）	放射性核素	D_2（TBq）
Am-241	6.E-02	Mo-99	2.E+01
Am-241/Be	6.E-02	Ni-63	6.E+01
Au-198	3.E+01	P-32	2.E+01
Cd-109	3.E+01	Pd-103	1.E+02
Cf-252	1.E-02	Pm-147	4.E+01
Cm-244	5.E-02	Po-210	6.E-02
Co-57	4.E+02	Pu-238	6.E-02
Co-60	3.E+01	Pu-239/Be	6.E-02
Cs-137	2.E+01	Ra-226	7.E-02
Fe-55	8.E+02	Ru-106（Rh-106）	1.E+01
Gd-153	8.E+01	Se-75	2.E+02
Ge-68	2.E+01	Sr-90（Y-90）	1.E+00
H-3	2.E+03	Tc-99m	7.E+02
I-125	2.E-01	Ti-204	2.E+01
I-131	2.E-01	Tm-170	2.E+01
Ir-192	2.E+01	Yb-169	3.E+01
Kr-85	2.E+03		

1 放射性释放量准则

运输和辐射源发生向环境大气释放的事件

7	
6	
5	释放超过D_2值2500倍的事件
4	释放超过D_2值250倍的事件

运输和辐射源环境释放事件的定级

放射源破损，向环境释放了100 TBq 的 Ir-192

1. 查找放射源的 D_2 值：
   - $D_2 = 20$

I-131	2.E-01
Ir-192	2.E+01
Kr-85	2.E+03

2. 计算释放量与D_2值的比
   - $100 \div 20 = 5$
3. 与分级准则比较，给事件定级
   - $5 < 250$；

4	释放超过D_2值250倍的事件

小于4级的准则，分级表以下0级。

放射性释放量准则汇总

7	超过几万TBq的 I-131	>50,000 TBq（$>5\times10^{16}$Bq）
6	几千到几万TBq 的I-131	5,000 – 50,000 TBq（5×10^{15} ~5×10^{16} Bq）
5	几百到几千TBq的 I-131 OR 超过D_2值的 2500倍	500 – 5,000 TBq（5×10^{14} ~5×10^{15} Bq）$>2500D_2$
4	几十到几百TBq的 I-131 OR 超过D_2值的250倍	50 – 500 TBq（5×10^{13} ~5×10^{14} Bq）$250D_2$~$2500D_2$

放射性释放量准则

- 事故对环境的实际影响（实际后果）；

事故早期阶段 → 根据已实际发生的情况 → 临时定级

- 与事故发生时的天气、季节、人口密度等无关；
- 事件级别 ≠ 应急响应（防护行动）

二、对人和环境影响的评定

1 放射性释放量准则

2 个人剂量准则

3 案例

2 个人剂量准则

- 实际受照剂量
- 可能受到的照射剂量

这里个人照射剂量是指从单次照射所致的照射剂量，而并非年累积剂量。（1级事件除外）

利用该准则对事件进行定级，不需考虑事件的场景，但事件场景却可能影响照射剂量。

2 个人剂量准则

个人照射剂量的估算：

- 实际受照场景
- 所采取的防护措施

外照射：时间、距离、防护；

内照射：

- 基本的假设条件

二、对人和环境影响的评定

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

2 个人剂量准则

- 最小定级：
  一个人
- 定级有可能升高
  超过一个人

A. 基于一个人的照射剂量的定级准则

4级：

（1）“发生致命的确定性效应；或

（2） 由于全身受到照射导致吸收剂量达到几Gy，可能发生致命的确定性效应。”

在明显受到高LET辐射的情况下，吸收剂量应考虑相应的相对生物效应。应使用相对生物效应加权吸收剂量来确定适当的INES定级。

A. 基于一个人的照射剂量的定级准则

3级：

(1) “发生或可能发生非致命的确定性效应；或

(2) 导致有效剂量超过工作人员的法定全身年剂量限值10倍的照射。”

A. 基于一个人的照射剂量的定级准则

2级：

（1）“一名公众成员受照有效剂量超过10mSv；或

（2） 一名工作人员受到的照射超过法定年剂量限值。”

考虑的剂量限值为所有法定剂量限值，包括全身有效剂量、皮肤剂量、四肢剂量和眼球晶状体剂量。

A. 基于一个人的照射剂量的定级准则

1级：

(1) “一名公众成员受到的照射剂量超过法定年剂量限值；或

(2) 一名工作人员受到的照射剂量超过剂量约束值；或

(3) 一名工作人员或公众成员受到的累积照射超过法定年剂量限值。”

A. 基于一个人的照射剂量的定级准则

4	发生致命的确定性效应 or 很可能发生致命的确定性效应，吸收剂量达到几Gy
3	发生或很可能发生致死性确定性效应 or 导致受照有效剂量超过工作人员法定全身年剂量限值10倍
2	一名公众成员受照有效剂量超过 10mSv or 一名工作人员受照剂量超过法定年剂量限值
1	一名公众成员受照剂量超过法定年剂量限值；or 一名工作人员受照剂量超过剂量约束值；or 一名工作人员或公众成员的累积照射超过法定年剂量限值

B. 多人受照情况下的定级准则

由受照射人数提高事件级别

- 对于潜在健康效应或随机效应
  - ≥10人 事件级别+1
  - ≥ 100人 事件级别+2
- 对于实际的健康效应或确定性效应
  - ≥ 几个人（3人） 事件级别 +1
  - ≥几十人（30人）事件级别 +2

多人受到不同程度的照射？

取按上述过程得出的最高事件定级

例如：

15名公众成员受照有效剂量为20mSv的事件

- 最低定级——2级；准则“一名公众成员受照有效剂量超过10mSv”
- 15人受照，事件级别提高1级，定为3级；
- 最终定级：3级

1个人受照有效剂量为20mSv；其他14人，剂量为1～10mSv的事件

- 最低定级，20mSv的1人定为2级；1~10mSv，定为1级；
- 超过10人受照1~10mSv，故事件级别提高1级，定为2级；
- 最终定级：2级

照射剂量	最低定级	受照人数	实际定级
发生或可能发生致死性确定性效应	4	几十人或以上	6*
		几人到几十人	5
		少于几人	4
全身吸收剂量达到几Gy而可能发生致命的确定性效应	4	几十人或以上	6*
		几人到几十人	5
		少于几人	4
发生或可能发生非致命的确定性效应	3	几十人或以上	5
		几人到几十人	4
		少于几人	3
个人照射剂量超过工作人员法定全身年剂量限值10倍	3	100人或以上	5
		10人及以上	4
		少于10人	3

照射剂量	最低定级	受照人数	实际定级
◆一名公众成员受照有效剂量超过10mSv；或 ◆一名工作人员受照有效剂量超过法定年剂量限值	2	超过100人	4
		超过10人	3
		少于10人	2
◆一名公众成员受照剂量超过法定年剂量限值；或 ◆一名工作人员受照剂量超过剂量约束值；或 ◆一名工作人员或公众成员的累积照射超过法定年剂量限值	1	超过100人	3
		超过10人	2
		少于10人	1

2. 对人和环境影响的评定

1. 放射性释放量准则
2. 个人剂量准则
3. 案例

案例—1

一座高放废物贮存罐的冷却系统失效，造成罐内贮存的废物温度升高。随后干硝酸盐和醋酸盐爆炸，其威力相当于75吨TNT。2.5米厚的混凝土盖子被抛到30米外。采取了包括撤离在内的应急行动，以防止产生严重的健康效应。释放最多的成分是1000TBq ^{90}Sr和13 TBq ^{137}Cs，并测得有300×50 km的大范围地区受到4 kBq/m^2 以上的^{90}Sr污染。

准则	说明
2.2释放的活度	从表2可知，^{90}Sr和^{137}Cs的放射性当量转换因子分别是20和40，所以放射性总释放量相当于20500 TBq ^{131}I。符合“相当于几千到几万TBq ^{131}I”，定为6级。
2.3个人剂量	事件已定为6级，故无需考虑。
根据对人和环境的影响评定的级别	6级

案例—2

一座石墨沸水堆由于临界事故和火灾导致的大规模放射性释放

由于设计缺陷和进行了错误的试验，导致反应堆超临界。试图关闭该反应堆，但能量出现峰值，一些燃料元件开始破裂，燃料元件碎片落到控制棒通道内。控制棒在只插入三分之一时就被卡住，因此无法阻止反应。反应堆功率提高到约30 GW，是正常运行时输出功率的10倍。燃料元件开始融化，蒸汽压力迅速增加，造成大量蒸气喷发。产生的蒸汽沿着控制棒通道垂直进入反应堆，使反应堆顶盖受到破坏，冷却管道断裂，之后在厂房顶部冲开了一个洞。氧气从洞口涌入，加之反应堆燃料和石墨的温度极高，引起石墨失火。火灾是导致放射性物质扩散和外围地区污染的一个重要原因。总共释放的放射性物质近1400万TBq，其中包括180万TBq ^{131}I、8.5万TBq^{137}Cs及其同位素、1万TBq ^{90}Sr和其他一些重要的核素。

准则	说明
2.2释放的活度	从表2可知，^{90}Sr和^{137}Cs的放射性当量转换因子分别是20和40，所以放射性总释放量相当于540万TBq^{131}I。符合“超过几万TBq ^{131}I”，定为分级表的最高等级7级。虽然还存在其他同位素，但由于给出核素的放射性已经相当于7级事故释放，因此没有必要将它们计算在内。
2.3个人剂量	因为事件已定为7级，故无需考虑。
根据对人和环境的影响评定的级别	7级

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

三、对设施的放射性屏障和控制影响的评定

1. 适用范围
2. 事件的定级准则
3. 案例

WEBSITE http://www.chinansc.cn/

三里岛核事故（TMI）

- 没有发生放射性大规模的释放；
- 纵深防御的最高定级是3级

人和环境的影响准则

纵深防御准则 ✗ 事故的严重程度及影响

第一类事件是：用于防止放射性物质大量释放的主要屏障发生严重损坏，例如堆芯熔化或核燃料后处理设施内的大量放射性物质包容屏障的丧失。在此类事件中，主要的设计保护失效，阻止大量放射性释放的唯一屏障是仅存的包容系统。

4、5级事件定级准则

A. 反应堆燃料损坏相关

B. 其他放射性屏障完整性相关

第二类事件是，防止大量放射性释放的主要屏障完好无损，但在处理大量放射性物质的设施内发生了放射性物质的大量溢出或剂量率显著增加的事件。此类事件因为多层屏障仍然保持完好，可根据纵深防御准则定为1级。但是，这类事件则意味着在放射性物质处理的管理控制方面的严重失误，存在发展成可对人和环境造成严重影响的潜在风险。

2、3级事件定级准则

C. 污染扩散事件

三、对设施放射性屏障和控制影响的评定

1 适用范围

- 在经批准的核设施内发生的事件，设施的场区边界按照许可证的要求明确界定。
- 只适用于有可能（但是可能性不大）发生可定为5级或更高级别的放射性物质释放事件的重要设施。

三、对设施的放射性屏障和控制影响的评定

1 适用范围

2 事件的定级准则

3 案例

A. 涉及反应堆（包括研究堆）燃料的事件

5级

- 导致动力堆中有超过几%的燃料熔化，或
- 超过几%的堆芯放射性总量从燃料组件中释放的事件。

4级

- 由于燃料熔化和／或燃料包壳破损而导致动力堆约0. 1%以上堆芯放射性总量从燃料组件中释放出来的事件。

研究堆损坏燃料所占比例应该基于3000MW（热功率）动力堆燃料数量计算的值。

A. 涉及反应堆（包括研究堆）燃料的事件

其他说明：

- ＜0.1%的堆芯放射性总量释放的燃料损坏或燃料性能退化事件 ⟹ 分级表以下0级。
- 堆芯放射性总量，并非只是“间隙存量”；
- 研究堆，基于3000MW（热功率）动力堆燃料数量计算得出其燃料损坏比例；
- 燃料损坏的程度不容易测量，应转化成可监测的量；
- 定级与一回路的状态无关。

B. 其他设施的放射性屏障损坏的事件

5级

导致设施发生放射性物质大量释放到设施边界范围内的高概率严重过量照射的事件。

大量释放=与堆芯熔化产生的释放相当

高概率=与继反应堆事故之后再发生从安全壳释放相似的概率。

4级

从一次包容结构中释放出活度几千TBq的放射性物质，且很可能对公众产生严重的过量照射的事件。

C. 放射性污染扩散的事件

3级

- 导致发生几千TBq活度的释放在设计未曾考虑到的区域内的事件，即使导致严重的公众照射的概率极低，要求采取纠正行动；或
- 导致在工作区内γ剂量率和中子剂量率的总和大于1 Sv/h的事件；

设计未曾考虑到的区域==设计基准中没有考虑到的受污染区域；
工作区== 不需要特殊许可的预期高辐射或高污染的区域；
工作区以外的高剂量率事件的定级，用纵深防御准则；
剂量率== 距源1m处测量的剂量率。

C. 放射性污染扩散的事件

2级

- 导致在工作区内γ剂量率加中子剂量率之和大于50 mSv/h的事件。或者
- 导致在设施内，且设计未曾考虑到的区域内出现大量放射性物质并且需要采取纠正行动的事件。”

设计未曾考虑到的区域==设计基准中没有考虑到的受污染区域；
工作区== 不需要特殊许可的预期高辐射或高污染的区域；
工作区以外的高剂量率事件的定级，用纵深防御准则；
剂量率== 距源1m处测量的剂量率。

这里的“大量”应该解释为：

(a) 活度相当于10TBq量级的 ^{99}Mo泄漏量的液态放射性物质泄漏量。

(b) 活度相当于1TBq 量级的^{137}Cs泄漏量的固态放射性物质泄漏量，另外表面污染和空气污染水平超过工作区允许值的10倍的情况。

(c) 包含在厂房内，活度相当于几十 GBq ^{131}I释放量的气态放射性物质释放量。

设施污染的放射性当量转换因子

核素	^{131}I-空气污染	^{137}Cs-固体污染	^{99}Mo-液体污染
Am-241	2000	4000	50 000
Co-60	2.0	3	30
Cs-134	0.9	1	20
Cs-137	0.6	1	12
H-3	0.002	0.003	0.03
I-131	1	2	20
Ir-192	0.4	0.7	9
Mn-54	0.1	0.2	2
Mo-99	0.05	0.08	1
P-32	0.3	0.4	5
Pu-239	3000	5000	57 000
Ru-106	3	5	60
Sr-90	7	11	140
Te-132	0.3	0.4	5
U-235(S)[a]	600	900	11 000
U-235(M)[a]	200	300	3000
U-235(F)[a]	50	90	1000
U-238(S)[a]	500	900	10 000
U-238(M)[a]	100	200	3000
U-238(F)[a]	50	100	1000
天然铀	600	900	11 000

三、对设施的放射性屏障和控制影响的评定

1 适用范围

2 事件的定级准则

3 案例

案例—1

在反应堆运行期间，探测到冷却剂活度略有增加，表明燃料发生了轻微损坏。然而，损坏程度不大，决定继续运行。根据反应堆冷却剂的活度，操纵员开始换料停堆，想从3400根燃料棒中找出少量出现破损的部分。然而，实际检查显示，约有200根（占总数的6%）燃料棒发生破损，但是没有发生燃料熔化或从燃料组件中释放大量的放射性核素。最终发现，燃料棒破损的原因是反应堆冷却剂中存在异物，导致燃料棒局部过热而破损。

准则	说明
2.2 释放的活度	不适用。无释放
2.3 个人剂量	不适用。无释放
3.2 设施的放射性屏障和控制	6%的燃料棒发生破损，导致约0.06%的堆芯放射性总量释放到冷却剂中。这低于4级标准，根据该标准，定为0级
根据实际后果评定的级别	分级表以下／0级（按照纵深防御准则，将给出更高的定级）

案例—2

一座后处理设施内发生的事件：

4名员工进入一个辐射控制区实施通风系统作业。作业包括从一座厂房内的一个房间中移出一个部件（消能箱），这座厂房内有一个钚处理设施。该设施自1957年以来就没有使用，一直处于休眠状态，准备退役。

工作人员佩戴防护服和监测装备。消能箱的切割进行了1小时40分钟，观察到有灰尘从消能箱上落下。当他们停止作业、离开辐射区时，通过个人污染监测设备，所有工作人员的服装上都检测到了污染。随后立即采取措施，包括对被污染人员实施工作限制，并通过生物测定技术进行剂量评估。初步估计的受照有效剂量小于11mSv。之后对相关人员的最大个人待积有效剂量的估计值为24～55 mSv。当时的个人年剂量限值为50 mSv。

准则	说明
2.2 释放的活度	不适用。
2.3 个人剂量	一名工作人员受照剂量大于年限值。受到这一剂量的人数小于10，所以由于所涉人数不超过10人，级别不提高，定为2级。
3.2设施的放射性屏障和控制	污染事件发生在一个已为潜在污染做好准备的区域（设计考虑到的区域）中的一个特定物项的退役期间。因此，本准则不适用。
根据实际后果评定的级别	2级

案例—3

一座核电站发生一起燃料过热的事故，导致约一半燃料细棒发生破损，并在随后释放了放射性物质（约一半燃料细棒发生破损，未发生显著的燃料熔化，可能释放0.5%的堆芯放射性总量）。

当地警方在与许可证持有者和监管部门协商之后，立即决定撤离设施周边半径2 km范围内的人群。结果，无人受到1mSv以上的照射。专家对设施释放的放射性物质进行评估显示，总活度约为20TBq，包含约10%的^{131}I、5%的^{137}Cs及其他惰性气体。

准则	说明
2.2释放的活度	采取撤离行动与定级无关。根据表2，ITBq^{137}Cs在放射学上相当于40 TBq^{131}I,因此总共释放的放射性当量42 TBq ^{131}I，接近于“几十到几百TBq^{131}I”的4级释放标准下的定级数值。
2.3个人剂量	所有的剂量均小于1 mSv，故根据个人剂量评定的级别为0级。
3.2设施的放射性屏障和控制	来自燃料的释放达到4级数值，即“约0.1%以上的动力堆堆芯放射性总量从燃料组件释放出来”，但是低于5级定义的值，即“百分之几以上的动力堆堆芯放射性总量的释放来自燃料组件。
根据实际后果评定的级别	4级

主 要 内 容

一、概述

二、对人和环境影响的评定

三、对设施的放射性屏障和控制影响的评定

四、对纵深防御影响的评定

- 运输和辐射源事件
- 动力堆功率运行中的事件
- 特定设施中的事件

四、对纵深防御影响的评定

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

适用于：辐射源、放射性物品运输有关的实践

不适用于：加速器和涉及放射性同位素生产和分发或使用Ⅰ类源的设施。

为确保辐射源运输和使用期间公众和工作人员的安全，需有良好的设计、控制得当的运行、行政控制手段和各种各样的保护系统（例如联锁、报警和实体屏障）。考虑到设备故障、人因失误和意外事件发生的可能性，在设置这些安全措施时应使用纵深防御方法。

纵深防御定级的原则

最大潜在后果	纵深防御最高定级
5—7级	3级
3—4级	2级
0—2级	1级

根据纵深防御对事件定级的步骤

A. 确定最大潜在后果

B. 确定纵深防御的上限

C .可用于预防、监测和缓解的安全措施的数目和有效性，包括非能动的和能动屏障的硬件和行政管理系统

D. 事件中有关安全文化方面的问题（附加因素）

A. 确定最大潜在后果

最大潜在后果

——根据源的类别A、源的D值得出，与事件的实际情况无关；

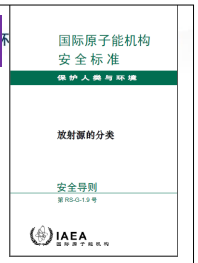
—— 假定所有安全措施都失效；

A/D值	0.01≤A/D< 1	1≤A/D<10	10≤A/D<1000	1000≤A/D
源的类别	4类	3类	2类	1类
最大潜在后果的定级	2	3	4	5[a]
纵深防御的最高定级	1	2	2	3

各核素的D值

核素	D（TBq）	核素	D（TBq）
Am-241	6E-02	Am-241/Be	6E-02
Au-198	2E-01	Cd-109	2E+01
Cf-252	2E-02	Cm-244	5E-02
Co-57	7E-01	Co-60	3E-02
Cs-137	1E-01	Fe-55	8E+02
Gd-153	1E+00	Ge-68	7.E-01
H-3	2.E+03	I-125	2.E-01
I-131	2.E-01	Ir-192	8.E-02
Kr-85	3.E+01	Mo-99	3.E-01
Ni-63	6.E+01	P-32	1.E+01
Pd-103	9.E+01	Pm-147	4.E+01
Po-210	6.E-02	Pu-238	6.E-02
Pu-239/Be	6.E-02	Ra-226	4.E-02
Ru-106（Rh-106）	3.E-01	Se-75	2.E-01
Sr-90（Y-90）	1.E+00	Tc-99^m	7.E-01
Ti-204	2.E+01	Tm-170	2.E+01
Yb-169	3.E-01		

放射源的分类



国际原子能机构IAEA：

2006年发布了RS-G-1.9号《放射源的分类》，将辐射源分为1、2、3、4、5类。

国务院第449号令：

第四条　国家对放射源和射线装置实行分类管理。根据放射源、射线装置对人体健康和环境的潜在危害程度，从高到低将放射源分为Ⅰ类、Ⅱ类、Ⅲ类、Ⅳ类、Ⅴ类，具体分类办法由国务院环境保护主管部门制定；将射线装置分为Ⅰ类、Ⅱ类、Ⅲ类，具体分类办法由国务院环境保护主管部门商国务院卫生主管部门制定。

国家环境保护总局　**2005年第62号《放射源分类办法》；**
2006年第26号《射线装置分类办法》

WEBSITE http://www.chinansc.cn/

类别	源[a]和实践	活度比[b]（A/D）
1	放射性同位素热电发生器（RTG） 辐照装置 远距放射治疗源 固定式多束远距放射治疗（γ刀）源	$A/D \geqslant 1000$
2	工业γ射线探伤源 高/中剂量率近距放射治疗源	$1000 > A/D \geqslant 10$
3	装有高活度源的固定式工业仪表[c] 测井仪表	$10 > A/D \geqslant 1$
4	低剂量率近距放射治疗源（眼部敷贴和永久性植入除外） 未装高活度源的固定式工业仪表[c] 骨密度仪 静电消除器	$1 > A/D \geqslant 0.01$
5	低剂量率近距放射治疗眼部敷贴和永久植入源 X射线荧光（XRF）分析仪 电子俘获设备 穆斯堡尔谱仪 正电子发射断层成像（PET）检查源	$0.01 > A/D$ 且 $A >$ 豁免水平[d]

源的类别	靠近单个源的风险	源的放射性物质因火灾或爆炸而漏散的事件中的风险
1	**对人员极度危险：**这种源，如果未得到安全管理或保安措施不到位，可能对操作它或者意外接触它几分钟的人造成永久性损伤。靠近这种无屏蔽放射性物质几分钟到1小时的时间，可能导致人员死亡。	这个量的放射性物质，如果漏散，也许可能——尽管不太可能——对近距离的人员造成永久性损伤或有生命危险。给几百米以外的人员会造成直接健康效应的风险很小或者没有，但是需要根据国际标准对污染区进行清理。对于大型源，需要清理的区域面积可能达到1平方千米甚至更大。[a]
2	**对人员非常危险：**这种源，如果未得到安全管理或保安措施不到位，可能对操作它或者意外接触它（从若干分钟到若干小时）的人造成永久性损伤。靠近这种无屏蔽放射性物质若干小时到若干天，可能导致人员死亡。	这个量的放射性物质，如果漏散，也许可能——尽管非常不可能——对近距离的人员造成永久性损伤或有生命危险。给百米或更远的人员会造成直接健康效应的风险很小或者没有，但是需要根据国际标准对污染区进行清理。需要清理的区域面积不可能超过1平方千米。[a]

3	**对人员危险**：这种源，如果未得到安全管理或保安措施不到位，可能对操作它或者意外接触它若干小时的人造成永久性损伤。靠近这种无屏蔽放射性物质若干天到若干周，可能会——尽管不太可能发生——导致人员死亡。	这个量的放射性物质，如果漏散，也许可能——尽管极不可能——对近距离的人员造成永久性损伤或有生命危险。给几米远的人员会造成直接健康效应的风险很小或者没有，但是需要根据国际标准对污染区进行清理。需要清理的区域面积不可能超过 1 平方千米的很小一部分。[a]
4	**对人员不太可能有危险**：极不可能有任何人因这种放射性物质而受到永久性损伤。但是，这种无屏蔽材料，如果未得到安全管理或保安措施不到位，那么可能——尽管不太可能——在许多小时内对操作它或意外接触它的人、或在许多周内靠近它的人造成暂时性损伤。	这个量的放射源物质，如果漏散，不可能给人员造成永久性伤害。[b]
5	**最不可能给人员造成危险**：没有人会因这种源受到永久性损伤。[b]	这个量的放射源物质，如果漏散，不可能给人员造成永久性伤害。[b]

A. 确定最大潜在后果

- 乏燃料——1类源
- 除加速器以外的其他射线装置：

(1). 所有安全措施都失效，不会发生确定性效应的装置——4类源

(2). 所有安全措施都失效，可能发生确定性效应的装置——2类或3类源

- 5类源，分级表以下0级

A. 确定最大潜在后果

若干源或若干运输货包：

- 如果安全要求降低只能影响单一物项，应使用受影响货包的存量，即货包/源的单项存量；（一件运输货包标签不合适）
- 如果安全要求降低可能影响所有物项，应使用总存量。（如火灾）

总D值

$$1/D = \sum f_i/D_i$$

$$A/D = \sum A_i/D_i$$

A. 确定最大潜在后果

一般步骤：

- 源活度已知→→A/D值
- 源实际活度未知→→剂量率+核素类别→→A/D值
- 源实际活度未知且剂量率无法测量→→源的用途

表Ⅳ.1 通用实践的分类

类别	通用的实践分类	典型同位素
1	放射性同位素温差电池	Sr-90, Pu-238
	辐照装置	Co-60, Cs-137
	远距离放射治疗	Co-60, Cs-137
	固定式多波束远距放射疗法（γ刀）	Co-60
2	工业γ照相机	Co-60, Se-75, Ir-192, Yb-169,Tm-170
	高/中剂量率近距放射治疗	Co-60, Cs- 137, Ir-192

A. 确定最大潜在后果

涉及包含裂变材料货包的事件：

- 防止临界所需安全措施失效→→货包作为1类源。
- 有一项与临界安全无关的措施失效：

(1)未辐照过的燃料→→A/D值(实际活度)

(2)乏燃料→→尽管实际的A/D值可以计算和应用，如果乏燃料的量非常少，一般应该使用1类源一列的数据。

B. 确定纵深防御的上限

最大潜在后果 → 原则 → 纵深防御最高级别

5-7级→ → 3级
3-4级→ →2级
0-2级→ →1级

C. 根据安全措施的有效性定级

安全文化

在组织和个人中将防护和安全问题作为最高优先事项，并根据其重要性予以相应重视的特征和态度的总和

指标实例：

- 未经事先批准而违反程序；
- 质量保证过程中的缺陷；
- 人因差错重复发生；
- 未能对放射性物质保持适当的控制，包括环境释放、污染扩散或剂量控制系统失效；
- 重发事件，有证据证明，运营商在第一次出事之后没有给以足够的重视以确保已经吸取教训且已经采取纠正措施，致使该事件重复发生。

(1)放射源/射线装置丢失、寻回相关

事件类型	根据源的类别进行的事件分级		
	Ⅳ类	Ⅲ类或Ⅱ类	Ⅰ类
失踪的放射源、射线装置或运输货包随后在受控制区域完好**找回**	1	1	1
寻回的源、射线装置（包括孤儿源和装置）或运输货包	1	1或2	2或3
丢失或被盗的放射源、射线装置或运输货包仍未找回	1	2	3
丢失或被盗的放射源、射线装置或运输货包的位置随后被确定，并证实没有发生意外照射，但是决定并获批准不回收这个源，因其处于安全或不可接近的位置（如水下）	1	1	1
投递错误的运输货包，但接收单位有处置货包所需的完善的辐射安全程序	0或1	1	1
投递错误的运输货包，但接收单位根本没有处置货包所需的辐射安全程序	1	1或2	2或3

(2) 安全措施功能降级相关

A. 无安全措施功能降级

虽然异常事件可能已经发生，但是从现有安全措施有效性看没有意义

典型事件	根据源的类别进行事件分级		
	Ⅳ类	Ⅲ类或Ⅱ类	Ⅰ类
·屏蔽和/或源容器的表面损伤或源泄漏，造成轻微表面污染和喷溅并有低水平个人污染发生。	1	1	1
·屏蔽和/或源容器的表面损伤或源泄漏，造成轻微表面污染和喷溅，虽然形成异常污染，但是几乎没有放射学意义。	0或1	0或1	0或1
· 在设计中用于应对这类事件的区域内发生污染。	0或1	0或1	0或1
· 可预见事件，针对此类事件具有有效的防止意外照射和恢复正常工况的安全程序。其中可以包括诸如辐射源（如工业射线照相γ源或近距离放射治疗源）未归还，但是按现有应急程序能安全回收这些源。	0或1	0或1	0或1
·运输货包没有或轻微损坏，剂量率没有增加。	0或1	0或1	0或1

(2) 安全措施功能降级相关

B. 安全措施部分有效

至少有一种安全措施仍然有效

典型事件	根据源的类别进行事件分级		
	Ⅳ类	Ⅲ类或Ⅱ类	Ⅰ类
• 已安装的可用于防止高剂量率照射的报警或安全系统部分失效。	0或1	1或2	
• 没有遵循安全程序（包括放射性监测和安全检查），但是其他现有安全措施（硬件）仍然有效	0或1	1或2	
• 包容系统明显降级或封闭不良	0或1	1或2	
• 包装或栓系不当，干预指示装置无效。	0或1	0或1	0或1

(2) 安全措施功能降级相关

C. 安全措施均失效

典型事件	根据源的类别进行事件分级		
	Ⅳ类	Ⅲ类或Ⅱ类	Ⅰ类
• 屏蔽丧失（例如因火灾或严重撞击使直接受源照射成为可能）。	1	1或2	2或3
• 报警和安全装置失效，使得进入高剂量率区域成为可能。	1	1或2	2或3
• 在无其他安全措施留存或所有其他安全措施都失效的场合不能监测辐射水平（例如检查在现场进行射线照相后γ源是否完全复位）。	1	1或2	2或3
• 源事故性外露而没有现成的有效程序来应对这种情况，或这种程序被忽视的事件。	1	1或2	2或3
• 在有明显照射可能性的场合发现包装物的屏蔽不充分或无屏蔽。	1	1或2	2或3

(3) 其他安全相关事件

事件类型	根据源的类别进行的事件分级		
	Ⅳ类	Ⅲ类或Ⅱ类	Ⅰ类
公众成员在一起事件中受到的剂量超过法定年剂量限值	1	1	1
工作人员或公众成员受到的累积剂量超过法定年剂量限值	1	1	1
记录缺失或有严重缺陷，例如源的存量、剂量测量安排中断	1	1	1
环境释放超过管理限值	1	1	1
不符合运输许可证条件	1	1	1

(3) 其他安全相关事件

事件类型	根据源的类别进行的事件分级		
	Ⅳ类	Ⅲ类或Ⅱ类	Ⅰ类
运输中不充分的放射性测量	0或1	0或1	0或1
货包／运输工具污染，造成的污染几乎没有放射学意义	0或1	0或1	0或1
货包/运输工具污染，若干测量表明污染超过适用限值，而且有可能使公众受到污染	1	1	1
运输文件、货包标签或运输工具标牌不正确或缺失，货包标识不正确或缺失	0或1	0或1	0或1
原以为空的货包中存有放射性品	1	1或2	1, 2或3
放射性物品类型错误或包装不当	0或1	1或2	2或3

案例—1

一座工厂使用一个^{192}Ir（1TBq）源的工业射线照相。在照相时，发生了源在照相位置的裸露。射线照相师带着检测仪重新进入此地时确认了辐射源的裸漏。检查受控区的屏蔽情况，发现屏蔽还存在，于是向国家主管部门发出求助。主管部门和射线照相师共同安排了对源的回收工作。在事件首次得到确认后12小时，源被成功地回放。事件（包括源的回收）造成的人员照射剂量（3个人）全都低于1mSv。

准则	说明
2.3 个人剂量	受照剂量低于1级准则。
4.2.1 最大潜在后果	^{192}Ir的D值是0.08 TBq，所以A/D是12（即2类源）。
4.2.2 安全措施的有效性	这是工业射线照相和应急计划中可预见的事件，预计有处理这种事的可用设备。射线照相师进行的监测也是有效的。根据表7 A部分第4段，“对于安全程序在防止意外照射和恢复正常工况方面有效的可预见事件”，级别可以是分级表以下/0级或1级。选择分级表以下／0级，因为没有迹象表明有安全文化问题。
最终定级	分级表以下／0级

案例—2

一家废金属公司向监管人员报告，其进料探测器发出辐射警报。监管人员使用手持测量设备在一个12 m容器的表面上测量到30mSv/h的高辐射水平。容器是由一家专门从事废品中放射源追踪和回收的公司卸下的。发现了三个相同的不锈钢源支架，每个包含一个^{137}Cs源，但是没有开关机构。其中有两个源支架有标识符号，分别是2GBq的^{137}Cs和8GBq的^{137}Cs源。三个源支架的表面剂量率大约分别是4.5mSv/h、4.2mSv/h和17mSv/h，而这些源的活度分别大约是1.85GBq. 1.85GBq和7.4GBq。容器在运输途中的时间接近一个月，但是三个源的始发地不能确定。这些源得到妥善保管，并被运送到一个适当的放射性废物设施。

准则	说明
2.3个人剂量	考虑到这些源在运输和装卸期间可能造成的人员照射，认为不大可能造成10mSv以上的照射剂量或者有10人或更多人受到照射（即1级）。
4.2.1最大潜在后果	已知两个源是^{137}Cs，而根据剂量率和活度测量，第三个源看来与两个已确认的源中较小的源一样。^{137}Cs的D值是1×10^{-1}TBq，源的总活度是11.1GBq。造成的A/D比为0.01≤A/D<1。因此是Ⅳ类源。
4.2.2安全措施的有效性	事件是发现了三个孤儿源。根据表6第2行，1级是恰当的。
最终定级	1级

案例—3

一台湿度—密度计丢失，推断是在一个建筑工地上被从卡车上偷走的。密度计中包含一个^{137}Cs源(0.47GBq)和一个^{241}Am/Be中子源(1.6GBq)。报告了国家主管部门，发布了新闻报道，并在周围地区进行了调查。几天以后找回了密度计，没有遭到破坏的迹象。

准则	说明
2.3 个人剂量	事件未造成人员照射。
4.2.1 最大潜在后果	必须按照附件Ⅲ的说明计算总的A/D值。^{137}Cs的D值是0.1 TBq，源的活度是0.47 GBq；^{241}Am/Be的D值是0.06，源的活度是1.6 GBq。总的A/D值是0.47/100+1.6/60=0.031。这样总的A/D值在0.01和1之间，所以源可以划为4类。
4.2.2 安全措施的有效性	根据表6第2行，1级是合适的。它的找回使事件可以重新评定为“丢失或被偷的放射源的位置随后被确定”（第4行），对于4类源仍然是1级。
最终定级	1级

案例—4

一个1TBq ^{137}Cs孤儿源无意中混入废金属，并在一家炼钢厂中融化。工厂中的50名雇员每人估计受照剂量0.3mSv。

准则	说明
2.2 释放的活度	据估计因熔化释放了10%的活度，造成0.1TBq ^{137}Cs的空气释放。^{137}Cs的D_2值是0.1TBq，所以释放远比5级准则规定的2500倍D_2值小。
2.3 个人剂量	受照剂量低于1级事件准则。
4.2.1 最大潜在后果	^{137}Cs的D值是1×10^{-1} TBq，而源的活度(A)是1TBq，造成的A/D为lOOO>A/D≥10。因此分类为2类源。
4.2.2 安全措施的有效性	根据表6第2行，级别应该是1级或2级。考虑到源熔化，最终定级根据表6应该是2级。
最终定级	2级

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

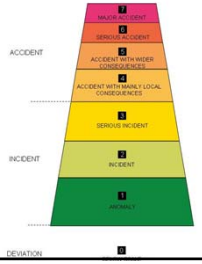
谢谢！

WEBSITE http://www.chinansc.cn/

核与辐射事件分级（INES）
----根据纵深防御影响的事件评定

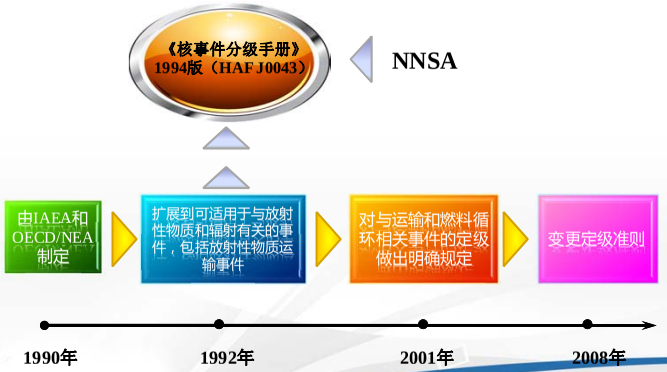
核与辐射事件分级（INES）

----根据纵深防御影响的事件评定



郑丽馨
核与辐射安全中心

INES的沿革

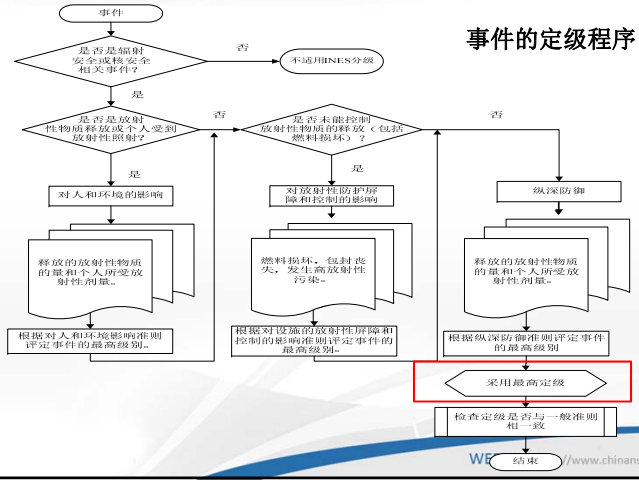


1990版本与2008版的主要差异

适用范围	核动力反应堆、研究堆、采矿和选矿设施、铀浓缩设施、燃料制造设施、乏燃料贮存和后处理设施、废物的预处理、贮存和处置设施等。 ☆ 不适用于与民用核工业无关的放射性装置或一般的放射性材料运输。	除了1990版包括的核设施之外，还涵盖了与放射性物质和辐射源的运输、贮存和使用有关的任何事件，不管事件是否在设施发生都适用，包括放射源或放射性货包的丢失或被盗和孤儿源的发现。
分级准则	（1）厂外影响准则：利用释放的放射性量或公众成员所受辐射量来表示； （2）厂内影响准则：即引起大量放射性物质释放的设施损坏程度、放射性物质释放或迁移到厂内屏蔽薄弱地点、以及工作人员的剂量； （3）纵深防御准则：适用于反应堆的纵深防御准则、非反应堆设施纵深防御准则。	（1）对人和环境的影响：按照对人和环境的影响为事件定级，要考虑对工作人员、公众成员和环境的实际放射影响，人剂量部分**增加了“考虑受照射个体数量的准则”**，根据受照人数的不同，将对定级进行调整； （2）设施放射性屏障和控制的影响：**增加了“放射性当量的计算”具体方法和各核素的转换因子；** （3）纵深防御：**新增运输和辐射源事件中对纵深防御影响的评定。**

纵深防御是保守设计、质量保证、监督活动、缓解措施和加强每个相继保护层次的总体安全文化的组合

事件的定级程序



描述和INES级别	人和环境	设施的放射性屏障和控制	纵深防御
特大事故 7级	·放射性物质大量释放，具有大范围健康和环境影响，要求实施所计划的和扩展的应对措施。		
重大事故 6级	·放射性物质明显释放，可能要求实施计划的应对措施		
影响范围较大的事故 5级	·放射性物质有限释放，可能要求实施部分所计划的应对措施。 ·辐射造成多人死亡。	·反应堆堆芯受到严重损坏。 ·放射性物质在设施范围内大量释放，公众受到明显照射的概率高。其发生原因可能是重大临界事故或火灾。	
影响范围有限的事故 4级	·放射性物质少量释放，除需要局部采取食物控制外，不太可能要求实施所计划的应对措施。 ·至少有1人死于辐射。	·燃料熔化或损坏造成堆芯放射性总量释放超过0.1%。 ·放射性物质在设施范围内明显释放，公众受到明显照射的概率高。	
重大事件 3级	·受照剂量超过工作人员法定年限值的10倍。 ·辐射造成非致命确定性健康效应（例如烧伤）。	·工作区中的照射剂量率超过1Sv/小时。 ·在设施内，设计预期之外的区域造成了明显的污染，公众受到明显照射的概率低。	·核电厂接近发生事故，安全措施全部失效。 ·高活度密封源丢失或被盗。 ·高活度密封源错误交付，并且没有准备好适当的辐射程序来进行处理。
一般事件 2级	·一名公众成员的受照剂量超过10mSv。 ·一名工作人员的受照剂量超过法定年限值。	·工作区中的辐射水平超过50mSv/小时。 ·设计中预期之外的区域内设施受到明显污染。	·安全措施明显失效，但无实际后果。 发现高活度密封无监管源、器件或运输货包，但安全措施保持完好。
异常 1级			·一名公众成员受到过量照射，超过法定限值。 ·安全部件发生少量问题，但纵深防御仍然有效。 ·低放放射源、装置或运输货包丢失或被盗。
无安全意义（分级表以下/0级）			

1 反应堆功率运行期间事件的评级

2 特定核设施中事件的评级

一、反应堆功率运行期间事件的评级

适用范围

反应堆

- 功率运行
- 热停堆
- 热备用
- 热启动

此类安全状态与功率运行状态很相似

美系技术规格书：

模式6：换料（开盖）

模式5：冷停堆T≤93℃

模式4：热停堆（93℃＜T＜177℃）

模式3：热备用（T>177℃）

模式2：热启动

模式1：功率

运行模式与标准运行工况对应表

运行模式	标准运行工况	一回路冷却剂装载量	一回路压力（MPa,绝对压力）（1）	一回路平均温度（℃）（1）	一回路硼浓度（ppm）	核功率
反应堆完全卸料模式（RCD）	所有核燃料在KX厂房		（2）	（2）		
换料停堆模式（RCS）	换料停堆工况	水闸门未就位：≥15米；水闸门就位：≥19.3米；	大气压力	10≤T≤60	2100~2300	0
维修停堆模式（MCS）	一回路充分打开维修冷停堆工况	≥LOW-LOI-RRA	大气压力	10≤T≤60	2100~2300	0
	一回路微开维修冷停堆工况	≥LOW-LOI-RRA	大气压力	10≤T≤60	2100~2300	0
	一回路卸压但封闭维修冷停堆工况	≥LOW-LOI-RRA	P≤0.5	10≤T≤60	2100~2300	0
RRA冷却正常停堆模式（NS/RRA）	正常冷停堆工况	一回路满水	0.5<P≤3.0	10≤T≤90	CB冷~2300	0
	单相中间停堆工况	一回路满水	2.4≤P≤3.0	90≤T≤180	CB冷~2300	0
	双相中间停堆工况RRA运行条件（RRA适用）	一回路满水，稳压器双相状态	2.4≤P≤3.0	120≤T≤180	CB冷~2300	0
蒸汽发生器冷却正常停堆模式（NS/SG）	双相中间停堆工况RRA运行条件（RRA不适用）	一回路满水，稳压器双相状态	2.4≤P≤3.0	160≤T≤180	CB冷~2300	0
	双相中间停堆工况蒸汽发生器冷却工况	一回路满水，稳压器双相状态	2.4≤P≤P11 或 160≤T≤P12		CB冷~2300	0
	热停堆工况	一回路满水，稳压器双相状态	P11≤P≤15.5 和 P12≤T≤294.4		CB热~2300	0
反应堆功率运行模式（RP）	反应堆临界阶段	一回路满水，稳压器双相状态	15.5±0.1	291.4 $\left(^{+1}_{-2}\right)$	逼近临界硼浓度	~0
	热备用	一回路满水，稳压器双相状态	15.5±0.1	291.4 $\left(^{+1}_{-2}\right)$	临界硼浓度	<2%Pn
	功率运行工况	一回路满水，稳压器双相状态	15.5±0.1	291.4≤T≤310	临界硼浓度	2%Pn≤P≤100%Pn

评级步骤

1. 判断是否发生真实的始发事件
2. 确定该始发事件所属的频率类别
3. 确定始发事件挑战的安全功能有效性的级别
4. 得出初步评级结果后，使用附加因素考虑是否提高评级

纵深防御与安全功能

对反应堆的运行安全来说，纵深防御要实现三个基本安全功能：
(1) 反应性控制；
(2) 堆芯冷却；
(3) 放射性物质包容。

这些功能由非能动系统（如管道、容器、实物屏障等）和能动系统（如泵、反应堆保护系统等）提供。某一个特定的安全功能可能由多个安全系统提供，即使一个安全系统不可用，该安全功能仍然有效。

安全功能	功能子项	措施	主要系统设备
反应性控制	停堆	手动、自动停堆	反应堆保护系统（RPR）紧急停堆部分
		注硼	高压安注系统
	防止重返临界	紧急注硼	高压安注系统
堆芯冷却	保持一回路完整性	防止一回路超压、超温	稳压器安全阀 主泵轴封注入 余热排出系统安全阀
	维持一回路水装量	安全注入	高压安注系统 安注箱 低压安注系统
	热阱	一次侧冷却	安注系统 稳压器安全阀
		二次侧冷却	辅助给水系统、主给水旁路系统 汽轮机旁路系统排大气部分（GCTa）
		余热导出	余热排出系统（RRA） 设备冷却水（RRI） 重要厂用水（SEC）
维持安全壳完整性	降压	安全壳喷淋、破口隔离	安全壳喷淋系统（EAS） 主蒸汽隔离阀（MSIV）

1. 安全功能有效性的分类

针对特定始发事件的安全功能的有效性范围很广，为了便于事件定级，可以把安全功能的有效性分为以下四类：

A 全部可用

B 达到运行限值和条件规定的最低要求

C 满足

D 不满足

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

A 全部可用

设计用来应对特定始发事件以限制其后果的所有安全系统和部件都是可用的（即多重性 / 多样性都有效）。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

B 达到运行限值和条件规定的最低要求

安全功能所需的每个安全系统的可用性满足运行限值和条件中（技术规格书）所规定的反应堆可连续功率运行（持续的时间可能有限）的最低要求。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

C 满足

至少有一个安全系统的可用性足以实现始发事件挑战的安全功能。

注意：某些情况下，B类和C类可能相同（除非所有的安全系统都满足运行限值和条件的要求，否则安全功能就不满足）。在其他情况下，C类可以低于运行限值和条件的要求。

还有一种情况，安全功能可能由于非安全系统可用而满足要求。如果已经证实（或已知）非安全系统在事件发生期间是可用的，就可以将他们考虑在内。但是应该谨慎将非安全系统考虑在内，因为它们的可用性通常没有采用与安全系统相同的控制和试验。

WEBSITE http://www.chinansc.cn/

D 不满足

没有一个安全系统能够实现某种始发事件挑战的安全功能。

注意：C类和D类可用性代表一系列的电厂状态（现实分析法），而A类和B类代表具体的可用性（保守分析法）。
实际的可用性可介于A类和B类之间（例如，可用性可能达不到全部可用的要求，但超过连续功率运行技术规格书的“最低要求”）

2. 始发事件的定义

始发事件是指导致偏离正常运行状态，挑战一项或多项安全功能的事件。在安全分析中，始发事件被用来评价所设置的安全系统的适当性，始发事件挑战了安全系统并要求它们发挥作用。

对纵深防御有影响的事件一般有两种可能的形式：
（1）某个始发事件，要求一些专设安全系统投入运行，这些专设安全系统是为了应对该始发事件的后果而设计的。

（2）没有始发事件，但是一个或多个安全系统的可用性降级了。

始发事件不包括依靠控制系统（而不是安全系统）纠正的小的电厂波动。然而，若控制系统不能使反应堆稳定下来，最后将导致始发事件。因此，始发事件可能与引发事件的异常不同；另一方面，若干个不同的事件序列常常可以合并成一起始发事件。

对于许多事件来说，有必要考虑一起以上的始发事件，其中的每一起事件都要定级。整个事件的级别取决于由始发事件定级最高的一个。例如，反应堆功率剧增就可能是挑战保护功能的始发事件，保护系统的成功触发就能导致停堆，然后把反应堆保护停堆视为挑战余热导出功能的始发事件。

确定始发事件的频率

定义了四类始发事件的频率：

- **预期始发事件**

在电厂运行寿期内预计会发生一次或多次的始发事件＞10^{-2}/堆年

- **可能发生的始发事件**

这类始发事件在电厂寿期内预期发生的频率是10^{-4}＜f ≤10^{-2} / 堆年

- **不大可能发生的始发事件**

这类事件是在设计电厂时考虑过的，可能比上述频率还低的始发事件（≤10^{-4} / 堆年）

- **超设计基准的始发事件**

这类事件是发生频率非常低的始发事件，通常不包括在电厂的安全分析中。

压水反应堆始发事件列表

➢ Ⅰ类：预期始发事件（预期瞬态）

- 反应堆紧急停堆；
- 化学补偿剂意外稀释；
- 主给水流量丧失；
- 由于能动部件（例如安全阀或卸压阀）的意外动作，致使反应堆冷却剂系统压力下降；
- 由于稳压器正常或辅助喷淋冷却造成反应堆冷却剂系统压力意外下降；
- 不妨碍反应堆受控停堆和降温的动力转换系统泄漏；（二回路蒸汽泄漏，如一个SG安全阀或泄压阀误开）
- 超过电厂技术规范书但低于单管完全断裂对应量的蒸汽发生器传热管泄漏；（SGTL）

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

- 不妨碍反应堆受控停堆和降温的反应堆冷却剂系统泄漏（化容系统能够补偿）；
- 厂外交流电源丧失（LOOP），包括电压和频率波动；
- 反应堆在一个燃料组件处于错误方向或位置情况时运行；
- 换料期间一个控制组件意外抽出；
- 小的燃料操作事件；
- 除反应堆冷却剂泵转子卡死外，反应堆冷却剂强迫流动完全丧失或中断。
- 一回路冷却剂装量增加（如误安注）；
- 二回路排热减少（汽轮机跳机）。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

➢ Ⅱ类：可能的始发事件（稀有工况）

- 小失水事故；
- 蒸汽发生器一根传热管完全断裂（SGTR）；
- 一个乏燃料组件坠落，但仅涉及该坠落组件；
- 超出正常补给能力的乏燃料池泄漏；
- 反应堆冷却剂通过多个安全阀或卸压阀排放；

➢ Ⅲ类：不大可能的始发事件（极限工况）

- 大失水事故，包括反应堆冷却剂压力边界内的合理最大管道断裂；
- 单个控制棒弹出；
- 能量转换系统大管道断裂，包括合理的最大管道断裂；（如主蒸汽管道破裂 MSLB，主给水管道破裂MFLB）
- 一个乏燃料组件坠落到其他乏燃料组件上；
- 主泵断轴卡死造成的冷却剂流量丧失。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

HAD102/01 核电厂设计中的始发事件分类

（见下表）

WEBSITE http://www.chinansc.cn/

事故归类	事故
(1)由二回路系统引起的排热增加	(a)给水温度降低； (b)给水流量增大； (c)蒸汽流量增大； (d)蒸汽发生器的一个卸压阀或安全阀的意外开启； (e)压水堆蒸汽系统安全壳内外管道故障
(2)由二回路引起的排热减少	(a)厂外负荷丧失； (b)汽轮机脱扣； (c)冷凝器真空丧失； (d)主蒸汽隔离阀关闭(沸水堆)； (e)蒸汽压力调节器故障(关闭)； (f)电厂辅助设备的非应急交流电源丧失； (g)正常给水流量丧失； (h)安全壳内外的给水管道破裂(压水堆)
(3)反应堆冷却剂系统流量减少	(a)包括泵的脱扣和控制器失灵在内的反应堆冷却剂丧失强迫流动； (b)反应堆冷却剂泵的转子卡住和泵轴断裂
(4)反应性和功率分布异常	(a)控制棒组件在次临界状态或低功率起动状态下的失控抽出； (b)控制棒组件在功率运行下的失控抽出； (c)控制棒误动作(系统误动作或运行人员差错)； (d)一条不用的反应堆冷却剂环路或再循环环路在不适当温度下的起动以及流量控制器失灵引起沸水堆堆芯流量增大； (e)化学和容积控制系统失灵(压水堆)引起反应堆冷却剂中硼浓度降低； (f)燃料组件意外装错位置和在错误位置下运行； (g)各种弹棒事故(压水堆)； (h)各种落棒事故(沸水堆)

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

(5)反应堆冷却剂装量的增加	(a)应急堆芯冷却系统意外运行和化学容积控制系统的失灵引起反应堆冷却剂装量增加
(6)反应堆冷却剂装量减少	(a)压水堆稳压器的一个卸压阀或沸水堆一个卸压阀的意外开启； (b)安全壳外装有反应堆冷却剂的小管线故障引起的放射后果； (c)蒸汽发生器传热管故障引起的放射后果(压水堆)； (d)安全壳外主蒸汽管线破损引起的放射后果(沸水堆)； (e)反应堆冷却剂压力边界内的各种假设的管道破裂引起的失水事故
(7)来自子系统或部件的放射性物质释放	(a)废气系统故障； (b)放射性废液系统泄漏或故障(向大气释放)； (c)装盛液体的储罐破损引起的假设放射性物质释放； (d)燃料装卸事故引起的放射后果； (e)乏燃料运输容器掉落事故
(8)未能紧急停堆的预计瞬态	

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

表4 有始发事件情况下，按纵深防御能力下降准则的严重程度分级规则

安全功能有效性	始发事件频率		
	(1) 预期始发事件	(2) 可能的始发事件	(3) 不大可能的始发事件
A 全部可用	0	1	2
B 达到运行限值和条件规定的最低要求	1或2	2或3	2或3
C 满足	2或3	2或3	2或3
D 不满足	3+	3+	3+

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

表5 无始发事件情况下，按纵深防御能力下降准则的严重程度分级规则

安全功能有效性	始发事件频率		
	(1) 预期始发事件	(2) 可能的始发事件	(3) 不大可能的始发事件
A 全部可用	0	0	0
B 达到运行限值和条件规定的最低要求	0	0	0
C 满足	1或2	1	1
D 不满足	3	2	1

WEBSITE http://www.chinansc.cn/

潜在事件的评级（如结构缺陷）

有些事件本身并不构成始发事件或导致安全系统的可用性降级，只是相当于增加了发生这种事件的可能性，例如发现结构缺陷或者已由操纵员终止的小泄漏。

最常见的一个潜在事件的例子是发现结构缺陷。如果这个缺陷在监督大纲的可接受范围之内，那么定为“分级表以下/0级”是合适的。

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

如果发现的缺陷大于监督大纲的预期，那么给该事件定级时需要考虑以下两个因素：
首先，要假定这个缺陷已导致某个部件失效，运用表4或表5确定该潜在事件的级别。

- 如果包含结构缺陷的部件的失效可能演变成始发事件，用表4给出该潜在事件的初步定级，即使缺陷或许是在停堆期间发现的，但也必须考虑它在其他模式下的影响。
- 如果该缺陷发生在安全系统中，只导致安全功能降级，则运用表5给出该潜在事件的初步定级。

注：如果缺陷没有导致实际失效，可根据失效的概率对以上的初步评级进行适当的降级。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

典型的分级表以下的0级事件

一般来说，先不考虑附加因素，以下几类事件是可以划分为“分级表以下 / 0级”的典型事件：

- 正常进行的反应堆保护停堆；
- 安全系统的误动作,但随后转为正常运行，并未对设施的安全性造成影响。

注：这方面的误动作可以包括由控制系统功能异常、仪表漂移或者个别人为差错导致的安全系统动作。然而，由电厂其他地方的非计划行动引起的物理参数变化触发的安全系统动作，不能视为安全系统的误启动。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

3. 对附加因素的考虑

有些特殊的情况可能会同时挑战纵深防御的不同层次，因此将其作为比初步定级提高一级的附加因素。

主要附加因素有：

（a）共因失效

（b）规程有问题

（c）安全文化缺陷

WEBSITE http://www.chinansc.cn/

使用附加因素应注意：

在使用附加因素而提高INES评级时，需要考虑以下几点：

(1)即使考虑所有的附加因素，事件的级别也只能提高1级；

(2) 上述的某些因素（例如共因失效）或许已在评定初步定级时考虑过，因此应注意不要重复计入此类故障。

(3) 事件不能提高到超过3级，取纵深防御的上限只适用于以下情况：假如再发生另一起事件（“预期始发事件”或又一个部件失效）就会发生事故。

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

□ 共因失效

共因失效是指若干个装置或部件由于一个特定的事件或原因都不能执行其功能。特别是，它能引起预定执行同一项安全功能的冗余部件或装置失效。这意味着整个安全功能的可靠性有可能远低于预期值。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

□ 规程有问题

由于规程有问题可能同时威胁纵深防御几个层次。因此，这种情况也有可能成为提高初步定级的理由。例如：
给运行人员发出的应对某起事件的指令错误或不合适（例如：1979年的三里岛事故期间就发生过这种情况。在安全注入已经启动的情况下操纵员使用的程序对于稳压器汽相冷却剂丧失的特殊情况并不适用）。
正常的监测操作未发现的异常或系统／设备的不可用时间远远超出测试间隔，暴露出监测大纲有缺陷。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

□ 安全文化缺陷

安全文化的定义是“存在于单位和个人中的各种特性和态度的综合，它建立一种超出一切之上的理念，即核电厂的安全问题由于它的重要性要保证得到应有的重视”。（INSAG 4对安全文化有更详细的介绍）

如果安全文化存在缺陷，理应将事件的级别提高1级。

鉴于因安全文化而提高级别，该事件必须存在以下安全文化问题的实际指标之一：

WEBSITE http://www.chinansc.cn/

① 违反运行限值和条件

安全文化缺陷中最容易定义的一个指标是违反运行限值和条件。

运行限值和条件描述的是能使反应堆的运行维持在安全要求之内的最低限度安全系统可用性，也可以包括反应堆在安全系统可用性已经降低的条件下进行有限时间的运行。大多数国家将运行限值和条件列入技术规格书中。此外技术规格书还描述了一旦运行限值和条件未满足要求时需采取的行动，包括允许修复和后撤的时间。

如果运行人员故意采取了导致电厂可用性超出运行限值和条件范围的行动，则由于有安全文化缺陷，应该考虑提高该事件的初步定级。

② 其他的安全文化缺陷

安全文化指标的另外一些例子包括：

- 未经事先批准违反程序；
- 质量保证过程存在缺陷；
- 人因差错重复发生；
- 一名公众在一起事件中受到的照射超过法定年剂量限值；
- 工作人员或公众受到的累积照射超过法定年剂量限值；
- 未能对放射性物质保持严格控制，包括环境释放、污染扩散或剂量控制系统失效；
- 如果有证据证明，操纵员在第一次出事之后没有给予足够的重视确保已经吸取教训或已经采取纠正措施，以致该事件重复发生。

实例 1 安全壳喷淋系统因阀门处在关闭位置而不可用

事件描述

该双机组电站每年必须将两座反应堆停堆，以便对共用的应急堆芯冷却系统（ECCS）和相关的自动安全动作进行试验。这些试验通常在两个反应堆中的一个冷停堆换料时进行。

10月9日，1号机组和2号机组进行了这些试验。10月14日，1号机组仍处在冷停堆状态准备换料，2号机组则恢复功率运行。11月1日，在进行安全阀月度检查时，发现安全壳喷淋泵出口侧的四个阀门处于关闭状态。调查发现这些阀门在10月9日进行测试后一直没有重新打开，违反了相关的试验程序要求。

因此，2号机组在喷淋系统不可用的情况下运行了18天。

结论是这起事件的原因是人因差错。

定级说明

准则	说明
2和3实际后果	本事件无实际后果。
始发事件频率	没有真实的始发事件。可能会挑战该降级安全功能的始发事件是大的失水事故（不大可能的始发事件）。
安全功能有效性	“包容”这项安全功能有效性降级。由于多样化的系统是可用的，因而可用性小于“达到运行限值和条件规定的最低要求”但大于“满足”。
初步定级	没有真实的始发事件，按照表5的C 3是合适的，给出的初步定级是1级。
附加因素	此故障是由人因差错引起的，但认为因安全文化缺陷而提高该事件的级别是不合适的（因为初步定级选择1级而不是0级时，已经考虑了违反运行限值和条件值这一事实）。
最终定级	1级

实例2 一回路小泄漏

事件描述

由于存在着监督大纲未预计到的一些缺陷（按照监督大纲这个部位是不检查的），在一根安全注入管线的非隔离部分发现了一处很小的泄漏（只能靠测量湿度才能探测到）。但类似的较小缺陷在其他的安全注入管线上也出现过。

定级说明

准则	说明
2和3实际后果	本事件无实际后果。
始发事件频率	按照潜在事件评级，如果该缺陷导致有关部件失效，就会发生大的失冷事故（“不大可能的始发事件”）。
安全功能有效性	对于这个假想的始发事件来说，安全功能（ECCS系统）有效性“全部可用”。
初步定级	按照处理结构缺陷的方法，使用表4的A3，给出初步定级的上限值为2级。由于只发生了一处泄漏（该管道实际上没有失效）因而该级别应该降1级。
附加因素	由于这些缺陷可能成为所有安全注入管线的共模故障，因而该级别被提高为2级。
最终定级	2级

实例3 保护系统动作引起停堆随后触发安注

事件描述

事件发生前，机组以满功率负荷稳定运行。23时42分，主控室突发“停堆断路器跳闸”等报警，经查发现7#、8#停堆断路跳闸，控制棒全部落到底，但未出现反应堆停堆信号，因此，汽轮发电机组未停，继续向电网供电。23时42分15秒，机组负荷为280MWe，反应堆功率为25MWt，此时操纵员手动停机，断开发电机出口开关2001B，进入应急规程E-0。至5月2日0时02分，主系统平均温度（Tavg）下降至268℃，操作员开始降主系统压力，降压过程中P-11指示灯亮起，但操纵员没有及时闭锁P-11，因而触发低压安注，低压安注所需设备中，除2#应急柴油发电机未能启动外，其它设备均正常启动。
0时05分，稳压器液位为5.0米，压力为14.2MPa，蒸汽发生器液位为10.8米，安注已复位，操纵员恢复系统至热停堆状态。由于安注将硼酸贮存箱的7000PPM浓硼水注入主系统，主系统的硼浓度从180PPM上升至480PPM。

定级说明

准则	说明
2和3实际后果	本事件无实际后果。
始发事件频率	先后发生了两起始发事件：反应堆紧急停堆和误安注，都是预期的始发事件。
安全功能有效性	针对紧急停堆，控制棒全部掉底后未出现反应堆停堆信号，所以反应堆保护系统的安全功能不是全部可用，但还是在运行限值和条件范围之内，因为部分通道不可用在技术规格书中允许一段时间修复，故安全功能是B。对于误安注，是典型的0级事件。
初步定级	有真实的始发事件，按照表4的B1给出的初步定级是1级或2级。
附加因素	无。
最终定级	1级

实例4 一回路水通过稳压器卸压箱爆破膜泄漏

事件描述

该机组已进入热停堆状态。为了进行余热排出系统修改后的测试，该系统已被隔离和部分排空，因而该系统不可用。

当时正在进行稳压器喷淋系统效率的定期试验，反应堆冷却剂系统的压力是159巴。大约在16：00，稳压器卸压箱高压警报被触发。容积控制箱水位下降，表明反应堆冷却剂泄漏，估计泄漏率为1.5m^3/h。一名工作人员进入反应堆大厅试图找到泄漏部位，认为泄漏来自反应堆冷却剂系统上的一个阀门（位于温度传感器旁通管路上的手动阀）的阀杆。这位工作人员转动手轮将阀门置于后座位置后认为该阀门没有泄漏（实际上该阀门并没有正确就位）。泄漏继续，18:00叫来了维修人员，但他们也没有找到泄漏源。

在此期间，稳压器卸压箱内的温度和压力继续升高。操纵员通过多次的补水和排水操作（即注入冷的补给水和将水排到反应堆冷却剂疏水回收箱）将温度保持在50℃以下。并联安装的两台泵将废水排出反应堆大厅，送往硼再循环系统水箱。

（待续）

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

（续）

大约在21:00，活度传感器指示反应堆大厅内的放射性增加，并于21:56时达到安全壳部分隔离的整定值，导致安全壳内核岛的通风和排水系统的阀门关闭。比时，废水不能再流向硼再循环系统。

卸压箱内的压力继续上升，直到爆破膜于21:22破裂。为了把稳压器卸压箱内的温度保持在50℃左右，不得不继续补水并持续到23:36。在次日凌晨01:45，反应堆大厅内的活度水平下降到安全隔离的整定值以下。

在02:32，反应堆冷却剂系统的压力为25巴，机组进入次临界热停堆状态，热量由蒸汽发生器排出，余热排出系统仍然不可用。

余热排出系统在10:45恢复工作。11:45，为了让反应堆冷却剂系统上泄漏的阀门切除，将该阀门的远程控制断开，从而停止泄漏。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

定级说明

准则	说明
2和3实际后果	本事件无实际后果。
始发事件频率	没有真实的始发事件。可能会挑战该安全功能的始发事件是大的失水事故（不大可能的始发事件）。
安全功能有效性	应对LOCA的安注系统虽然全部可用，但有一个阀门错误打开且未被识别，因此“包容”这项安全功能有效性降级。由于多样化的系统是可用的，因而可用性小于“达到运行限值和条件规定的最低要求”但大于“满足”。
初步定级	没有真实的始发事件，按照表5的C3是合适的，给出的初步定级是1级。
附加因素	此故障是由人因差错引起的，但认为因安全文化缺陷而提高该事件的级别是不合适的，因为初步定级选择1级而不是0级时已经考虑了违反运行限值和条件值这一事实）。
最终定级	1级

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

实例5 美国戴维斯-贝斯核电厂反应堆压力容器封头腐蚀

事件描述

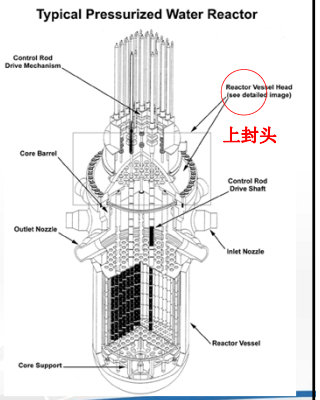
2002年3月7日，在对戴维斯－贝斯核电厂反应堆压力容器（RPV）封头上的CRDM管座进行超声波检查时， 发现在RPV封头上靠近3号CRDM管座处，存在一个孔穴缺陷。电厂对CRDM周围的反应堆压力容器顶部情况进行了检查，包括移除CRDM，清理反应堆压力容器顶部硼结晶。清除完硼结晶后发现：在反应堆压力容器顶部，3号CRDM管座下滑的位置，存在一个被腐蚀的大孔穴。孔穴从管座处扩展约18cm，最宽处宽度约15cm，深16.8cm。腐蚀延伸到封头基材，最终到达封头内名义厚度为1cm的不锈钢堆焊层。约10cm范围内不锈钢堆焊层出现向上鼓起1.5cm，表明运行时在反应堆冷却剂系统（RCS）在15.2MPa的工作压力下，不锈钢堆焊层已经屈服。

WEBSITE http://www.chinansc.cn/

背景介绍

压水堆核电厂反应堆压力容器封头，依照ASME规范由低合金钢制成，内表面堆焊一层不锈钢。压力容器封头装有69个贯穿管座，其中61个用于控制棒驱动机构CRDM，7个备用，1个作为压力容器封头排气管。每个管座外径约为4英寸（101.6mm），其材料为镍基合金（Alloy600），相关的焊接金属为合金82或182（Alloy 82/Alloy 182），相邻管座中心距约为12英寸(304.8mm)。在压水堆电厂的一回路冷却剂和运行应力作用下，这些镍基合金会在焊接位置出现裂纹，这个过程被称为“一回路冷却剂应力腐蚀开裂PWSCC”。

1990年以来该电厂就已多次发现CRDM泄漏问题，但管理层未重视，修改检查大纲对缺陷部位进行检查。



定级说明

准则	说明
2和3实际后果	本事件无实际后果。
始发事件频率	按照潜在事件评级，如果该缺陷导致有关部件失效，就会发生大的失冷事故（“不大可能的始发事件”）。
安全功能有效性	对于这个假想的始发事件来说，安全功能有效性“全部可用”。
初步定级	按照处理结构缺陷的方法，使用表4的A3，给出初步定级的上限值为2级。由于腐蚀孔穴离封头不锈钢堆焊层只剩1cm厚度，虽然封头没有实际失效，但失效的概率非常大，因而不对初步评级降级。
附加因素	1990年以来该电厂就已多次发现CRDM泄漏问题，但管理层未重视，没有修改检查大纲对缺陷部位进行进一步检查，反映其安全文化存在问题，故提高1级。
最终定级	3级

二、特定核设施中事件的评级

适用范围

反应堆
- 停堆期间
- 退役期间

研究堆

核燃料循环设施

加速器
- 直线加速器
- 回旋加速器

生产和运输放射性同位素的设施

使用I类放射源的设施

厂区其他事件，如废物贮存或维护设施

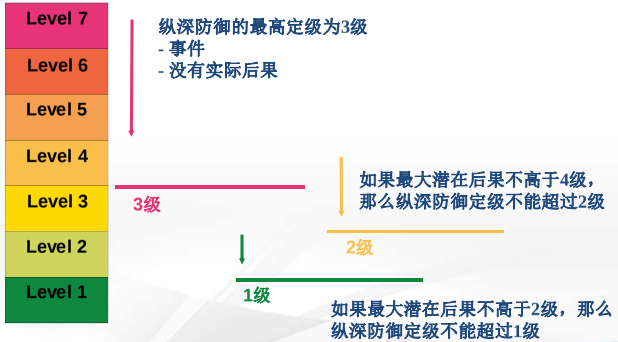
纵深防御定级的方法论

确定事件定级的上限：根据最大潜在后果

初步定级：根据对安全保护层的挑战和安全措施的降级

最终定级：根据附加因素

上限



确定最大潜在后果

本评定方法所涵盖的装置中，放射性物质的总量和事件的时间跨度存在很大差异。定级过程确定了三类最大的潜在后果：5-7级、3-4级和1-2级。
在对最大潜在后果进行定级时，应考虑下述总原则：

① 任何一个厂址都可能含有若干座设施，每座设施执行着各种不同的任务。最大潜在后果不是仅限于所发生的事件，而是适用于在设施内进行的所有操作。

② 必须考虑事件可能涉及的放射性总量、相关物质的物理和化学性质，以及放射性可能扩散的机制。

③ 应考虑如果与该事件相关的所有安全措施都有缺陷的话可能发生的事故。

④ 在考虑工作人员受照的后果时，最大潜在后果通常应以个体受照情况为基础，因为若干工作人员全都受到最高可信水平的照射的情况极不可能发生。

举例说明：

(1)对于与维护屏蔽室入口联锁装置相关的事件，最大潜在后果可能与工作人员的计划外照射有关。如果进入屏蔽室，并且没有采取任何缓解措施，辐射水平高到足以导致确定性效应或死亡，那么最大潜在后果的定级为3级或4级。

(2)对于发生在小型研究堆（即功率约为1 MW或更低）中的事件，尽管存在着放射性存量大量扩散的物理机制（临界事件或燃料丧失冷却），但放射性总量很小，以致即使所有的安全措施都失效，最大潜在后果的定级大概也不会高于4级。

(3) 对于动力堆停堆期间发生的事件，存在着放射性存量大量扩散的物理机制（通过冷却剂丧失或临界事件），如果所有安全措施都失效，最大潜在后果的定级可能会超过4级。

(4) 对于后处理设施和其他钚化合物处理设施，存在着放射性存量大量扩散的物理机制（通过临界事件、化学爆炸或火灾），如果所有安全措施都失效，最大潜在后果的定级可能会超过4级。

(5) 对于铀燃料制造和浓缩装置，其释放可能具有化学和放射学方面的安全问题。必须强调的是，氟和铀的毒性造成的化学风险超过了放射性风险。但事件分级只考虑放射性危害的评价。因此，铀或铀化合物的释放不会造成超过4级的严重后果。

(6) 对于加速器，最大潜在后果可能与计划外的个人照射有关。如果辐射水平足够高，以致当人员进入限制区时可导致确定性效应甚至死亡，那么最大潜在后果的定级为3级或4级（根据第2.3节的个人剂量准则）。

(7) 对于辐照装置，大部分事件将与计划外的照射有关。当所有的防护行动均失效时，如果潜在的辐射水平足够高，以致导致确定性效应甚至死亡，那么最大潜在后果的定级为3级或4级。对于拥有防止放射性物质扩散的安全系统（例如消防系统）的Ⅰ类放射源设施，如果发生事件，潜在的释放可能相当大，足以产生高达5级的最大潜在后果。

安全保护层

- ✓ 确保设施安全的安全措施即为“安全保护层”，如联动装置、行政措施、操纵员行为、规程等。
- ✓ 安全保护层是一些非能动的设计、能动的部件或行政控制措施，包括监督程序。
- ✓ 确定剩余安全保护层的数量及有效性，同时考虑每个安全保护层的完整性。

确定安全保护层的数目

确定安全保护层

对涉及各种安全措施的事件进行定级的基本方法，是将各种安全措施分成单独的和独立的安全保护层。因此，如果2个单独的信号是通过一个联锁装置传送的，那么这2个信号与联锁装置一起构成一个安全保护层。另一方面，如果冷却功能是由2台独立的100%容量的泵提供的，则应视为2个独立的安全保护层，除非它们共用一套非冗余的支持系统。

在考虑将**行政管理措施**作为安全保护层时，如运行或应急规程，须核对程序的独立性，以及程序的可靠性。准备和执行该规程的可用时间，对规程的可靠性具有重要影响。

- 独立性：核对可将单独的程序视为独立程序的**范围**；
- 可靠性：核对程序的可靠性是否足以被视为一个安全保护层。

包容

在某些情况下，包容本身即构成一个或多个安全保护层，但是使用时必须要慎重。如上述中所说，定级过程就是将最大潜在后果判定为以下三个类别之一：5-7级、3-4级和1-2级。

如果在其他安全措施失效后包容系统能够发挥作用，并将最大潜在后果降低到一个较低的水平，那么可以将包容系统看成是一个安全保护层。另一方面，如果包容的效果不足以改变最大潜在后果的类别，则不宜将其作为附加的安全保护层。

高完整性安全保护层

在某些情况下，可能存在着**高完整性的安全保护层**，例如：

- 合格的燃料转运容器
- 反应堆压力容器
- 基于经过验证的自然、非能动的安全措施，如对流冷却

在这些情况下，由于这些安全保护层已被证明具有极高的完整性或可靠性，因而在运用这一指导时，采用与其他安全保护层同样的方式来对待显然是不合适的。

行政管理措施通常满足不了高完整性安全保护层的要求，但如果有很长的时间可以用于采取纠正行动，并且有各种选择，那么某些操作规程也可视为高完整性安全保护层。

※如果只剩下一个安全保护层，但它符合高完整性安全保护层的所有要求那么初步定级定为分级表以下/0级是比较合适的。如果安全保护层的可操作性超出了许可限值，可以定为1级

高完整性安全保护层

特征：

- 能应对所有相关的设计基准故障；
- 在设施安全正当性中被确认需要极高水平的可靠性或完整性；
- 通过适当的监测或检查能识别出完整性的任何降级；
- 有明确的手段应对已发现的安全保护层降级，通过预定规程或较长的可用时间。

可用时间

- 在某些情况下，执行纠正措施的可用时间或许明显大于所需时间，因而可以利用附加的安全保护层。
- 如果有执行所需行动的规程，那么就可以考虑这些附加的安全保护层。
- 如果安全保护层的不可用时间与安全保护层部件的定期试验间隔相比非常短（例如在月度试验中某个部件的不可用时间为若干小时），应考虑降低该事件的初步定级。

安全保护层方法

上限: 确定最大潜在后果

初步定级: 确定剩余安全保护层的数目，根据下表确定初步定级

最终定级: 考虑附加因素

剩余的安全保护层数目	最大潜在后果[a]		
	（1） 5、6、7级	（2） 3、4级	（3） 2级或1级
A 3个以上	0	0	0
B 3	1	0	0
C 2	2	1	0
D 1或0	3	2	1

a这些级别不能因为附加因素而提高，因为它们已经是纵深防御的上限。

结构缺陷

定级方法：

- 首先，应假定缺陷已导致部件失效，运用前述的指导对潜在事件进行定级。
- 然后，应根据缺陷将导致部件失效的可能性，以及考虑附加因素，对定级进行调整。

如果缺陷在可接受范围之内，评定为**分级表以下／0级**是合适的。

附加因素

利用始发事件方法和安全保护层方法确定了事件的**初步定级**。有些特殊的情况可能会同时挑战纵深防御的不同层次，因此将其作为比初步定级提高一级的附加因素。

- 附加因素是那些预示着纵深防御严重降级的方面：
  - 共因失效
  - 规程有问题
  - 安全文化缺陷
- **初步定级最大能够提高1级**

共因失效

共因失效是指由于单一特定的事件或原因引起的多个设备或部件无法执行其功能。特殊性在于它能引起预定要执行相同安全功能的多重部件或设备失效。这可能意味着整个安全功能的可靠性比预期的低得多。因此，

- 一起影响一个部件并确定为可能影响其他类似部件的共因失效事件的严重性要高于部件随机失效事件。
- 由于缺乏信息或误导信息而引起的某些系统运行困难事件也可以考虑根据共因失效提高级别。

规程有问题

由于规程有问题，可能会同时要求几个纵深防御层次起作用。因此，这种规程问题也有可能成为提高初步定级的原因。（例如：1979年的三里岛事故期间就发生过这种情况。在安全注入已经启动的情况下操纵员使用的程序对于稳压器汽相冷却剂丧失的特殊情况并不适用）。

- 给运行人员发出的应对某起事件的指令错误或不合适；
- 监督大纲中的显著不足：
  - 通过常规程序不能发现的异常；
  - 系统／设备的不可用时间远远超出试验间隔

安全文化缺陷

安全文化的定义是“存在于单位和个人中的各种特性和态度的综合，它建立一种超出一切之上的理念，即核电厂的安全问题由于它的重要性要保证得到应有的重视”。（INSAG 4对安全文化有更详细的介绍）

- 良好的安全文化有助于预防事件的发生；
- 缺乏安全文化，有可能导致运行人员不按设计要求去做；
- 如果安全文化存在缺陷，可能会导致事件级的别提高1级；
- 事件必须被看做是存在安全文化问题的一个实际指标。

① 违反运行限值和条件

安全文化缺陷中最容易定义的一个指标是违反运行限值和条件。

运行限值和条件描述的是能使反应堆的运行维持在安全要求之内的最低限度安全系统可用性，也可以包括反应堆在安全系统可用性已经降低的条件下进行有限时间的运行。大多数国家将运行限值和条件列入技术规格书中。此外技术规格书还描述了一旦运行限值和条件未满足要求时需采取的行动，包括允许修复和后撤的时间。

如果运行人员故意采取了导致电厂可用性超出运行限值和条件范围的行动，则由于有安全文化缺陷，应该考虑提高该事件的初步定级。

② 其他的安全文化缺陷

安全文化指标的另外一些例子包括：

- 未经事先批准违反程序；
- 质量保证过程存在缺陷；
- 人因差错重复发生；
- 一名公众在一起事件中受到的照射超过法定年剂量限值；
- 工作人员或公众受到的累积照射超过法定年剂量限值；
- 未能对放射性物质保持严格控制，包括环境释放、污染扩散或剂量控制系统失效；
- 某种事件重复发生，是否表明营运单位在初次事件发生后既没有给予足够的重视以吸取教训，也没有采取纠正措施。

验证定级

- **小事件**

0级：无安全意义（OL&C 内的较小偏离）

1级：超出运行许可范围（OL&C）的异常

- **安全层的显著降级**

2级：安全措施明显失效的事件

3级：接近事故—安全措施全部丧失，再有一个失效就会导致事故

用安全保护层方法分析特定事件的指导原则

1. 反应堆停堆期间冷却系统失效的事件

大多数反应堆的安全系统用于处理功率运行期间发生的始发事件。热停堆或启动工况下的事件与功率运行中的事件十分类似，因此应按照始发事件方法进行定级。

一旦反应堆停堆，只需要一部分安全系统来确保安全功能，通常有较长的时间可以利用。另一方面，从多重性或多样性的角度来看，在这一段时间里，人员采取的行动可以部分替代安全措施。

反应堆停堆期间采用安全保护层方法定级。定级主要考虑因素包括：可用的冷却系列的数目、可用于采取纠正措施的时间和用于冷却压力容器的任何管道的完整性。

2. 影响乏燃料水池的冷却系统故障事件

运行数年以后，乏燃料水池的放射性总量可能很高。在这种情况下，按照纵深防御准则对影响乏燃料水池的事件定级，定级范围可以从0级一直到3级。如果事故造成放射性向环境释放，则根据放射性释放总量评级，级别可定为4级或4级以上。

由于水装量很大，同时衰变热相对较低，通常有很多时间来采取纠正措施处理有关乏燃料水池冷却恶化的事件。因此，乏燃料水池冷却系统有点小毛病或小的泄漏是典型的分级表以下／0级事件。

运行工况不符合运行限值和条件、温度的急剧上升或乏燃料水池冷却剂水位急剧下降，应定为1级事件。

冷却剂大面积沸腾或燃料元件开始裸露可以定为2级事件。燃料元件明显大面积裸露应定为3级。

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

3. 临界控制

按照一般的指导原则：

- 在许可限值内对临界安全规范的微小偏差，应定为分级表以下／0级。
- 超出许可限值的运行至少应定为1级。
- 如果安全措施进一步失效或设施条件稍有改变就会发生临界事件，而且最大潜在后果为3级或4级，那么该事件应定为2级。如果最大潜在后果可能为5级或更高，那么该事件应定为3级。
- 如果仍然有一个以上的安全保护层起作用，那么定为较低的级别是合适的，应使用安全保护层事件定级表（表11）来确定相应的级别。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

4. 屏蔽区域门的联锁

一般通过在门上安装辐射剂量控制联锁装置、使用进入批准程序以及进入前的辐射剂量率检查来防止误入通常屏蔽的场所。
屏蔽门联锁保护装置失效可能是由于失电和/或探测器故障、有关的电子设备故障或人为失误造成。

这类事件的最大潜在后果限制在4级，因此发生安全措施失效可能造成事故发生的事件应定为2级。在一些措施已经失效但附加安全保护层（包括管理进入许可的行政管理措施）仍然有效的场合发生的事件，通常应定为1级。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

5. 装卸事件和重物跌落

① 不涉及燃料组件的装卸事件
装卸事件或起吊设备故障的影响，取决于所涉及的材料、事件发生的地点，以及受影响的或可能受到影响的设备。

在跌落的重物可能造成放射性物质泄漏，事件的定级应考虑最大潜在后果和发生这种泄漏的可能性。在跌落的重物只引起有限的损坏、但引起更坏后果的概率较大的情况，事件应按照纵深防御原则定为最大潜在后果的最高级别。

在设施寿期内预期会发生的较小的装卸事件，应定为分级表以下/0级。

WEBSITE http://www.chinansc.cn/

② 与燃料装卸有关的事件

在装卸新的铀燃料元件时，发生不涉及装卸乏燃料的事件，并且该事件对乏燃料元件或安全相关设备没有造成损坏的风险，那么该事件是典型的分级表以下／0级事件。

对于乏燃料的装卸，单根燃料元件的放射性贮量显然要比乏燃料池或堆芯的放射性贮量低得多，因此最大潜在后果也较低。对于在设施寿期内预期会发生的事件，只要不影响乏燃料元件的冷却且只造成少量释放或不造成释放，那么该事件就是典型的分级表以下／0级事件。

涉及以下几种情况的事件应考虑定为1级：

- 设施寿期内的非预期事件；
- 运行工况超出许可限值；
- 冷却能力的有限降低不影响燃料元件棒的完整性；
- 燃料元件棒的完整性受到机械损伤，但冷却能力没有降低。

对于因燃料元件的显著升温而导致燃料元件完整性受到损害的事件，定为2级可能是合适的。

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

6. 电源丧失

为了给厂外电源丧失或厂内供电系统失效的事件进行定级，要考虑仍然有效的电源的范围、断电持续时间和最大潜在后果。特别重要的是必须要考虑恢复供电前允许的持续时间。

对于某些设施来说，即使持续几天完全断电也不会给安全造成不利的影响；这些设施中的这类事件一般应定为分级表以下/0级或1级，因为在可用时间内应该有多种手段用于恢复供电。如果安全系统的可用性一直超出许可限值，则定为1级是合适的。

来自普通电网的供电部分丧失或全部丧失，但能从备用系统获得供电，这是在设施寿期内“预期”会发生的事件，因此应定为分级表以下／0级。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

7. 火灾和爆炸

在设施内或临近地区发生的火灾或爆炸，只要没有影响任何安全措施降级的可能性，就可以排除在分级表之外或定为分级表以下／0级。由安装的防火系统扑灭的火灾，应定为同样的级别。

如果造成任何安全系统降级，则定级取决于最大潜在后果，以及留存的安全保护层的数目及其有效性，

由规程不完备或安全文化差所导致的涉及低放废物的火灾或爆炸，均应定为1级。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

8. 污染物未经许可释放或扩散

根据安全文化缺陷（“未能对放射性物质保持适当控制”）的规则，将因放射性物质转移而使区域的污染水平超过调查水平的任何事件定为1级是合适的。导致区域的污染水平高于许可限值的事件也应定为1 级。对比较严重的安全措施失效进行定级，应考虑假定所有安全措施都失效时的最大潜在后果和剩余安全保护层的数目来确定。

违反许可限值进行排放的事件至少应定为1 级。

WEBSITE http://www.chinansc.cn/

9. 剂量控制

有时，当放射性控制规程和管理措施不当，可能会出现工作人员接受计划外的照射（内照射和外照射）的情况。根据安全文化附加因素“未能对放射性物质保持适当控制”的规则，这类事件可定为1 级。如果事件导致的累积剂量超过许可限值，由于违反了许可限值，那么该事件至少应定为1 级。

一般来说，附加因素的指导原则不应该用于提高与剂量控制失效有关的事件的初步定级为1 级的事件。否则，就会发生未造成剂量的事件被定为与实际已引起显著超剂量限值的照射事件一样的级别。但是，如果没有或只有1 个有效的安全保护层，且安全措施时效导致的最大潜在后果为3 级或4 级，那么按纵深防御准则定为2 级是合适的。

10. 通风、过滤和净化系统的失效

在处理大量放射性物质的设施中，可能会设置多达3个单独的但又相互关联的通风系统。在不同容器、屏蔽室／手套箱和操作区之间维持一个压力梯度，同时保持足够的流量通过屏蔽室操作区界墙上的缝隙，来阻止放射性物质的反向扩散。此外，设置了净化系统，如高效微粒空气（HEPA）过滤器或涤气器，以使向大气的排放减少到预先规定的限值以下，并阻止反向扩散到较低活度水平的区域。

给失去这些系统的事件定级时，第一步是确定所有安全措施失效时的最大潜在后果。这就应当考虑放射性物质的总量及其在设施内外扩散的可能方式。还必须要考虑惰性气体浓度减小或爆炸性混合物积累的可能性。在大多数情况下，除非可能发生爆炸，否则最大潜在后果不大可能超过4 级，因此按纵深防御原则的最高级别将是2 级。

第二步是确定留存安全保护层的数目，包括通过停止工作以防止产生更多放射性的规程。

11. 外部灾害

诸如外部火灾、洪水、海啸、外部爆炸、飓风、龙卷风或地震等的外部灾害事件，可按其他事件相同的方法，通过考虑留存的安全措施的有效性来定级。

对于灾害防护专用系统失效的事件，应评估安全保护层的数目，包括灾害在系统不可用期间发生的可能性。对于大多数设施而言，由于这类灾害事件预期发生频率低，因此定级不宜超过1级。

12. 冷却系统失效

重要冷却系统失效应采用和电气系统失效相似的方法定级，考虑最大潜在后果、留存安全保护层的数目、以及恢复冷却的可用时间。

在高放废液或钚贮存冷却系统失效的情况下，对于相当长时间内仅剩一个安全保护层的事件，可能定为3级是合适的。

实例 1 由冷却剂压力升高引起的停堆冷却丧失

事件描述

停堆冷却由冷却剂经两条单独的吸入管线进入两台余热排出（RHR）热交换器。循环提供，其中每条吸入管线上各有2个隔离阀。每条管线上的阀门由单独的压力传感器控制，并可在控制室远程操作。此时，一回路是封闭的，蒸汽发生器还可用，用以确保由余热排出功能丧失后升温变得十分缓慢。安全注入不可用，高压安注泵（HPSI）已与上充泵隔离，卸压阀则可用于控制一回路压力。

事件为冷却剂压力升高导致隔离阀关闭。控制室报警通知运行人员隔离阀已关闭，降低压力后阀门重新打开。温度没有超过运行限值和条件中规定的上限值。

定级说明

准则	说明
2和3实际后果	该事件无实际后果。
最大潜在后果	发生在反应堆停堆期间事件的最大潜在后果是5-7级。
确定安全层数	有4个硬件保护层确保蒸汽发生器可用，而且有充裕的时间用于采取必要的行动，甚至足以允许实施对RHR系统的维修。由于有很长的时间可供使用，因此重新打开阀门的操作可被视为比一个安全层次更加可靠，并且所有4个安全层次均可被认为是独立的。
初步定级	根据表，定为分级表以下／0级。
附加因素	无附加因素
最终定级	分级表以下／0级

实例 2 由压力传感器误动作引起的停堆冷却丧失

事件描述

停堆冷却是由冷却剂经装有2个隔离阀的一根吸入管道进入一台余热排出（RHR）热交换器循环提供的。阀门可在控制室进行操作。一回路是打开的，腔内充满水。反应堆已停堆一周，因此冷却剂的任何升温将非常缓慢。蒸汽发生器因工作需要已经打开，因此不可用。安全注入不可用，高压安注（HPSI）泵已与上充泵隔离，卸压阀则可用于控制一回路压力。

压力传感器假动作，引起隔离阀关闭。控制室报警通知运行人员隔离阀已关闭，经核实压力升高是假信号后重新打开了阀门。温度没有超过运行限值和条件的上限，大约需要10个小时才能达到运行限值。

准则	说明
2和3实际后果	该事件无实际后果。
最大潜在后果	发生在反应堆停堆期间事件的最大潜在后果是5-7级。
确定安全保护层数量	就余热导出这一安全功能而言，有2个安全保护层。第一个是RHR系统；第二个是可用于补水的时间很长，需要补水主要是因为水和热量会通过蒸发损失掉，需要补水以保持水位。 以下原因可认为第二个安全保护层是一个高度可靠的安全保护层： – 有很长时间可供采取行动（达到运行限值至少需要10个小时） – 可采取多种方法添加更多的水（例如低压安全注入，消防水管），但必须控制硼的浓度。 – 在安全论证中，这个安全保护层是公认的一个关键安全装置。 此外，如需要的话，有充裕的可用时间实施对RHR系统的维修。
初步定级	定为分级表以下/0级。
最终定级	分级表以下／0级

实例3 核电厂期间全厂失电12分钟事件

事件描述

2012年2月9日，核电厂1号机组处于换料大修冷停堆阶段，三路厂外电源（一路来自主变，两路来自辅变）只有一路来自主变的电源正常连接，其他两路来自辅变A、B的电源处于检修状态，两台应急柴油机之一处于检修状态，另一台处于备用状态，第三台柴油机处于手动启动状态。

2月9日20点39分，一个工人在执行发电机出口断路器的电气保护试验时，犯了一个错误，导致供应厂外电源的主变高压侧开关误跳，全厂丧失厂外电。此时，备用应急柴油机由于异物导致空气启动电磁阀打不开，应急柴油机启动失败，核安全相关设备失去电源，包括堆芯冷却和乏燃料水池的冷却。12分钟后，恢复来自主变的厂外电源，各系统和设备很快恢复正常功能和状态。断电期间，堆芯冷却剂温度从36.9℃升高到58.3℃，乏燃料水池水温从21℃升高到21.5℃。

该事件后果：没有安全影响，没有放射性物质释放。

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

定级说明

准则	说明
2和3实际后果	该事件无实际后果。
最大潜在后果	发生在反应堆停堆期间的事件的最大潜在后果是5-7级。
确定安全保护层数量	余热排出系统是唯一的硬件安全保护层，但由于全厂断电丧失。剩下的一个软件安全保护层是依赖运行人员通过规程恢复供电。但由于一回路温度上升较快，约1小时后将沸腾，留给运行人员的可用时间不多，因此该安全层不能看作是一个高完整性的安全保护层。
初步定级	根据表6，本事件的初步定级是3级。
附加因素	无
最终定级	3级

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

谢 谢！

WEBSITE
http://www.chinansc.cn/

核电厂人因事件发生的机理及数字化仪控对人因可靠性的影响

2018年核设施经验反馈专项培训班

核电厂人因事件发生的机理及数字化仪控对人因可靠性的影响

邹衍华　博士

人因工程与安全管理研究所
湖南工学院
2018.3.6

Outlines

1. 研究团队简介
2. 核电厂人因事件发生的机理
3. DCS对人因可靠性的影响
4. 人因失误预防综合建议

1 研究团队简介

湖南工学院　人因工程与安全管理研究所

- 所长：张力教授
- 现有固定及流动研究人员21人，其中教授6人、副教授11人、讲师4人（多学科背景交叉互补）
- 博士及硕士研究生20余人
- 国家核安全局技术支持单位
- 荣获多项国防科工委及湖南省科技进步奖
- 是国内最早一批开展核电领域人因可靠性研究的专业团队

主要研究方向

- 人因可靠性分析
- 防人因失误与安全管理
- 人机系统（界面）评价与优化
- 人误数据采集与数据系统开发
- 作业绩效评估与提升
- 系统安全分析与安全人机工程

主要应用领域

- 核电厂
- 电力系统
- 大型复杂人机系统/工业企业

团队所承担的国家自然科学基金项目

- 复杂人-机系统中人员可靠性研究(1995)
- 人因事故分析理论与方法研究(1998)
- 人误分析技术及应用研究(2002)
- 考虑组织与管理因素的人因可靠性分析方法及应用（2005）
- 复杂工业系统数字化对人因可靠性的影响（2008）
- 大规模数字化控制系统中人的认知行为研究（2010）
- 数字化工业系统人因可靠性分析方法研究（2013）
- 核电厂数字化主控室操纵员情境意识可靠性研究（2013）青年
- 核电厂数字化主控室操纵员作业行为动态可靠性分析方法研究（2015）青年
- 核电厂数字化主控室操纵员班组情境意识可靠性研究（2016）
- 功率持续快速变化下核电厂操纵员人因可靠性分析方法研究（2017）

团队所承担的部分国防军工项目

- 复杂人-机系统中人员可靠性研究(1995)
- 核电站人员可靠性基础研究(1994)
- 反应堆系统人因事件分析与预防方法(2000)
- 人因可靠性技术（2002）
- 人误因素辨识与原因分析技术研究（2005）

团队所承担的环保部核与辐射安全监管项目

- 运行核电厂日常运行和大修监管活动中人因类技术支持及研究（2010,2013,2014,2015,2016,2017）

团队所承担的工程项目

- 大亚湾核电站：人因可靠性分析（1998-1999）
- 岭澳核电站： 人因可靠性分析(2000-2001)
- 秦山核电站：人因可靠性分析(2001-2003)； PSR中人因安全因素评审（2001-2004）
- 秦山第三核电站：人因可靠性分析（2007-2009）
- 中广核核电运营公司：岭东核电站DCS+SOP人因可靠性分析（2010-2014）
- 华东电网：高级调度中心人因可靠性研究（2010-2011）
- 中广核工程公司：主控室人机界面评价（2010）
- 中船重工701所 ：×××人因可靠性分析方法（2012-2013）
- 中国航天员科研训练中心（2017）

实验平台

- 人因工程实验室拥有200余台套仪器设备，其中10万元以上的大型仪器设备30多台套，仪器设备总值1000余万元，系统建立了人体生理测量、工程心理学、人体三维测量与仿真、动作捕捉与作业行为与分析、认知测试与分析、人机界面设计与评估、产品可用性测试、作业绩效分析、疲劳测试、工业控制系统仿真、眼动轨迹追踪与脑电测试等系统。

科研平台

- 大型复杂人机系统人误预警技术湖南省工程实验室
- 国家能源核电运营及寿命管理技术研发中心—安全人因工程实验室
- 湖南省自然科学基金创新研究群体“大型复杂人-机系统人因可靠性研究”
- 湖南省应用基础研究基地
- 湖南省科技厅产学研创新平台

Outlines

1. 研究团队简介
2. 核电厂人因事件发生的机理
3. DCS对人因可靠性的影响
4. 人因失误预防综合建议

2 核电厂人因事件发生的机理

- 对核电厂这一类的大规模复杂社会-技术系统而言，必须对系统可能发生的失效/人因失误进行广泛深入的研究，以预防和减少灾难性事故的发生。
- 随着科学技术的发展，系统变得更加复杂和自动化，但不管系统自动化程度有多高，人在系统的设计、安装、操作和维修等过程中依然发挥重要的作用。
- 系统的自动化程度以及软硬件的可靠度不断提高，降低了设备的失效率，但却提高了人的相对失误概率。
- 从根本上来说，在技术可靠性已得到显著提高的情况下，引发严重事故的主要原因还是人因失误及未能预见的自然灾害。（三哩岛核事故、切尔诺贝利核事故、福岛核事故）

- “当今世界工业企业事故中，约有 85%以上的事故直接或间接源于人的因素”；
- “由于人的不安全行为而导致的事故占事故总数的70 %～90 %”；
- “大亚湾核电厂和秦山核电厂运行经验反馈也显示人因失效事件在执照运行事件中占有很大的比重，约为75%”.....
- 通过国家核安全局经验反馈平台收集了313份运行事件报告，经过分析、筛选，其中有162份属于人因事件，人因事件率为51.76%
- 通过WANO数据库收集了1364份事件报告，经过分析、筛选，其中有878份属于人因事件，人因事件率为64.37%
- 因此，人因失误已成为引发核电厂事故的最根本的原因之一。

2.1 人因失误的概念

- “认为作用于系统的人的行为没有或没有充分满足系统的要求就称为人误。”—Rigby 该定义严格根据系统的要求进行定义，没有考虑到人的自身局限性，也没有考虑人的认知失误。
- “人误就是超出系统可接受的界限范围的人的任何一个动作。”—Swain & Guttman；“能够或有可能引发不期望事件的所有人的行为或疏忽。”—Swain；由 Swain 的定义可知，人已被看作是技术系统中的一个组成部分。
- “当人的行为超出系统可接受的限度，那么该行为就是人误”—Leplat

--上述定义都是从工程应用角度根据系统的性能限制来定义人因失误的。

- “人误就是计划中的心理和身体行为序列在执行后没能达到意向中的结果，并且这种失效不能归因于随机触发因素的干扰作用”—Reason
- Reason 认为人是技术系统中的一个信息处理组分，该定义是从心理学角度进行定义的。尽管该定义想尽力从人的角度来定义人误且尽量包括人的认知失误，但它还是没有考虑到人的局限性。
- “人误一直存在于工作系统中，它具有引起工作系统处于非期望或者错误状态的特性，它的产生导致系统需求处于没有满足或未能充分满足的状态，个人是工作系统的一个组分，并与工作中的其他组分相互作用，工作系统中的所有成分相互依赖，相互影响。”—Sträter
- 该定义从技术系统的局限性和人的局限性两方面对人误进行了定义，但也没有涉及所有的人误。

- 根据上述多个定义，可知人误的定义是多种多样的，人们看待问题的角度不同就有不同的定义。不管如何定义，人因失误一般具有以下三个基本的性质：

✓ 人工操作是一个有组织的机体，它像系统的硬件和软件一样具有失效率与容许度。

✓ 人误包括隐性失误(认知失误)和显性失误(行为失误)。隐性失误是导致显性失误的原因之一，也是人误分析不可或缺的重要组成部分，如进行失

人因失误 vs 人为失误

✓ 人误

后果来判定某

误。

- 简而言之，人误就是人的认知失误和行为失误，人的认知功能和行为响应没有达到正确和预期的标准。人误主要有如下一些特点。

✓ 人的失误的重复性。人的失误常常会在不同甚至相同条件下重复出现，其根本原之一就是人的能力与外界要求的不匹配。人的失误不可能完全消除，但可以通过有效手段尽可能地避免；而一般的部件或设备，一旦发现失效原因，往往可以通过修改设计加以克服。

✓ 人引发的失效的潜在性。大量事实说明这种潜在失误一旦与某种激发条件相结合就会酿成难以避免的灾难。（三哩岛事故）

✓ 人的失误行为往往是情境环境(Context)驱使的。人在系统中的任何活动都离不开当时的情境环境。硬件的失效、虚假的显示信号和紧迫的时间压力等的联合效应会极大地诱发人的不安全行为。

✓ 人的行为的固有可变性。人的行为的固有可变性是人的一种特性，也就是说，一个人在不借助外力情况下不可能用完全相同的方式(指准确性、精确度等)重复完成一项任务。起伏太大的变化会造成绩效的随机波动而足以产生失效，这种可变性也是人员发生错误行为的重要原因。

✓ 人因失误的可修复性。人因失误会导致系统的故障或失效，然而也有许多情况说明，在良好反馈装置或人员冗余条件下，人有可能发现先前的失误并给予纠正。此外，当系统处于异常情况下，由于人的参与，往往可以得到缓解或克服，使系统恢复正常工况或安全状态。在核电厂概率安全评价(PSA)中，人的恢复因子的计算直接影响核电厂风险值的结果。

✓ 人具有学习的能力。

2.2 人因失误机理与模型

- 对历史灾难性事故原因的认识，经历了从技术、人误到组织错误这样一个认识过程。
- 最初针对技术失效发展的故障树和事件树分析技术，能模拟事故的发展历程，但缺乏分析的指导性框架，不同的分析人员可能得到不同的分析结果。
- 三哩岛核电站事故之后，认为灾难性事故的产生源于人误，人被看作是问题的起源，并对人误开展了广泛的研究，发展了各种***人因失误模型***来描述***人因失误机理***。
- 大致可归结为：个体失误模型、班组失误模型、组织错误模型以及复杂社会-技术系统模型。

➢个体失误模型

- 个体失误模型是对单个人的心智过程分析的建模研究。
- 这些模型属于“人因失误方法”(Person approach)，偏重对单个人因失误机理的描述。
- 如 Rasmussen 的决策阶梯(Step-ladder)模型和技能-规则-知识级模型、Reason 的通用失误模拟系统、Hollnagel的简单认知模型，Rouse W.B 和 Rouse S.H 的操作员行为模型以及何旭洪等建立的核电厂操纵员认知行为模型等。
- 由于人的固有局限性，决定了人在不同条件下行为的不确定性和随机性，而现今发展的个体失误模型都是基于假设和经验建立起来的，对操纵员的复杂认知过程的认识可以说不尽人意。

➢班组失误模型

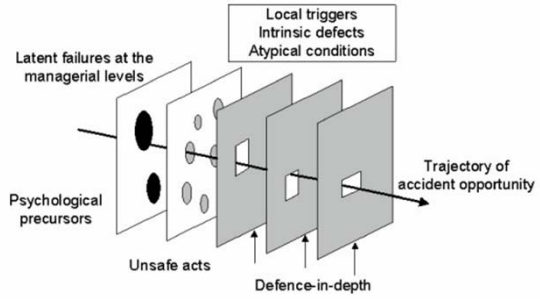
- 高风险组织的很多工作都需要班组成员共同完成，需要整个班组的协同诊断和决策。因此，在评价这类系统的安全和可靠性时需要考虑班组行为绩效。
- 班组失误模型偏重于将班组成员看作一个整体，对其认知机理和行为可靠性进行研究。
- Sasou和Reason对班组失误进行了定义和分类，并对班组失误与行为形成因子之间的关系进行了讨论。
- Rouse 等发展一个具体的心理模型，对班组交流、协作与班组绩效做出原理性解释提供了基础。

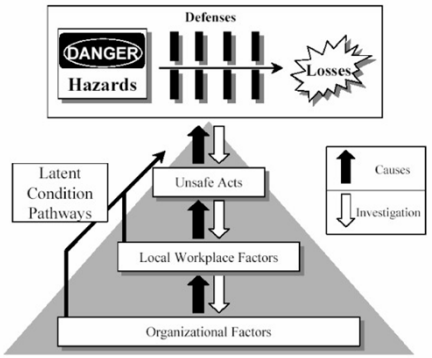
- Sasou K 等结合核电站模拟机，定性研究了非正常状态下作业人员失误与检查人员、管理人员决策能力之间的关系，建立了班组行为仿真系统模拟班组决策过程并对班组行为进行了分类。
- Shu Yufei 等开发了一个班组行为模型。它包括四个子模型，即任务模型、事件模型、班组模型和人-机界面模型，以此来确定班组认知处理的情境环境。
- [illegible]决策(D)和执行(A)，对班组内部交互和影响进行了[illegible]化。

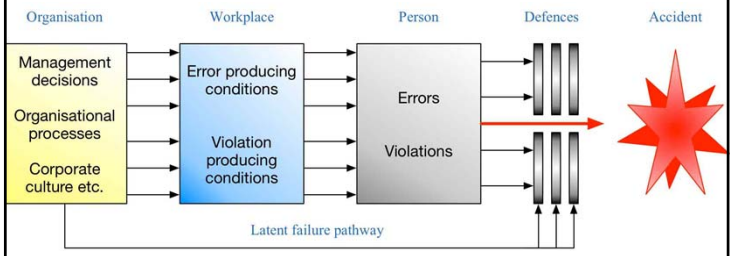
上述对班组认知行为机理和失效的研究只停留在面上，对班组的认知和交互过程进行了简化，因而没有进一步深入到班组的复杂机理和可靠性研究。如只考虑影响班组绩效的某个方面(如班组交流)，对于班组认知行为的解释也只是静态的，没有考虑到外部和内部环境的动态易变性，即班组可靠性具有时变性。

➢组织失误模型

- “人误是结果，不是原因，人误的产生是由其上游的因素—工作环境和组织因素引起的”—Reason
- 复杂技术系统安全的主要关注点已由硬件失效和单个的人误转移到组织管理领域内的潜在失效，并发展了各种系统方法(System approach)，如典型的被广泛采用的 Reason 的组织事故因果(瑞士饼)模型，该模型能很好地模拟出组织事故中各事件之间的相互关系，有助于识别组织事故的根原因。
- 但是该模型没有对模型中的各组分(如组织的潜在错误、不利的工作条件、不安全行为等)进行详细的分类，只给出了大概的分析框架，没有对各模块中的因素之间的因果关系进行说明，也没有说明“屏障”存在何处？屏障如何被突破？并且没有对“人的方法”和“系统方法”进行有效整合。



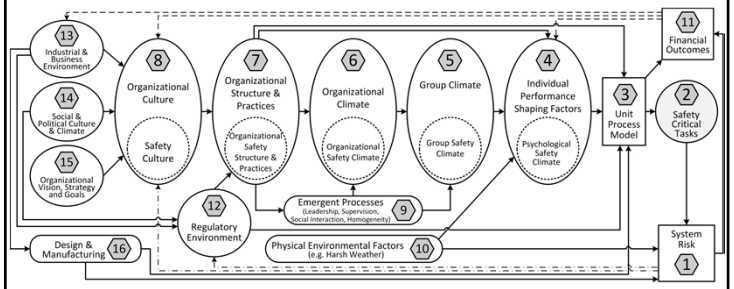




➢复杂社会技术系统模型

- “事故因果是一个涉及整个社会-系统的复杂过程，应该包括最高层的立法者、政府部门到最低层的员工”—Rasmussen
- Rasmussen 建立的社会-技术系统模型主要由六个层级组成，即政府、安全委员会或研究学会、公司、管理部门、员工以及工作组成。
- Leveson N.从系统论和控制论的角度建立了一般的社会-技术系统模型。模型由系统开发和系统运行阶段共两部分构成，每一部分由若干层级构
- 上述模型及分类对于识别复杂社会-技术系统的因果机理做出了贡献，但是模型中各组分的构成过于粗糙，更具体的系统中各组分的因果关系还需进一步研究，缺乏人因失误与组织情境环境之间的因果对应方面的研究等。

的风险或危[illegible]，并将它们分解成包括人、软件、硬件以及环境因素等更为具体的风险贡献因素。



Socio - Technical Risk Analysis (SoTeRiA) Theoretical Framework

2.3 人因失误分类

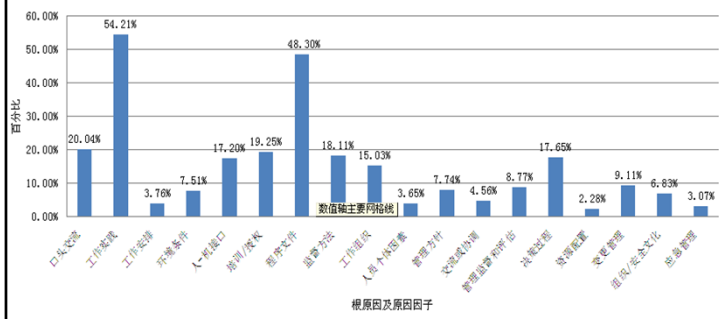
- 人因失误的分类方法/体系，总体上来说，可以分为两大类：一类是工程分类法，一类是认知行为分类法。
- Meister分类，将人因失误分为设计失误、操作失误、装配失误、检查失误、安装失误和维修失误等。
- Swain 将人因失误行为分为执行型错误（Error of Commission, EOC）和遗漏型失误（Error of Omission, EOO）。EOC是指某项任务或步骤没有正确执行，或者是执行了某项错误任务或任务不需要的动作；EOO指人在完成一项任务时忘记并遗漏遗漏整个任务或遗漏任务中的某一项或几项。

- Rasmussem 提出的S-R-K模型，技能型（Skill-based），规则型（Rule-based），知识型（Knowledge-based）。
- 技能型失误：指在我们的能力范围之内，也是在我们熟悉的、经常性的工作中出现的失误，是一种无意识的行为疏忽或过失。导致这类失误的原因通常是熟悉的环境和频繁的日常工作使大脑处于放松状态，注意力未集中在当前的工作上，或注意力仅集中于某一点而忽视其他方面。
- 规则型失误：指执行根据经验、培训或书面指令积累而成的程序时出现的失误，程序型失误又可分为 3 种类型：不恰当的程序（程序本身有问题）、程序的错误运用（程序是对的，使用方面有问题）、不遵守程序。
- 知识型失误：指在从事超出了我们知识范围的工作中出现的失误，主要发生在工作人员无章可循却需要做出决定或判断时。

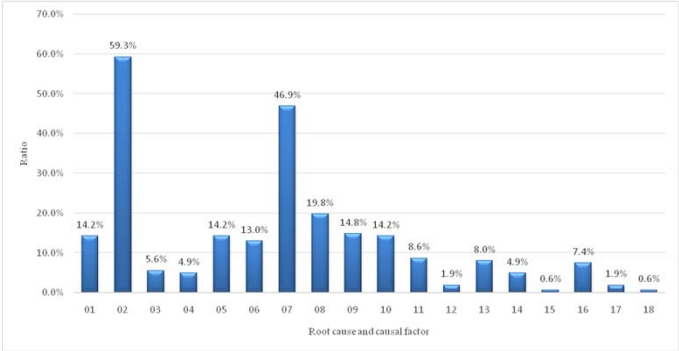
- Reason以关系分类法的观点，在Rasmussem的SRK模型基础上，用概念法提出一种概念分类方案，将所有的失误分为偏离（slip）、疏忽（lapse）、错误 (mistake)。
- Reason将人的失误归于两大类：①执行已形成意向计划过程中的失误，称为疏忽和过失；②在建立意向汁划中的失误，称为错误或违反。疏忽和过失常常发生在技能型动作的执行过程中，主要是因为人丧失注意力或由于作业环境的高度自动化性质所导致。错误往往比较隐蔽，短时间内较难被发现和恢复，当面对与自己已形成的判断或概念不相容的信息时，往往会给予排斥，坚持先前的观点或决策，因此，错误的恢复途径比较困难，也是要着力加以防范的失误类型。
- 在考虑人对系统失效的贡献中，Reason将失误分为两类：①激发失误，它对系统产生的影响几乎是立刻和直接的；②潜在失误，它可能在系统中潜伏较长时间，往往与设计人员、决策人员和维修人员的行为有关。

2.4 诱发核电厂人因事件的主要因素

- 采用WANO提供的根本原因和原因因子分类体系，对所收集的人因事件进行分析。
- 人员行为相关因子。该因子包含口头交流、工作实践、工作安排、环境条件、人-机接口、培训/授权、程序文件、监督方法、工作组织、人员个体因素10个方面。
- 管理相关因子。该因子包含管理方针、交流或协调、管理监督和评估、决策过程、资源配置、变更管理、组织/安全文化和应急管理 8 个方面。
- 设备相关因子。该因子包含设计配置和分析、设备技术规范/制造和安装、维修/实验/监督、设备性能4个方面。



各类根原因及原因因子所占比例（WANO）



各类根原因及原因因子所占比例（国内）

- 对比两部分的数据发现，人因事件主要是由工作实践、程序文件、培训/授权等几个因素促成。
- 造成人因事件发生的主要原因为：未严格执行操作监护制度、未有效实施自检、未开展独立验证、没有遵守相应的沟通交流规程、工前会对程序的审查和风险的分析不足、缺乏严谨的工作习惯和质疑的工作态度、与程序不一致时没有采取独立的验证工具、规程缺失不足、人员的工作实践经验不足。

- 此外，对所收集的样本数据分布进行了相关性分析、聚类分析，以及关联规则挖掘后，发现以下现象和结论。

✓ 口头交流同工作实践、工作组织，环境条件同交流或协调，培训授权同监督方法、管理监督和评估、应急管理、管理方针，人员个体因素同资源配置，这些因素间表现出较为明显的相关性，尤其是培训授权与管理相关的四个因子间所表现出来的紧密联系更进一步说明良好的培训是便捷有效管理的基础。

✓ 口头交流、工作实践、程序文件这3个因素非常重要，并且它们经常捆绑性地同时出现。这说明，如果核电厂拟进行其中某一方面的改进工作，就必须同时考虑其他与之关联性很强的因素，否则其改进很可能无效。

✓ 培训授权受到多因素的制约，培训工作是一个系统性的工作，只靠单一的措施是不行的，需要多方面的支持。

✓ 聚类分析发现，工作实践、程序文件这两个因素无论是在聚集为几类时都是独自成为一类，这与其在各年度根原因统计中所具有的高比例性相关；工作安排与人员个体因素、交流或协调等几个因素聚为一类说明好的工作安排计划应该充分考虑人员个体因素，班组协调沟通能力；由于人机接口设计不合理或者人系统界面设计不友好所导致人因事件在各年度均占有较大的比例，而好的工作组织和监护方法将大大降低这类人因事件的发生，所以人机接口、工作组织、监督方法这几个因素聚为一类。

✓ 相关性分析发现，（1）对于一些具体的任务，如果没有明确的规程或文件指引，并且操纵员缺乏工作实践，则很容易导致人因事件的发生，这时很容易激发“工作实践”和“培训授权”两个因素之间的负效应；（2）人机接口设计不良，加之操纵员缺乏工作实践，很容易造成人因事件，特别是在数字化主控室；（3）在操纵员个人技能不足的情况下，没有适用的文件和程序会加速人因事件的发生；（4）紧急情况下，如果缺乏明确的规程指引，则操纵班组需要对系统当前状况进行足够的沟通交流，否则很可能会导致事故的发生。

Outlines

1. 研究团队简介
2. 核电厂人因事件发生的机理
3. DCS对人因可靠性的影响
4. 人因失误预防综合建议

3 DCS对人因可靠性的影响

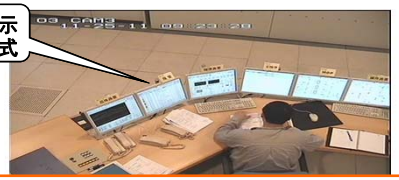
- 依托“岭东核电站DCS+SOP人因可靠性分析”项目，以及国家自然科学基金项目（70873040，71071051，71371070，71301069），从2010年1月至2014年12月，历时五年，项目组在岭澳2期核电站开展的DCS+SOP-HRA研究。

- 研究背景：
- 数字化控制系统（DCS）的采用使得核电站的运行控制更加集中化、自动化与精确化，提高了系统的效率与安全性。但是DCS也带来了较基于模拟技术、传统控制系统新的、更复杂的与更深层次的人因问题，如：主控室人机接口更加多样化且高度集中；操纵员作业任务、作业模式、作业负荷和作业行为发生巨大变化；运行班组结构及其运行机制较模拟主控室有显著差异。

- 事故处理规程也在原理、结构等方面发生了重大变化，如由基于单一事件的事件导向法事故规程EOP（Event Oriented Procedures），发展为基于电厂系统物理状态的状态导向法事故规程SOP（State Oriented Procedures)。
- 核电厂主控室数字化以及采用新的事故规程后引起的以上变化，势必导致新的人因可靠性问题，给操纵员操作带来潜在不利影响，可能出现新的失误模式与风险。
- 以下主要介绍DCS后操纵员的认知行为变化以及失误模式的变化、DCS-MCR人员绩效的主要影响因素、DCS-MCR团队合作/班组交流。

3.1 DCS vs 模拟技术主控室的技术变化：人因相关

- 显示方式
- 报警方式
- 操作规程
- 控制方式
- 人-机界面



显示方式

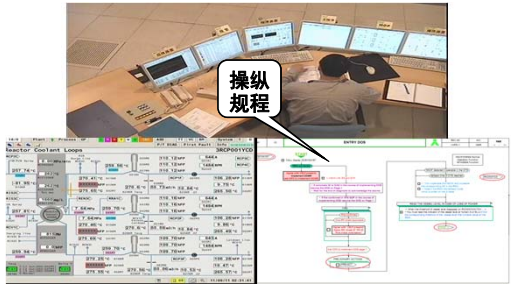
- **传统系统----基于模拟技术**
  - 测量仪表
  - 模拟图
  - 记录仪
- **数字化系统----基于计算机技术**
  - 操纵员工作站VDU，主控室大屏幕
  - 运行参数，流程图，操作画面
  - 画面显示采用多种导航形式

- 显示方式
- 报警方式
- 操作规程
- 控制方式
- 人-机界面

报警方式

- 数字化报警系统更具灵活性和多样性

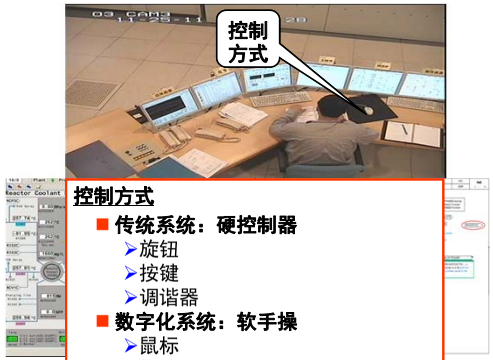
- 显示方式
- 报警方式
- 操作规程
- 控制方式
- 人-机界面



操作规程

- 传统系统：纸质打印文档
- 数字化系统：电子化/计算机化

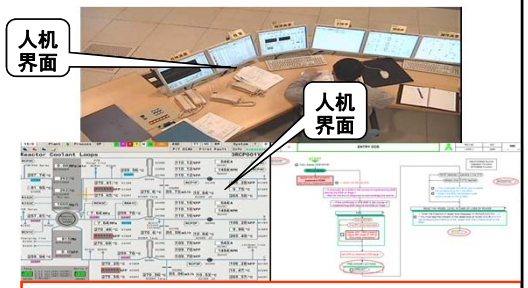
- 显示方式
- 报警方式
- 操作规程
- 控制方式
- 人-机界面



控制方式

- 传统系统：硬控制器
  - 旋钮
  - 按键
  - 调谐器
- 数字化系统：软手操
  - 鼠标
  - 软按钮
  - 软控制器

- 显示方式
- 报警方式
- 操作规程
- 控制方式
- 人-机界面



人-机界面

- 人-机接口多样化
- 人-机接口高度集中
- 信息容量比传统界面大很多倍
- 传统人-机界面发展为人-系统界面

数字化主控室给人因带来至少五个方面变化

- 人-机界面→→人-系统界面
- 作业模式
- 认知行为
- 运行组织结构和运行机制
- 人误模式和机理

□较传统的自动化系统新的、更复杂、更深层次的人因问题

- 国际共识：
  - 需要探索DCS下人因可靠性规律
  - DCS需要新的HRA方法

✓ 2016年10月2日-7日，在韩国首尔举行的的第13届国际概率安全评价及管理会议上，应邀在**HRA Special Session**中，报告了与该研究有关的工作，引起了国际上许多研究机构和学者的关注。“Human Reliability Analysis for Digitized Nuclear Power Plants--Case Study on LingAo II”

✓ 2017年11月，维也纳，IAEA组织召开的技术研讨会“Technical Meeting on the Development of the Safety Report on Human Reliability Assessment for Nuclear Installations”，并代表中国作题为“HRA for Digitalized MCR in China”的技术报告。

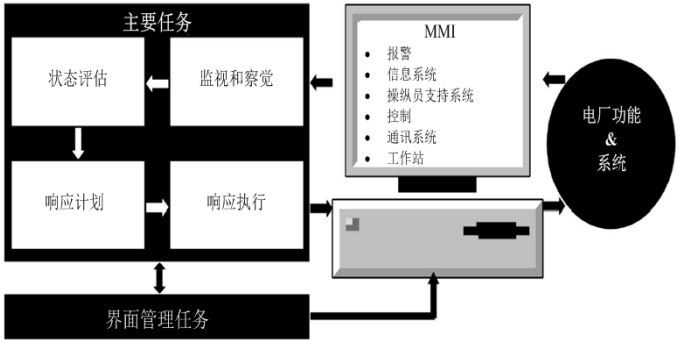
3.2 DCS操纵员认知行为变化与特征

- DCS操纵员需要完成两类任务
  - 第一类任务

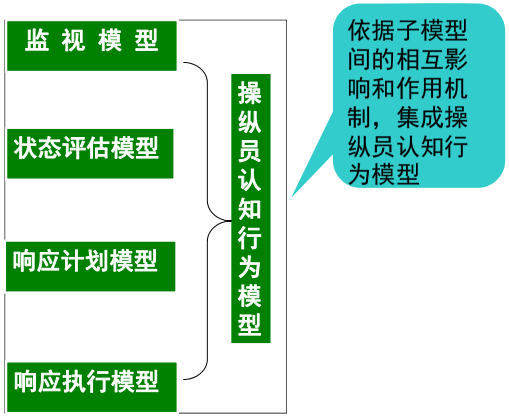
    操纵员直接为监控系统运行而需完成的任务：监视/检测、状态评估、响应计划、响应执行
  - 第二类任务

    不直接监控系统运行的那些任务：界面管理任务，包括浏览与访问信息，数据搜索，页面配置与管理等
- 两类任务有着不同的工作模式和认知行为模式
- 界面管理任务支持和保障完成第一类任务，同时与第一类任务也相互交互，产生了额外的认知负荷和操作负荷。增加新的人因失误源，可能出现新的人误模式，如模式混淆、情境意识丧失

DCS操纵员认知行为过程



■ DCS中人的认知行为模型



- 核电厂主控室数字化（DCS）以后，人机界面发生了巨大变化，操纵员获得信息的方式和获得的信息的显示方式发生改变，引致操纵员获取、储存、加工和输出信息的方式发生改变，即操纵员的认知行为亦发生较大改变。主要有：

✓ DCS中操纵员的认知负荷与传统控制室相比有较大的变化；人员在操纵员班组中的作用和功能发生变化；操纵员班组成员之间的交流机制和交流方式改变；操纵员执行规程的行为模式发生了改变。

✓ DCS人机界面扩大了操纵员可用数据的来源，提供给操纵员更多系统可用信息，操纵员亦可更加灵活地对信息进行组合以判断系统的状态，从而DCS降低了操纵员收集和整合信息的认知负荷。经过培训后，操纵员可以很快地适应新的人机界面。

✓ DCS中操纵员角色转变成监视性控制。操纵员认知行为过程包括四个阶段：监视/察觉，状态评估，响应计划和响应执行。

✓ 为了完成以上四个阶段的认知任务，DCS中，操纵员需要执行界面管理任务。这新增的界面管理任务产生了额外的认知负荷和操作负荷，增大操纵员发生人因失误的机会，如模式混淆、情境意识丧失。

✓ 由于界面管理任务带来的认知负荷，操纵员在执行主任务过程中常常自动地实施一些操纵策略，带来新的风险，如对信息进行核实的意愿降低；采取特定的操作等。

✓ 班组在事故处理中为了实现信息共享，增加了操纵员的交流，也增加了操纵员交流过程中的失误机会。

✓ DCS较模拟控制系统中，知识型行为增加，执行型失误增加。特别是DCS中，由于呈现给操纵员的信息的显示、信息布局和信息量等更加容易导致疏忽型失误。

✓ 操纵员具有很强的偏好，如习惯性地忽略规程步骤，同时操纵员执行规程中跳项的现象大量存在。

✓ DCS至少在5个方面对操纵班组产生了影响：班组绩效，班组交流，情景意识，电子规程和二类任务管理。

✓ 操纵员在执行SOP过程中，监视部分和响应执行部分的工作负荷均显著高于状态评估和响应计划，而监视与响应执行间无显著性差异，状态评估与响应计划间也无显著性差异。同RO1相比，协调员除响应执行阶段工作负荷略低于RO1外，其余各阶段工作负荷均高于RO1，从协调员自身看，四个认知阶段的工作负荷无显著性差异。

- ✓ 在岭澳2核电站，由于操纵员基于工作站工作，其操作行为难以被其他操纵员观察（除非操作失误并有信息反馈），操作存在监管缺失，由此造成的人因事件相对有所增加。
- ✓ 对操作绩效的主要影响因素：屏幕管理，系统复杂性，交流干扰，系统画面或规程中内容呈现的有限性，操作员对系统的熟悉程度，规程标记，DCS下的系统问题，班组和操纵员水平。

DCS操纵员行为观察与分析

- 数据来源
  - 主控室现场观察---10余个运行班
  - 模拟机培训观察--- 2011年至2014年，20个运行班组（20×5×6小时）
  - 模拟机培训录像分析---60小时
  - 模拟机实验---4个序列
  - 实验室实验---数十项
  - 事件报告和小偏差报告---500余份，人因小偏差400余个
  - 访谈和问卷调查---100余次

- 有研究认为数字化控制室会导致交流模式的改变，而这些改变会产生交流减少的负面影响。但从分析结果来看，DCS下班组人员交流或许有所减少，但其交流效率可能会更高。在做重要行为决策时，班组中存在较多的交流。
- 操纵员使用的屏幕和系统画面相对较多且切换频繁，界面管理任务占用了操纵员较多的注意力资源并对操作绩效产生影响，增加失误概率，养成良好的界面管理习惯对提高操作效率是有益的。
- 规程标记。共记录到标记次数476次，失误11次，尽管从数据上看失误率只有2.3%，但由于数据采集手段的不足，真实的失误率肯定会更高，更为重要的是，规程标记需要在紧张的事故处理过程中频繁的在多个屏幕之间移动，且在屏幕间切换时会有一点延时，对操作员操作效率产生影响。

界面管理任务对一类任务的影响

- 界面管理占用了大量时间，增加了工作负荷

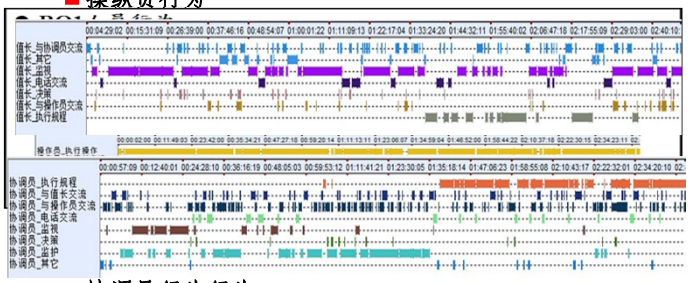
  某电厂主控室值长反映：事故状态下DCS界面管理占了50%的时间
- 通过模拟机观察和操纵员访谈，发现：

  1）操纵员对于界面管理任务普遍存在一定的畏避心理。

  2）操纵员似乎不太愿意按照设计者的思路进行二类管理任务的执行，而是采取自己认为有效的策略。

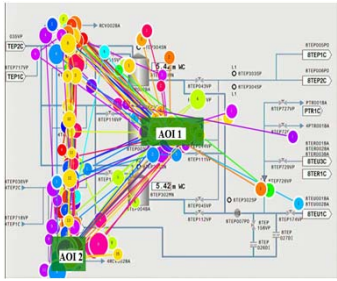
■ DCS操纵员行为观察

- DCS主控室人员行为观察分析
  - 操纵员行为

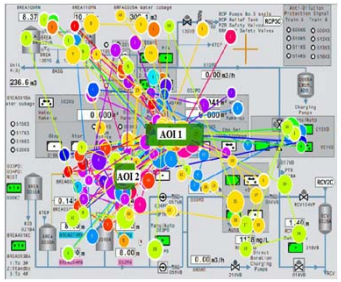


  - 协调员行为行为

■ 颜色和形状特征显著眼动分析

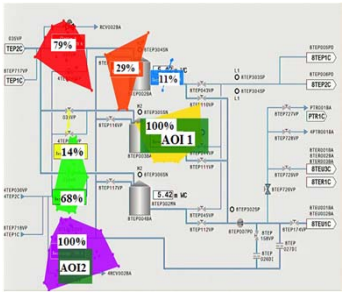


打开TEP界面中被试注视轨迹图

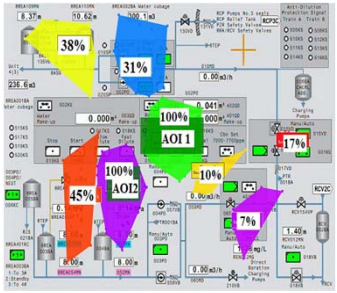


打开REA界面中被试注视轨迹图

■ 颜色和形状特征显著眼动分析

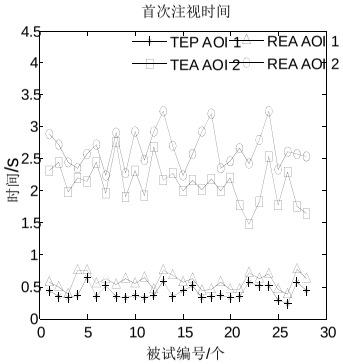


打开TEP界面集簇图

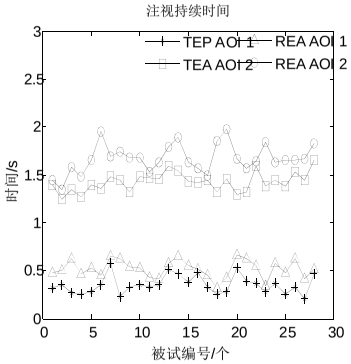


打开REA界面集簇图

■ 颜色和形状特征显著眼动分析



不同被试在REA界面对AOI 1和AOI 2首次注视时间



不同被试在TEP界面对AOI 1和AOI 2首次注视时间

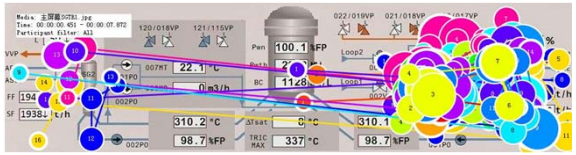
■ 培训效果分析

LOCA事件培训前被试注视热点图

LOCA事件培训后被试注视热点图

■ 操纵员监视行为测试

●SGTR1事件培训后所有被试注视点路径图



●TEP界面眼动轨迹图

■ 监视转移失误实验

图 3.1 数字化主控室操纵员操作平台

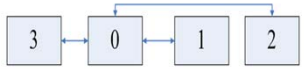
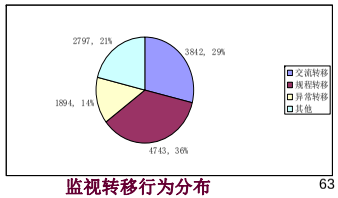


图 3.2 操纵员屏幕间转移过程示意图

表 4.3 稳态视觉注意力向量

规程页面	屏幕 0	屏幕 1	屏幕 2	屏幕 3
PRE-ACT	0.56	0.21	0.17	0.06



监视转移行为分布

- 监视行为转移类型及分布。对岭澳2核电站4个班组16名操纵员，每班3小时，共20个班次，总计60个小时的操纵行为进行观察、访谈，总共观察到13276次监视转移，对所获得的数据进行分析，发现操纵员的监视行为主要存在三种转移类型：规程转移、异常转移、交流转移。
- 规程转移是指基于系统操作规程的转移，异常转移是指系统发生异常后报警信号或参数变化引起的监视转移，交流转移是指基于班组其他成员的提醒而发生的监视转移。
- 这3种转移类型所占总转移次数的百分比分别为：交流转移29%、异常转移14%、规程转移36%，不能归入前三种类型的转移占21%。

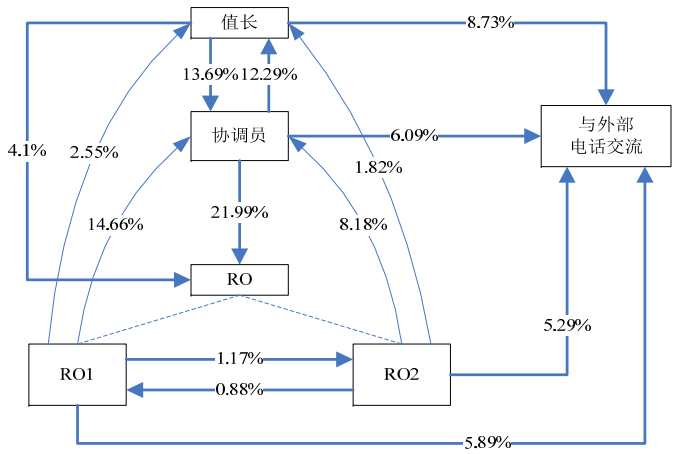
- ✓ 交流转移较为均匀地分布在整个班次运行过程中。当电厂处于复杂事故状态时操纵员进入复杂事故操纵而执行SOP规程，此时主控室操纵员及主控室外工作人员需要进行更多的信息交换，交流转移的次数略有增加。
- ✓ 规程转移占总转移量的比例最高，达36%。电厂处于正常运行状态和小故障运行状态时，规程转移出现的次数较少；当电厂处于复杂事故状态时，主控室操纵员要执行大量有关SOP规程的工作，此时会出现大量的规程转移。
- ✓ 异常转移的次数较少，仅占总转移量的14%。异常转移随机分布在整个班次运行周期之内。异常转移虽然次数较少，但发现并解决异常状态是操纵员非常重要的工作，故异常转移在监视转移类型中具有重要地位。

- ✓ 其他形式的转移在电厂处于正常运行状态和小故障运行状态时次数较多，而在电厂处于复杂事故状态时略有减少。虽然其他形式的转移所占数量较多（21%），但其对操纵员与电厂的影响却远远不及规程转移、异常转移与交流转移。
- ✓ 在数字化主控室中，由于纸质规程更多是起到补充DCS系统中规程的不足或扩充DCS显示屏显示信息量的作用，故屏幕内规程转移的次数远远高于屏幕外规程转移的次数。
- ✓ 电厂处于复杂事故状态时，RO1、RO2都会执行SOP规程。由于RO1在此期间执行规程的工作较RO2更为重要，而RO2较RO1需要更多的兼顾监视、稳定系统状态的工作。故此时RO1的规程转移量高于RO2，RO2的异常转移量高于RO1。

3.3 DCS-MCR团队合作、班组交流

- DCS引起主控室运行班组组织结构、运行机制变化
  - 运行班组构成，成员间关系
  - 操纵员任务分配机制
  - 班组成员之间的交流机制和交流方式
- 讨论：
  - 班组结构
  - 成员职能
  - 交流网络与频度
  - 交流内容特征
  - 主要交流模式
  - 交流失效分布/特征
  - 交流模式对人误的影响

- 交流网络与频度。有研究认为数字化控制室会导致交流模式的改变，因为传统控制室要走到操纵员身边，而现在在各自的工作台，就可以访问到需要的由数字化系统共享的系统信息，这些改变会使得交流减少。但从观察分析结果来看，DCS下班组人员交流或许有所减少，但其交流效率可能会更高。在做重要行为决策时，班组中存在较多的交流。他们通过各自的方式从不同的视角监视系统获取信息，通过交流很好的形成一个团队，分工明确。



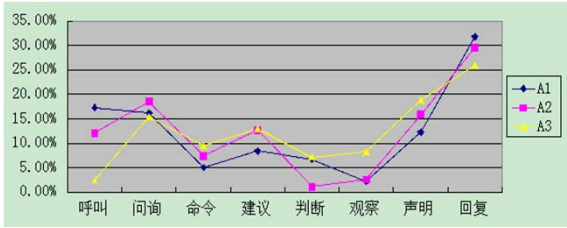
- 交流内容、交流方式、交流及时性是影响运行班组成员间交流有效性的三大因素。
- 操纵班组在事故状态下执行SOP规程时交流的主要内容是电厂状态参数、系统功能和设备、规程。其中，参数交流所占比例最大（超过40%），体现了SOP状态导向、非针对特定事故的特征，也揭示出在DCS下操纵班组的交流内容更关注团队的控制目标，即电厂的状态及其特性参数。而参数控制目标的实现依赖于系统功能和设备的动作，故其在交流比例中为第二位（超过20%）。
- 主要交流模式为呼叫、问询、声明、回复，另外还有命令、判断和观察，但使用很少。其中，呼叫模式主要与规程相关，问询模式与参数、系统功能和设备、规程三者均相关。

- 交流模式对人因失误的影响主要包括：因“呼叫”的缺失导致信息接收者对交流请求的忽视，交流请求的重复造成任务执行的延迟（如造成监视和规程判据信息获取的延迟）；对参数“问询”，“判断”，“观察”性交流不足增加了操纵员的注意力资源负担，导致操纵班组对电厂情境意识的不足，影响了操纵班组的决策；对参数的“声明”和“回复”不足影响操纵班组的响应计划和执行（对电厂控制目标的及时评价和操纵班组对下一步工作目标的规划和重要步骤的协同一致）。对系统功能和设备的“判断”性沟通不足造成“命令”性指令的目标冲突并影响操纵员的自主操控过程。

■ 班组成员主要交流模式--- 实验结果（1）

➢ A工况下各操纵班组沟通模式

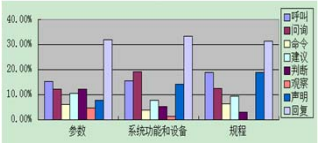
1）各组沟通类别的总分布结果



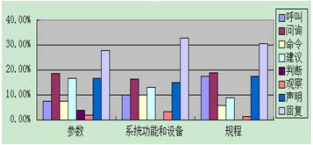
A1，A2，A3各组关于沟通的功能类别分布趋势具有相似性。“问询”，“建议”，“声明”，“回复”是各组主要的沟通类别，“命令”，“判断”“观察”类别在各组中的分布比例较低。各组关于沟通类别的分布比例并不完全一致，

■ 班组成员主要交流模式--- 实验结果（2）

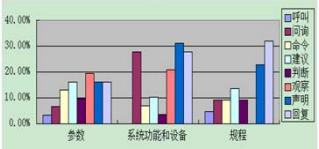
A工况下各操纵班组沟通模式
2）各组沟通主题的类别分布结果



A1



A2



A3

从A1，A2，A3沟通主题的分布特征中，我们发现：参数的沟通类别特征主要为“建议”，“判断”和“观察”；而系统功能和设备，规程的沟通类别特征主要体现在“问询”和“声明”。

3.4 人因失误模式变化

- 重点研究了DCS以后操纵员基于新的人机接口的低认知水平的人员行为，包括正常运行工况下的日常操作活动等基础人员行为，主要为 1) 操作失误；2)规程执行；3）交流通讯；4）巡盘监盘； 5）人机界面；6）看错输错；7) 报警响应等7类人员行为。同时也关注DCS中发生的具有更高意识水平的人员行为（KB行为）。
- 将人误类型归纳为5大类39种：监视/检测失误（7种），状态评估失误（5种），响应计划失误（3种），响应执行失误（6种），界面管理失误（18种）。

- 在监视阶段，主要失误模式为信息定位丧失、没有监视到、监视延迟和未能认识，引起这些失误的原因主要涉及“信息所在的画面被覆盖”、“需要的信息在画面中的位置不固定”、“信息之间的关联性由成百上千的一张张画面被分隔，操纵员看起来需要完成复杂的‘拼图游戏’一样来对信息进行关联”，这些数字化主控室的新特征增加了操纵员的认知负荷。，这也是操纵员不能遵从特定的行为规范的原因之一。
- 在状态评估阶段，主要失误模式为：状态的误解、未能对状态做出解释、不充分的解释和原因辨识失误。引发这些问题的原因主要包括人机界面的问题、技术系统的问题，特别是“巨量信息，有限显示”。
- 在响应计划阶段，主要失误模式有：计划跟随失误、计划选择失误，其主要原因在于时间压力。
- 在响应执行阶段有，主要失误模式有：目标定位错误、操作遗漏、调节失误、操作延迟、操作方向错误、不充分的信息交流、错误的信息交流。引发这些失误的原因涉及“人机界面问题，如画面的相似性”、“技术系统问题，如系统反馈延迟”、“由任务的复杂性和紧急性带来的负荷”、“班组结构，如变化的班组交流路径和角色”等。

Type	Proportion
Work Preparation	9.5%
File Management	15.8%
Work Practice	18.8%
Operation Error	6.7%
Procedure Performing	6.1%
Communication	10.7%
Panel Surveillance	4.2%
Human-Machine Interface	5.8%
Input error	1.2%
Alarm Response	2.1%
Others	19.1%

- 新人误模式1： KB-SLIP. 传统控制室人机界面的SB行为（技能级行为），如按按钮，旋动选择键等SB行为失误在DCS中有可能转化为需要较高意识水平的KB行为（知识级行为）。无论从产生的原因、还是从动作的表征来看，这一类行为失误不能归于Rasmussen的SLIP和LAPSE，这是在DCS中出现的一种新型的人因失误模式，命名为KB-SLIP。此类失误模式在DCS中发生频率较高（约占操作失误的17%）。
- 新人误模式2：事故状态下操纵员执行他自己以为是正确的动作，或者执行操纵员认为比自动设备更好的动作和引入不该引入的动作。此外还有页面配置失误、误点击鼠标、数据输入错误、目标识别失误与信息搜集失误等传统模拟技术主控室不存在的失误模式。
- 新人误模式3：误点击鼠标、数据输入错误、页面配置错误等。

- 操作失误模式分布发生变化。THERP手册认为，操纵员执行操作时的主要失误模式为EOO（error of omission，遗漏型失误）。但本项目研究数据表明，EOC（error of commission，执行型失误）占整体失误的59%，而EOO只占21%。由于DCS的显示操纵控制特征，执行型失误贡献较显著。
- 人误的原因发生变化。THERP认为，执行规程时EOO的原因往往是“规程过长”，研究发现，DCS中EOO的原因大部分是“执行规程的时间过长”，或者是“执行规程的形式复杂”，例如，别的成员或者班组已经执行完规程的某一部分，而新的班组继续接手执行。
- 界面管理任务对执行主任务和人误影响大。界面管理不当常常使得 “巨量信息，有限显示”对于操纵员变成“巨量信息，有限获得”，导致执行任务时操纵员所需要获得的某些信息被遗漏；界面管理任务确实增加了操纵员的工作负荷。另外，由于界面管理任务的存在，操纵员发生EOO和EOC失误的可能性有上升。EOO失误可能性升高的主要原因是需要的信息未能有效获得（被掩盖）；EOC失误可能性升高的主要原因是在错误的对象上进行操作。

Outlines

1. 研究团队简介
2. 核电厂人因事件发生的机理
3. DCS对人因可靠性的影响
4. 人因失误预防综合建议

4 人因失误综合预防建议

- 从人员个体因素角度；
- ✓ 从人机界面设计的角度；
- ✓ 从界面管理任务的角度；
- ✓ 从培训的角度；
- 从组织因素角度；
- ✓ 加强班组情景意识，形成主控室多层人因失误预防体系；
- ✓ 减少诱发人因失误情景的产生；
- ✓ 预防或减少失误的风险以及发生失误后的后果；
- ✓ 学习型组织；

4.1 从人机界面设计的角度

- 从人机界面设计的角度对人因失误预防，其主要目标是防止基于计算机软控制操作的人因失误，包括两个方面：软操作的信息显示和人 - 系统交互。
- 软控制操作的信息显示的人机界面设计需要满足以下几个目标：

1. 由于DCS中是多个操纵员协调操作，所以基于计算机界面的操作必须允许操纵员保持对他人操作的情景意识，以保证各个操纵员之间不会互相干扰。
2. 信息显示必须使得操纵能够迅速评价控制系统中的单个部件的状态，以及单个部件与其他部件之间的关系。
3. 操纵员必须能够清楚地辨识所操作的对象，包括其位置，大小，颜色，标识。

4. 操纵员能够从控制输入区域获得所输入的控制操作在系统中的反馈显示。
5. 对于就地现场及其他特定场合，界面设计必须能够满足操纵员在某种特定环境下对于信息的阅读和输入，例如，操纵员带手套或者操纵员穿辐射防护服的情况。

- 人 - 系统交互的人机界面设计需要满足以下几个目标：

1. 操纵员能够清楚地选定和判断所操作的区域和对象。
2. 操纵员能够实时地获得操纵员的操作的系统反馈，包括指令是否已经发出，系统是否在执行发出的指令，系统接受了指令是否响应，是否达到了操作的预期目标。
3. 系统响应时间。总的系统响应时间是指提交一个输入指令到获得系统反馈之间的时间。系统响应时间的设计会影响操纵员对于电厂的控制能力。

- 由于操纵员在计算机界面上的操作绝大多数是一种SB行为，所以操纵员的注意力和记忆力对失误的产生会有很大影响。
- 由于基于计算机人机界面显示狭窄，操纵员对计算机信息阅读和输入的空间维度单一，而电厂本身需要显示的信息或需要输入的操作类型复杂；除此之外，计算机界面的信息显示结构相对传统控制室复杂，信息获得更多的是模型驱动的，因此，在传统控制室人机界面中是属于低意识水平的SK和RB行为，（按键，旋钮或者移动调节点等），在DCS中有可能会转变成KB行为。
- 从人机界面的设计的角度而言，总的原则是尽量使得在DCS界面中的人员行为变成SB和RB行为，这就包括例如控件的布置，控件的大小设置，控件操作的反馈等的数量要小，布局要符合人员的习惯特征等。

4.2 从界面管理任务的角度

- 操纵员执行界面管理任务的行为属于SB或者RB行为，行为中的失误类型为SLIP或者LAPSE，行为失误的原因是由于操纵员在执行界面管理任务过程中记忆失误或者注意失误。
- 操纵员对于界面管理任务执行的方式或者执行的过程都非常熟悉，失误往往发生在操纵员处于高工作负荷的情况下，例如，工作计划安排紧或者在DCS执行事故处理。
- 界面管理任务的执行需要进行大量的屏幕选择及导航，因此，操纵员应该对屏幕选择和导航所在的数据空间的位置有一个清楚的即时判断。

4.3 从培训的角度

- 三大目标：
- ✓ 一是提高操纵员的基本技能，也就是SB和RB行为；
- ✓ 二是提高操纵员对于事故的处理能力，也就是培养操纵员如何使用好现有的人机界面系统来对事故进行处理；
- ✓ 三是培养操纵员班组各个成员保持共享情景意识的能力，也就是培养操纵员班组的交流通讯技能。

- ✓ 对于在传统控制室的一些基本操作，如按钮，读表，调节等，在数字化控制室中变成了导航，选屏，控件操作等。
- ✓ 传统控制室中固定的物理布局可以形成固定而且稳定的心智模型，而DCS中导航，选屏以及控件位置在计算机屏幕上灵活布置，这样不能形成稳定的心智模型。如果事故状态下，操纵员处在较高工作负荷的情况下，操纵员的人因失误发生的可能性要增大。
- ✓ 避免因工作负荷等原因而使得DCS缺陷被放大；
- ✓ 培训操纵员的交流技能，包括交流时机，交流手段，交流反馈等以提高操纵班组的情景意识；要特别注意强调值长和安工在保持整个运行班组情景意识方面的作用。

邹衍华
博士/副教授
人因工程与安全管理研究所 副所长
湖南工学院
Email：zouyanhua@163.com
电话：13974701136

认 识 根 本 原 因 分 析

中广核 CGN
核能服务 Nuclear Power Services
苏州热工研究院有限公司
Suzhou Nuclear Power Research Institute Co.,Ltd.

认识根本原因分析

——根本原因分析基本概述

二O一八年二月

© Copyright 2018 SNPI

自我介绍

姓名：关建军
单位：苏州热工研究院有限公司/设备管理部
/ 经验反馈与RCA研究所
工作职责：事件调查与根本原因分析
联系方式：0755-84476618
电邮：guanjianjun@cgnpc.com.cn

© Copyright 2018 SNPI

01 为什么要做RCA分析？

© Copyright 2018 SNPI

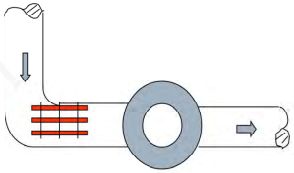
因果关系（因果律或原因链）

© Copyright 2018 SNPI

【案例】RRI泵叶片汽蚀及泵振动问题（来源：大亚湾核电站）

事件描述：

- 大亚湾核电站调试期间，发现RRI系统设备冷却水泵在LOCA流量下发生汽蚀现象，同时RRI水泵振动异常
- 当时分析认为振动与汽蚀是泵吸入口部分有漩涡所造成。在泵的入口管道安装内置式稳流器，以消除泵的汽蚀问题
- 但运行结果表明，稳流器无助于问题的解决

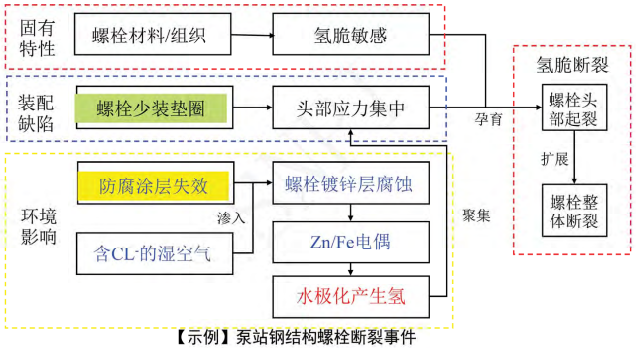


泵位置结构示意图

很多公司在设备发生故障后，都能够很快修复，但难以发现故障的根本原因，所以，类似故障会再次发生。

© Copyright 2018 SNPI

【案例分析】



【示例】泵站钢结构螺栓断裂事件

© Copyright 2018 SNPI

为什么做RCA分析？

- 识别引发事件的不安全行为或不安全状态
- 确定引发事件的管理体系、人的行为和设备存在的缺陷
- 制定纠正行动以防止事件重发

© Copyright 2018 SNPI

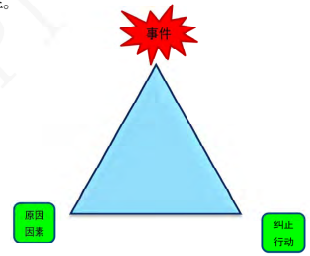
根本原因分析（RCA）

RCA分析是一套系统、科学和结构化的问题分析与解决方法。

RCA分析目的找出事件/问题背后的事实和真相，以制定适当和有效的纠正行动，防止事件重发或降低其发生的可能性。

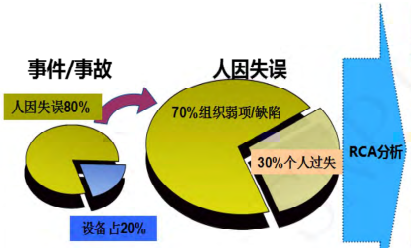
RCA分析用于确认：

- 发生了什么？
- 事件是如何发生的？
- 为什么会发生？
- 采取的措施？
- 是否可用防止事件重发？



© Copyright 2018 SNPI

根本原因分析



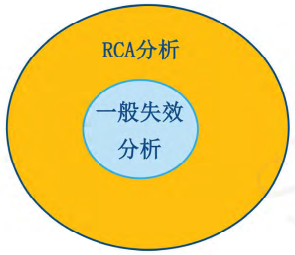
设备方面：
消除设备的潜在隐患，降低或避免故障的发生。通过RCA制定出更合理的维护策略，提高设备的可靠性。

人因方面：
明确人的失误机理和根本原因，有效防范并减少人因失误。

管理方面：
消除管理系统的缺陷，优化管理组织结构和提升安全文化水平。

© Copyright 2018 SNPI

RCA分析与一般失效分析的区别



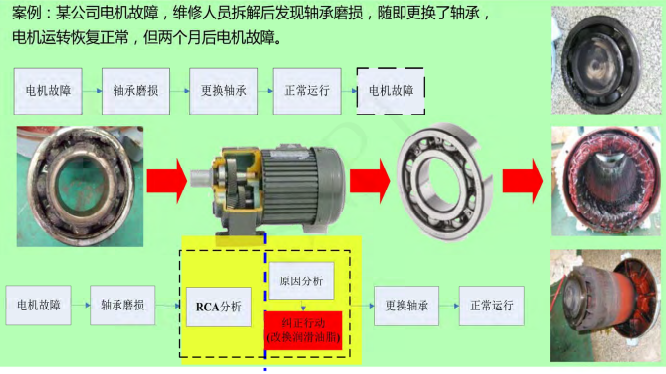
一般失效分析往往是针对事件给出单维度或单层级的分析，而非深层次、广范围的系统分析，缺乏有效的治本措施。

RCA 分析不只是注重故障与原因的内在关联，找出问题的根源与形成机理，还要在更高的层面上来解决问题，避免故障的重发。

RCA分析找出组织、系统或流程中及系统设计等存在的缺陷，并采取适当有效的纠正行动。

© Copyright 2018 SNPI

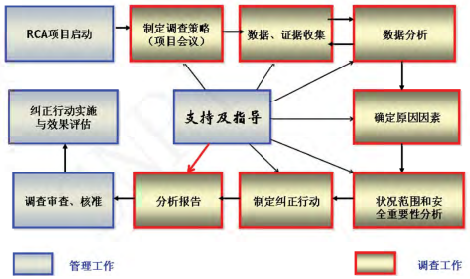
案例：某公司电机故障，维修人员拆解后发现轴承磨损，随即更换了轴承，电机运转恢复正常，但两个月后电机故障。



© Copyright 2018 SNPI

RCA分析特点

系统性：
RCA分析是一种系统性分析方法，有完整的分析体系和流程作指导。



© Copyright 2018 SNPI

RCA分析特点

规范性：

RCA分析从项目组织到完成故障模式鉴别等一系列活动，具有规范的操作流程，分析方法具有统一模式，便于理解和准确地评估。

序号	可能的故障模式	支持的证据	反对的证据	可能性
1	中间轴材料缺陷	无	轴材料分析与设计要求相符。	低
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
4	中间传动齿轮组安装缺陷	无	大小齿轮固定力矩正常，放松装置安装到位（解体未有松动），齿轮轴向窜动及其与曲轴齿轮的啮合间隙符合程序要求。	低
5	外部异物	无	在油箱底部仅发现齿轮碎片，未发现其它异物存在。	低

柴油机中间齿轮轴断裂原因分析

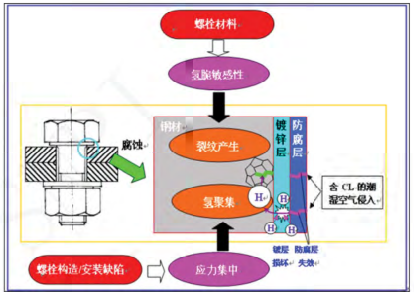
© Copyright 2018 SNPI

RCA分析特点

逻辑性：

RCA分析是深层次的因果关系链分析，注重探索事物的内在关联与发展机理，提供了一个鉴定和证实特定问题以及判定原因的逻辑思维方法。

故障逻辑推理



© Copyright 2018 SNPI

RCA分析特点

有效性：

RCA分析具有重要产品输出“纠正措施”，从根源上解决问题，避免故障重发,同时通过效果分析与评价可以充分验证和改进分析效果。

序号	原因（需与原因因素图对应）		纠正行动	类	级	负责单位/签字	技术性关闭	完成期	有效性验证时间
1	根本原因	电机轴翻修工艺缺陷	升版电机翻修工艺件。	[illegible]	[illegible]	[illegible]	文件升版	2012.3.31	2012.9.31
2	促成因素	皮带张紧力偏大	确认皮带张紧力的合理值，升版维修程序。	B	I	MRM	文件升版	2012.3.31	2013.3.31
3	扩展行动	MRM 学习事件报告，做好经验反馈	[illegible]	[illegible]	[illegible]	MRM	学习完成	2012.3.31	
		MOT 修改[illegible]为正式的程序。	[illegible]	B	II	MOT	文件提交	2012.06.31	
		MOT 组织复查[illegible]应技术管理细则。	[illegible]	B	II	MOT	文件提交	2012.12.31	

纠正行动

改进措施

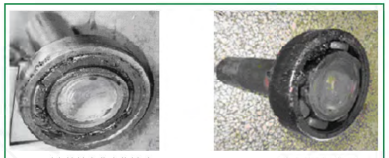
效果评估

© Copyright 2018 SNPI

RCA分析特点

全面性：

RCA成果可以作为经验反馈，推广至相同或者类似设备，避免同类设备的失效。



1040#钢 旋转弯曲疲劳断裂　　45#钢 旋转弯曲疲劳断裂

典型旋转弯曲断裂宏观形貌

RCA分析为个人、团体或组织提供了事件相关的经验和技术知识，有助于防止将来发生类似的问题。学习并加以有效运用此类知识，乃是RCA分析的目的之一，也为供应商持续改进设备的设计与制造提供了重要参考。

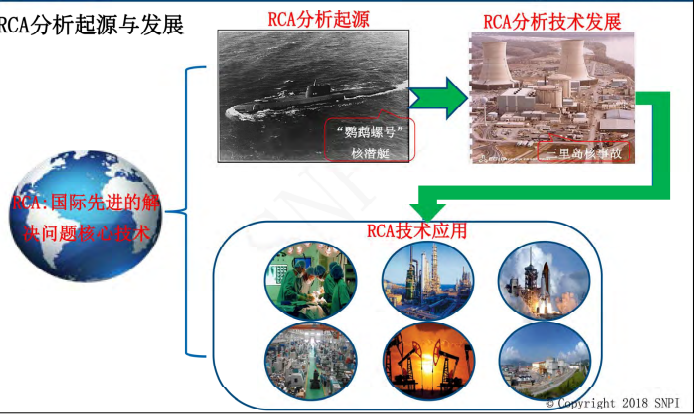
© Copyright 2018 SNPI

© Copyright 2018 SNPI

02 RCA分析起源与发展

© Copyright 2018 SNPI

RCA分析起源与发展



© Copyright 2018 SNPI

三里岛核事故

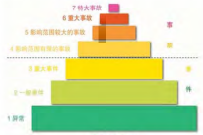
1979年3月28日凌晨4时，美国宾夕法尼亚州的三里岛核电站第2反应堆严重损坏（堆芯部分融化），导致向厂外有限度释放放射性物质，需部分的实施当地应急计划。此事故定级为5级（具有厂外风险的事故）。直接经济损失达100-200亿美元

事故影响

1、三里岛核电站事故后美国30年来未建新的核电站

2、创建了INPO（美国核电运行研究院）——RCA手册

3、对核电站的主控设计及事故管理做出改进



国际核事件分级表INES

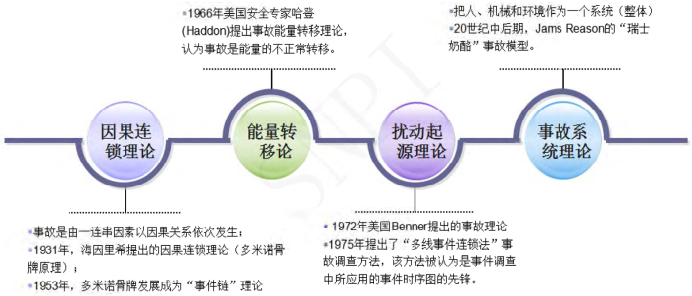
© Copyright 2018 SNPI

国际上常用的RCA分析方法

- 安全重要事件小组评价（ASSET）
- 管理疏忽和风险树（MORT）
- *人员绩效增强系统（HPES）*
- 人员绩效增强系统（HPES）衍生方法：K-HPES,J-HPES,UK-HPES,HPIP,MTO,AEB,PRCAP,CERCA,CAS-HPES等
- 组织学习型安全法（SOL）
- 三脚架分析（TRIPOD BETA）
- STEP方法
- 矫正的RCA分析系统（Takano，Japan）
- HF协同型RCA方法（GRS, Germany）
- 控制变化原因分析 (3CA)
- 人-技术-组织调查(MTO)
- FRAM分析
- CAS-HEAR分析
- 人员行为评估流程 (HPEP)
- PAKS根本原因分析程序(PRCAP)
- 安全融入组织学习(SOL)
- 事故演化与屏障作用(AEB)
- 减少失误的系统方法(SAFER)
- 人因心理学根本原因分析方法
- 商业产品 RCA方法（TapRoot®、REALITY CHARTING®Apollo、REASON®、PROACT®）

© Copyright 2018 SNPI

RCA与事故致因理论



© Copyright 2018 SNPI

RCA分析方法

对根本原因分析及其定义有着不同的陈述和意见；

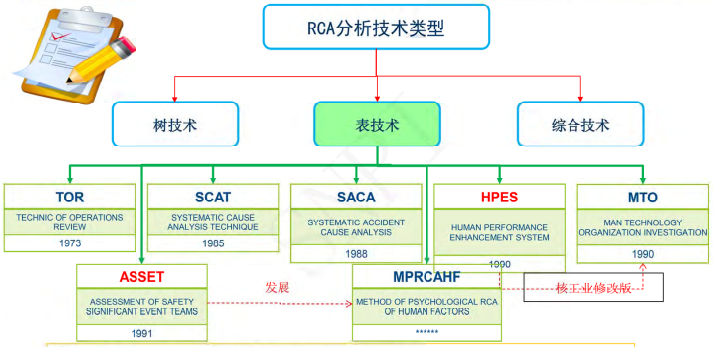
共有的基本理念是：**致力于探究根本原因和纠正行动与事件/问题之间的联系。**

共识：即根本原因分析是一种方法论（methodology）。它是一种问题分析和解决方法，这种方法可应用于不同的领域和环境。

由于没有单一最好的方法来应对所有的事件。因此，对待事件问题选择何种方法是实际工作所面临的问题。

针对某一事件，按照其性质和复杂性可采用不同的技术/工具来开展RCA分析

© Copyright 2018 SNPI



特点：文件化、界面简化，检查单化 。信息收集及分析需要大量时间。

© Copyright 2018 SNPI

ASSET分析

事件RCA分析表格

DISTURBANCES TO
(NUCLEAR INSTALLATIONS)

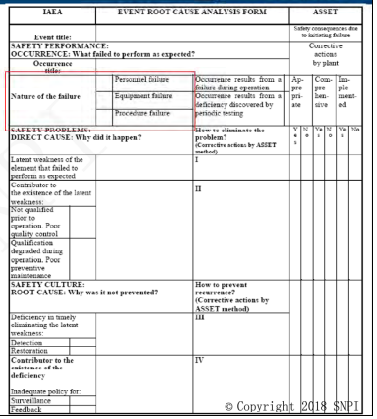
SAFETY PERFORMANCE
(1) WHAT HAPPENED? ***EVENTS***

OCCUR AND RECUR
BECAUSE OF

SAFETY PROBLEMS
(2) WHY DID IT HAPPEN? ***DIRECT CAUSES***

DUE TO

SAFETY CULTURE
(3)WHY WAS IT NOT PREVENTED? ***ROOT CAUSES***



RCA分析技术类型

- 树技术
- 检查表技术
- 综合技术

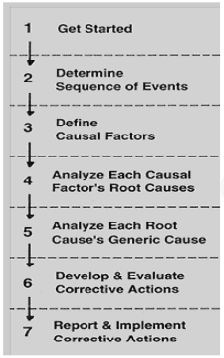
ABS	MORT	APOLLO	CTM	SRP
CAUSE AND EFFECT TREES	MANAGEMENT OVERSIGHT AND RISK TREE	ROOT CAUSE ANALYSIS	CAUSAL TREE METHOD	SAVANNAH RIVER PLANT RCA
1960s-1980s	1980 F C F C	1980	1983	1988 M O R T

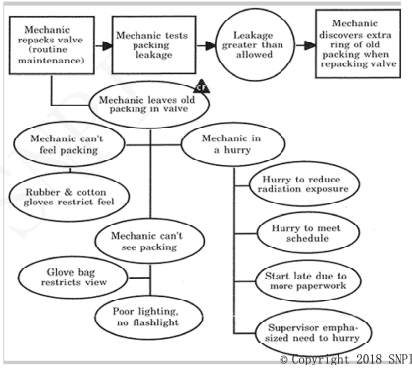
REASON	ERCAP	HPIP	TapRoot	PRCAP
Root cause analysis	EVENT ROOT CAUSE ANALYSIS PROCEDURE	HUMAN PERFORMANCE INVESTIGATION PROCESS	ROOT CAUSE ANALYSIS	PAKS ROOT CAUSE ANALYSIS PROCEDURE
1997	1993	1994	1991	1970S

特点：结构化、系统化　　比较复杂、需要专项技能培训

© Copyright 2018 SNPI

TapRooT® System分析技术



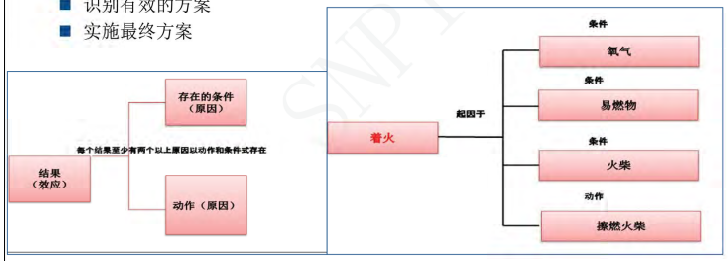


© Copyright 2018 SNPI

APOLLO®分析技术

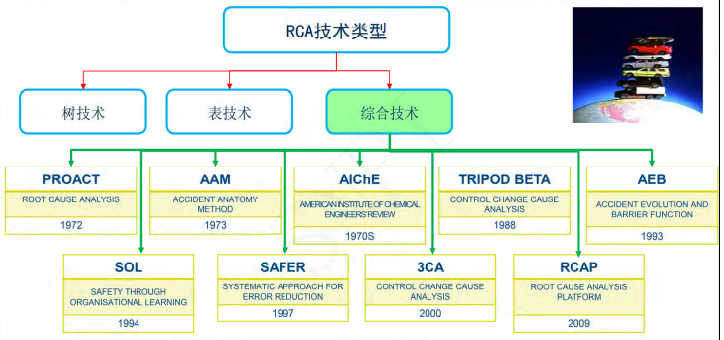
APOLLO根本原因分析四个步骤：

- 界定问题
- 创建因果表
- 识别有效的方案
- 实施最终方案



© Copyright 2018 SNPI

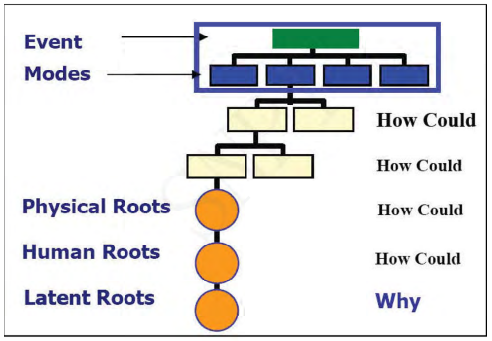
RCA技术类型



特点：综合树技术和表技术或者其他技术

© Copyright 2018 SNPI

PROACT®分析技术



© Copyright 2018 SNPI

RCA分析起源与发展

RCA技术共同特征：

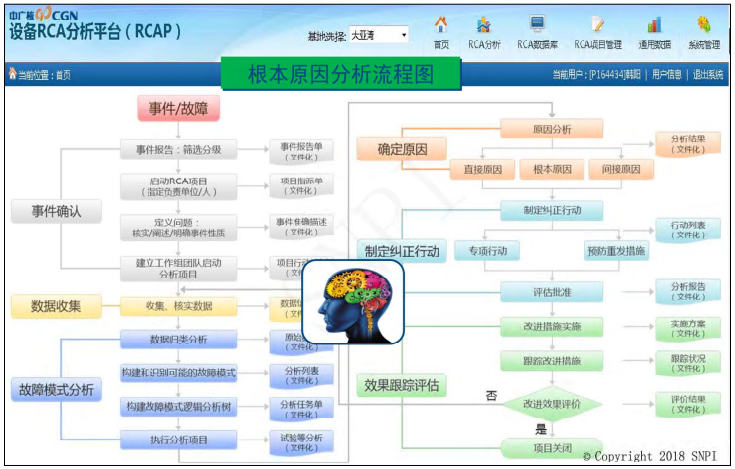
- RCA技术大多数起源于美国；
- 构建或描述事件时序和过程状态；
- 识别事件时序中的关键事件和条件；
- 系统地调查管理和组织方面的失效因素；
- 具有信息结构化的软件系统和数据库。

© Copyright 2018 SNPI

根本原因分析方法的应用

- RCA分析能够应用于突发的事故调查分析
- RCA 能够用于潜在的长期存在的问题（设备、组织）分析
- RCA能够分析生产过程存在问题,实现持续改进,提高系统的安全性和可靠性
- RCA分析能够在不同层面开展事件调查分析（Cummings & Worley, 2005）
  - ✓ 组织层面（Organization Level）
  - ✓ 团队层面（Group Level）
  - ✓ 个人层面（Individual Level）

© Copyright 2018 SNPI



03 RCA分析的基本术语

© Copyright 2018 SNPI

RCA分析基本术语

事件【EVENT】

- 事件的一般定义：事物在一段时间内所经历的变化。
- 事件（RCA）定义：**一个实时发生的事情(通常是不期望或非计划发生的事情），可能有突发的情形和严重的结果。**

例如：管道断裂、电机扫膛、阀门拒动、电源失电等均可作为设备事件；走错间隔、误碰开关、打闸不及时等都可认定为人因事件。

事件的严重程度决定是否需要进行根本原因分析。

© Copyright 2018 SNPI

RCA分析基本术语

核电站可能存在的严重事件

- 非计划停机停堆
- 反应性管理或控制错误事件
- 影响核安全和电厂可靠性的状况或趋势
- 危害人身安全等意外事故

。。。

不期望或不可接受的事件、行为活动、项目或因素等，依其重要程度需要采取适当的管理措施来防止或预防事件的重发。

© Copyright 2018 SNPI

RCA分析基本术语

原因/原因因素（Cause /Causal Factor）

任何能够导致事件发生的条件或状态，或增大事件严重性的情形和条件，其情形影响着结果。

原因因素通常归于：设备或材料（制造）问题、程序问题、人因错误、设计问题、培训不足、管理缺陷、外部因素等。

© Copyright 2018 SNPI

RCA分析基本术语

直接原因（Direct Cause）

直接原因：是直接/立即导致事件发生的原因因素(原因链中的第一个原因)，它直接跟事件有关。导致事件发生的失效、行为、疏忽、状态或条件。

例如：泄漏事件的直接原因是某个管道焊缝失效或阀门出现泄漏；电机轴未对中事件直接原因是在对中时操作误差。

根本原因（Root Cause）

引起事件或问题产生的最基本的原因因素，该原因因素是可以被识别，如果此原因被消除或纠正，这种事件和类似的事件在未来就不会再发生。

© Copyright 2018 SNPI

RCA分析基本术语

促成原因（Contributing Cause）

对导致事件的情形和条件有贡献或加剧促成结果出现的原因因素。即其增加了事件发生的可能性或严重性，但其本身不会引起事件发生，消除它并不能预防事件的重发。

例如:

1）卡住的浮控开关妨碍了操作员看清水箱的水位；

2）严重泄漏事件，促成原因是泄漏检测和处理方面存在培训不足才导致了比其它泄漏更为严重的事件。

© Copyright 2018 SNPI

RCA分析基本术语

显性原因(Apparent Cause)

----显性原因是通过可用的信息能够容易确定的原因因素。这种原因不需要做进一步或更深入的调查就可以认定，即原因是明显的或显而易见的。

----基于有限调查所获信息的事件或问题的最可能的原因。

共性原因（Common Cause）

引起或促成类似事件发生或趋势的共性原因因素。例如：不良照明引起的阀门装配错误事件。

© Copyright 2018 SNPI

RCA分析基本术语

纠正行动（Corrective Action）

- 纠正行动是指为了消除事件根本原因、促成因素或改善事件后果和其他不利条件所采取的改进行动，包括所有其它用于改进企业生产管理和运行质量而采取的措施。

纠正行动包含一些主要的定义，例如预防重发等。

- 预防重发：消除了引发事件或问题的根本原因，就会避免这类事件的再次发生。例子：维修程序的不充分（——需要修订程序）。
- 重发事件：以前发生过的事件，或经过分析评价后，与历史事件根本原因相同的事件。

© Copyright 2018 SNPI

RCA分析基本术语

RCA分析【ROOT CAUSE ANALYSIS】

根本原因分析（ROOT CAUSE ANALYSIS）是一套系统、科学、结构化的问题分析与解决方法。其具有客观、公正、权威和有效性的特点。

设备事件根本原因分析是通过系统化、逻辑化、规范化的分析方法，来找出设备失效的故障机理和根本原因，通过制定和实施有效的纠正行动，以保证系统设备的原有功能，防止类似事件的重复发生。

© Copyright 2018 SNPI

RCA分析基本术语

- **直接原因（Direct Cause）：立即/直接导致事件发生的原因因素** (在原因链中的第一个原因)。
- **促成原因（Contributing Cause）：**促成事件发生但其本身不会引发事件的原因因素 (在直接原因之后的原因) 。

  注意:对于一个简单的问题/事件可能没有促成原因。
- **根本原因（Root Cause）：**事件的基本原因因素，可用被识别和纠正。如果纠正将能够防止重发 (原因链中“最后”的原因)。

© Copyright 2018 SNPI

04 RCA分析管理体系

© Copyright 2018 SNPI

怎样做RCA分析？

- 如何面对“事件”？
- 如何识别“问题”？
- 如何找出“原因”？
- 如何避免“重发”？

管理体系__人员授权__方法与工具

© Copyright 2018 SNPI

BP德州炼油厂爆炸事故

- 2005年3月23日BP德州炼油厂发生爆炸事故；
- 美国化工安全与危害调查局（CSB）3月25日成立专项调查小组；
- CSB 2005年8月17日发布事故初步调查结果；
- BP公司独立调查小组2005年12月正式报告；
- CSB 2007年3月提交最终调查分析报告。

问题思考？

- 炼油厂爆炸的原因是什么呢？
- 使用了哪些调查技术？
- 根本原因分析时间要求？

BP德州炼油厂爆炸事故

异构化装置主管的失职和值班工人没有遵循书面程序的规定，是事故发生的根本原因。对上述失职行为我们不能视而不见。

——BP 北美公司总裁罗斯-费拉里

“调查结果表明英国石油公司在组织决策、安全监督和企业安全文化中存在系统性疏漏，如果不加以改正，这种疏漏可能会导致更多严重事故。”

—— CSB 主席卡罗琳·梅里特

© Copyright 2018 SNPI

根本原因分析

CRITICAL FACTOR	IMMEDIATE CAUSE	MGMT SYSTEM CAUSE (Root Cause)	CULTURAL ISSUES	CORRECTIVE ACTION
• CF-1. Loss of Containment (6.2.1)	• Violation by Individual • Violation by Supervisor • Improper decision making or lack of judgment • Defective safety devices • Inadequate equipment	• Poor judgment • Inadequate training effort • Inadequate leadership • Inadequate adjustment/ repair/ maintenance • Inadequate enforcement of Policies/Standards/ Procedures	• Business Context (6.3.1) • Safety as a Priority (6.3.2) • Inability to See Risk (6.3.4)	• See Recommendations for Other Critical Factors, especially: • Leadership (7.1.1) • Supervision (7.1.2) • Individual Performance (7.1.4) • Training (7.1.8) • Organization (7.1.9)

根本原因：BP 集团公司没有提供有效监督的企业安全文化和重大事故预防程序。

© Copyright 2018 SNPI

美国墨西哥湾原油泄漏事件

© Copyright 2018 SNPI

事件调查分析的目的

Do Not Look for Someone to Blame!

请记住三个基本的事实：

- 事件/事故的发生都是有原因的
- 如果根本原因被消除就可以防止事故的发生
- 除非将原因消除，否则同样的事件仍会发生

© Copyright 2018 SNPI

请说明如何来管理及启动事件调查分析?

根本原因调查分析流程：

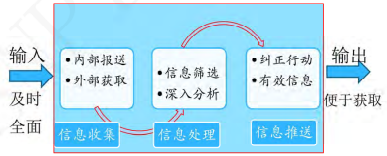
- 发起调查
- **实施调查分析**和形成报告
- 评审和批准调查报告

© Copyright 2018 SNPI

核电行业经验反馈管理体系

事件根本原因分析属于公司经验反馈管理系统范畴

- 公司经验反馈管理政策和上层文件
- 经验反馈管理体系和目标
- 经验反馈管理组织机构
- 经验反馈管理运作流程
- 经验反馈管理事件分级准则
- 事件/问题RCA启动原则
- 纠止行动管理、分级、分类
- 根本原因分析启动和管理

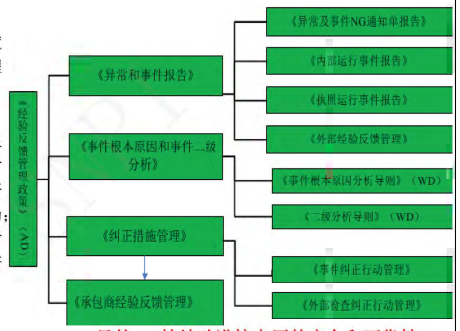


经验反馈管理系统模型

© Copyright 2018 SNPI

经验反馈管理体系：管理政策和管理程序

- 公司管理政策倡导和执行高度透明的安全文化，制定管理程序要求和鼓励所有员工发现、报告公司一切偏差事件；
- 公司自上而下形成事件管理组织机构和相应的执行流程，对发现的问题/事件能够及时开展动积极响应和推动纠偏行动；
- 为员工提供行之有效的RCA方法培训及保证事件调查分析所需的资源。

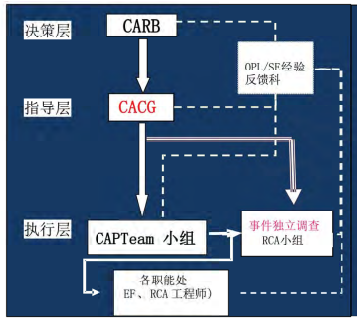


目的： 持续改进核电厂的安全和可靠性

© Copyright 2018 SNPI

参考核电厂经验反馈管理运作体系

组织管理架构



CARB—纠正行动审查委员会

CACG—纠正行动协调组

CAPT—电站内外部事件及纠正行动审查评议小组

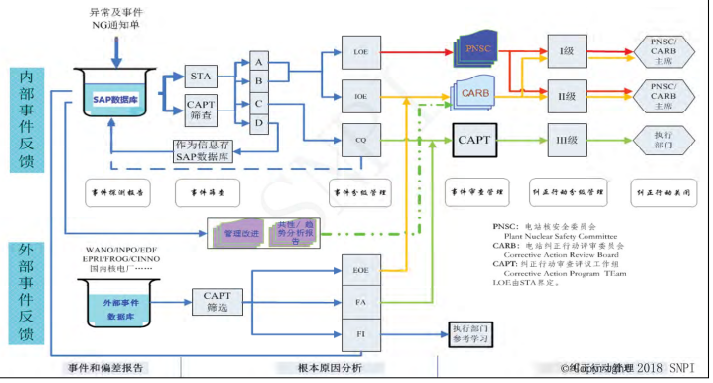
OPL/SE—执照申请处经验反馈科

设备RCA小组：独立调查分析重要设备事件

事件独立调查小组：独立调查跨部门人因事件

© Copyright 2018 SNPI

经验反馈管理运作流程



PNSC：电站核安全委员会 Plant Nuclear Safety Committee
CARB：纠正行动评审委员会 Corrective Action Review Board
CAPT：纠正行动审查评议工作组 Corrective Action Program TTeam
LOE由STA界定。

©纠正行动管理 2018 SNPI

哪些事件/问题需要RCA？

调查分析类型

- 事件响应（迅速调查）
- 根本原因调查（分析）
- 显因调查分析
- 共因分析(趋势调查)
- 快速人因行为调查
- 快速设备失效调查

RCA分析原则

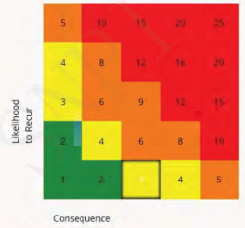
	程度	不确定性		
		高	中	低
事件后果	高	根本原因	根本原因	显性原因
	中	根本原因	显性原因	仅有纠正措施
	低	显性原因/共因分析	仅有纠正措施	仅有纠正措施/实施接近正确的纠正措施

© Copyright 2018 SNPI

Severity Calculator

Likelihood to Recur: Extremely low | Low | Possible | Likely | Very Likely

Consequence: Insignificant cost | Low cost | Moderate costs | High costs | Dangerously high costs



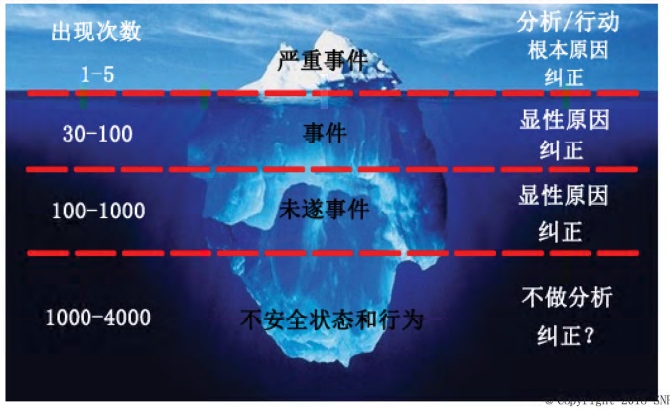
Recommended Analysis Type

Fishbone

Level 2 - Fishbone analysis. There is a modest level of risk. It is recommended to have key staff spend a few hours and assess the problem or potential problem beyond the surface level. Look for issues that can be avoided or find the major problems that created the situation. make recommendations that can be communicated clearly and quickly.

© Copyright 2018 SNPI

核电厂事件数量和分析类型



© Copyright 2018 SNPI

RCA项目管理

- 采用项目管理模式
- 委派有分析资格的人员担任组长
- 主要成员需受到过专业调查分析的培训
- 提供所需资源的支持
- 根据需要寻求外部专家支持

RCA定期会议

启动通报会 → 定期分析会 → 分析评审会

组建项目组 | 调整分析策略 | 明确及落实行动

© Copyright 2018 SNPI

RCA分析人员资质与职责

© Copyright 2018 SNPI

RCA分析人员资质与职责

© Copyright 2018 SNPI

事件根本原因分析成功的基础

RCA分析需要：

1）管理体系的正常运作和领导层的参与和支持

2）RCA小组团队全力协作和集体智慧的发挥

3）良好的安全文化基础，以防止事件重发来代替责怪、惩罚文化

RCA 团队

© Copyright 2018 SNPI

【案例】：酸循环屏蔽泵电动机故障

（案例来源：PROCESS ENGINEERING）

事件描述：

◆一台用于酸循环的屏蔽泵电动机故障，主电源熔断器烧毁了，必须立即采取措施。

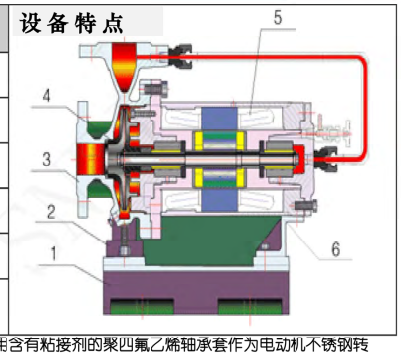
◆这是一台价格昂贵的进口泵，由不锈钢制成，使用含有粘接剂的聚四氟乙烯轴承套作为电动机不锈钢转子的导套，其润滑剂是酸性的，经过轴承套和屏蔽套后回到吸入式过滤器中。

◆电气技术人员诊断后认为电动机定子中发生短路，并更换了熔断器。在检查叶轮和泵体时发现叶轮与口环俱有明显的磨损，于是设备工程师决定更换整个机组。

© Copyright 2018 SNPI

序号	部件名称
1	底盘
2	底板
3	泵体
4	叶轮
5	屏蔽电机
6	支架

设备特点



泵材料：不锈钢。结构特点：使用含有粘接剂的聚四氟乙烯轴承套作为电动机不锈钢转子的导套。

© Copyright 2018 SNPI

诊断和处理

故障现象：

——电动机主电源熔断器烧毁

——叶轮与口环明显磨损

诊断结果：

——电动机定子绕组发生短路

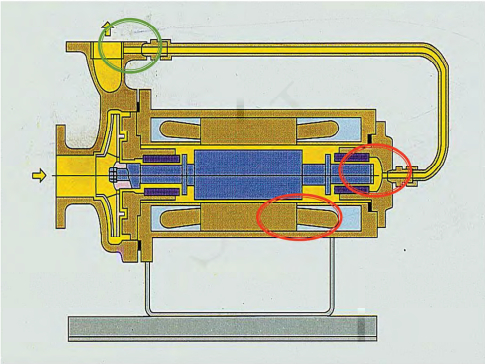
处理措施：更换主电源熔断器、更换整个电动机泵组

结　果：几个星期后，同样的问题再次发生

由于修理费用昂贵，且影响正常的生产运行活动，高层管理人要求调查此事。

© Copyright 2018 SNPI

屏蔽泵的结构示意图



© Copyright 2018 SNPI

电动机定子绕组短路原因?

- 电动机定子绕组为什么会短路?
- 为什么酸会泄漏到屏蔽套内?
- 为什么转子和屏蔽套会发生摩擦?
- 为什么转子轴承和轴承套之间会发生摩擦?

  ——因为较软的聚四氟乙烯轴承套中有细小的金属片；
- 为什么在此处有金属片存在?

  ——是吸入式过滤器破损造成细小物质进入到泵和润滑剂通道中去。

© Copyright 2018 SNPI

分析思考?

1. 请考虑事件的直接原因，并制定纠正行动?
2. 设备问题：更换过滤器可以解决问题
3. 对事件还需要哪些调查?

© Copyright 2018 SNPI

谢谢聆听!

© Copyright 2018 SNPI

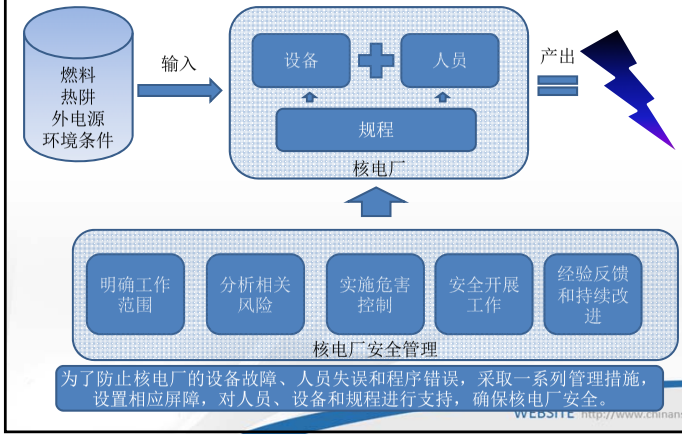
核电厂事件原因分析平台简介

核电厂事件原因分析平台简介

核与辐射安全中心
焦峰
jiaofengnsc@126.com

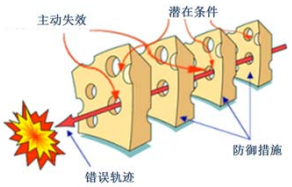
事件原因分析

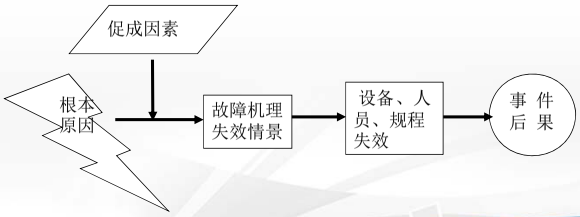
监管机构的事件原因分类：



为了防止核电厂的设备故障、人员失误和程序错误，采取一系列管理措施，设置相应屏障，对人员、设备和规程进行支持，确保核电厂安全。

事件原因分析



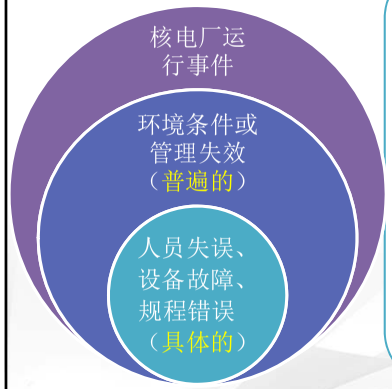


事件的原因因素

事件的影响因素并非并列关系，它们彼此之间可能存在引起和被引起的关系，它们对核电厂安全运行的影响深度和影响广度也不尽相同。

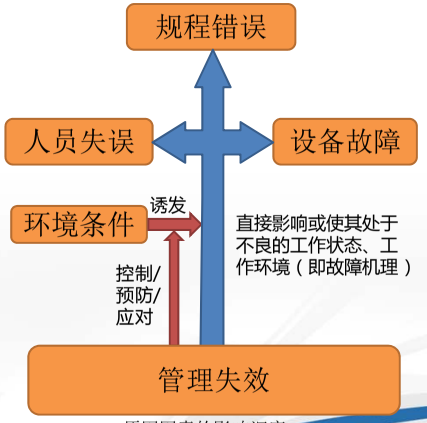
事件的原因因素

原因因素的影响范围



在原因因素的影响范围方面，引起事件的人员失误、设备故障或规程错误影响范围最小，往往局限在当班工作人员当时进行的操作、同一台设备或同类型设备的失效等方面。而核电厂运行的环境条件和安全管理的影响范围更广。

事件原因分析



原因因素的影响深度

在原因因素影响深度方面，安全管理比其他三种影响因素更深刻。几乎每一起事件都能够通过制定和实施相应的管理措施避免。

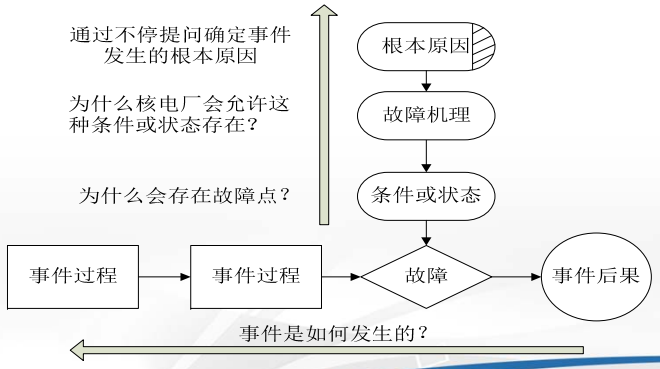
事件的原因因素

WANO归纳的核电厂三大组织要素的影响因素

1、人因影响因素	2、设备影响因素	3、管理影响因素
口头交流	设计配置和分析	管理方针
工作实践	设备的规范、制造、运输、安装和施工	沟通或协调
人员工作日程安排	维修/试验/监督	管理监督和评价
环境条件	设备性能	决策流程
人机接口		资源分配
培训/资格评定		变动管理
书面程序和文件		组织文化/安全文化
监督方法		应急管理
工作组织		

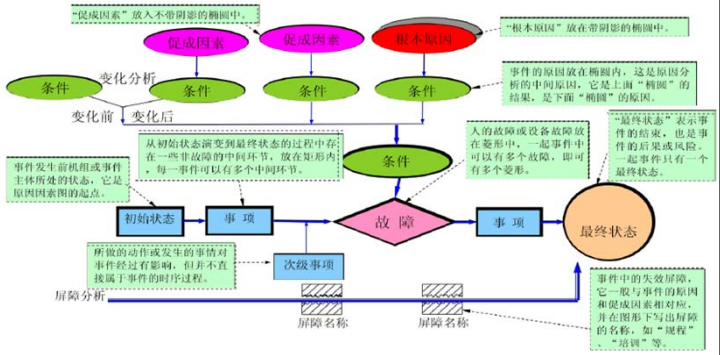
事件原因分析

事件和原因因素图（ECF）分析法基本逻辑

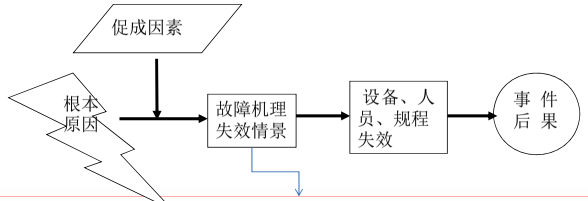


事件原因分析

ECF分析以其方便清晰的特点成为原因分析的骨干或主要展现形式



原因分析过程的参考指引



原因分析方法为事件调查和分析人员提供了分析事件原因的框架，但调查中需要思考的问题和调查方向依靠调查人员的经验和总结。为此，指南总结了相关的背景知识，作为参考指引指导事件分析过程。

故障机理或失效情景是中间原因而非最终的根本原因。针对这些中间原因进一步分析核电厂的安全管理体系为何允许这些失效情景或故障机理存在，这些深层次原因就是事件发生的根本原因或促成原因。

原因分析过程的参考指引

人因失误征兆矩阵

任务要求（T）	个人素质（I）
时间压力（紧急任务） 高工作强度（大量记忆） 同时的、多项的行动 重复动作/单调 不可挽救的行为 要求进行解释 未明确目的、角色或者责任 缺乏标准或标准不明确	对任务不熟悉/第一次任务 知识匮乏（思维错误模型） 未使用过的新工艺 不准确的沟通习惯 不熟练/经验不足 解决问题能力不足 不安全的态度 生病或者疲劳/身体长期的不适或者损伤
工作环境（W）	**人的天性（N）**
分散注意力/打断 改变/偏离规程 混乱的显示信息/控制命令 应急措施 设备/系统的响应被隐藏 非预期的设备状态 缺少备用的指示 私人思怨	压力 行为模式 先入为主的假设 自大/过于自信 思维模式(倾向) 对危险的感知不准确 心理上的认知捷径或者偏差 有限的短期记忆

原因分析过程的参考指引

人员违规问题分析

不知道		不能遵守		不愿遵守	
从来都不知道	这通常表明培训不到位或管理体系失效以致未能将指令传达至工作员工层面。	缺乏资源	经费不足是不遵守规则的常见原因。当调查违规问题时，事件调查组应考虑这类方向。	没有奖励	调查人员可能需要确定如果按照要求做或把工作做好是否能得到奖励。可能没有奖励机制促使人员遵守规则。
忘记了	通常是局部的个人失误。不能反映体系缺陷，但是可能表明需要增加培训频次或开展复训。	不知道该怎么办	这类问题关注缺乏知识（也就是对如何完成一项工作的了解）。	没有处罚	该问题关注如果强制执行处罚，是否能够迫使遵守。
隐含的任务	这可能是因为缺少经验或没有详细的指令。	不可能	确定该工作是否能够完成。如果有足够资源、知识和意愿，工作人员或工作组是否能够满足特定要求？	不同意	在某些情况中，有些人拒绝按照标准执行或服从他们不同意/认为不切实际的要求。

原因分析过程的参考指引

规程缺陷的原因分析

工作程序和文件
无适用文件
技术性错误
技术不完备
未包括注意事项
未根据当前设计进行更新
没有正式发布
措词不清或过于复杂
格式缺陷
使用说明不足或未提供
技术审查过程不充分
未说明遵守规程的职责
未提供充分的安全评价

原因分析过程的参考指引

设备缺陷的原因分析

在进行设备缺陷原因分析时，要注意故障机理（模式）分析与根本原因分析的区别。

- 故障机理分析：引起故障的物理、化学变化等内在原因，就是故障机理（模式）。

一台设备发生故障，其故障机理可能是：

- 过载破裂（脆化）
- 振动
- 疲劳破裂（包括腐蚀疲劳）
- 腐蚀或磨蚀
- 水锤
- 电气部件失灵
- 其他

原因分析过程的参考指引

- 设备缺陷的根本原因分析关注的是导致故障机理存在的深层次原因。核电厂设备经历了设计、加工、安装、调试、运行、维护等多个环节，如果这些活动存在缺陷，则有可能导致设备处于故障机理环境中，进而引起设备失效。例如，WANO将设备根本原因分为：
  - 设计配置和分析
  - 设备的规范、制造、运输、安装和施工
  - 维修/试验/监督
  - 设备性能
- 在开展设备缺陷的根本原因分析之前，必须首先确定设备的故障机理。

设备缺陷原因分析

设备缺陷的故障模式分析和根本原因分析逻辑清晰，主要难点在于确定设备的故障模式。如果最终故障模式无法确定，则电厂应对所有可能的原因因素提出纠正措施。

如果设备缺陷的根本原因出现在设计、制造等环节，超出核电厂营运单位的控制范畴，那么核电厂营运单位应考虑的是，在设备进厂前质量控制和运行维护是否存在缺陷。例如设备的安全等级、驻厂质量监督、设备厂家资质、役前检查、在役检查的频度和要求、预防性维修等方面。

原因分析过程的参考指引

安全管理缺陷分析

在核电厂生产过程中健全的安全管理体系在以下五个方面执行其安全管理职能，从而建立阻断事件发展的屏障：

① 定义工作范围

将任务转化成工作，设定期望，明确任务及其优先级，分配资源。

② 分析危险

对与工作有关的危险进行识别、分析和归类。

③ 制定并实施风险控制

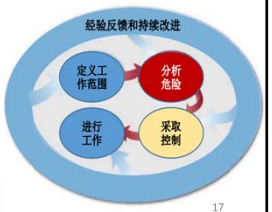
制定并明确适用的标准、政策、规程和要求；明确防止/减轻危害的措施；并且将这些措施落实到位。

④ 在控制之下开展工作

确保工作准备充分，并且安全地开展工作。

⑤ 提供反馈和持续改进

收集工作控制措施是否充分的信息，找出可以改进工作和计划的机会，开展独立的工作监督。



常见的安全管理缺陷

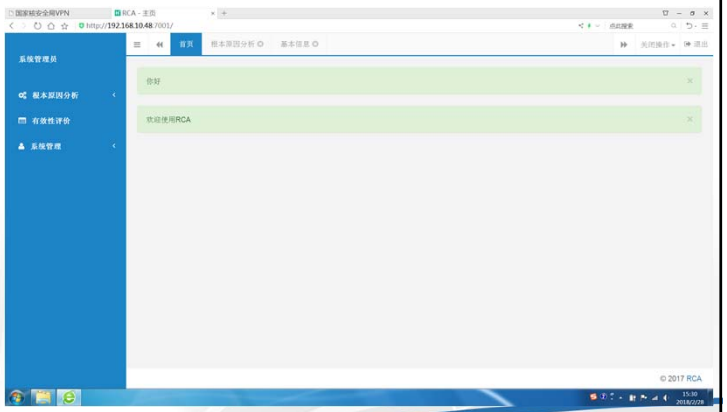
分类	薄弱环节
培训	对于技术型任务工作人员的资格培训的有效性： 只关注低级别的认知知识。 未涉及管理培训。 培训和实际的设备、工作流程和工作规程不匹配。
交流	增加对关键步骤的标注，以避免对指令的误解： 未能增加对三段式沟通的使用。 未能对工作流程中不清楚的优先级和预期结果采用特殊的唯一ID进行标示。 角色和责任分配不明确。
计划安排	对意外失效事件的准备工作： 未考虑到可能出现多个组件失效的情况。 未能提供需要的材料或者流程。 资源的调度： 未考虑是否会对邻近设备造成误操作或者损伤。 未进行具体的工作。 未对具体的问题分配足够的资源。

常见的安全管理缺陷

设计或流程变更	设计改变过程中的工作人员： 培训不足。 对于流程出错的突发事件缺少应对方案。
价值观、优先级、方针	管理方针中加入足够的规定流程或者安全措施： 将计划置于过高的优先级。 能够容忍工况或者性能的降级。 管理者未能意识到相关程序的必要性和重要性。
流程的改进和投用	流程改进和投用中的人员因素： 未对程序进行验证和确认。 完成任务时未遵循修改后的流程。 想当然地用臆测代替流程。 忽略了流程中的必要内容。

常见的安全管理缺陷

监管介入	调查中的观察和指导工作： 未能纠正不好表现或者未能贯彻好的表现。 未对责任和义务进行明确分配或者分配混乱。 调查过程缺乏监督。
组织交流	为确定工作优先级的交流： 组织间缺乏明确的交流渠道。 缺少自评监测的各个过程之间出现目标和需求的冲突。 各个过程之间缺少交流。
工作实践	加强设立和配备用于错误预防的工具和技术。



案例分析一

国内某电厂2号机组主给水泵B控制卡件故障导致自动停堆事件

2015年6月14日，国内某电厂保持满功率运行。10：23：40主给水B泵DCS HS2M102控制卡件3082MB故障，主给水B泵失去控制信号，主给水流量迅速下降。为避免蒸汽发生器水位低低停堆，主控操纵员果断启动主给水C泵，并手动控制将流量迅速恢复正常值2000t/h左右，由于给水流量的恢复，高加内的蒸汽被重新冷凝，高加液位迅速上涨，因为正常疏水阀门开启较慢，且冷凝高加壳侧压力同步下降，疏水能力下降，液位很快触发高信号。随后5B、5A高加三高信号动作，高加解列，主控操纵员立即在DEH中以30MW/min的速率执行快速降功率。高加解列后，主给水温度由234℃降至158℃，使得一回路冷端温度降低引入正反应性，一回路核功率上升。

10：26：53，超功率ΔT保护达到108%定值，停堆信号触发，机组停堆停机。操纵员执行DEC故障诊断规程，根据DEC程序引导执行I1事故规程“反应堆紧急停堆”，稳定机组状态在热停堆状态。

案例分析一

APA B泵失效原因

10：23：40主给水B泵的控制卡件DCS系统中3082MB卡件故障，型号为HS2M102，由一块底板加两块面板组成。后现场检查确认发现该卡件已停止工作。对于此次故障的卡件，在每年大修期间，均进行过测试并且合格；最近一次检修为2014年6月21日，210大修期间对该卡件进行通道测试，结论合格。

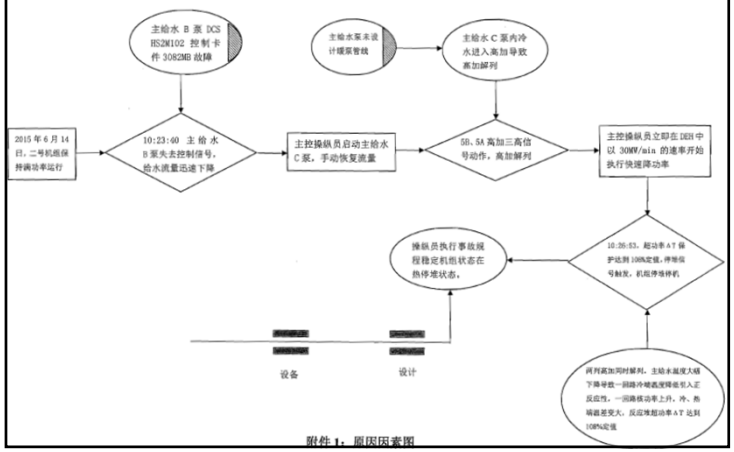
高加解列原因

主给水B泵控制失效后，出力降为0，因无跳泵信号，备用主给水C泵无自动启动信号，主给水流量迅速减小，进入高加的给水减少使得高加在短时间内加热的蒸汽冷凝变少，压力上升，液位下降。主控操纵员确认给水B泵故障后，立即启动主给水备用C泵，将主给水流量恢复正常，蒸汽发生器水位不再下降。在流量恢复的过程中，由于正常运行状态下主给水备用C泵及相关管线内水温较低（60℃），C泵紧急启动后，这一部分冷水直接进入高加，加剧了高加液位的波动。正常流量给水重新进入高加，将高加内聚集的蒸汽冷凝，从而产生大量凝结水，壳侧压力降低，汽水分离再热器的疏水也由于高加的压力降低，疏水到高加的流量加大，高加液位上升迅速，并触发高、高高、高高高液位信号，导致高加解列。

案例分析一

直接原因：
主给水B泵DCS系统控制卡件3082MB故障导致B泵出力下降
手动启动主给水C泵后，C泵内冷水进入高加及主给水流量大幅变化导致两列高加液位三高解列
两列高加同时解列，主给水温度大幅下降导致一回路冷端温度降低引入正反应性，一回路核功率上升，冷、热端温差变大，反应堆超功率ΔT达到108%，停堆信号触发，机组停堆停机。
根本原因：
主给水B泵DCS控制卡件3082MB故障
主给水C泵内冷水进入高加导致高加解列
促成因素：
高加解列后，冷水进入蒸汽发生器，引起一回路冷热端温差变大。
1、事件序列见打印材料；
2、请运用ECF分析法对该事件进行分析；
3、对于事件序列有疑问或需要进一步调查的问题，请列出问题提纲。

案例分析一



附件 1：原因因素图

案例分析二

2015 年6 月24 日晚，某电厂3 号机组85%Pn 功率运行，为配合电气维修人员进行计划内工作“控制棒驱动机构电源的 2 号电动发电机组定期检查”，运行人员在停运控制棒驱动机构电源的2 号电动发电机组后，由于误合2 号发电机（3RAM002AP） 出口断路器（3RAM601JA），导致控制棒驱动机构电源的2 台发电机（3RAM001/002AP）过流保护动作跳闸，控制棒驱动机构动力电源失电导致控制棒落棒，触发RPN 功率量程中子通量变化率高保护动作，引起3 号机组反应堆自动停堆。

案例分析二

在操纵员执行事故规程（SOP）稳定机组状态过程中，核电厂多次违反规程未将一回路硼化到维修冷停堆硼浓度（2300ppm）。6 月27 日上午，操作设备的运行人员承认是由于人因误操作导致机组停堆，6 月27 日重新启动控制棒驱动机构电源3RAM 系统，20:58 分机组退出SOP 处理规程，事件结束。

练习要求：

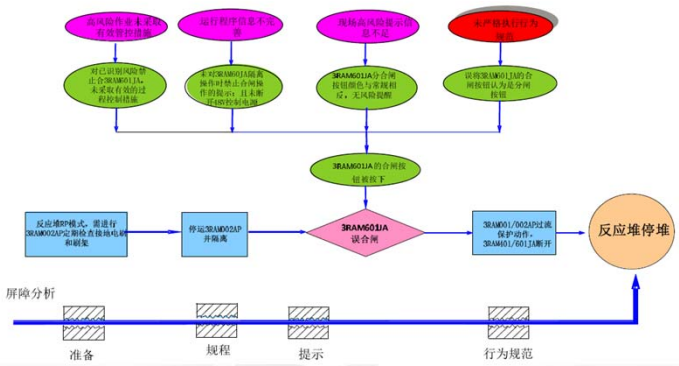
1、事件序列见打印材料；

2、请分组讨论事件过程；

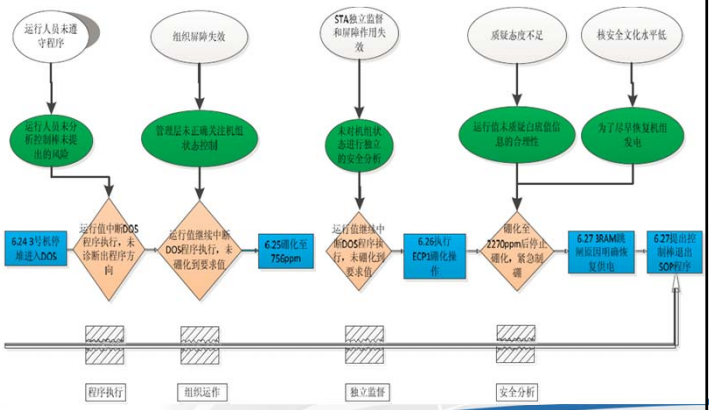
3、请运用ECF分析法对该事件进行分析；

4、对于事件序列有疑问或需要进一步调查的问题，请列出问题提纲。

案例分析二



案例分析二



案例分析三

主汽门突然故障关闭导致停机停堆事件

2015年7月25日国内某电厂1号机组处于满功率功率运行。

8：28，2#主汽门（1GSE002VV）突然关闭，汽机功率突降至525MW，主控立即通知现场人员就地检查，同时立即开始以30MW/min降功率至300MW。期间主控安排查找故障原因，发现2#主汽门（1GSE002VV）油缸下部液压模块本体处大量漏油且无法隔离，导致汽机调节油系统控制油大量泄漏。

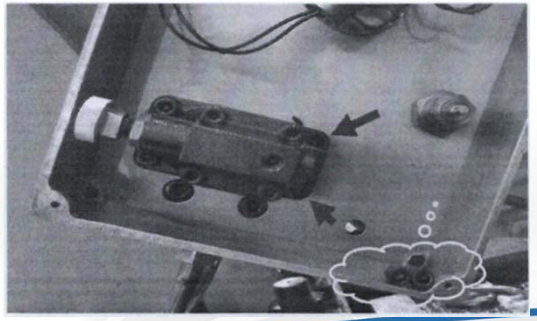
9：08根据现场反馈主控以30MW/min开始降功率至30MW。

9：17主控室手动打闸停运汽轮发电机组。

9:22在汽机打闸后GCT-C处于温度模式下未能调节开启，后操作员稳定状态过程中GCT-C也未调节开启，操纵员未及时发现此异常。随着一二回路的温差升高，GCT-C第一组3个阀门达到快开动作定值（6℃）第一组三个阀门同时快速保护开启，蒸汽压力迅速降低，蒸发器产生气泡，触发虚假水位至高高水位保护定值，2号蒸汽发生器液位高高（P14）与和功率大于10%（P7）叠加符合产生停堆信号导致反应堆自动停堆。停堆后主控执行DEC规程，后通过I1规程稳定机组在热停堆状态。

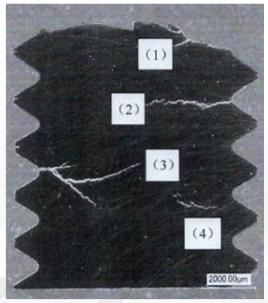
案例分析三

经调查发现2#主汽门为油压驱动，油压失去导致阀门突然关闭。现场检查发现，卸荷阀远离其针型阀调节手轮侧两个固定螺栓头部发生断裂，卸荷阀与控制块密封面上的O型圈被冲出，且发生断裂破碎，密封失效导致汽轮机调节油系统（EH）油大量泄漏。



案例分析三

螺栓断裂的原因：根据实物测绘按照14MPa油压测算单只螺栓受拉应力大约在39.11MPa，该负荷远远低于螺栓材料的抗拉强度及屈服强度，断裂螺栓进行理化材料分析发现断口表面残存有相当数量的腐蚀产物，这两个断口的裂纹已经存在较长时间。螺栓断裂是因为它们在空气中发生了氢致应力腐蚀。



案例分析三

主汽门有动机预防性维修项目5年解体检查一次，长燃料循环后改为3C，2015年7月2日，大修机组启动过程中曾发现2#主汽门无法开启，当时紧急对主汽门油动机的卸荷阀及其O型密封圈进行更换，未对卸荷阀的4个固定螺栓进行更换。

GCT-C阀门开启问题：在机组满功率运行期间，GCT-C阀门在温度模式下自动运行，控制信号来自“反应堆冷却剂平均温度与代表汽机负荷大小的温度之差”。当温差信号大于3度时，产生阀门调节开信号；温差大于6度时，第一组3个阀门动作定值达到最快速保护开启。根据GCT-C阀门动作趋势记录发现3至6度温差区间阀门未出现调节开启信号。

查询KDO和KIT系统趋势和数据，GCT-C阀门调节开的控制信号均未出现，现场1GCT121VV阀门也未动作过。GCT-c控制由KRG卡件实现，电厂检查卡件接线未发现异常，判断“压力模式和温度模式切换开关下游的继电器卡件”即1GCT503CC开关在T模式位置，1GCT402XR2卡件继电器触点未正常闭合，导致控制回路不同。后续试验缺陷未复现，怀疑为偶发故障。

案例分析三

事件直接原因

汽机停机：1GSE002VV卸荷阀螺杆断裂，2号主汽门1GSE002VV大量漏油突然关闭。

停堆：GCT-c卡件故障最终由蒸汽发生器水位高高与核功率高于10%叠加产生停堆信号

事件根本原因：

断裂螺栓强度超过12.9级，强度较高的螺栓对氢十分敏感，在环境中发生“氢致应力腐蚀”。1GCT402XR2失效故障。

1、事件序列见打印材料；

2、请运用ECF分析法对该事件进行分析；

3、对于事件序列有疑问或需要进一步调查的问题，请列出问题提纲。

谢 谢！

核电厂异常重要性判定程序(SDP)

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

核电厂异常重要性判定程序(SDP)

环境保护部核与辐射安全中心

2017年3月

WEBSITE
http://www.chinansc.cn/

核电厂异常重要性判定程序（Significance Determination Process，SDP）是美国核管会（NRC）最先开发使用的一套基于风险指引技术的核电厂安全事项重要性判定程序。

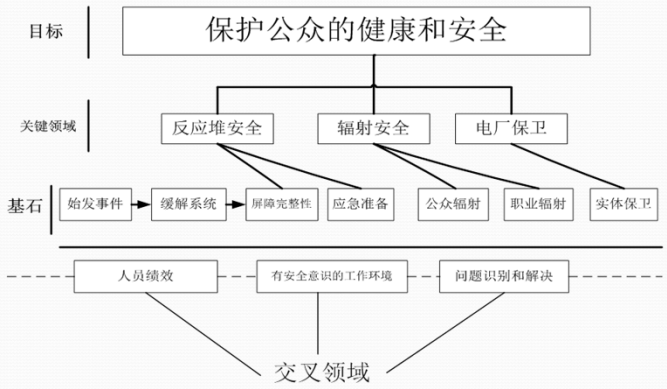
是反应堆监管程序（ROP）核电厂性能评估的两大技术支柱（性能指标体系PIs和异常重要性判定程序SDP）。

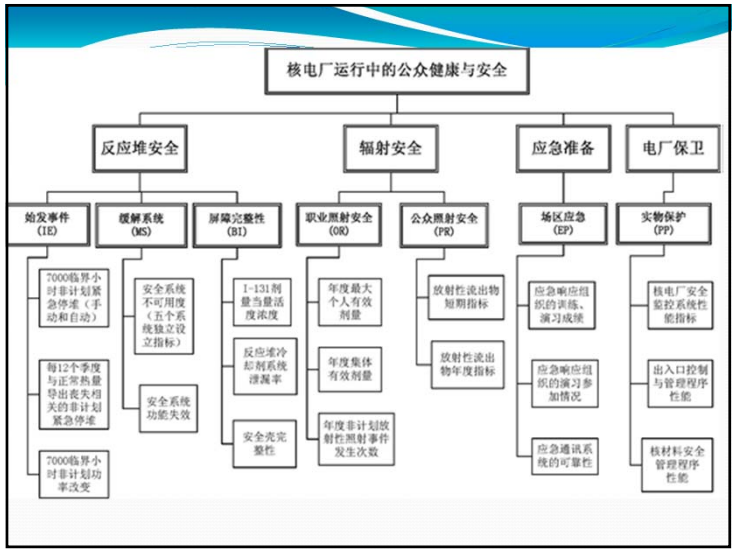
主要内容

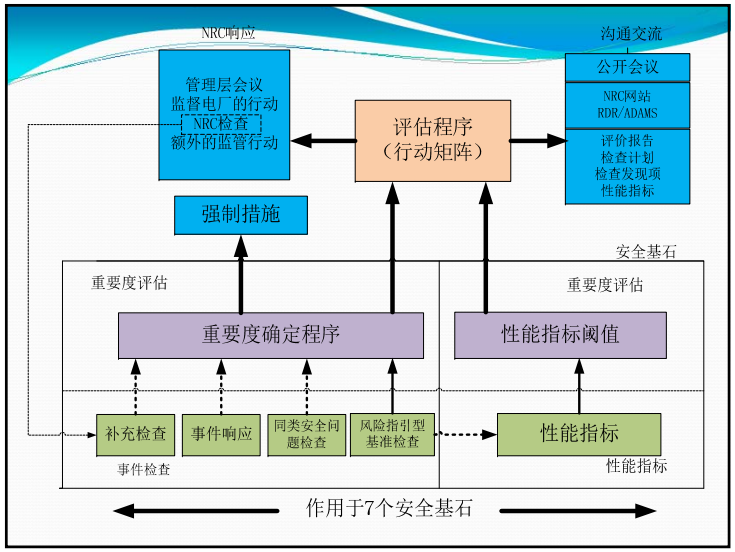
- SDP的背景和概述
- SDP框架
- 功率工况SDP
- 停堆工况SDP
- 火灾工况SDP
- 其他SDP评估程序

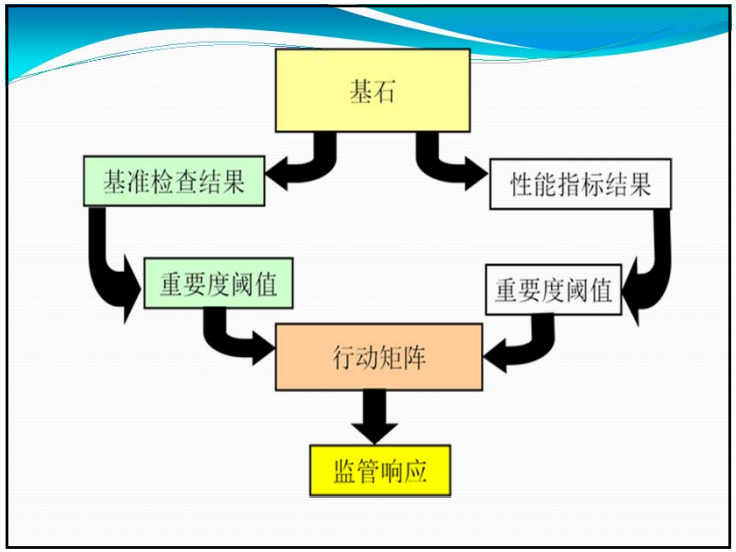
SDP的背景和概述

核电厂异常重要性判定程序（Significance Determination Process，SDP）是由美国核管会（NRC）监管体系和理念的体现，是完成NRC监管目标的重要工作程序。





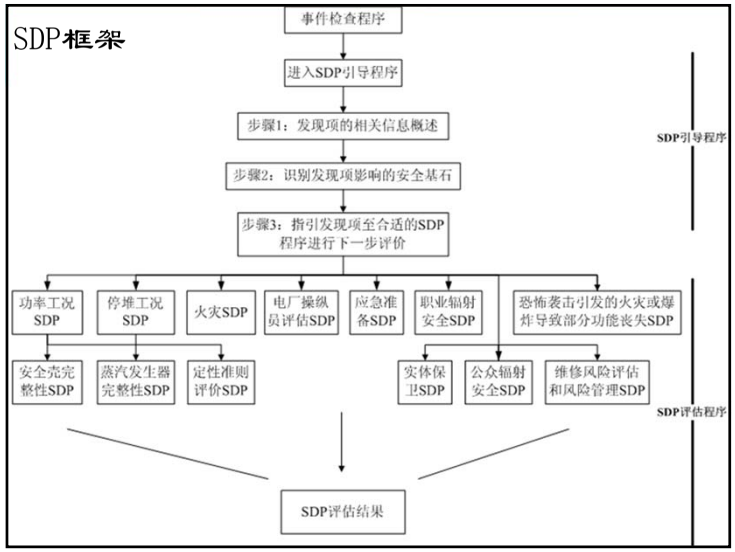




SDP在核电厂安全状态评估中的使用

使用SDP的目的有四个方面：

- 使用适当的风险阈值确定安全事项的安全重要程度；
- 提供客观、公用的平台，以便核安全管理者与业主、营运单位对检查安全事项的潜在安全重要程度进行沟通，以便达成共识；
- 为安全事项的及时评估或强制措施的制定提供合理的依据；
- 提供核电厂特定风险信息，并用于风险指引型检查程序的执行。



安全事项相关信息表

支持性文档和参考资料：
安全事项的清晰描述：
对功能降级和系统缺陷的实际描述：
安全事项与功能降级或系统性缺陷的逻辑关系：

始发事件	缓解系统	屏障完整性
❒ A. 一回路LOCA始发事件贡献项——（稳压器加热套管的一回路泄漏、反应堆压力容器管道穿透、控制棒驱动机构管嘴、先导式安全阀、界面LOCA事件等。） ❒ B. 瞬态始发事件贡献项——（反应堆/汽机跳闸，丧失厂外电源，丧失重要厂用水（RRI/SEC）、主蒸汽管道/主给水管道降级/破口、直流电源降级/丧失、仪用压缩空气丧失、一回路/二回路瞬态事故） ❒ D.蒸汽发生器传热管破裂 ❒ E.外部事件贡献项（局限于火灾和内部水淹）	❒ A. 缓解系统 ❒ 堆芯衰变热移出功能降级 ❒ 短期热移出功能降级 ❒ 一回路（例如，安全注入） ❒ 高压安注 ❒ 低压安注 ❒ 二回路（如，主给水、辅助给水、排放阀） ❒ 长期热移出功能降级（如，安全壳地坑再循环） ❒ B. 外部事件缓解系统（地震/火灾/水淹/严重气候的防护功能降级） ❒ C. 反应性控制系统功能降级（包括反应堆保护系统） ❒ 不受控的控制棒移动 ❒ 一回路冷却剂误稀释或冷却剂误注入 ❒ 反应性管理（例如，超过执照许可的功率限制、需求和控制）	❒ A. 在电厂扰动情况下，一回路边界作为缓解该扰动的一个来源。（事件有：承压热冲击） **注**：所有有关一回路边界的其它事件，如泄漏，在始发事件中考虑 ❒ B. 反应堆安全壳屏障降级 ❒ 实际存在破口或旁通 ❒ 热移出、氢或压力控制功能降级 ❒ C. 控制室、辅助厂房/反应堆厂房或乏燃料厂房屏障的降级 ❒ D. 乏燃料水池 ❒ 乏燃料水池水装量和/或温度（如，冷却） ❒ 燃料储运
应急准备	**职业辐射**	**公众辐射**
❒ 未能服从计划标准或风险重要计划标准 ❒ 实际事件执行问题	❒ 保持辐射剂量在合理范围的计划或工作控制 ❒ 暴露或过度暴露问题 ❒ 评估辐射损害的能力	❒ 放射性排出物的释放程序 ❒ 放射性环境监控程序 ❒ 放射性材料控制程序 ❒ 放射性材料运输程序
实体保卫		
❒ 安全和防护措施的检查程序		

如果安全事项和与之相关的功能降级或系统缺陷存在于电厂的：
1.应急准备安全基石，停止。转向应急准备SDP评估程序。
2.职业辐射安全基石，停止。转向职业辐射安全SDP评估程序。
3.公众辐射安全基石，停止。转向公众辐射安全SDP评估程序。
4.实体保卫安全基石，停止。转向实体保卫SDP评估程序。
5.始发事件、缓解系统或屏障完整性安全基石，继续下列问题。

阅读A到E，用“是”或“否”回答问题。如果A到E的回答结果均为“否”，直接转向功率工况SDP评估程序。

A. 停堆、换料和强制停堆
安全事项是否属于停堆期间的操作、事件或功能降级？
□ a. 如果“是”，停止，转向停堆工况SDP评估程序。
□ b. 如果“否”，继续下面的问题。

B. 电厂操纵员资格：
安全事项是否涉及操纵员执照授权程序或模拟程序逼真度？
□ a. 如果“是”，停止，转向电厂操纵员SDP评估程序。
□ b. 如果“否”，继续下面的问题。

C. 维修风险评估：
安全事项是否涉及功率或停堆工况执行维修活动执照申请评估和风险管理？
□ a. 如果“是”，停止，转向维修风险评估SDP评估程序。
□ b. 如果“否”，继续下面的问题。

D. 安全事项是否涉及保持或恢复堆芯冷却、安全壳完整性和乏燃料水池冷却能力的缓解措施？
□ a. 如果“是”，停止，转向恐怖袭击引发的火灾或爆炸导致部分功能丧失SDP评估程序。
□ b. 如果“否”，继续下面的问题。

E. 火灾防护：
1. 安全事项违背火灾防护策略？
□ a. 如果“否”，停止，转向功率工况SDP评估程序。
□ b. 如果“是”，继续下面的问题。
2. 安全事项是否涉及：
（1）火灾防护和易燃物、点火源或热操作的管控；
（2）固定的防火系统或限制火灾的能力；
（3）或影响在火灾情况下达到或保持安全停堆条件的能力。
□ a. 如果“是”，停止，转向火灾SDP评估程序。
□ b. 如果“否”，停止，转向功率工况SDP评估程序。

1) 功率工况SDP评估程序；
2) 停堆工况SDP评估程序；
3) 火灾SDP评估程序；
4) 电厂操纵员评估SDP评估程序；
5) 安全壳完整性SDP评估程序；
6) 蒸汽发生器完整性SDP评估程序；
7) 应急准备SDP评估程序；
8) 职业辐射安全SDP评估程序；
9) 公众辐射安全SDP评估程序；
10)实体保卫SDP评估程序；
11)维修风险评估和风险管理SDP评估程序；
12)恐怖袭击引发的火灾或爆炸导致部分功能丧失SDP评估程序；
13)定性准则评价SDP评估程序。

ΔCDF < 1E-6
1E-6 < ΔCDF < 1E-5
1E-5 < ΔCDF < 1E-4
ΔCDF > 1E-4

绿灯表示无安全影响；白灯表示低微安全影响；黄灯表示中度安全影响；红灯表示显著安全影响。

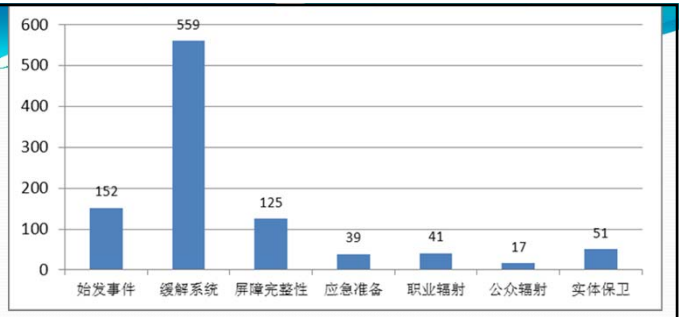
NRC的SDP运作流程主要包含以下几个步骤：

1）对安全事项的初始描述和判定

2）初始重要度复审

3）安全事项初始重要度判定过程中核电厂方面的意见

4）安全事项安全重要度的最终确定



在2012年2季度到2013年1季度期间，共检查出安全事项984个，平均每个机组约10个；其中始发事件安全基石安全事项152个，占总数的15.4%；缓解系统安全基石安全事项559个，占总数的56.8%；屏障完整性安全基石安全事项125个，占总数的12.7%；应急准备安全基石安全事项39个，占总数的4%；职业辐射安全基石安全事项41个，占总数的4.2%；公众辐射安全基石安全事项17个，占总数的1.7%；实体保卫安全基石安全事项51个，占总数的5.2%。

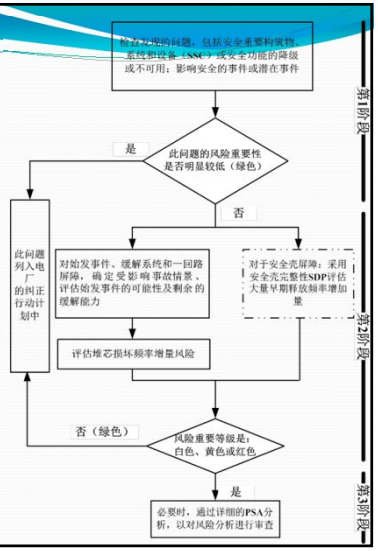
功率工况SDP

功率工况SDP包含三个阶段的工作：

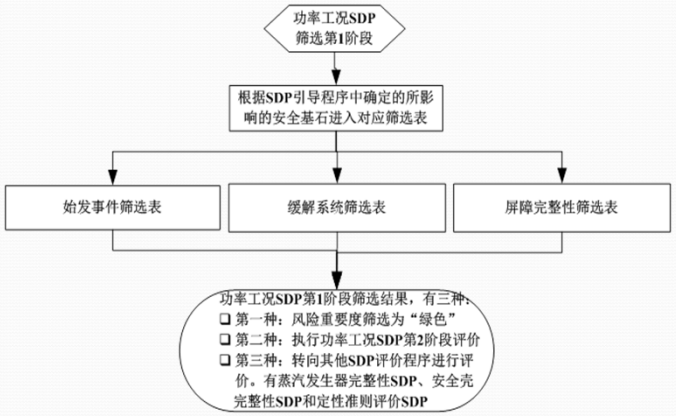
第1阶段：安全事项的特征描述和初步筛选；

第2阶段：风险重要度的评估；

第3阶段：进行详细的概率安全评估，以确定第2阶段的重要度判定是否合理。



功率工况SDP第1阶段实施流程



始发事件筛选表

A. LOCA始发事件

1. 通过对功能降级进行合理评估，判断安全事项所导致的结果是否会产生大于一回路小破口的泄漏率？
   - □ a. 如果“是”，停止，转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，继续下面的问题。
2. 通过对功能降级进行合理评估，判断安全事项是否会影响LOCA事故的缓解系统，最终导致其丧失全部功能。
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，其风险重要度为“绿色”。

B. 瞬态始发事件

1. 安全事项是否导致反应堆紧急停堆以及使核电厂向稳定的停堆状态过渡所需要的缓解系统功能丧失（如丧失冷凝器、丧失主给水）？其他事件还包括高能管道破裂、内部水淹和火灾。
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，其风险重要度为“绿色”。

C. 支持系统始发事件

1. 安全事项是否包括全部或部分支持系统功能的丧失？支持系统功能的丧失可能导致始发事件发生或增加始发事件的发生频率，或影响缓解系统功能，例如丧失厂外电、丧失直流电、丧失交流电、丧失设备冷却水系统、丧失重要厂用水系统和丧失仪表用压缩空气系统。
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，其风险重要度为“绿色”。

D. 蒸汽发生器传热管破裂

1. 安全事项是否包括蒸汽发生器传热管降级事件，即一根传热管不能承受三倍稳态满功率运行状态下压力？
   - □ a. 如果“是”，停止。转向蒸汽发生器完整性SDP评估程序。
   - □ b. 如果“否”，继续下面的问题。
2. 是否一个或多个蒸汽发生器违反“事故泄漏”的性能标准（例如包含超过了设计基准事故状态下规定的事故泄漏的性能标准）？
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估，蒸汽发生器完整性SDP评估程序中适用的部分内容可以作为参考。
   - □ b. 如果“否”，其风险重要度为“绿色”。

D. 外部始发事件

安全事项是否会影响火灾或内部水淹始发事件的发生频率？
- □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
- □ b. 如果“否”，其风险重要度为“绿色”。

缓解系统筛选表

A. 缓解SSC及其功能（不包含反应性控制系统）

1. 如果安全事项影响缓解SSC的设计或技术规格书规定的限制条件，SSC是否能够维持其可操作性或功能？
   - □ a. 如果“是”，其风险重要度为“绿色”。
   - □ b. 如果“否”，继续下面的问题。
2. 安全事项是否表明丧失系统和/或功能？
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，继续下面的问题。
3. 安全事项是否导致缓解系统最少一列丧失的时间大于技术规范所允许的时间，或两个独立的安全系统丧失的时间大于技术规范所允许的时间？
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，继续下面的问题。
4. 安全事项是否导致一个或多个未包含在技术规范中，但在核电厂维修大纲中定义为高安全重要的设备功能丧失大于24小时？
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，其风险重要度为“绿色”。

B. 外部事件缓解系统（地震/火灾/水淹/恶劣气象保护设备）

1. 安全事项是否会导致用于缓解地震、水淹或极端气象等始发事件的设备或功能的丧失或降级？（例如地震缓冲器、水淹屏障等）
   - a) a. 如果“是”，转向“始发事件筛选表”。
   - b) b. 如果“否”，其风险重要度为“绿色”。

C. 反应性控制系统

1. 安全事项是否会影响单个反应堆保护系统（RPS）停堆信号和其他冗余的停堆信号或多样的停堆手段？（例如，其他RPS启动停堆信号，控制棒下插或手动停堆）
   - □ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。
   - □ b. 如果“否”，继续下面的问题。
2. 安全事项是否会导致操纵员对反应性的控制不当（例如，反应堆功率超过功率限值、未能预见和控制反应性的改变）？
   - □ a. 如果“是”，停止。转向定性准则评估SDP。
   - □ b. 如果“否”，继续下面的问题。
3. 该安全事项是否会导致操纵员对反应性的控制出现误操作（例如，反应堆功率超过功率限值、未能提醒和控制反应性的改变）？
   - □ a. 如果“是”，停止。转向定性准则评估SDP。
   - □ b. 如果“否”，其风险重要度为“绿色”。

D. 火灾防护

1. 安全事项是否影响消防队训练和资格授权，或消防队人员配置？
   - □ a. 如果“是”，检查是否涉及以下一项或多项；
   - ● 消防队在消防演习中具备在需要的时间内消除火险的能力，且该安全事项对于消防队响应火灾的能力并无重大影响。
   - ● 在安全事项存在的时间里，消防队所宣称的人手不足的时间小于2小时。
   - □ b. 如果以上的至少有一项符合，其风险重要度为“绿色”。
   - □ c. 如果“否”，继续下面的问题。
2. 安全事项是否影响消防队对火灾的响应时间？
   - □ a. 如果“是”，是否涉及以下一项或多项；
   - ● 消防队的响应时间由于现因别的其他措施得被缓解，例如易燃物存放未超过限制、火灾防护系统功能正常、安全停堆功能未受影响。
   - ● 安全事项影响的高火灾风险区域备有自动灭火系统。
   - ● 核电厂具备充分的现地火灾保护补偿措施。
   - □ b. 如果以上至少有一项符合，其风险重要度为“绿色”。
   - □ c. 如果“否”，继续下面的问题。
3. 安全事项是否影响灭火器、消防软管、消防水龙头？
   - □ a. 如果“是”，检查是否涉及以下一项或多项；
   - ● 防火屏障并未降级，且火灾状况不需要使用水进行灭火。
   - ● 灭火器或消防软管知时间丧失，且因这有置有其他灭火器或水龙头。
   - □ b. 如果以上至少有一项符合，其风险重要度为“绿色”。
   - □ c. 如果“否”，停止。转向定性准则评估SDP。

屏障完整性筛选表

A. 一回路边界（例如导致压力增加的热冲击事件）

□ 停止，转向功率工况SDP第2阶段评估。

B. 安全壳

1.安全事项是否表明实际的安全壳旁路（阀门、气闸门等）、安全壳隔离系统和热移出设备开启？

□ a. 如果“是”，停止。转向安全壳完整性SDP。

□ b. 如果“否”，继续下面的问题。

2.安全事项是否导致安全壳内氢气复合器的功能降低？

□ a. 如果“是”，停止。转向安全壳完整性SDP。

□ b. 如果“否”，其风险重要度为“绿色”。

C. 控制室、辅助厂房、反应堆厂房或乏燃料厂房

1. 安全事项是否导致控制室、辅助厂房或乏燃料水池的放射性屏障功能降级？

□ a. 如果“是”，其风险重要度为“绿色”。

□ b. 如果“否”，继续下面的问题。

2.安全事项是否导致控制室对烟或有毒气体的屏障功能降级？

□ a. 如果“是”，停止。转向功率工况SDP第2阶段评估。

□ b. 如果“否”，其风险重要度为“绿色”。

D. 乏燃料水池

1. 安全事项是否会对乏燃料水池的衰变热移出能力有不利影响，从而导致乏燃料水池温度超过许可的最大限值？

□ a. 如果“是”，停止。转向定性准则评估SDP。

□ b. 如果“否”，继续下面的问题。

2.安全事项是否由燃料转运过失、燃料组件跌落、储存桶跌落或是起重机在乏燃料水池上方操作引起燃料包壳机械损伤以及可发觉的放射性泄漏所导致？

□ a. 如果“是”，停止。转向定性准则评估SDP，职业放射安全SDP评估程序中适用的部分内容可以作为参考

□ b. 如果“否”，继续下面的问题。

3.安全事项是否会导致乏燃料水池水装量下降至许可限值以下？

□ a. 如果“是”，停止。转向定性准则评估SDP。

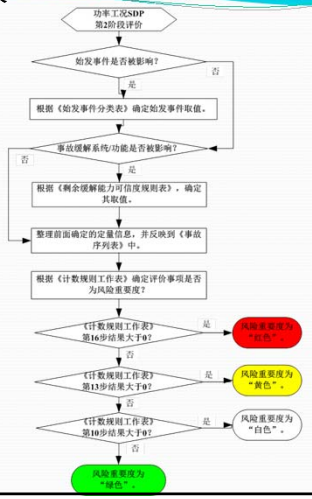
□ b. 如果“否”，继续下面的问题。

4.安全事项是否会影响乏燃料水池的中子吸收、燃料棒束的错误放置或硼浓度？

□ a. 如果“是”，停止。转向定性准则评估SDP。

□ b. 如果“否”，其风险重要度为“绿色”。

功率工况SDP判定第2阶段



功率工况SDP第2阶段判定模型建立

SDP第2阶段分析过程实际上是利用简化的PSA模型，最大的一个特点是故障树不在SDP模型中出现，这一点带来的影响是，SDP 模型的事件树要把功能事件当作一个基本事件来对待。一个完整的SDP模型是以若干张表单的形式呈现的，要使它能够实现对安全事项风险重要度的分析，必须包括以下要素：

1. SDP始发事件；
2. SDP始发事件与系统相关性；
3. SDP功能事件；
4. SDP功能事件缓解能力确定；
5. SDP事件树和事件序列表。

SDP的计算及简化原理

（1）如果A事件和B事件相互独立，那么A事件和B事件同时发生的概率是A事件发生概率和B事件发生概率的乘积：

$$P(AB)=P(A)\cdot P(B)$$

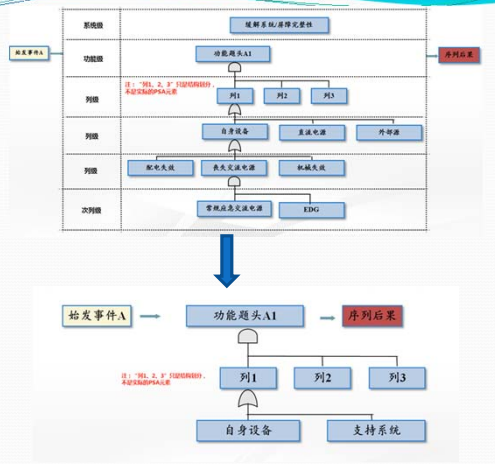
（2）在SDP中，认为始发事件、功能事件失效以及操纵员恢复动作是独立事件；

（3）一个事故序列的发生概率就是始发事件可能性、功能事件失效概率以及操纵员恢复动作失效概率的乘积，由于它们都转化成了对数，因此，将这些对数值相加，即得到事故序列发生概率的对数值。

$$\lg P(ABC)=\lg[P(A)P(B)P(C)]=\lg P(A)+\lg P(B)+\lg P(C)$$

（4）失效概率的量级化

为了简化评估过程，SDP将故障树简化到了列级，所谓列级就是该要素一旦失效，就意味着至少一列失效。



SDP计算简化的方案

假设一座核电厂的基准CDF是CDF_0，它既是一个年化的CDF，又是一个瞬时CDF。在T_0这段时间内（T_0即为暴露时间，这里进行了归一化处理）核电厂发生了一个安全事项，它导致核电厂的瞬时CDF发生了变化，增大到CDF_1，那么核电厂这一年的CDF也发生了变化，新的CDF的计算公式如下：

$$CDF = T_0 \times CDF_1 + (1 - T_0) \times CDF_0$$
$$= CDF_0 + T_0 \times (CDF_1 - CDF_0)$$

则ΔCDF应为

$$\Delta CDF = CDF - CDF_0$$
$$= T_0 \times (CDF_1 - CDF_0)$$

把CDF展开为所有CD序列之和，CD序列又可分解为始发事件发生频率和功能事件的失效概率之积，所以CDF_0和CDF_1应为：

$$\Delta CDF = T_0 \bullet (CDF_1 - CDF_0)$$
$$= T_0 \bullet [(\sum_{n=1}^{N_1} IEF'_n \bullet P'_n + \sum_{m=1}^{N-N_1} IEF_m \bullet P_m) - (\sum_{n=1}^{N_1} IEF_n \bullet P_n + \sum_{m=1}^{N-N_1} IEF_m \bullet P_m)]$$
$$= T_0 \bullet \sum_{n=1}^{N_1} (IEF'_n \bullet P'_n - IEF_n \bullet P_n)$$

同是，SDP中对始发事件频率和功能题头失效概率都进行了量级化处理，并将SDP将安全事项的暴露时间T0划分为3天以内、3-30天、30天以上三个区间，分别对应暴露时间水平T_{0L}为2、1、0。

$$\Delta CDF_L = -log_{10}\left[\sum_{n=1}^{N1}(T_0 \cdot IEF'_n \cdot P'_n)\right]$$
$$= -\sum_{\text{SDP 量级求和}} (T_{0L} + IEL'_n + PL'_n)$$

其中，T_{0L}为暴露时间对应的暴露时间水平，IEL为事故序列的始发事件水平，为了方便使用，将T_{0L}合并到IEL中，始发事件的IEL不再是定值，而是随着暴露时间水平变化而变化的值。

SDP在功能事件处理上的简化

SDP功能事件的概念同PSA功能事件的概念是一样的，同样具有成功准则，但是SDP功能事件被当作基本事件来处理。

这样带来的一个问题就是在没有故障树支持的条件下如何确定功能事件这个“基本事件”的失效概率。

- 一种情况下，功能事件的输入本来就是一个基本事件，比如人因事件，则直接根据基本事件的失效概率为这个功能事件指定一个数值。
- 另一种情况下，功能事件的输入是一颗故障树，这颗故障树代表着一个前沿系统，SDP为这种情况设计了一种特别的解决方法。SDP为前沿系统指定一种类型，这个类型与系统的复杂程度和冗余度有关，决定了功能事件失效概率的量级，**这个量级称之为功能事件的缓解能力。**
- 剩余缓解能力是指受到安全事项影响的功能事件变化后的缓解能力。

“功能系统剩余缓解能力准则表” 规定了前沿系统或人因事件的剩余能力因子，以数字表示，数字越大说明该功能的能力越强，即对后果的缓解能力越强。

- 可信的缓解能力是以系统列的形式定义的，同时也要考虑核电厂PSA报告中特定的成功准则。
- 而剩余缓解能力的大小主要取决于系统和操纵员行为的可用性和可靠性，但在分析中不考虑其支持系统的可用性。
- 如果系统的列存在不同的特点导致它们缓解事故的可靠性不同，那么这些列就要分别定义。例如，辅助给水系统的电动泵列和汽动泵列就要分别定义。各个功能系统剩余缓解能力数值将在事故序列分析中参与计算。

剩余缓解能力的类型	剩余缓解能力可信度：x = -log10(失效概率)
失效列恢复： 操纵员恢复失效设备的行为，而且这些设备是事件发生后可以恢复的。操作行为可以是在主控室，也可以是主控室之外，当认为其为可信的剩余缓解能力时，它的失效概率约为1E-1。只有满足以下的准则才认为是可信的： (1) 有足够的时间实施这些操作； (2) 环境条件允许到达操作的区域； (3) 有用于指导操作行为的程序； (4) 在相似的事故情景下有依据程序进行的培训； (5) 用于完成这些操作的任何设备都是可用的，且处于备用状态。	1
一列自动蒸汽驱动： 一套相关设备，其中包含一个汽动驱动设备且能提供100%的指定安全功能。当这一列被确信为剩余缓解能力时，则因失效、试验或维修导致一列不可用的概率假定为：1E-1。	1
完成功能的1列设备： 一套相关设备（如泵、阀门、开关等），它们一起能够完成100%的制定安全功能。当这一列被确信为剩余缓解能力时，则因失效、试验或维修导致这些设备不可用的概率假定为：1E-2。	2
1个多列系统： 一个由两列或多列组成的系统，认为他们之间存在共因失效模式。当这一系统被确信为剩余缓解能力时，则不论该系统有多少列，其因失效、试验或维修导致系统中设备不可用的概率假都定为：1E-3。	3
2个不同的列： 一个系统由两列组成，且两列之间不存在共因失效模式。当这一系统被确信为剩余缓解能力时，则因失效、试验或维修导致系统中设备不可用的概率假都定为：1E-4。	4（＝2+2）
操纵员行为的可信度： 事故处理期间，由操纵员执行的重要操作（如通过充-排方式移出一回路的热量等）。这些操作行为使用三类人员失误概率（HEP）表征可信度。这些类别是： (1) 操作行为＝1，代表人员操作失效概率在5E-2~0.5之间； (2) 操作行为＝2，代表人员操作失效概率在5E-3~5E-2之间； (3) 操作行为＝3，代表人员操作失效概率在5E-4~5E-3之间。	1、2或3

核电厂发生的安全事项有一个持续时间，即从它刚出现到事件分析时这段时间，称之为安全事项的暴露时间。安全事项只在暴露时间内对核电厂的CDF产生影响。因此，需要根据安全事项的持续时间来修改始发事件的发生概率。

SDP将安全事项的暴露时间划分为3类，“>30天”近似等于1年，“3-30天”近似等于1/10年，“<3天”近似等于1/100年，将安全事项的暴露时间乘以始发事件频率，即得到始发事件可能性（IEL）。

始发事件分类表					
类型	始发事件频率	始发事件组	始发事件可能性 $X=-\log_{10}$（始发事件频率）		
I	$>10^{-1}$ /堆年	主给水丧失（LMFW）、二回路变化引起的瞬态（STRANS）、其他瞬态（TRANS）	1	2	3
II	10^{-2}~10^{-1} /堆年	部分（安全段）丧失热阱（LHS2）、部分（公用段）丧失热阱（LHS3）、丧失压缩空气（LOIA） 丧失厂外电源（LOOP）、30V列直流电源（LDDD）	2	3	4
III	10^{-3}~10^{-2} /堆年	给水管道破口（FWLB）、48V A列直流电源丧失（LDCA）、48V B列直流电源丧失（LDCB）、48V C列直流电源丧失（LDCC）、125V A列直流电源丧失（LDBA）、安全壳内主蒸汽管道破口（MSLB1）、安全壳外主蒸汽隔离阀上游破口（MSLB2）、安全壳外主蒸汽隔离阀下游破口（MSLB3）、蒸汽发生器传热管断裂（SGTR）、小破口失水事故（SLOCA）	3	4	5
IV	10^{-4}~10^{-3} /堆年	全部丧失热阱（LHS1）、中破口失水事故（MLOCA）、蒸汽管小破口叠加1根蒸汽发生器传热管断裂（SSGTR1）	4	5	6
V	10^{-5}~10^{-4} /堆年	给水丧失相关的未停堆的瞬态（ATWT2）、大破口失水事故（LLOCA）、稳压器汽相SEBIM阀破口失水事故	5	6	7
VI	$<10^{-5}$ /堆年	其他未停堆的瞬态事件（ATWT1）、界面LOCAV-LOCA（ISLOCA）、蒸汽管小破口叠加10根蒸汽发生器传热管断裂（SSGTR2）	6	7	8
安全事项存在的时间（天）			>30	3~30	<3

SDP始发事件的确定

1)合并

- 对功能题头进行简化后，将事件树进程基本一致的始发事件进行合并，并以最不利工况进行包络。
- 合并后的始发事件频率为被合并始发事件频率之和。

2)删除

- 将频率极小且造成的CDF小于10^{-10}的始发事件进行删除。

PSA始发事件	始发事件描述	处理方式	对应的SDP始发事件	说明
LLOCA1A	大破口	不做处理	LLOCA	该两棋树的主要差异为中压安注箱的注入方式不一样，采用包络的形式将“完好的1台中压安注箱成功M03”调整为“2/2台中压安注箱成功注入M02”，除此之外，其他完全相同。
LLOCA2A	压力容器直接注入管线大破口	将“完好的1台中压安注箱成功M03”调整为“2/2台中压安注箱成功注入M02”		

始发频率量级化

始发事件频率的范围								
始发事件频率	＞1	1E-1～1	1E-2～1E-1	1E-3～1E-2	1E-4～1E-3	1E-5～1E-4	1E-6～1E-5	＜1E-6
始发事件可能性	0	1	2	3	4	5	6	7

将经过合并和删除后的始发事件频率进行量级化处理，引入始发事件水平（IEL）来代替始发事件频率（IEF），IEL=-log（IEF的量级），如始发事件频率为2.8E-3次/年时，其IEL为3。如果安全事项造成始发事件频率上升，通常情况下，SDP将其处理为将IEL提高一个等级，例如，某安全事项会造成IEL为3的丧失厂外电（LOOP）事件频率上升则提高一个等级，按照IEL为2进行计算。

SDP始发事件清单

序号	始发事件组编码	始发事件描述	始发事件频率	备注
1	ATWT1	其他ATWT	1.65E-06	30/48/125V直流电源丧失、厂外电源丧失的瞬态
2	ATWT2	给水丧失相关的ATWT	8.55E-05	压缩空气丧失、主给水丧失、二次侧引发的瞬态以及其他导致停堆的瞬态
3	ISLOCA	界面LOCAV-LOCA	1.50E-07	
4	LDBA	125V A列直流电源	9.70E-04	A列125V直流电源
5	LDCA	丧失直流电源LCA	5.63E-03	A列48V直流电源
6	LDCB	丧失直流电源LCB	5.63E-03	B列48V直流电源
7	LDCC	丧失直流电源LCC	2.30E-03	C列48V直流电源
8	LDDD	30V列直流电源	1.10E-02	30V直流电源
9	LHS1	全部丧失热阱	1.00E-04	丧失最终热阱
10	LHS2	部分丧失热阱(安全段)	7.40E-02	丧失RRI安全段
11	LHS3	部分丧失热阱(公用段)	1.00E-02	丧失RRI公用段
12	LLOCA	大破口失水事故	1.00E-04	一回路大破口
13	LMFW	主给水丧失	5.00E-01	丧失主给水
14	LOIA	丧失压缩空气	1.20E-02	丧失压缩空气
15	LOOP	丧失厂外电源	2.50E-02	丧失厂外电源
16	MLOCA	中破口失水事故	3.00E-04	一回路中破口
17	MSLB1	安全壳内主蒸汽管道破口	1.10E-03	安全壳内蒸汽管道破口，不分大小破口，全部合并，并且包括给水管道破口
18	MSLB2	安全壳外主蒸汽隔离阀上游破口	1.01E-03	安全壳外主蒸汽隔离阀上游破口
19	MSLB3	安全壳外主蒸汽隔离阀下游破口	6.00E-03	安全壳外主蒸汽隔离阀下游破口
20	SGTR	蒸汽发生器传热管断裂	6.72E-03	蒸汽发生器传热管破裂，合并原先的1/2根SGTR
21	SLOCA	小破口失水事故	2.00E-03	一回路小破口，合并原先的BS1A和BS2A
22	SORV	稳压器汽相SEBIM阀破口失水事故	5.90E-05	稳压器安全阀卡开
23	SSGTR 1	蒸汽管小破口叠加1根蒸汽发生器传热管断裂	4.80E-05	蒸汽管道小破口叠加1和2根SGTR，不考虑大破口叠加SGTR，因为其贡献很小
24	SSGTR 2	蒸汽管小破口叠加10根蒸汽发生器传热管断裂	1.00E-06	蒸汽管道小破口叠加10根SGTR
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

始发事件分类表					
类型	始发事件频率	始发事件组	始发事件可能性 $X=-\log_{10}$（始发事件频率）		
Ⅰ	$>10^{-4}$ /堆年	主给水丧失（LMFW）、二回路变化引起的瞬态（STRANS）、其他瞬态（TRANS）	1	2	3
Ⅱ	10^{-2}~10^{-1} /堆年	部分（安全段）丧失热阱（LHS2）、部分（公用段）丧失热阱（LHS3）、丧失压缩空气（LOIA） 丧失厂外电源（LOOP）、30V列直流电源（LDDD）	2	3	4
Ⅲ	10^{-3}~10^{-2} /堆年	给水管道破口（FWLB）、48V A列直流电源丧失（LDCA）、48V B列直流电源丧失（LDCB）、48V C列直流电源丧失（LDCC）、125V A列直流电源丧失（LDBA）、安全壳内主蒸汽管道破口（MSLB1）、安全壳外主蒸汽隔离阀上游破口（MSLB2）、安全壳外主蒸汽隔离阀下游破口（MSLB3）、蒸汽发生器传热管断裂（SGTR）、小破口失水事故（SLOCA）	3	4	5
Ⅳ	10^{-4}~10^{-3} /堆年	全部丧失热阱（LHS1）、中破口失水事故（MLOCA）、蒸汽管小破口叠加1根蒸汽发生器传热管断裂（SSGTR1）	4	5	6
Ⅴ	10^{-5}~10^{-4} /堆年	给水丧失相关的未停堆的瞬态（ATWT2）、大破口失水事故（LLOCA）、稳压器汽相SEBIM阀破口失水事故	5	6	7
Ⅵ	$<10^{-5}$ /堆年	其他未停堆的瞬态事件（ATWT1）、界面LOCAV-LOCA（ISLOCA）、蒸汽管小破口叠加10根蒸汽发生器传热管断裂（SSGTR2）	6	7	8
安全事项存在的时间（天）			>30	3~30	<3

系统和设备与始发事件相关性表

影响的系统	主要设备	支持系统	始发事件
辅助给水系统	电动泵A列、气动调节阀	30V（LDA）直流电源、48V（LCA、LCB）直流电源、125V（LBA、LBB）直流电源、仅用压缩空气系统（SAR）	除了MLOCA、LLOCA、30V直流丧失、以及A列电源丧失的所有始发事件
	电动泵B列、气动调节阀	30V（LDA）直流电源、48V（LCA、LCB）直流电源、125V（LBA、LBB）直流电源、仅用压缩空气系统（SAR）	除了MLOCA、LLOCA、30V直流丧失、以及B列电源丧失的所有始发事件
	一台汽动泵、气动调节阀（供水）、气动隔离阀（汽机供气）	30V（LDA）直流电源、仅用压缩空气系统（SAR）	除了MLOCA、LLOCA和30V直流丧失的所有始发事件
安全壳喷淋系统	两台安注泵（EAS001PO/EAS002PO）、电动阀	48V（LCA、LCB）直流电源、125V（LBA、LBB）直流电源、6.6KV（LHA/LHB）交流电源	一回路破口
重要厂用水系统	A列：SEC001PO/SEC003PO B列：SEC002PO/SEC004PO	48V（LCA、LCB）直流电源、125V（LBA、LBB）直流电源、6.6KV（LHA/LHB）交流电源、仅用压缩空气	热阱丧失相关的始发事件、涉及安全壳喷淋再循环和余热排出功能的始发事件
应急柴油机	LHP001AP、LHQ001AP、LHA002JA、 LHB002JA	48V（LCA、LCB）直流电源、125V（LBA、LBB）直流电源，EDG润滑油系统、冷却系统以及通风系统	涉及厂外电源丧失的始发事件

SDP功能事件的确定

方式 1——删除

示例 1：停堆功能（A01，A03，A04，A07）

理由：在 PSA 模型的事件树中，停堆功能失败则转到停堆保护拒动（ATWS）继续分析，SDP 模型中已经把 ATWS 当作始发事件处理，因此在 SDP 模型其他事件树中不需要再出现停堆功能事件。

示例 2：开启的 1 组稳压器安全阀回座失败（S01）

理由：这个功能事件的失效引发稳压器安全阀泄漏事件（SORV），将在 SORV 事件树中分析，而在主蒸汽管道安全壳内破口 SDP 事件树中不考虑。

方式 2——合并

示例 1：不同的“高压/中压安注”

理由：不同情境的高压/中压安注，按照主要设备配置相同进行合并，而不区分发生的事故情景。

方式 3——拆分

示例 1：充-排冷却（H05）

理由：该功能题头中包括 1/3 稳压器安全阀开启（SRV01）、高压安注直接注入（HPSI）、高压安注冷端再循环（HPR01）和执行充排操作的人因事件（LODC-H2）四个事件题头。为了更好地模化其影响，将该充排冷却题头（H05）拆分为四个题头在事件树里体现。

人员失误概率的范围

HEP	5E-2～5E-1	5E-3～5E-2	5E-4～5E-3
缓解能力	1	2	3

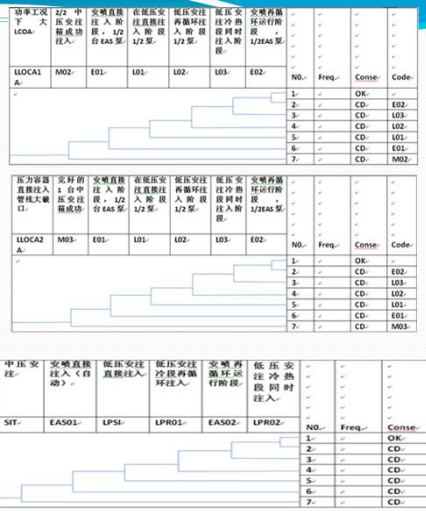
人因事件编码	推述	PSA人因分析值	能力等级初值
ATWT下的人因事件			
ATWT-H1	ATWS事故后操纵员使用SPI规程使反应堆重返次临界	2.90E-04	3
蒸汽管道破口的人因事件			
MSLB-H2	蒸汽管道破口事故后58分钟内，操纵员执行U1规程对一回路Feed-Bleed	2.00E-02	2
MSLB-H3	安全壳内/外蒸汽管道破口未引发蒸汽发生器传热管破裂	1.00E-02	2
MSLB-H4	操纵员手动停安注	4.24E-04	3
直流电源丧失的人因事件			
LODC-H1	30分钟内通过LLJ和另一机组LNE360CR恢复LNE360CR的供电	5.50E-03	2
LODC-H2	操纵员根据U1规程，在78分钟内手动执行feed-bleed操作	2.22E-03	3
LODC-H3	操纵员就地调节ASG流量	2.00E-05	3
LDBA-H1	实施RCV泵的保护措施	4.82E-02	2
LDBA-H2	9RIS011PO手动投用	5.20E-04	3
丧失厂外电源的人因事件			
LOOP-H1	根据U1规程，105分钟内操纵员未能手动执行feed-bleed操作	5.23E-03	2
LOOP-H2	实施从相邻机组LNE360CR供电	3.25 E-4	3
LOOP-R	电源恢复	6.02E-01	1
LMFW事故下的人因事件			
LMFW-H1	事故后78分钟内，操纵员使用H2规程成功进行充排操作	2.22E-03	3
LOCA事故下的人因事件			
MLOCA-H1	事故后18分钟内，操纵员采用了U1规程对一回路进行快速降温降压	3.73E-01	1
SLOCA-H1	事故后60分钟内，操纵员按照A1.1规程以56C/h执行快速降温降压	5.50E-04	3
SLOCA-H2	高压安注失效后30分钟内，操纵员采用了U1规程进行快速降温降压	1.68E-01	1
SLOCA-H3	操纵员在78分钟内采用U1规程对一回路实施充排冷却	2.52E-03	3
SGTR事故下的人因事件			
SGTR-H1	执行A3规程隔离破损蒸汽发生器	2.46E-02	2
SGTR-H2	执行U1规程对一回路实施快速降压	2.03E-03	3
SGTR-H3	执行U1规程对一回路实施充排操作	2.22E-03	3
SGTR-H4	操纵员执行A3规程在37分钟内平衡一二回路压力	2.00E-04	3

功能事件编码	功能事件	成功准则
A03	ATWT信号	~~ATWT信号由两种不同类型的信号组成（给水流量低信号和中子注入率高信号），任何一组信号成功触发即成功。~~
A05	慢化剂温度系数<k	根据PSA分析，慢化剂温度系数<k的概率为1.71E-1。
C01	通过9RIS011PO方式上充补水	发生轴封破口，通过9RIS011PO方式上充补水
G01	二次侧冷却(一台泵一个GCT)	ASG系统有4列，两列电动泵，两列汽动泵。此功能事件的成功准则是一台电动泵或一台汽动泵，同时必须1/4GTCa可用。
G02	二次侧冷却（二台泵二个GCT)	ASG系统有4列，两列电动泵，两列汽动泵。此功能事件的成功准则是两台电动泵或两台汽动泵，同时必须2/4GTCa可用。
G03	二次侧冷却（一台泵一个GCTA）	由于A列直流电源故障，只有B列电动泵和汽动泵可用，成功准则是一台泵，同时必须1/4GTCa可用。
G04	二次侧冷却（一台泵一个GCTA）	ASG系统有4列，两列电动泵和两列汽动泵。此功能事件的成功准则是一台电动泵或一台汽动泵，同时必须1/4GTCa可用，并且考虑人员操作。根据PSA人因分析，有规程指导的流量调节失效概率为2.0E-5，与两列设备失效同量级。
G05	二次侧冷却(一台泵一个GCT)	由于B列直流电源故障，只有A列电动泵和汽动泵可用，成功准则是一台泵，同时必须1/4GTCa可用。

根据剩余缓解能力准则，确定功能事件的剩余缓解能力。

功能事件编码	缓解能力类型	缓解能力初值
A03	1个多列系统	3
A05	操作员动作	1
C01	完成功能的1列设备	2
G01	2个不同的列系统	4
G02	1个多列系统	3
G03	2个不同的列系统	4
G04	1个多列系统	3
G05	2个不同的列系统	4

SDP事件树的建立



象的安全功能：	每一安全功能完全可信的缓解能力：
全壳喷淋直接注入（EAS01）	安全壳喷淋系统有 2 列，一列运行成功即可，系统是自动启动。
全壳喷淋再循环（EAS02）	安全壳喷淋系统有 2 列，一列运行成功即可，系统是自动切换。
压安注冷段再循环（LPR01）	低压安注由 2 列构成，一列从地坑取水，并向一回路冷段注入。
压安注冷热段同时再循环（LPR02）	低压安注由 2 列构成，一列从地坑取水，并向一回路冷段注入。
压安注直接注入（LPSI）	低压安注由 2 列构成，一列从换料水箱取水，并向一回路冷段注入。
压安注（SIT）	安注箱属于非能动设备，投入无需操纵员的干预。此功能题头的成功准则为：2/2 个安注箱及注入管线成功即可。

	选择受影响的功能	基准分	始发事件可能性	每一受影响的事故序列的剩余缓解能力评估	失效列的恢复	结果	LERF 因子
	LLOCA+EAS01 8 ＋ 3	11					
	LLOCA+EAS02 8 ＋ 3	11					
	LLOCA+LPR01 8 ＋ 3	11					
	LLOCA+LPR02 8 ＋ 3	11					
	LLOCA+LPSI 8 ＋ 3	11					
	LLOCA+SIT 8 ＋ 4	12					

事故序列分析表

步骤	操作指令/指示	得分
（1）	输入风险重要序列值等于9的个数。	
（2）	第（1）步的结果除3，并把所得结果记入下一轮。	
（3）	输入风险重要序列值等于8的个数。	
（4）	第（3）步结果与第（2）步结果相加。	
（5）	第（4）步的结果除3，并把所得结果记入下一轮。	
（6）	输入风险重要序列值等于7的个数。	
（7）	第（6）步结果与第（5）步结果相加。	
（8）	第（7）步的结果除3，并把所得结果记入下一轮。	
（9）	输入风险重要序列值等于6的个数。	
（10）	第（9）步结果与第（8）步结果相加。	
（11）	第（10）步的结果除3，并把所得结果记入下一轮。	
（12）	输入风险重要序列值等于5的个数。	
（13）	第（12）步结果与第（11）步结果相加。	
（14）	第（13）步的结果除3，并把所得结果记入下一轮。	
（15）	输入风险重要序列值等于4的个数。	
（16）	第（15）步结果与第（14）步结果相加。	

- 如果第16步结果大于0，则检查安全事项的风险重要性是高安全重要度，用“红色”表征。
- 如果第13步结果大于0，则检查安全事项常的风险重要性至少是重要的安全重要度，用“黄色”表征。
- 如果第10步结果大于0，则检查安全事项的风险重要性至少是中等安全重要度，用“白色”表征。
- 如果第10、13和16步结果都是0，则检查安全事项的风险重要性是非常低的安全重要度，用“绿色”表征。

第2阶段的评估结果：绿色 白色 黄色 红色

功率工况SDP判定第3阶段

1. **安全事项的审查和分析：** 在充分了解事件的基础上，确定原因和重要因素，从PSA角度了解安全事项的背景。
2. **将安全事项映射到PSA逻辑结构上：** 安全事项及其相关信息与PSA模型建立联系。
3. **定量化：** 评估故障概率，修改PSA可靠性模型。
4. **计算结果：** 重新计算所有相关事故序列的ΔCDF。
5. **结果判定：** 将计算结果与风险重要度判定准则进行对比，判定安全事项的最终风险重要度。

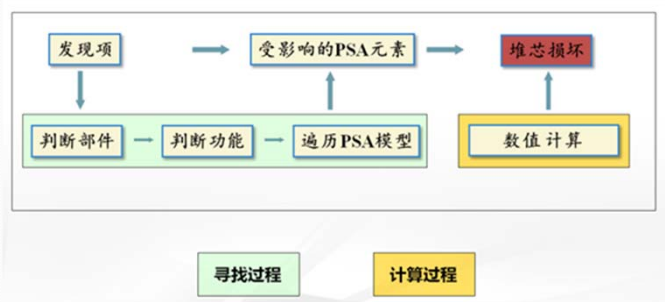
表 4-1 颜色标识所代表的风险（定性）

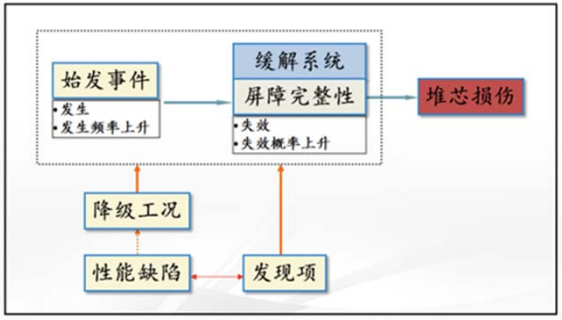
颜色	风险大小程度
绿色	表示安全性能完全满足相关安全基石的目标，电厂性能没有重大偏离
白色	表示安全性能偏离期望的正常范围，安全裕量略有下降，但是满足安全基石的目标
黄色	表示安全性能下降明显，安全裕量有所下降，安全基石目标有所下降
红色	表示安全裕量大幅度降低，连续运行有可能将不能确保公众的健康与安全

表 3-2 颜色表示所代表的风险（定量）

颜色	风险大小程度（定量）
绿色	ΔCDF≤1.0E-6 或 ΔLERF≤1.0E-7
白色	1.0E-6＜ΔCDF≤1.0E-5 或 1.0E-7＜ΔLERF≤1.0E-6
黄色	1.0E-5＜ΔCDF≤1.0E-4 或 1.0E-6＜ΔLERF≤1.0E-5
红色	ΔCDF≥1.0E-4 或 ΔLERF≥1.0E-5

与PSA分析过程的对比





停堆工况SDP

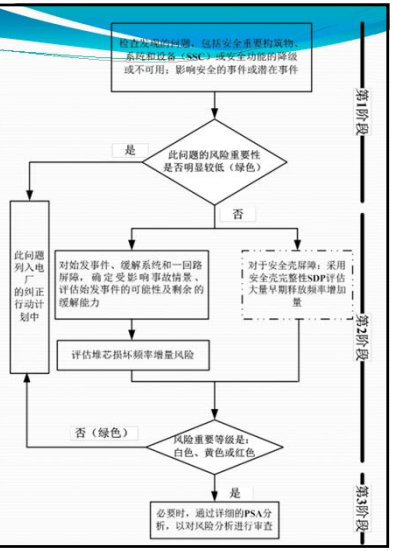
停堆工况SDP主要评估核电厂3个安全基石的性能状态，包括始发事件、缓解系统和屏障完整性。

第1阶段：安全事项的特征描述和初步筛选；

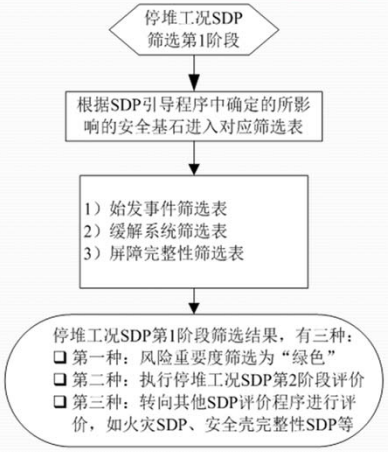
第2阶段：风险重要度的评估；

第3阶段：进行详细的概率安全评估，以确定第2阶段的重要度判定是否合理。

，



停堆工况SDP第1阶段



始发事件筛选表

A.停堆始发事件

1.安全事项所 导致的结果是否会增加停堆始发事件的发生可能性？

- □ a. 如果“是”，停止，转向停堆工况SDP第2阶段评估。
- □ b. 如果“否”，继续。

B.LOCA始发事件

1.破口位置是否无法探测或无法隔离，并且在24小时内将导致正常的安全功能失效（如，水位降低导致余热排出泵无法正常工作）？

- □ a. 如果“是”，停止，转向转向停堆工况SDP第2阶段评估。
- □ b. 如果“否”，继续。

2.一回路水装量受泄漏影响下降，在影响余 热排出系统功能前，是否能够自动停止泄漏？

- □ a. 如果“是”，继续。
- □ b. 如果“否”，停止，转向转向停堆工况SDP第2阶段评估。

C.瞬态始发事件

1.丧失厂外电（LOOP）和丧失余热导出系统（LORRA）事件发生时，堆芯燃料是否处于淹没状态？

- □ a. 如果“是”，继续。
- □ b. 如果“否”，停止，转向停堆工况SDP第2阶段评估。

2.丧失厂外电（LOOP）时，恢复厂外电的时间是否大于一回路水蒸发导致燃料原件裸露出水面的时间？

- □ a. 如果“是”，停止，转向停堆工况SDP第2阶段评估。
- □ b. 如果“否”，继续。

3.丧失液位控制（LOLC）时，一回路是否没有处于满水状态？

- □ a. 如果“是”，停止，转向停堆工况SDP第2阶段评估。
- □ b. 如果“否”，继续。

D.外部事件始发事件

1.安全事项是 否会影响火灾或内部水淹始发 事件 的频率并可能导致停堆始发事件 的发生？

- □ a. 如果“是”，停止，转向第3阶段评估。
- □ b. 如果“否”，其风险重要度为“绿色”。

缓解系统筛选表

A. 缓解设备、备用和部件（SSC）和功能

1.如果安全事项是缓解系统设计或功能被旁路，带旁路运行的缓解系统是否能够维持其可操作性和非故缓解功能？

- □ a. 如果“是”，其风险重要度为“绿色”。
- □ b. 如果“否”，继续。

2.安全事项是否表示丧失系统安全功能？

- □ a. 如果“是”，停止，转向停堆工况SDP第2阶段评估。
- □ b. 如果“否”，继续。

1. 安全事项是否表示以下情形的实际功能丧失，即最少一列丧失时间大于技术规范所允许的时间，或两个独立的安全系统丧失的时间大于技术规范所允许的时间？
   - □ a. 如果“是”，停止，转向停堆工况SDP第2阶段评估。
   - □ b. 如果“否”，继续。
3. 反应堆水池注水时，安全事项是否表示以下情形的实际功能丧失，即一个或多个技术规范中不包含的，在电厂停堆过程中高安全重要度设备功能丧失>24小时？
   - □ a. 如果“是”，停止，转向停堆工况SDP第2阶段评估。
   - □ b. 如果“否”，继续。
4. 反应堆水池未注水时，该安全事项是否表示以下情形的实际功能丧失，即一个或多个技术规范中不包含的，在电厂停堆过程中高安全重要度设备功能丧失>4小时？
   - □ a. 如果“是”，停止，转向转向停堆工况SDP第2阶段评估。
   - □ b. 如果“否”，继续。
5. 反应堆水池未注水时，该安全事项是否导致一回路水位监测系统降级或反应堆测量热电偶降级？
   - □ a. 如果“是”，停止，转向停堆工况SDP第2阶段评估。
   - □ b. 如果“否”，继续。

A. 外部事件缓解系统（消防/火灾/水淹/恶劣天气保护降级）

1.安全事项是否包含专用于缓解地震，水淹或恶劣天气始发事件的设备或功能的丧失或降级？

- □ a. 如果“是”，停止，转向第3阶段。
- □ b. 如果“否”，继续。

A. 火灾消防员

1.安全事项是否包括消防队训练和资格授权，或消防队人员配置？

- □ a. 如果“是”，检查以下几项是否有一项或多项被涉及。
  - 消防队在消防演习中具备在需要的时间内消除火险的能力，且该安全事项对于消防队响应火灾的能力并无重大影响。
  - 在所有任务时间中，消防队所面临的人手不足的事件短于2小时。
- □ 如果没有以上内容，停止，执行定性筛选SDP程序。
- □ 如果至少有一项，继续。
- □ b. 如果“否”，继续。

2.安全事项是否包括对消防队响应火灾时间的影响？

- □ a. 如果“是”，检查以下几项是否有一项或多项被涉及。
  - 消防队的响应时间由于纵深防御的其他元素而被缓解，例如易燃物存放未超过限制，火灾防护系统功能正常，安全停堆功能未受影响。
  - 该安全事项包括高火灾风险重要度区域，具备自动灭火系统
  - 电厂具备充分的就地火灾保护补偿措施
- □ 如果没有以上内容，停止，执行定性筛选SDP程序。
- □ 如果至少有一项，继续
- □ b. 如果“否”，继续

3.安全事项是否包括灭火器，灭火水龙带，灭火水龙头？

- □ a. 如果“是”，检查以下几项是否有一项或多项被涉及
  - 防火屏障并未降级，且火险状况不需要使用灭速行灭火
  - 灭火器或水龙带如时间丢失，且附近有其他灭火器、水龙头
- □ 如果没有以上内容，停止，执行定性筛选SDP程序
- □ 如果至少有一项，绿色

屏障完整性筛选表

A. 一回路边界或燃料包壳

- □ 如果安全事项是燃料棒放置位置错误则为“绿色”。

1. 低温超压—安全事项是否包含一个由于疏忽导致的安注或者在低温超压时，释放阀（PORV）或安全阀无法在需要的时候正常动作？
   - □ a. 如果“是”，停止，转向第3阶段。
   - □ b. 如果“否”，继续。
2. 冷冻密封—安全事项是否会导致冷冻密封的潜在失效增加，或者导致余热排出系统出现破口或导致其他丧失冷却剂事件发生？
   - □ a. 如果“是”，停止，转向第3阶段。
   - □ b. 如果“否”，继续。
3. 蒸汽发生器下封头—安全事项是否导致下封头安装问题，导致蒸汽发生器下封头降级或功能性丧失？
   - □ a. 如果“是”，停止，转向第3阶段。
   - □ b. 如果“否”，继续。
4. 安全事项是否导致潜在的一回路硼稀释？
   - □ a. 如果“是”，停止，转向定性SDP分析。
   - □ b. 如果“否”，继续。

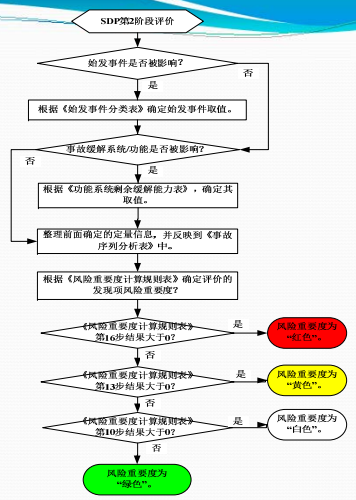
5.安全事项是否导致排水口隔离功能降级？

- □ a. 如果“是”，停止，转向第3阶段。
- □ b. 如果“否”，继续。

A. 安全壳

1. 该安全事项是否表示安全壳关闭或隔离能力的降级？
   - □ a. 如果“是”，停止，转向安全壳完整性SDP。
   - □ b. 如果“否”，继续。
2. 该安全事项是否标示着反应堆安全壳物理完整性的降级（阀门，贯穿件，封堵结构）？
   - □ a. 如果“是”，停止，转向安全壳完整性SDP。
   - □ b. 如果“否”，继续。
3. 该安全事项是否标示着反应堆安全壳物理完整性的降级（阀门，贯穿件，封堵结构）？
   - □ a. 如果“是”，停止，转向安全壳完整性SDP。
   - □ b. 如果“否”，其风险重要度为绿色。

停堆工况SDP第2阶段



电厂运行状态划分

POS-B1	如果为了便于LPSD工作而将某一LPSD 进程的若干POS归并成组，那么归并过程和POS的最终定义必须确保归并成的组选择了最严格的或最有约束性的特征（对CD 或 LER而言）。 该过程必须考虑始发事件的类型和频率。 说明： POS 组的持续时间等于组内各个POS 的持续时间之和。 POS 组的频率不等于组内各个POS 的频率之和。 建议对电厂状态采取归并的方法而不是筛选淘汰的方法，因为即使某个电厂状态的持续时间很短，但是条件堆芯损坏概率有可能很高，如果被筛选掉，则可能会遗漏掉重要的堆芯损坏贡献项。 POSs可以根据相似的参数例如温度、压力、衰变热以及衰变热移出机制进行归并。

POS	名称	机组状态			温度控制	起始点		结束点
		水位	温度/℃	压力/MPa				
POS 1	NS/RRA	IN PZR	10≤T≤180	0.5≤P≤3.0	RRA，SG 备用	下	RRA 接入（M3）	进入维修冷停堆（M10）
						上	离开维修冷停堆（M60）	RRA 隔离（M70）
POS 2	人孔关闭的维修冷停堆	PZR 满水	10≤T≤60	0.1≤P≤0.5	RRA，SG 备用	下	进入维修冷停堆（M10）	人孔打开（M12）
						上	人孔关闭（M53）	离开维修冷停堆（M60）
POS 3	人孔打开的维修冷停堆	PZR 水位+2m→法兰面水位→反应堆水池满水	10≤T≤60	0.1	RRA，PTR 备用	下	人孔打开（M12）	反应堆水池满水（M20）
						上	一回路开始排水（M50）	人孔关闭（M53）

火灾工况异常重要性（SDP）评估程序

火灾SDP适用于机组在功率工况下的风险评估，包括3个评估阶段。

第1阶段：火灾安全事项特征描述和初步筛选。评估人员需要辨别安全事项，并对安全事项的特征进行准确描述，采用确定论和概率论方法进行评估，并对低重要度（绿色）的事项进行初步筛选；

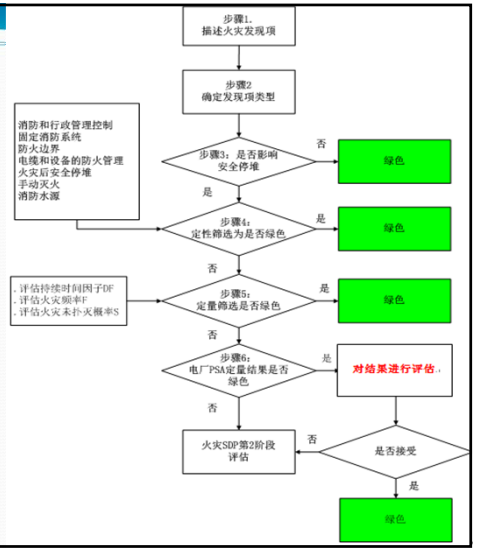
第2阶段：进一步通过确定论和概率论方法对安全事项风险进行评估。此阶段是在第1阶段的基础上，进一步对第1阶段评估的非“绿色”安全事项做进一步的细化评估，以便进一步确定安全事项风险重要度等级（绿白黄红）；

第3阶段：该阶段是风险重要度的最终确定。对安全事项进行详细的概率安全评估，审查第2阶段所得的风险重要度评估结果（非“绿色”安全事项）并对其进行必要的细化。从技术特点上，第3阶段属于完全的概率安全评估（PSA）方法，需要运用核电厂火灾PSA模型进行详细分析。

火灾SDP第1阶段评估方法

火灾SDP的第1阶段是一个对火灾安全事项进行初步筛选的分析处理过程，其首要目的是对低风险重要度的安全事项进行初步筛选，其共包含6个分析步骤，流程图见图。

1) 火灾安全事项特征的描述；
2) 火灾实际或潜在影响；
3) 对安全停堆能力的影响；
4) 定性筛选；
5) 初始定量筛选；
6) 风险重要度初步筛选。



火灾实际或潜在影响

安全事项的火灾实际或潜在影响是从7个方面做综合分析，参见表，以确定安全事项类别。

类别	内 容
防火和行政管理控制相关	➢ 易燃物和可燃物管理程序； ➢ 行政管理措施，例如工作许可证程序； ➢ 热加工作业的防火检查； ➢ 现场巡视或定期防火检查； ➢ 相关的培训程序；
固定式消防系统相关	➢ 火灾探测系统； ➢ 固定式灭火系统（自动或手动启动）；
火灾限制和防火屏障相关	➢ 两个防火区域之间的防火屏障； ➢ 密封贯穿件； ➢ 消防水喷淋； ➢ 防火和或烟气挡板； ➢ 防火门设置；
电缆或设备防火屏障相关	➢ 电缆、电缆线槽或单个设备的火灾防护而安装的非能动设备； ➢ 电缆线槽或设备防火屏障； ➢ 设备或电缆的辐射隔热部件； ➢ 实体防火隔离；
火灾后安全停堆相关	➢ 火灾后安全停堆分析中涉及的系统或设备； ➢ 火灾后安全停堆可信赖的系统或设备； ➢ 火灾后安全停堆必需设备； ➢ 火灾后安全停堆的相关分析假设； ➢ 火灾后核电厂相关的应急响应规程； ➢ 涉及操纵员手动的操作规程； ➢ 远程停堆能力（如主控室不可用的情况下）； ➢ 控制或保护系统电路失效模式和影响（如：误动作问题）；
手动消防相关	➢ 消防软管； ➢ 消防灭火器； ➢ 消防预案；
消防水供应相关	➢ 消防水泵； ➢ 消防水管路； ➢ 消防水水源；

对安全停堆能力的影响

通过以下问题判断火灾安全事项是否影响反应堆的安全停堆能力。

问题 1：反应堆是否能达到和保持安全停堆（热停堆或冷停堆）的状态？

如果是——筛选为绿色，无需进一步分析

如果不是——继续下一个问题。

如果是，请提供支持的信息，可能需要的文件：

问题 2：安全事项被确定为“低”降级等级？

如果是——筛选为绿色，无需进一步分析

如果不是——继续定性筛选。

提供指定“低”降级等级的解释：

注：降级等级是指安全事项（实际或潜在缺陷）导致安全相关系统或设备能力下降的程度，可以分为低降级、中降级和高降级，其定义如下：

低降级表示的是相关系统或设备性能和可靠性，受安全事项影响最小，即安全事项影响的系统、设备或辅助系统功能能够维持必需的安全功能和响应能力。

中降级表示是相关系统或设备性能和可靠性，受到了较大的影响，出现了性能或可靠性的重大降级，但仍能在后续的事件后果缓解过程中发挥一定的作用。

高降级表示，相关系统或设备性能和可靠性严重降级，以至于只能极少或者根本发挥不了任何安全功能。在风险重要度的计算中，如果存在系统或设备的高降级，在评估中对相应的系统或设备、相应的火灾防护屏障将给予不信任，即其所保护的安全重要系统和设备将完全暴露在火灾的威胁之下。

定性筛选

1防火和行政管理控制

问题1：火灾安全事项的影响是否只限制在非安全相关设备？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题2：火灾安全事项的影响是否限制在仅仅一列安全相关设备，其他列安全相关设备仍能完成其安全功能？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题3：如果火灾安全事项与可燃物或易燃物的存在有关，可燃物或易燃物的充分燃烧是否可能影响火灾屏障或安全停堆分析的结论？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题4：如果火灾安全事项与可燃物或易燃物的存在有关，可燃物或易燃物是否包括可以在环境温度下自燃的材料？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题5：如果火灾安全事项与可燃物或易燃物的存在有关，且存放在不符合安全要求的容器内，可燃物或易燃物是否是多于1加仑低燃点的（燃点值低于200°F）的易燃或可燃液体？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题6：如果火灾安全事项与可燃物或易燃物的存在有关，可燃物或易燃物是否包括超过1磅的易燃气体？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题7：火灾安全事项是否与点火源（例如，使用移动式加热器或吸烟引起的）的存在有关？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题8：火灾安全事项与未能执行动火工作许可证有关，而这个工作可能会影响安全重要设备？

是 – 继续SDP第2阶段定量筛选；

否 – 继续初始定量筛选]。

2固定式消防系统

问题1：如果火灾安全事项导致消防灭火系统（如自动喷淋或消防供水系统）异常，该灭火系统是否仍然可以在着火区域内保护停堆有关的安全重要系统和设备（例如安全停堆过程中所需安全设备的供电电缆）？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题2：火灾安全事项的影响是否限制在非安全相关设备？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题3：火灾安全事项的影响是否限制在仅仅一列安全相关设备，其他列安全相关设备仍能完成其安全功能？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题4：如果火灾安全事项涉及火灾探测系统（不用于自动启动灭火系统），该火灾安全事项是否会导致火灾探测延时超过5分钟，并且期间火灾是否足以破坏重要的安全相关设备？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题5：火灾安全事项是否仅仅只影响消防队快速到达火灾区域？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题6：如果火灾安全事项影响到固定式灭火系统，但在没有该固定式灭火系统的帮助下，是否仍然可以应对由非可燃物或易燃物引起的火灾？

是 –筛选为“绿”，不要求进一步分析；

否 –继续下一个问题。

问题7：受影响的固定式灭火系统是否仍然可以扑灭火灾，使重要安全相关设备免受火灾的影响？

是 –筛选为“绿”，不要求进一步分析；

否 – 继续初始定量筛选。

3防火屏障

问题1：对于涉及防火屏障的事项，其火灾载荷耐火的持续时间不少于1.5小时？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题2：降级的防火屏障，其火灾载荷的耐火持续时间是否仍能够保持1小时或更长时间？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题3：防火屏障两侧是否都有功能齐全的自动灭火系统？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题4：火灾安全事项是否不会影响本防火区以外的设备（安全停堆所需的设备）？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题5：对于涉及贯穿防火屏障的设备（如管道），该设备是否既不会燃烧也不会传播火灾（如电缆导管）？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题6：对于有关防火屏障缺陷的火灾安全事项，确定相邻隔间内的重要安全相关设备（例如，来自不同安全停堆列）是否可能会受到通过火灾屏障缺陷蔓延过来火灾的影响？

是 –继续初始定量分析；

否 –筛选为“绿”，不要求进一步分析。

4局部的电缆或设备保护

问题1：自动灭火系统是否能够保护安全重要的设备和电缆免受火灾安全事项的影响？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题2：火灾区域是否有功能齐全的火灾探测系统，并且防护屏障可以提供至少20分钟的耐火等级？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续火灾SDP第2阶段定量筛选。

5火灾后的安全停堆

问题1：由于电气电路问题，火灾是否可能引起着火区域外的二次火灾发生？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题2：在火灾发生后24小时内，火灾是否能够影响到核电厂为维持机组稳定状态所必需的系统和设备？

是 – 继续下一个问题；

否 – 筛选为“绿”，不要求进一步分析。

问题3：火灾是否导致安全停堆所需相关部分系统和设备的不可用？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题4：火灾安全事项是否导致电厂无法达到机组稳定状态？

是 – 继续SDP第2阶段定量筛选；

否 – 继续下一个问题。

问题5：火灾安全事项是否导致在1小时内必须的安全措施的执行的延迟，其延时超过10分钟？

是 – 继续SDP第2阶段定量筛选；

否 – 继续初始定量分析。

6手动消防

问题1：火灾安全事项是否与热加工作业没有准备手提式灭火器有关？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题2：火灾安全事项是否与消防预案有关？

是 – 筛选为“绿”，不要求进一步分析；

否 – 继续下一个问题。

问题3：火灾安全事项是否与消防演习不足或者灭火的设备缺失有关？

是 – 继续火灾SDP第2阶段定量筛选；

否 – 继续初始定量分析。

7消防水供应

问题1：所需的消防水的流量是否仍然满足灭火要求？

是 –筛选为“绿”，不要求进一步分析；

否 –继续初始定量分析。

初始定量筛选

1指定一个持续时间因子（DF）

持续时间因子是反映防火功能降级的持续时间长短的一个重要参数，如表所示。如果防火功能降级的持续时间大于30天，持续时间因子DF一般选取为1。

降级持续时间	持续时间因子值（DF）
＜3 天	0.01
3 – 30 天	0.1
＞30 天	1

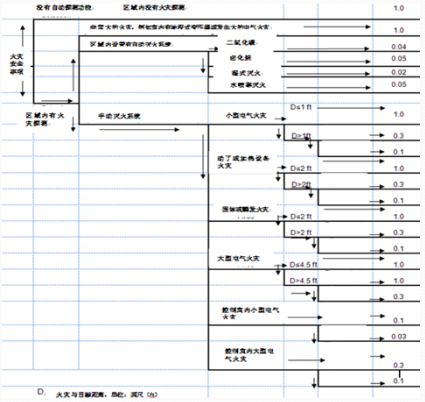
2评估火灾区域的火灾频率（F）

评估火灾区域可以作为点火源的设备，其火灾频率的取值，见表，该表的数据来自NRC火灾评估导则CR6850，仅作为参考。

位置	点火源	通用火灾频率
电池室	电池	7.5E-04
安全壳（PWR）	反应堆冷却泵	6.1E-03
安全壳（PWR）	可燃物或热能释放	2.0E-03
控制室	控制板件	2.5E-03
控制/辅助、反应堆厂房	焊接和切割引起的电缆火灾	1.6E-03
控制/辅助、反应堆厂房	焊接和切割引起的可燃物火灾	9.7E-03
控制/辅助、反应堆厂房	可燃物	3.9E-03
柴油发电机室	柴油发电机	2.1E-02

3火灾未扑灭概率（S）

火灾未扑灭概率（S）是在火灾区域内因火灾未能被扑灭，而导致安全相关系统和设备被破坏的可能性。S值的选择基于未扑灭火灾事件树和工程经验的判断。一个火灾安全事项的S值由下图描述火灾安全事项的最佳决策路径来确定。



以1E-6为阈值，定量筛选堆芯损坏频率的变化量（ΔCDF）。该值由火灾区域的持续时间因子DF乘以火灾频率F、未扑灭概率S和条件堆芯损坏概率CCDP得到。

$$\Delta CDF \approx DF \times F \times S \times CCDP$$

如果事项会影响多个火灾区域，那么初始第1阶段筛选ΔCDF值基于所有受影响的火灾区域的火灾频率总和，如下：

$$\Delta CDF \approx DF \times \Sigma (F_{AREA} \times S_{AREA}) \times CCDP$$

- 如果Δ CDF低于1E-6，该火灾安全事项筛选为“绿”并结束分析（不要求进行第2阶段析）。
- 如果Δ CDF高于或等于1E-6，那么该火灾安全事项不筛选为“绿”，继续第2阶段的定量筛选分析。

风险度初步评估

问题 A：火灾安全事项的风险评估表明 ΔCDF 小于 1E-6，这个评估结果是否被接受？

O 是 – 筛选为“绿”，不要求进一步分析

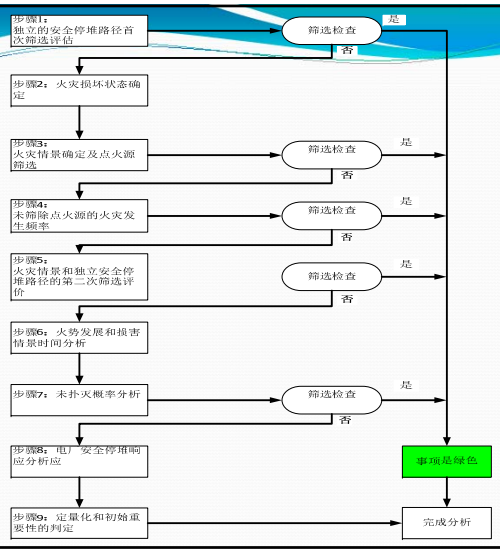
O 否 – 继续 SDP 第 2 阶段评估

评估：

火灾SDP第2阶段

第1阶段筛选后未能判定为低风险（绿色）的事项有些将会传递到第2阶段做进一步的定性和定量化分析。第2阶段共分为9个步骤，分别是：

1) 独立的安全停堆路径首次筛选评估
2) 火灾损坏状态确定
3) 火灾情景确定及点火源筛选
4) 未筛除点火源的火灾发生频率
5) 火灾情景和独立安全停堆路径的第二次筛选评估
6) 火势发展和损害情景时间分析
7) 未扑灭概率分析
8) 电厂安全停堆响应分析
9) 定量化和初始重要性的判定



1独立的安全停堆路径首次筛选评估

火灾安全事项发现后，评估人员所关注的应是安全事项对安全停堆功能的影响，即机组是否能够在火灾发生后或假定的火灾情景下，机组能够达到或维持在安全停堆状态。所以在火灾SDP评估时应确定安全停堆的路径有哪些。在美国核电厂火灾防护程序中，可能的火灾区域对安全停堆路径的影响都是有相应的分析的。

◆ 确定安全停堆路径的不可用度因子

剩余缓解能力的类型	不可用度因子
蒸汽驱动的系统列：相关设备能提供100%特定安全功能的蒸汽驱动设备，该列由于失效、试验或维修而不可用时的概率为1E-1。	0.1
可提供100%的特定安全功能的相关设备（如泵、阀和断路器等），该设备由于失效、试验和维修而不可用的概率约为1E-2。	0.01
操纵员行动的可信度：操纵员进行的主要操作时的失误概率（HEPs），有三个类别来估算，这些类别是： 操纵员行动=1.0，表示不给予信任 操纵员行动=0.1，表示失效概率在5E-2和0.5之间 操纵员行动=0.01，表示失效概率在5E-3和5E-2之间 可信度是基于以下准则进行确定： 1) 有足够的操作时间； 2) 环境的准入条件允许进行手动操作； 3) 有明确的规程指导操纵员操作； 4) 操纵员接受过相应的培训； 5) 所操作的设备均处于可用状态。	1.0, 0.1 或 0.01

- 受火灾效应（如烟或高温）或二氧化碳固定灭火系统排放影响的手动操作，在评估中是不给予信任的；
- 核电厂有相关规程规定的，并有明确要求的手动操作，在评估中应给予信任；
- 如果安全事项对于执行这些手动操作的可行性和可靠性有影响，安全停堆的不可用度因子都等于1.0。

指定事项类别	ΔCDF筛选值 中降级	ΔCDF筛选值 高降级
防火和行政管理控制相关	N/A	
固定式消防系统相关	1E-5	
火灾限制相关	1E-5	1E-6
局部电缆或设备保护相关	1E-5	
火灾后安全停堆相关	1E-6	

2火灾损坏状态确定

基于火灾SDP第1阶段评估步骤2中给定的火灾安全事项类别，分析和确定火灾损坏状态（FDS）。FDS是在火灾SDP分析过程中假设的火灾发展和造成破坏的4个不同阶段，4个火灾阶段描述如下：

- FDS0：只有点火源或起火的可燃物和易燃物被损坏，评估中不将FDS0作为一个风险贡献项在火灾SDP中进行分析。
- FDS1：火灾造成的危害发生在点火源附近，例如未受防火屏障保护的设备或电缆。
- FDS2：火灾造成大范围的破坏，包括火灾区域内未受防火屏障保护的设备或电缆，局部降级的防火屏障，以及耐火极限小于1小时的防火屏障所保护的设备或电缆。
- FDS3：火灾造成的危害蔓延到附近的防火区域内，相应的防火屏障严重降级。例如，墙体、防火门和密封贯穿件等。

事项类型或类别:	FDS1	FDS2	FDS3
防火和行政管理控制相关	保留	保留	保留
固定式消防系统相关	保留	保留	保留
火灾限制相关	不保留	不保留	保留
局部电缆或设备保护相关 中降级 高降级	 不保留 保留(1)	 保留 保留	 保留 保留
火灾后安全停堆相关	保留	保留	保留

注1：对于一个高降级的防火屏障，被保护的设备或电缆被认定为为完全裸露于火灾下，并且假定为在FDS1情景中就被破坏了。

3火灾情景确定及点火源筛选

筛除不会使火灾蔓延并且不会对火灾区域内的系统和设备造成破坏的点火源；同时还要确定未筛除的点火源，及其导致的火灾具体蔓延程度和其损坏情景。

4未筛除点火源的火灾发生频率（F）

对每个未筛除点火源的火灾频率进行进一步评估，以反映某个火灾限制相关和其他行政控制程序的变化，并且评估某些补偿措施的有效性。

首先，判断是否有火灾频率增加的可能性。对于火灾频率的增加仅适用于某些类型的点火源，例如热加工作业和易燃或可燃物。一般如果火灾安全事项指定的事项类别是“防火和行政管理控制相关”，则需要进行火灾频率的调整。

其次，如果补偿措施安排到位并被认为是可以降低被分析的点火源的火灾发生频率。

将所有评估后的点火源的情景的火灾频率相加以生成所评估的火灾区域的火灾频率的更新值。然后再将所评估的火灾区域的火灾频率的更新值带入到ΔCDF的计算与相应的阈值进行比较来确定是否无需进一步分析。

5火灾情景和独立安全停堆路径的第二次筛选评估

一旦定义了电厂损坏情景，在此情景基础上对已确定有效的安全停堆路径进行再评估，需要评估以下几个方面：

① 确定火势增长和损坏情景；

② 确定火势增长和损坏情况；

③ 确定核电厂损坏状态情景；

④ 评估火灾情景中安全停堆路径的独立性。

如果给定最差情况损坏状态，指定的安全停堆路径受到了影响，但仍是可行的，应重新计算ΔCDF值，并与相应的阈值进行对比。如果在给定最差情况下，安全停堆路径被认为在任何给定的点火源引起的火灾情景中都不起作用，那么继续步骤6的分析。

6火势发展和损害情景时间分析

需分析火灾情景中火灾的发展情况，以评估达到相关的FDS的时间，分别对FDS1、FDS2和FDS3情景下火灾的暴露时间进行确定。

7未扑灭概率分析

需要量化每个火势增长和其涉及的损坏情景的火灾未扑灭概率（PNS），考虑的因素有火灾探测、固定式灭火系统、电厂人员和消防队响应等。

8电厂安全停堆响应分析

根据假定火势的发展和损害情景，分析核电厂的安全停堆的有效性（包括所需的操纵员恢复行动）。需考虑被信任的系统及其功能、控制室外人员行动和手动操作的失效概率等因素，计算每个火灾情景的CCDP。

9定量化和初始重要性的判定

计算所关注的FDS情景将最终量化，并给出火灾事项的初始判定的重要性程度，其ΔCDF是以下因子的乘积。

$\Delta CDF = DF \times \sum[F_i \times \prod PNS_i \times CCDP_i]$

DF：时间持续因子

F_i：点火源的火灾频率

PNS_i：未扑灭概率

频率范围/堆年	基于ΔCDF 的SDP
$\geq 10^{-4}$	红色
$< 10^{-4}$ - 10^{-5}	黄色
$< 10^{-5}$ - 10^{-6}	白色
$< 10^{-6}$	绿色

火灾SDP第3阶段评价主要是使用特定电厂标准化PSA模型进行评价，主要用于评价第1阶段直接跳转过来的事件，以及第2阶段评价结果为白、黄、红色，也就是事项导致的风险增量ΔCDF>10E-6的情况。这一阶段是风险重要度验证再确定阶段，如果结果证明其实风险重要度高事件，以此结果为依据则需要管理人员必须采取相应的管理行动。

其他SDP程序

1电厂操纵员评估SDP评估程序

电厂操纵员SDP用于评估与电厂操纵员活动相关安全事项的风险重要性。这些安全事项的来源主要是电厂操纵员的任职资格考试。分析认为，电厂操纵员在考试中的表现能够很大程度上代表其在实际操作中的表现。

2维修风险评估和风险管理SDP评估程序

维修风险评估和风险管理SDP用于评估核电厂与在功率工况和停堆工况下进行维修活动时核电厂风险评估和风险管理相关安全事项的风险重要性。维修风险评估和风险管理SDP的评价过程主要以定量评价为主。

3恐怖袭击引发的火灾或爆炸导致部分功能丧失SDP评估程序

恐怖袭击引发的火灾或爆炸导致部分功能丧失SDP的目的是评估与在恐怖袭击引发的火灾或爆炸导致的核电厂安全重要系统大面积不可用的情况下，为了保持和恢复堆芯冷却、安全壳完整性和乏燃料水池冷却能力，而实施的导则和策略相关安全事项风险重要性，评估过程由一系列定性评估组成。

4职业辐射安全SDP评估程序

职业辐射安全SDP的目的是评估在民用核设施正常运行期间放射性材料对工作人员的健康和安全相关安全事项的风险重要性。职业辐射安全SDP以合理的辐射剂量为基准，运用一系列定性和定量的评估步骤，最终评估得出此类安全事项的风险重要性。

5公众辐射安全SDP评估程序

公众辐射安全SDP的目的是评估与在民用核设施正常运行期间放射性材料对公众健康和安全相关安全事项的风险重要性。公众辐射安全SDP从放射性废气废水排出物的处理、放射性材料的加工和运输以及放射性环境监控、放射性材料控制程序等几个方面对不同的相关安全事项进行一系列定性和定量的评估，最终评估得出此类安全事项的风险重要性。

6实体保卫SDP评估程序

核电厂为防止非法盗取核材料以及针对核电厂的人为破坏而采取特殊保护措施，形成多层的实体保卫。实体保卫SDP的目的是评估电厂实体保卫的探测、延迟和响应等环节存在漏洞的情况下，为了保持核电厂防止外部入侵的能力，而实施的导则和策略相关的保卫事项风险重要性，评估过程由一系列的定性评估组成。

7定性准则评价SDP评估程序

有时，安全事项的影响范围比较大，而又没有比较恰当SDP判定程序相对其进行分析。同时也无法利用PSA进行风险判定，因为安全事项的情况是复杂的，原因和影响都不能在PSA中利用模型化的方式表达出来。在这种情况下SDP提供了一种基于工程判断和确定论的风险识别程序，即定性准则评价SDP对其进行判定。

8应急响应准备SDP评估程序

应急响应准备SDP的目的是运用定性评价的原则，评估与应急准备安全目标和性能预期相关的安全事项的风险重要性。

9安全壳完整性SDP评估程序

安全壳完整性SDP用于评估导致早期大量放射性物质释放增量（ΔLERF）指标增加安全事项的风险重要性。安全壳完整性SDP主要评价3个安全基石的性能状态：始发事件、缓解系统和屏障完整性，以ΔLERF指标为依据，通过定量分析的方法确定相关安全事项的风险重要性。

10蒸汽发生器完整性SDP评估程序

蒸汽发生器完整性SDP用于评估在在役检查过程中识别出的与蒸汽发生器完整性相关安全事项的风险重要性。主要通过蒸汽发生器完整性SDP矩阵完成风险重要性的评估过程。

总结

SDP是美国NRC ROP程序中重要的工作程序，与性能指标体系共同构建了整个ROP监管的技术基础。

SDP不是PSA的简化，他是一套完整的核电厂异常重要性判定流程，通过定性和定量两种手段，来确定事项的重要程度，PSA方法只是SDP判定程序中一种技术方法。

SDP作为工作程序，着重于分析过程的严密性和客观性，提高了监督管理者分析问题和解决问题的能力。

SDP需要其他工作程序的配合，例如RCA来帮助其确定核电厂真正的缺陷。

谢 谢！

SDP 软件工具的应用及案例分析

SDP软件工具的应用及案例分析

环境保护部核与辐射安全中心

事件评价与经验反馈部

1 SDP应用情况

2 暴露时间

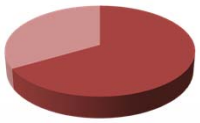
3 3种状况实例分析

4 详细计算过程

SDP应用

SDP在美国的使用

截至2012年，全美国共有104台机组



2种技术路线，却有4个反应堆系统供应商，超过80种的不同设计

机组运行时间长且多、设备老旧、设计多元化

美国核能监管委员会于2000年施行了新的基于风险指引框架的反应堆监督程序（ROP）来监管运行核电厂。SDP便是这套监管程序的主要技术支柱之一。

SDP应用

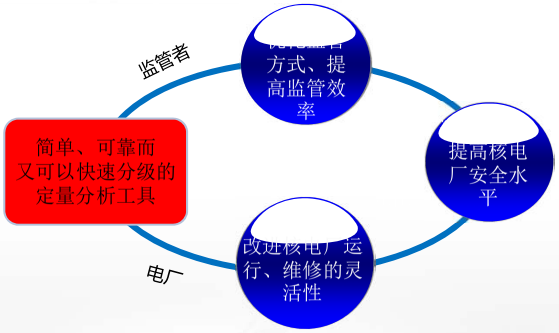
SDP在美国的使用

根据NRC 使用情况统计结果，美国核电厂每年所需关注的核事件不足1000 个，安全重要度较高的事项不足4%。

重要度较低 → 核电厂营运单位自行处理

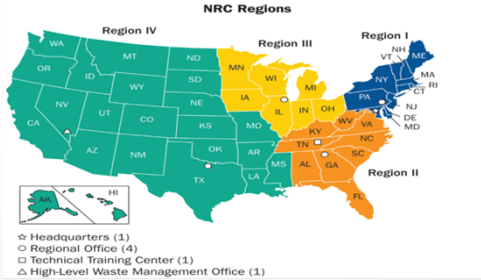
重要度较高 → NRC关注

SDP应用



SDP应用

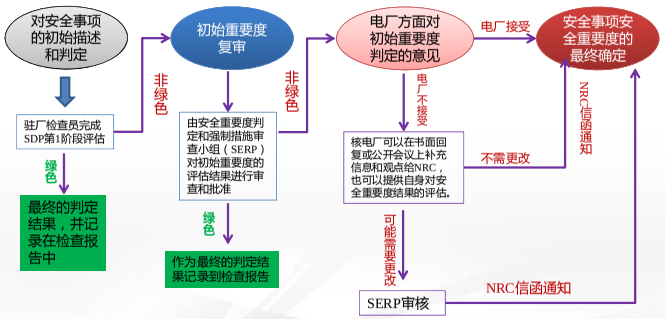
NRC SDP运作流程



目前，美国近100个在运反应堆分布在65个厂区，NRC在每个厂区平均设置有两个驻厂监督员，全年共对约3000个事件进行检查，与电厂讨论后形成相应的报告。

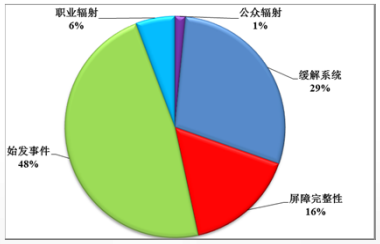
SDP应用

NRC SDP运作流程



我国近4年的运行事件评价结果

- 安全基石分布

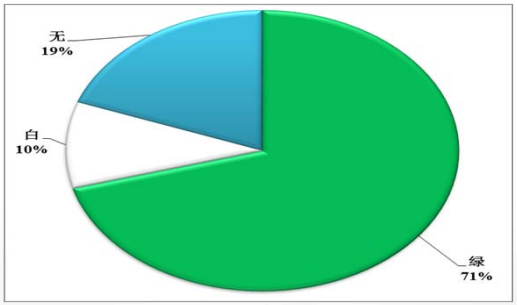


从上图可以看出，始发事件是受冲击最频繁的安全基石。

我国近4年的运行事件评价结果

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

➢ 重要度分布

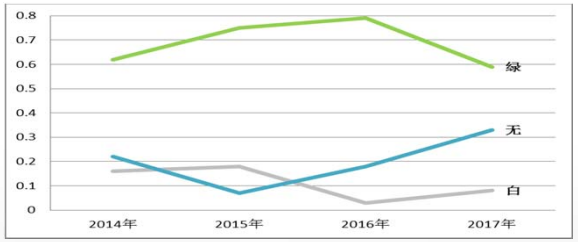


从上图可以看出：
SDP 评估结果中包含有绿、白2类重要度，这表征着虽然都是运行事件，但是其重要度却存在差别，所以基于SDP 评估结果，可以优化核安全监管方式、提高监管效率。

我国近4年的运行事件评价结果

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

➢ 时序分布

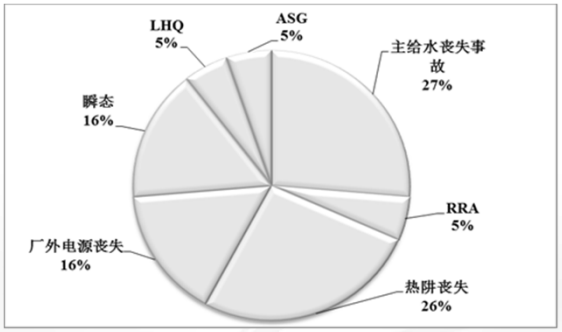


总体上我国高重要度运行事件的占比（指占当年运行事件总量的比例）在降低，尤其是15年到16年间呈明显下降。

我国近4年的运行事件评价结果

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

➢ 事件重要度大于“绿色”的原因分布



环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

2 暴露时间

暴露时间

- 暴露时间（T）：T是指被分析地结构、系统或设备失效或降级的持续时间。暴露时间理论上应该是运行模式下的时间，停堆状态下不应该包含在暴露时间里，除非技术规范里要求停堆状态下该设备系统可用。
- t时间：t是指最近成功功能运行到未成功功能运行或失效发现的时间。
- 维修时间：PRA定义的维修时间为“设备失效直到恢复可用期间”。“恢复可用”是指维修已完成并且维修后已成功执行相关试验以证明其安全功能可用。

暴露时间

根据设备运行情况将暴露时间分为两类：

- 1.备用或周期性运行设备的暴露时间
  - 1）设备最近一次试验或计划外功能运行时已发生失效
    暴露时间=t+维修时间
  - 2）在上次运行后任何时刻发生的设备失效
    暴露时间=t/2+维修时间
  - 3）设备运行失效的暴露时间
    - a）平均（运行时间）>PRA要求时间（24H）
    - b）平均（运行时间）<PRA要求时间（24H）
- 2连续运行设备的暴露时间

备用或周期性运行设备的暴露时间

设备最近一次试验或计划外功能运行时已发生失效

这类情况的暴露时间（T）为从最近一次成功运行到未成功运行的时间加上维修时间，即T=t+维修时间。该计算方法适用于备用或周期性运行设备的失效，并且其降级机理为备用阶段时非逐渐影响设备。

下述情况需要考虑使用t：

1）失效开始时间已知。指的是设备在最后一次试验或计划外功能运行时发生失效（例如设备固定时发生的失效）。

2）失效开始时间未知或未评估失效根本原因。指的是失效机理未知或失效的根本原因评估不充分或不完全，无法确定失效根本原因。

备用或周期性运行设备的暴露时间

设备最近一次试验或计划外功能运行时已发生失效

- 认为失效发生在最近一次成功运行期间或之后立即的依据包括以下5点：
- 最近一次试验或运行时设备即将不可用，但却由于人因失误导致设备失效。
- 仅发生在设备上次运行或改变状态时的机械故障导致的失效。
- 替代部件存在缺陷，但通过了初次运行。
- 试验导致设备失效的事件（如：水锤）一直存在直到设备未成功运行才发现。
- 由于泵内进入异物，泵启动后不足以提供足够的扬程。但上次试验时泵可用。碎片最有可能接近吸入管线或在里面，并从上次成功运行这段时间内造成了堵塞。

备用或周期性运行设备的暴露时间

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

在上次运行后任何时刻发生的设备失效

这类情况的暴露时间（T）等于设备从最近一次成功运行期间的二分之一加维修时间，即T= t/2+维修时间。这种暴露时间的计算方法适用于备用或周期性运行设备的失效，但其降级机理为备用阶段时逐渐影响设备。如：不确定实际失效时间的自然失效。

以下2种情况应该考虑使用t/2：

1）专家进行全面的根本原因分析后，排除失效发生在最近一次功能运行，但经仔细审查后，不确定最近一次运行之后失效的开始时间。

2）专家不确定失效的开始时间，但已知道失效机理和原因。

备用或周期性运行设备的暴露时间

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

在上次运行后任何时刻发生的设备失效

认为失效发生在上次成功运行和发现时间之间的依据包括以下2点：

没有强有力的证据表明：失效的原因与最近一次成功运行有关。

失效机理是由环境条件（如：腐蚀等）引起的。

备用或周期性运行设备的暴露时间

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

设备运行失效的暴露时间

这种暴露时间确定方法适合于备用或周期运行设备的失效，并且其降级机理是在设备运行期间影响设备。（如：运行期间因降级导致失效发生，并且认为与运行时间呈线性比例。）另外，该降级机理对处于备用状态的设备基本无影响。在这两种情况下，暴露时间始于设备不再具有能力运行PRA任务时间（如24小时）。这类情况的暴露时间分成两种：

备用或周期性运行设备的暴露时间

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

平均（运行时间）>PRA要求时间（24H）

开始时间已知或未知。该情况的暴露时间开始于设备不再具有能力运行PRA任务时间（24小时）。

例子A—设备监督试验期间在9月30日失效前累计运行36h。开始于1月1日，维修时间忽略不计，根据失效之前24小时（PRA任务时间）的运行时长可以得出暴露时间为6个月。

1月	2月	3月	4月	5月	6月	7月	8月	9月
4小时	4小时	4小时	4小时	4小时	4小时	4小时	4小时	4小时
情况开始			暴露时间6个月				运行时发生失效	

备用或周期性运行设备的暴露时间

平均（运行时间）<PRA要求时间（24H）

若已知降级开始时间，并且在开始时间和失效时间之间的累积运行时间小于PRA任务时间（24h）。暴露时间起始于开始时间，终止于设备经维修恢复投运的时间。

例子B—设备监督试验期间累计运行9小时，已知起始时间和失效时间9月30日，维修时间忽略不计，暴露时间为9个月

1月	2	3	4	5	6	7	8	9
1小时	1小时	1小时	1小时	1小时	1小时	1小时	1小时	1小时
情况开始							运行时发生失效	
暴露时间为9个月								

持续运行设备失效的暴露时间

持续运行设备的失效通常是在运行时（例如，正常运行的厂用水泵），暴露时间一般为PRA任务时间（即24小时）。

最大暴露时间

最大暴露时间（T）通常仅限于一年，即使，条件可能已经存在了一年以上（例如，从安装，修改，或建造起，设计上存在的缺陷）

3 3种状态实例分析

3种状况实例分析

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

1、性能缺陷仅导致始发事件

状况1：这类性能缺陷会导致后续始发事件的发生，但并未影响其它的系统、设备和构筑物。

处理方式：针对这类情况采用相关始发事件的条件堆熔损坏概率（CCDP）来进行估算。在使用SDP第二阶段计算时，将发生的始发事件（例如一般瞬态、失去主给水等）设定为1.0，便得到堆熔损坏频率的变化值(ΔCDF)。

3种状况实例分析

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

1、某核电站1号机组主变A相故障导致反应堆自动保护停堆

事件描述：2009年10月31日02时34分19秒，某核电站1号机组主变A相1BAT11重瓦斯保护动作跳闸，由于220kV厂外电源线路处于电网处于检修状态，导致1号机组失去厂外电源。反应堆自动保护停堆正确动作，所有控制棒顺利落入堆芯，反应堆进入次临界状态。触发DA11和 DA21启动信号，所有4台应急柴油发电机与2台机组柴油发电机正确启动并且出口开关合闸，设备分级带载成功启动，相关设备先后启动稳定导出堆芯热量。同日16:35前，先后恢复220kV厂外电和4条厂用正常母线，20:08到20:43分别停运1#、2#、3#、4#应急柴油发电机和5#、6＃机组柴油发电机。

SDP第二阶段的定量评价：该事件中实际发生了丧失厂外电的始发事件，所以在第二阶段中将丧失厂外电的始发事件置为1，即提高4个量级，得到的ΔCDF的量级为1.0E-5，所以该发现项的风险重要度判定为黄色。

3种状态实例分析

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

2、性能缺陷增加始发事件发生频率

状况2：导致构筑物、系统和设备不可用的性能缺陷可能会增加始发事件的发生频率，但并未导致始发事件实际发生。某些设备故障，尤其是辅助系统中设备（如厂用水、设备冷却水、仪表空气等）的故障可能导致系统失效概率上升。如果系统失效可触发始发事件，则系统失效概率上升就可能导致始发事件的发生频率增加。

处理方式：针对这类情况，在使用SDP第二阶段计算时，一般将对应的始发事件频率提高一个量级。

3种状态实例分析

环境保护部核与辐射安全中心 Nuclear and Radiation Safety Center

2、某核电厂因海生物涌入取水口导致反应堆紧急停堆

事件描述：国内某核电厂处于满功率运行状态，泵站监测到CFI旋转滤网反冲洗水中毛虾数量较多。随后，循环水过滤系统CFI 032TF和CFI 031TF旋转滤网相继因压差高4信号导致循环水泵CRF002PO和CRF001PO停运，进而导致凝汽器真空下降，触发汽轮机停机，同时叠加P10信号，反应堆紧急停堆（C8+P10+凝汽器真空低）。期间，SEC系统流量、泵及电机运行正常，SEC海生物捕集器压差正常。本事件的发现项为未设置应对小型海生物涌入的拦截装置。

SDP第二阶段的定量评价：由于CFI系统不仅为机组凝汽器提供冷却水，同时还为SEC系统提供水源，所以虽未影响SEC系统的带热能力，但触发了反应堆紧急停堆，可以认为该发现项对CFI系统功能和稳定性影响程度较大，会导致丧失最终热阱的频率增加。该事件的发现项为设计缺陷。故取暴露时间大于30天。根据暴露时间和对始发事件的分析，所以将始发事件的最终热阱丧失频率增加1个量级，得到的ΔCDF的量级为10^{-6}，所以该发现项的风险重要度判定为白色。

3种状况实例分析

3、发现项导致缓解系统的设备失效

状况3：该性能缺陷会导致缓解系统中一列或多列设备的不可用，进而降低了核电厂对始发事件的应对和缓解能力，这类系统包括：安注系统、安全壳喷淋系统、辅助给水系统、大气排放阀、应急柴油发电机组、重要厂用水系统等。

处理方式：针对这类情况，在使用SDP第二阶段计算时，需要将缓解系统中失效的设备置为不可用。

实例分析

3、某核电厂执行PT 3LHP 001(低负荷试验)时应急柴油发电机未启动

事件描述：2011年2月12日，运行二处当班值按照计划执行定期试验PT 3LHP 001（柴油发电机组低负荷运行性能试验），发现A列应急柴油发电机启动失败，记录柴油机不可运行的I0，多次重新启动，仍旧失败。 2月13日，经过机械检查，确认为A列空气分配器错位导致进气顺序错乱。调整到正确顺序后柴油机启动成功，消除I0。
3月10日，再次执行3LHP柴油发电机组低负荷试验时，柴油机两次均未成功启动，故障现象与之前空气分配器错位相似。厂家服务人员现场检查后,更换了带来的新的空气分配器并调整到正确顺序，柴油机启动成功。经过设备厂家和电厂的合作调查，最终确认该批次空气分配器产品在制造、安装环节存在缺陷。

SDP第二阶段的定量评价：该发现项导致LHP不能启动，所以将A列LHP置为不可用。由于该试验的周期为1个月。由于相邻两次试验全都失败。故取暴露时间大于30天，得到的ΔCDF的量级为10-6，所以该发现项的风险重要度判定为白色。

4 详细计算过程

实例计算1

1、某核电厂RCV002PO泵轴平衡推力卡环缩颈处断裂

3月7日，某核电厂处于RP模式（核功率0.5%Pn），主控室发现RCV002PO跳闸；3月10日，对RCV002PO进行解体检查，3月12日确认RCV002PO非驱动端轴承烧毁，泵轴在平衡推力卡环缩颈处断裂，并3月13日维修完成，恢复可用。
事件后果：RCV002PO 卡轴损坏造成安全设备不可用；倒电完成之前 RCV B列不可用，一列高压安注功能失效；RCV系统冗余性降低，容易失去主泵轴封，可能会造成机组瞬态。

定性筛选阶段

RCV002PO不可用可能导致瞬态，并且一列高压安注失效，影响堆芯短期热移出功能，通过引导程序始发事件筛选表和缓解系统筛选表，RCV002PO不可用影响的安全基石是始发事件和缓解系统，由于影响两个安全基石所以需要进入功率工况SDP第二阶段评价。

评价阶段

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

1）首先分析RCV002PO不可用是否会直接导致始发事件发生。在该事件中，RCV 冗余性降低，主泵轴封丧失概率增大，可能造成机组瞬态，所以该发现项会导致其他瞬态始发事件发生概率提高。

2）其次分析RCV002PO不可用是否影响其他始发事件的缓解能力。在该事件中，RCV002PO不可用导致一列高压安注功能失效，所以该发现项影响应对热阱丧失和SGTR事故等的缓解能力。

3）然后分析RCV002PO不可用是否引起人因事故。在该事件中，RCV002PO不可用并没有引起人因事故。

4）接着分析该事件的存在时间。该缺陷存在起始日期是2014年3月7日，3月13日恢复可用，故RCV002PO暴露时间大于3天，小于30天。

根据以上分析，根据事件直接引发的始发事件和受影响的始发事件，从26颗事件树中找出所有受影响的题头事件，并根据事件实际情况，判断每个题头事件的成功准则是否满足，从而打分评价每个题头事件的剩余缓解能力。

WEBSITE http://www.chinansc.cn/

1、受影响的题头事件表

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

题头事件	题头事件名称	剩余缓解能力	成功准则	说明
HPR01	高压安注冷段再循环	3	由两个相同列组成。1/2成功	RCV001PO 为 A 列，RCV002PO和RCV003PO为B列，RCV002PO不可用，不会影响RCV003PO可用。所以各题头事件成功准则满足，各题头事件剩余能力不变。
HPR02	高压安注热段再循环	3	由两个相同列组成。1/2成功	
HPR03	高压安注冷段再循环	2	A列直流电源丧失故障，只有B列泵可用。	
HPSI	高压安注直接注入	3	由两个相同列组成。1/2成功	
HPSI01	高压安注直接注入	2	A列直流电源丧失故障，只有B列泵可用。	
J04	正常轴封注入	3	轴封注入由两列上充泵及其注入管线构成。	

WEBSITE http://www.chinansc.cn/

2、始发事件分类表

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

	始发事件频率	始发事件类型	始发事件可能性 $X=-\log_{10}$（始发事件频率）		
Ⅰ	> 1 per 1-10 yr	主给水丧失（LMFW）、二回路变化引起的瞬态（STRANS）其它瞬态（TRANS）	1	2	3
Ⅱ	1 per 10-10^2 yr	部分(安全段)丧失热阱（LHS2）、部分(公用段)丧失热阱（LHS3）、丧失压缩空气（LOIA） 丧失厂外电源（LOOP）、30V列直流电源（LDDD）	2	3	4
Ⅲ	1 per 10^2-10^3 yr	给水管道破口（FWLB）、48V A列直流电源丧失（LDCA）、48V B列直流电源丧失（LDCB）、48V C列直流电源丧失（LDCC）、125V A列直流电源丧失（LDBA）、安全壳内主蒸汽管道破口（MSLB1）、安全壳外主蒸汽隔离阀上游破口（MSLB2）、安全壳外主蒸汽隔离阀下游破口（MSLB3）、蒸汽发生器传热管断裂（SGTR）、小破口失水事故（SLOCA）	3	4	5
Ⅳ	1 per 10^3-10^4 yr	全部丧失热阱（LHS1）、中破口失水事故（MLOCA）、蒸汽管小破口叠加1根蒸汽发生器传热管断裂（SSGTR1）	4	5	6
Ⅴ	1 per 10^4-10^5yr	给水丧失相关的未停堆的瞬态（ATWT2）、大破口失水事故（LLOCA）、稳压器汽相SEBIM阀破口失水事故	5	6	7
Ⅵ	< 1 per 10^5yr	其他未停堆的瞬态事件（ATWT1）、界面LOCAV-LOCA（ISLOCA）、蒸汽管小破口叠加10根蒸汽发生器传热管断裂（SSGTR2）	6	7	8
事件/缺陷存在的时间（天）			>30	3~30	<3

由于影响始发瞬态事件，一个高年，分为1

WEBSITE http://www.chinansc.cn/

3、序列表

核电厂SDP工作表——ATWT事件序列

需求的安全功能：	每一安全功能完全可信的缓解能力：
蒸发器的大气旁路阀和安全阀回座（MSSV）	根据PSA故障树分析，未回座的失效概率在3.0E-4，因此，剩余能力因子是4。
稳压器安全阀组打开（SRV01）	由三组稳压器安全阀组，2组稳压器安全阀组打开即可。
辅助给水供水（ASG03）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵。
稳压器安全阀回座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
ATWT直流次临界（ATWT-H1）	ATWT瞬态事故下操纵员使反应堆重返次临界，主要是通过按停堆按钮或停控制棒电源，属于人员操作。
辅助给水箱补水（ATWT-H2）	操纵员根据辅助给水箱的水位信号向辅助给水水箱补水，属于人员操作。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	ATWT1+ASG03 8 + 4	12	ATWT1+ASG03	
2	ATWT1+ATWT-H1 8 + 3	11	ATWT1+ATWT-H1	
3	ATWT1+ATWT-H2 8 + 3	11	ATWT1+ATWT-H2	
4	ATWT1+MSSV 8 + 4	12	ATWT1+MSSV	
5	ATWT1+SRV01 8 + 2	10	ATWT1+SRV01	
6	ATWT1+SRV03+EAS03 8 + 4 + 3	15	ATWT1+SRV03+EAS03	
7	ATWT1+SRV03+HPR01 8 + 4 + 3	15	ATWT1+SRV03+HPR01 7+4+3	14
8	ATWT1+SRV03 8 + 4	12	ATWT1+SRV03	

核电厂SDP工作表——ATWT事件序列

需求的安全功能：	每一安全功能完全可信的缓解能力：
ATWT信号（A08）	ATWT信号由两种不同类型的信号组成（给水流量低信号和中子注入率高信号），任何一组信号成功触发即成功。
控制棒自动调节（A09）	参考PSA模型及数据分析，控制棒自动调节失效概率是0.1。
蒸发器的大气旁路阀和安全阀回座（MSSV）	根据PSA故障树分析，未回座的失效概率在3.0E-4。因此，剩余能力因子是4。
稳压器安全阀组打开（SRV01）	由三组稳压器安全阀组，2组稳压器安全阀组打开即可。
辅助给水供水（ASG03）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵。
稳压器安全阀回座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
ATWT直流次临界（ATWT-H1）	ATWT瞬态事故下操纵员使反应堆重返次临界，主要是通过按停堆按钮或停控制棒电源，属于人员操作。
辅助给水箱补水（ATWT-H2）	操纵员根据辅助给水箱的水位信号向辅助给水水箱补水，属于人员操作。
ATWT手动注入DEC规程（ATWT-H3）	ATWT瞬态事故下操纵员没有根据报警正确进入DEC规程，而不是H2规程。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	ATWT2+A08 7 + 4	11	ATWT2+A08	
2	ATWT2+A09 7 + 1	8	ATWT2+A09	
3	ATWT2+ASG03 7 + 4	11	ATWT2+ASG03	
4	ATWT2+ATWT-H1 7 + 3	10	ATWT2+ATWT-H1	
5	ATWT2+ATWT-H2 7 + 3	10	ATWT2+ATWT-H2	
6	ATWT2+ATWT-H3 7 + 3	10	ATWT2+ATWT-H3	
7	ATWT2+MSSV 7 + 4	11	ATWT2+MSSV	
8	ATWT2+SRV01 7 + 2	9	ATWT2+SRV01	
9	ATWT2+SRV03+EAS03 7 + 4 + 3	14	ATWT2+SRV03+EAS03	
10	ATWT2+SRV03+HPR01 7 + 4 + 3	14	ATWT2+SRV03+HPR01 6+4+3	13
11	ATWT2+SRV03+HPSI 7 + 4 + 3	14	ATWT2+SRV03+HPSI	

核电厂SDP工作表——125V交流电源丧失（LDBA）事件序列

需求的安全功能：	每一安全功能完全可信的缓解能力：
额外电源供（LGR）	在LBA丧失事故下，自动切换到LGR供电。
RRI/SEC自动切换（I02）	在LBA丧失事故下，RRI/SEC自动切换到B列。
辅助给水供水（ASG06）	由于A列直流电源故障，只有B列电动泵和汽动泵可用，成功准则是一台泵。
稳压器安全阀回座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
充排操作（LODC-H1）	直流电源丧失时操纵员实施一回路实施充排操作
高压安注直接注入（HPSI01）	因A列直流电源丧失故障，只有B列可用。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR03）	因A列直流电源丧失故障，只有B列可用。
安全壳喷淋再循环（EAS04）	因A列直流电源丧失故障，只有B列可用。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LDBA+ASG06+EAS04 5 + 4 + 2	11	LDBA+ASG06+EAS04	
2	LDBA+ASG06+HPR03 5 + 4 + 2	11	LDBA+ASG06+HPR03 4+4+2	10
3	LDBA+ASG06+HPSI01 5 + 4 + 2	11	LDBA+ASG06+HPSI01 4+4+2	10
4	LDBA+ASG06+LODC-H1 5 + 4 + 2	11	LDBA+ASG06+LODC-H1	
5	LDBA+ASG06+SRV02 5 + 4 + 3	12	LDBA+ASG06+SRV02	

核电厂SDP工作表——48V A列直流电源丧失事件序列

需求的安全功能：	每一安全功能完全可信的缓解能力：
辅助给水供水（ASG06）	由于A列直流电源故障，只有B列电动泵和汽动泵可用，成功准则是一台泵。
稳压器安全阀回座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
充排操作（LODC-H1）	直流电源丧失时操纵员实施一回路实施充排操作
高压安注直接注入（HPSI01）	因A列直流电源丧失故障，只有B列可用。
稳压器安全阀组打开（SRV04）	由于A列直流电源故障，所以只有一组稳压器安全阀组可用
高压安注冷段再循环（HPR03）	因A列直流电源丧失故障，只有B列可用。
安全壳喷淋再循环（EAS04）	因A列直流电源丧失故障，只有B列可用。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LDCA+ASG06+EAS04 5 + 4 + 2	11	LDCA+ASG06+EAS04	
2	LDCA+ASG06+HPR03 5 + 4 + 2	11	LDCA+ASG06+HPR03 4+4+2	10
3	LDCA+ASG06+HPSI01 5 + 4 + 2	11	LDCA+ASG06+HPSI01 4+4+2	10
4	LDCA+ASG06+LODC-H1 5 + 4 + 2	11	LDCA+ASG06+LODC-H1	
5	LDCA+ASG06+SRV04 5 + 4 + 2	11	LDCA+ASG06+SRV04	

核电厂SDP工作表——48VDC分析（标准电厂长期失去厂用电事件）

需要的安全功能：	每一安全功能完全可信的缓解能力。
主给水旁路供水（ARE）	主给水旁路有三条，根据成功准则要求，一个旁路向蒸汽发生器供水就满足要求。为了配合供水，还需要1台电动主给水泵或3台凝结水泵供水。
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
充排操作（LODC-H1）	直流电源丧失时操纵员实施一回路实施充排操作
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LDCC+ARE+ASG01+EAS03 5 + 3 + 4 + 3	15	LDCC+ARE+ASG01+EAS03	
2	LDCC+ARE+ASG01+HPR01 5 + 3 + 4 + 3	15	LDCC+ARE+ASG01+HPR01 4 + 3 + 4 + 3	14
3	LDCC+ARE+ASG01+HPSI 5 + 3 + 4 + 3	15	LDCC+ARE+ASG01+HPSI 4 + 3 + 4 + 3	14
4	LDCC+ARE+ASG01+LODC-H1 5 + 3 + 4 + 2	14	LDCC+ARE+ASG01+LODC-H1	
5	LDCC+ARE+ASG01+SRV02 5 + 3 + 4 + 3	15	LDCC+ARE+ASG01+SRV02	

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

核电厂SDP工作表——30VDC分析（标准电厂长期失去厂用电（LDDD）事件）

需要的安全功能：	每一安全功能完全可信的缓解能力。
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
充排操作（LODC-H1）	直流电源丧失时操纵员实施一回路实施充排操作
直流电源切换（LODC-H2）	操纵员将LDA供切换至URA，为调节阀供电
稳压器安全阀回座（SRV03）	稳压器安全阀租由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀租，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LDDD+ASG01+EAS03 4 + 4 + 3	11	LDDD+ASG01+EAS03	
2	LDDD+ASG01+HPR01 4 + 4 + 3	11	LDDD+ASG01+HPR01 3 + 4 + 3	10
3	LDDD+ASG01+HPSI 4 + 4 + 3	11	LDDD+ASG01+HPSI 3 + 4 + 3	10
4	LDDD+ASG01+LODC-H1 4 + 4 + 2	10	LDDD+ASG01+LODC-H1	
5	LDDD+ASG01+SRV02 4 + 4 + 3	11	LDDD+ASG01+SRV02	
6	LDDD+LODC-H2+EAS03 4 + 3 + 3	10	LDDD+LODC-H2+EAS03	
7	LDDD+LODC-H2+HPR01 4 + 3 + 3	10	LDDD+LODC-H2+HPR01 3 + 3 + 3	9
8	LDDD+LODC-H2+HPSI 4 + 3 + 3	10	LDDD+LODC-H2+HPSI 3 + 3 + 3	9
9	LDDD+LODC-H2+LODC-H1 4 + 3 + 2	9	LDDD+LODC-H2+LODC-H1	
10	LDDD+LODC-H2+SRV02 4 + 3 + 3	10	LDDD+LODC-H2+SRV02	

WEBSITE http://www.chinansc.cn/

核电厂SDP工作表——失去厂用电（LOHS）事件

需要的安全功能：	每一安全功能完全可信的缓解能力。
主蒸汽隔离（POS）	根据PSA模型分析，停运主泵的方式居多，其失效概率为1.5E-9。
稳压器安全阀回座（SRV03）	稳压器安全阀租 由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
正常轴封注入（X4）	轴封注入由两列上充泵及其注入管线构成，一列运行即可。
实施RCV防护措施（LOHS-H1）	操纵员实施保护RCV的两项措施，以保证泵运行可靠性。
充排操作（LOHS-H2）	在失热阱事故下，操纵员实施一回路实施充排操作
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀租，1组稳压器安全阀组打开即可。
稳定密封的可能性（IOS）	参考PSA分析，产生较大轴封破口的概率为0.1。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
再循环密封复热冲（LOHS-R）	对于复水口丧失事故，虽然有程序规定恢复热阱，但是根据PSA模型分析，热阱恢复的失效概率0.92，因此，该功能的剩余能力很不充分。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LHS1+ASG01+EAS03 6 + 4 + 3	13	LHS1+ASG01+EAS03	
2	LHS1+ASG01+HPR01 6 + 4 + 3	13	LHS1+ASG01+HPR01 5 + 4 + 3	12
3	LHS1+ASG01+HPSI 6 + 4 + 3	13	LHS1+ASG01+HPSI 5 + 4 + 3	12
4	LHS1+ASG01+LOHS-H2 6 + 4 + 2	12	LHS1+ASG01+LOHS-H2	
5	LHS1+ASG01+LOHS-R 6 + 4 + 1	11	LHS1+ASG01+LOHS-R	
6	LHS1+ASG01+SRV02 6 + 4 + 3	13	LHS1+ASG01+SRV02	
7	LHS1+IO4+ASG01 6 + 3 + 4	13	LHS1+IO4+ASG01 5 + 3 + 4	12
8	LHS1+IO4+EAS03 6 + 3 + 3	12	LHS1+IO4+EAS03 5 + 3 + 3	11
9	LHS1+IO4+HPR01 6 + 3 + 3	12	LHS1+IO4+HPR01 5 + 3 + 3	11
10	LHS1+IO4+HPSI 6 + 3 + 3	12	LHS1+IO4+HPSI 5 + 3 + 3	11
11	LHS1+IO4+LOHS-R 6 + 3 + 1	10	LHS1+IO4+LOHS-R 5 + 3 + 1	9
12	LHS1+LOHS-H1+ASG01 6 + 2 + 4	12	LHS1+LOHS-H1+ASG01	
13	LHS1+LOHS-H1+IO5+EAS03 6 + 2 + 1 + 3	12	LHS1+LOHS-H1+IO5+EAS03	
14	LHS1+LOHS-H1+IO5+HPR01 6 + 2 + 1 + 3	12	LHS1+LOHS-H1+IO5+HPR01 5 + 2 + 1 + 3	11
15	LHS1+LOHS-H1+IO5+HPSI 6 + 2 + 1 + 3	12	LHS1+LOHS-H1+IO5+HPSI 5 + 2 + 1 + 3	11
16	LHS1+LOHS-H1+IO5+LOHS-R 6 + 2 + 1 + 1	10	LHS1+LOHS-H1+IO5+LOHS-R	
17	LHS1+POS 6 + 9	15	LHS1+POS	
18	LHS1+SRV03 6 + 4	10	LHS1+SRV03	

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

核电厂SDP工作表——失去厂用电（RHR）事件（LHS2）序列

需要的安全功能：	每一安全功能完全可信的缓解能力。
主蒸汽隔离（POS）	根据PSA模型分析，停运主泵的方式居多，其失效概率为1.5E-9。
稳压器安全阀回座（SRV03）	稳压器安全阀租由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
实施RCV防护措施（LOHS-H1）	操纵员实施保护RCV的两项措施，以保证泵运行可靠性。
充排操作（LOHS-H2）	在失热阱事故下，操纵员实施一回路实施充排操作
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀租，1组稳压器安全阀组打开即可。
稳定密封的可能性（IOS）	参考PSA分析，产生较大轴封破口的概率为0.1。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LHS2+ASG01+EAS03 4 + 4 + 3	11	LHS2+ASG01+EAS03	
2	LHS2+ASG01+HPR01 4 + 4 + 3	11	LHS2+ASG01+HPR01 3 + 4 + 3	10
3	LHS2+ASG01+HPSI 4 + 4 + 3	11	LHS2+ASG01+HPSI 3 + 4 + 3	10
4	LHS2+ASG01+LOHS-H2 4 + 4 + 2	10	LHS2+ASG01+LOHS-H2	
5	LHS2+ASG01+SRV02 4 + 4 + 3	11	LHS2+ASG01+SRV02	
6	LHS2+LOHS-H1+ASG01 4 + 2 + 4	10	LHS2+LOHS-H1+ASG01	
7	LHS2+LOHS-H1+IO5+EAS03 4 + 2 + 1 + 3	10	LHS2+LOHS-H1+IO5+EAS03	
8	LHS2+LOHS-H1+IO5+HPR01 4 + 2 + 1 + 3	10	LHS2+LOHS-H1+IO5+HPR01 3 + 2 + 1 + 3	9
9	LHS2+LOHS-H1+IO5+HPSI 4 + 2 + 1 + 3	10	LHS2+LOHS-H1+IO5+HPSI 3 + 2 + 1 + 3	9
10	LHS2+POS 4 + 9	13	LHS2+POS	
11	LHS2+SRV03+ASG01 4 + 4 + 4	12	LHS2+SRV03+ASG01	
12	LHS2+SRV03+EAS03 4 + 4 + 3	11	LHS2+SRV03+EAS03	
13	LHS2+SRV03+HPR01 4 + 4 + 3	11	LHS2+SRV03+HPR01 3 + 4 + 3	10
14	LHS2+SRV03+HPSI 4 + 4 + 3	11	LHS2+SRV03+HPSI 3 + 4 + 3	10

WEBSITE http://www.chinansc.cn/

[illegible]SBO事故序列——[illegible]（LOHS）序列

[illegible]	每一安全功能完全可信的缓解能力。
[illegible]	根据PSA模型分析，停运主泵的方式很多，其失效概率为1.5E-9。
稳压器安全阀组座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
阀阀阀门类阀信号（J01）	该功能主要隔离设备冷却水系统公用列，保证重要用户的冷却水。根据PSA模型分析，阀阀阀门类失效概率是：5.0E-3。
主泵[illegible]（LOHS-H1）	操纵员实施保护RCP的再启动，以保证泵运行可靠性。
关闭主泵（LOHS-H2）	发失热排事故下，操纵员实施一回路实施充排操作
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
[illegible]（SRV02）	由三组稳压器安全阀组，1组稳压器安全阀组打开即可。
[illegible]（J05）	参考PSA分析，产生较大轴封破口的概率为0.1。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

序号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LHS3+ASG01+EAS03 4 + 4 + 3	11	LHS3+ASG01+EAS03	
2	LHS3+ASG01+HPR01 4 + 4 + 3	11	LHS3+ASG01+HPR01 3 + 4 + 3	10
3	LHS3+ASG01+HPSI 4 + 4 + 3	11	LHS3+ASG01+HPSI 3 + 4 + 3	10
4	LHS3 +ASG01+LOHS-H2 4 + 4 + 2	10	LHS3+ASG01+LOHS-H2	
5	LHS3+ASG01+SRV02 4 + 4 + 3	11	LHS3+ASG01+SRV02	
6	LHS3+I01+ASG01 4 + 2 + 4	10	LHS3+I01+ASG01	
7	LHS3+I01+J05+EAS03 4 + 2 + 1 + 3	10	LHS3+I01+J05+EAS03	
8	LHS3+I01+J05+HPR01 4 + 2 + 1 + 3	10	LHS3+I01+J05+HPR01 3 + 2 + 1 + 3	9
9	LHS3+I01+J05+HPSI 4 + 2 + 1 + 3	10	LHS3+I01+J05+HPSI 3 + 2 + 1 + 3	9
10	LHS3+LOHS-H3+ASG01 4 + 3 + 4	11	LHS3+LOHS-H3+ASG01	
11	LHS3+LOHS-H3+J05+EAS03 4 + 3 + 1 + 3	11	LHS3+LOHS-H3+J05+EAS03	
12	LHS3+LOHS-H3+J05+HPR01 4 + 3 + 1 + 3	11	LHS3+LOHS-H3+J05+HPR01 3 + 3 + 1 + 3	10
13	LHS3+LOHS-H3+J05+HPSI 4 + 3 + 1 + 3	11	LHS3+LOHS-H3+J05+HPSI 3 + 3 + 1 + 3	10
14	LHS3+P05 4 + 9	13	LHS3+P05	
15	LHS3+SRV03+ASG01 4 + 4 + 4	12	LHS3+SRV03+ASG01	
16	LHS3+SRV03+EAS03 4 + 4 + 3	11	LHS3+SRV03+EAS03	
17	LHS3+SRV03+HPR01 4 + 4 + 3	11	LHS3+SRV03+HPR01 3 + 4 + 3	10
18	LHS3+SRV03+HPSI 4 + 4 + 3	11	LHS3+SRV03+HPSI 3 + 4 + 3	10

WEBSITE http://www.chinansc.cn/

[illegible]SBO事故序列——[illegible]（LMFW）序列

[illegible]	每一安全功能完全可信的缓解能力。
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
稳压器安全阀组座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
充排操作（LMFW-H1）	操纵员实施一回路实施充排操作，启动安注和打开稳压器安全阀
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

序号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LMFW+ASG01+EAS03 3 + 4 + 3	10	LMFW+ASG01+EAS03	
2	LMFW+ASG01+HPR01 3 + 4 + 3	10	LMFW+ASG01+HPR01 2 + 4 + 3	9
3	LMFW+ASG01+HPSI 3 + 4 + 3	10	LMFW+ASG01+HPSI 2 + 4 + 3	9
4	LMFW+ASG01+LMFW-H1 3 + 4 + 3	10	LMFW+ASG01+LMFW-H1	

[illegible]SBO事故序列——[illegible]（LOIA）序列

[illegible]	每一安全功能完全可信的缓解能力。
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
稳压器安全阀组座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
充排操作（LMFW-H1）	操纵员实施一回路实施充排操作，启动安注和打开稳压器安全阀
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

序号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LOIA+ASG01+EAS03 4 + 4 + 3	11	LOIA+ASG01+EAS03	
2	LOIA+ASG01+HPR01 4 + 4 + 3	11	LOIA+ASG01+HPR01 3 + 4 + 3	10
3	LOI A+ASG01+HPSI 4 + 4 + 3	11	LOIA+ASG01+HPSI 3 + 4 + 3	10
4	LOIA+ASG01+LMFW-H1 4 + 4 + 3	11	LOIA+ASG01+LMFW-H1	
5	LOIA+ASG01+SRV02 4 + 4 + 3	11	LOIA+ASG01+SRV02	

WEBSITE http://www.chinansc.cn/

[illegible]SBO事故序列——厂外失电事故序列（LOOP）序列

[illegible]	每一安全功能完全可信的缓解能力。
辅助给水供水（ASG02）	对于全厂断电事故，ASG系统只有汽动泵可用。
稳压器安全阀组座（SRV03）	稳压器安全阀组由安全阀和隔离阀构成，当一回路压力降到某一值后，两个阀门会相继关闭，所以只要一个阀门关闭即可保证稳压器的完整性。
EDG系统（EDG）	该功能由一台汽轮机及其发电机构成
LOOP事故（LOOP-H1）	LOOP事故下，操纵员实施一回路实施充排操作
不间断电源入（DI）	该功能由一台水压试验装置注入装置构成。
物质液位的可靠性（D5）	参考PSA分析，产生较大轴封破口的概率为0.1。
交流电源恢复（LOOP-R）	全厂断电事故下，电源恢复程序程序，允许时间0.5小时。根据PSA分析，交流电源的恢复失效概率0.02。因此该功能剩余能力因子为1。
辅助给水供水（ASG03）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

序号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	LOOP+ASG01+EAS03 4 + 4 + 3	11	LOOP+ASG01+EAS03	
2	LOOP+ASG01+HPR01 4 + 4 + 3	11	LOOP+ASG01+HPR01 3 + 4 + 3	10
3	LOOP+ASG01+HPSI 4 + 4 + 3	11	LOOP+ASG01+HPSI 3 + 4 + 3	10
4	LOOP+ASG01+LOOP-H1 4 + 4 + 3	11	LOOP+ASG01+LOOP-H1	
5	LOOP+ASG01+SRV02 4 + 4 + 3	11	LOOP+ASG01+SRV02	
6	LOOP+EDG+ASG02+ASG04 4 + 3 + 1 + 2	10	LOOP+EDG+ASG02+ASG04	
7	LOOP+EDG+ASG02+J03+ASG04 4 + 3 + 1 + 2 + 2	12	LOOP+EDG+ASG02+J03+ASG04	
8	LOOP+EDG+ASG02+J03+HPSI 4 + 3 + 1 + 2 + 3	13	LOOP+EDG+ASG02+J03+HPSI 3 + 3 + 1 + 2 + 3	12
9	LOOP+EDG+ASG02+J03+LOOP-R 4 + 3 + 1 + 2 + 3	11	LOOP+EDG+ASG02+J03+LOOP-R	
10	LOOP+EDG+ASG02+LLS+ASG04 4 + 3 + 1 + 1 + 2	11	LOOP+EDG+ASG02+LLS+ASG04	
11	LOOP+EDG+ASG02+LLS+HPSI 4 + 3 + 1 + 1 + 3	12	LOOP+EDG+ASG02+LLS+HPSI 3 + 3 + 1 + 1 + 3	11
12	LOOP+EDG+ASG02+LLS+LOOP-R 4 + 3 + 1 + 1	10	LOOP+EDG+ASG02+LLS+LOOP-R	
13	LOOP+EDG+ASG02+LOOP-R 4 + 3 + 1 + 1	9	LOOP+EDG+ASG02+LOOP-R	
14	LOOP+EDG+ASG02+SRV03 4 + 3 + 1 + 4	12	LOOP+EDG+ASG02+SRV03	
15	LOOP+EDG+J03+HPSI 4 + 3 + 2 + 1 + 3	13	LOOP+EDG+J03+HPSI 3 + 3 + 2 + 1 + 3	12
16	LOOP+EDG+J03+LOOP-R 4 + 3 + 2 + 1 + 1	10	LOOP+EDG+J03+LOOP-R	
17	LOOP+EDG+LLS+J03+HPSI 4 + 3 + 1 + 1 + 3	12	LOOP+EDG+LLS+J03+HPSI 3 + 3 + 1 + 1 + 3	11
18	LOOP+EDG+LLS+J03+LOOP-R 4 + 3 + 1 + 1 + 1	10	LOOP+EDG+LLS+J03+LOOP-R	
19	LOOP+EDG+LLS+LOOP-H2 4 + 3 + 1 + 3	11	LOOP+EDG+LLS+LOOP-H2	
20	LOOP+EDG+LLS+LOOP-H2+ASG04 4 + 3 + 1 + 3 + 2	13	LOOP+EDG+LLS+LOOP-H2+ASG04	
21	LOOP+EDG+LLS+LOOP-H2+HPSI 4 + 3 + 1 + 3 + 3	14	LOOP+EDG+LLS+LOOP-H2+HPSI 3 + 3 + 1 + 3 + 3	13
22	LOOP+EDG+LLS+LOOP-H2+LOOP-R 4 + 3 + 1 + 3 + 1	12	LOOP+EDG+LLS+LOOP-H2+LOOP-R	
23	LOOP+EDG+SRV03 4 + 3 + 4	11	LOOP+EDG+SRV03	

sc.cn/

[illegible]SBO事故序列——[illegible]（LOCA）序列

[illegible]	每一安全功能完全可信的缓解能力。
[illegible]（EAS01）	安全壳喷淋系统有2列，一列运行成功即可。系统是自动启动。
[illegible]（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
失水事故（LOCA-H1）	LOCA事故下操纵员没有该停安注
高压安注直接注入（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
阀门失效操作（LOCA-H2）	操纵员使用二次侧对一回路实施降温降压操作
二次侧热量冷却（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵。同时必须2/3TCs可用。
中压安注（HPI）	中压安注有3个安注箱注入管线，对于主回路上游破口，只有两列可用；因此该功能的剩余能力是3。
低压安注直接注入（LPSI）	低压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入
低压安注冷段再循环（LPR01）	低压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS02）	安全壳喷淋系统有2列，一列运行成功即可。系统是自动启动。

序号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	MLOCA+EAS01 6 + 3	9	MLOCA+EAS01	
2	MLOCA+EAS02 6 + 3	9	MLOCA+EAS02	
3	MLOCA+HPR01+ASG05 6 + 3 + 2	11	MLOCA+HPR01+ASG05 5 + 3 + 2	10
4	MLOCA+HPR01+EAS02 6 + 3 + 3	12	MLOCA+HPR01+EAS02 5 + 3 + 3	11
5	MLOCA+HPR01+LOCA-H2 6 + 3 + 1	10	MLOCA+HPR01+LOCA-H2 5 + 3 + 1	9
6	MLOCA+HPR01+LPR01 6 + 3 + 3	12	MLOCA+HPR01+LPR01 5 + 3 + 3	11
7	MLOCA+HPR01+LPR02 6 + 3 + 3	12	MLOCA+HPR01+LPR02 5 + 3 + 3	11
8	MLOCA+HPR01+SIT 6 + 3 + 3	12	MLOCA+HPR01+SIT 5 + 3 + 3	11
9	MLOCA+HPR02+ASG05 6 + 3 + 2	11	MLOCA+HPR02+ASG05 5 + 3 + 2	10
10	MLOCA+HPR02+EAS02 6 + 3 + 3	12	MLOCA+HPR02+EAS02 5 + 3 + 3	11
11	MLOCA+HPR02+LOCA-H2 6 + 3 + 1	10	MLOCA+HPR02+LOCA-H2 5 + 3 + 1	9
12	MLOCA+HPR02+LPR02 6 + 3 + 3	12	MLOCA+HPR02+LPR02 5 + 3 + 3	11
13	MLOCA+HPR02+SIT 6 + 3 + 3	12	MLOCA+HPR02+SIT 5 + 3 + 3	11
14	MLOCA+HPSI+ASG05 6 + 3 + 2	11	MLOCA+HPSI+ASG05 5 + 3 + 2	10
15	MLOCA+HPSI+EAS02 6 + 3 + 3	12	MLOCA+HPSI+EAS02 5 + 3 + 3	11
16	MLOCA+HPSI+LOCA-H2 6 + 3 + 1	10	MLOCA+HPSI+LOCA-H2 5 + 3 + 1	9
17	MLOCA+HPSI+LPR01 6 + 3 + 3	12	MLOCA+HPSI+LPR01 5 + 3 + 3	11
18	MLOCA+HPSI+LPR02 6 + 3 + 3	12	MLOCA+HPSI+LPR02 5 + 3 + 3	11
19	MLOCA+HPSI+LPSI 6 + 3 + 3	12	MLOCA+HPSI+LPSI 5 + 3 + 3	11
20	MLOCA+HPSI+SIT 6 + 3 + 3	12	MLOCA+HPSI+SIT 5 + 3 + 3	11
21	MLOCA+LOCA-H1 6 + 3	9	MLOCA+LOCA-H1	
22	MLOCA+SIT 6 + 3	9	MLOCA+SIT	

WEBSITE http://www.chinansc.cn/

表格7 SDP工作表——安全注入和余热排出系统（MSLB1）序列

最终安全功能	每一安全功能完全可信的缓解能力：
主蒸汽隔离阀（MSIV）	事故蒸汽发生器回路的主蒸汽隔离阀关闭会其他回路的关闭即可。相当于两列。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
安全壳喷淋直接注入（EAS01）	安全壳喷淋系统有2列，一列运行成功即可，系统是自动启动。
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵。
事故蒸汽发生器隔离和水箱补水（MSLB-H1）	主蒸汽管道破裂事故下，事故蒸汽发生器隔离并向辅助给水水箱补水
充排操作（MSLB-H2）	主蒸汽管道破裂事故下，操纵员实施一回路实施充排操作
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀相，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS02）	安全壳喷淋系统有2列，一列运行成功即可，系统是自动切换。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	MSLB1+ASG03+EAS02 5 + 4 + 3	12	MSLB1+ASG03+EAS02	
2	MSLB1+ASG03+HPR01 5 + 4 + 3	12	MSLB1+ASG03+HPR01 4 + 4 + 3	11
3	MSLB1+ASG03+MSLB-H2 5 + 4 + 1	10	MSLB1+ASG03+MSLB-H2	
4	MSLB1+ASG03+SRV02 5 + 4 + 3	12	MSLB1+ASG03+SRV02	
5	MSLB1+HPSI 5 + 3	8	MSLB1+HPSI 4 + 3	7
6	MSLB1+MSIV+EAS01 5 + 3 + 3	11	MSLB1+MSIV+EAS01	
7	MSLB1+MSIV +EAS02 5 + 3 + 3	11	MSLB1+MSIV+EAS02	
8	MSLB1+MSIV+HPR01 5 + 3 + 3	11	MSLB1+MSIV+HPR01 4 + 3 + 3	10
9	MSLB1+MSIV+HPSI 5 + 3 + 3	11	MSLB1+MSIV+HPSI 4 + 3 + 3	10
10	MSLB1+MSIV+MSLB-H2 5 + 3 + 1	9	MSLB1+MSIV+MSLB-H2	
11	MSLB1+MSIV+SRV02 5 + 3 + 3	11	MSLB1+MSIV+SRV02	
12	MSLB1+MSLB-H1+EAS02 5 + 3 + 3	11	MSLB1+MSLB-H1+EAS02	
13	MSLB1+MSLB-H1+HPR01 5 + 3 + 3	11	MSLB1+MSLB-H1+HPR01 4 + 3 + 3	10
14	MSLB1+MSLB-H1+MSLB-H2 5 + 3 + 1	9	MSLB1+MSLB-H1+MSLB-H2	
15	MSLB1+MSLB-H1+SRV02 5 + 3 + 3	11	MSLB1+MSLB-H1+SRV02	

表格7 SDP工作表——安全注入和余热排出系统（MSLB2）序列

最终安全功能	每一安全功能完全可信的缓解能力：
主蒸汽隔离阀（MSIV）	事故蒸汽发生器回路的主蒸汽隔离阀关闭会其他回路的关闭即可。相当于两列。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
辅助给水供水（ASG03）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵。
事故蒸汽发生器隔离和水箱补水（MSLB-H1）	主蒸汽管道破裂事故下，事故蒸汽发生器隔离并向辅助给水水箱补水
充排操作（MSLB-H2）	主蒸汽管道破裂事故下，操纵员实施一回路实施充排操作
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀相，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	MSLB2+ASG03+EAS03 5 + 4 + 3	12	MSLB2+ASG03+EAS03	
2	MSLB2+ASG03+HPR01 5 + 4 + 3	12	MSLB2+ASG03+HPR01 4 + 4 + 3	11
3	MSLB2+ASG03+MSLB-H2 5 + 4 + 1	10	MSLB2+ASG03+MSLB-H2	
4	MSLB2+ASG03+SRV02 5 + 4 + 3	12	MSLB2+ASG03+SRV02	
5	MSLB2+HPSI 5 + 3	8	MSLB2+HPSI 4 + 3	7
6	MSLB2+MSIV+EAS03 5 + 3 + 3	11	MSLB2+MSIV+EAS03	
7	MSLB2+MSIV+HPR01 5 + 3 + 3	11	MSLB2+MSIV+HPR01 4 + 3 + 3	10
8	MSLB2+MSIV+HPSI 5 + 3 + 3	11	MSLB2+MSIV+HPSI 4 + 3 + 3	10
9	MSLB2+MSIV+MSLB-H2 5 + 3 + 1	9	MSLB2+MSIV+MSLB-H2	
10	MSLB2+MSIV+SRV02 5 + 3 + 3	11	MSLB2+MSIV+SRV02	
11	MSLB2+MSLB-H1+EAS03 5 + 3 + 3	11	MSLB2+MSLB-H1+EAS03	
12	MSLB2+MSLB-H1+HPR01 5 + 3 + 3	11	MSLB2+MSLB-H1+HPR01 4 + 3 + 3	10
13	MSLB2+MSLB-H1+MSLB-H2 5 + 3 + 1	9	MSLB2+MSLB-H1+MSLB-H2	
14	MSLB2+MSLB-H1+SRV02 5 + 3 + 3	11	MSLB2+MSLB-H1+SRV02	

表格7 SDP工作表——安全注入和余热排出系统（MSLB3）序列

最终安全功能	每一安全功能完全可信的缓解能力：
主蒸汽隔离阀（MSIV）	事故蒸汽发生器回路的主蒸汽隔离阀关闭会其他回路的关闭即可，相当于两列。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
辅助给水供水（ASG03）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵。
充排操作（MSLB-H2）	主蒸汽管道破裂事故下，操纵员实施一回路实施充排操作
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀相，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对FB情况下的再循环，需要操纵员启动，根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	MSLB3+ASG03+EAS03 5 + 4 + 3	12	MSLB3+ASG03+EAS03	
2	MSLB3+ASG03+HPR01 5 + 4 + 3	12	MSLB3+ASG03+HPR01 4 + 4 + 3	11
3	MSLB3+ASG03+MSLB-H2 5 + 4 + 1	10	MSLB3+ASG03+MSLB-H2	
4	MSLB3+ASG03+SRV02 5 + 4 + 3	12	MSLB3+ASG03+SRV02	
5	MSLB3+MSIV+EAS03 5 + 3 + 3	11	MSLB3+MSIV+EAS03	
6	MSLB3+MSIV+HPR01 5 + 3 + 3	11	MSLB3+MSIV+HPR01 4 + 3 + 3	10
7	MSLB3+MSIV+HPSI 5 + 3 + 3	11	MSLB3+MSIV+HPSI 4 + 3 + 3	10
8	MSLB3+MSIV+MSLB-H2 5 + 3 + 1	9	MSLB3+MSIV+MSLB-H2	
9	MSLB3+MSIV+SRV02 5 + 3 + 3	11	MSLB3+MSIV+SRV02	

表格7 SDP工作表——安全注入和余热排出系统（SGTR）序列

最终安全功能	每一安全功能完全可信的缓解能力：
二次侧快速冷却（ASG05）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵，同时必须2/3GTCs可用。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
充排操作（SGTR-H1）	SG TR事故下，操纵员实施一回路实施充排操作
蒸汽发生器降压（SGTR-H2）	SG TR事故下，破损蒸汽发生器充满前降压到释放阀整定压力之下
蒸汽发生器后降压（SGTR-H3）	SG TR事故下，破损蒸汽发生器充满后降压到释放阀整定压力之下的操作
隔离破损蒸汽发生器（SGTR-H4）	SG TR事故下隔离非破损蒸汽发生器
余热排出冷却（SGTR-H5）	SG TR事故下实施蒸汽发生器将堆芯冷却至RRA连接
辅助给水供水（SGTR-H6）	SG TR事故下辅助给水箱补水
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀相，1组稳压器安全阀组打开即可。
蒸汽发生器主蒸汽安全阀组（MSSV）	根据PSA故障树分析，未开座的失效概率在3.0E-4，因此，剩余能力因子是4。
喷雾（SPAY）	一回路降压可以由主喷淋或辅助喷淋实现，所以剩余能力因子为4。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
余热排出系统（RRA）	余热排出系统有2个相同组成，一列运行成功即可。

编号	选择受影响的功能	基准分	每一受影响的事故序列的剩余缓解能力评价	结果
1	SGTR+ASG05+EAS03 5 + 2 + 3	10	SGTR+ASG05+EAS03	
2	SGTR+ASG05+HPR01 5 + 2 + 3	10	SGTR+ASG05+HPR01 4 + 2 + 3	9
3	SGTR+ASG05+HPSI 5 + 2 + 3	10	SGTR+ASG05+HPSI 4 + 2 + 3	9
4	SGTR+ASG05+SG TR-H1 5 + 2 + 2	9	SGTR+ASG05+SGTR-H1	
5	SGTR+ASG05+SRV02 5 + 2 + 3	10	SG TR+ASG05+SRV02	
6	SGTR+HPSI+SGTR-H2 5 + 3 + 1	9	SGTR+HPSI+SGTR-H2 4 + 3 + 1	8
7	SGTR+HPSI+SGTR-H4 5 + 3 + 3	11	SGTR+HPSI+SGTR-H4 4 + 3 + 3	10
8	SGTR+HPSI+SG TR-H6+RRA 5 + 3 + 3 + 3	14	SGTR+HPSI+SGTR-H6+RRA 4 + 3 + 3 + 3	13
9	SGTR+HPSI+SPAY 5 + 3 + 4	12	SGTR+HPSI+SPAY 4 + 3 + 4	11
10	SG TR+SG TR-H2+SGTR-H3 5 + 1 + 3	9	SGTR+SGTR-H2+SG TR-H3	
11	SGTR+SGTR-H2+SGTR-H4+RRA 5 + 1 + 3 + 3	12	SG TR+SG TR-H2+SGTR-H4+RRA	
12	SGTR+SGTR-H2+SGTR-H4+SGTR-H5 5 + 1 + 3 + 3	12	SGTR+SGTR-H2+SGTR-H4+SGTR-H5	
13	SGTR+SGTR-H2+SGTR-H6+RRA 5 + 1 + 3 + 3	12	SG TR+SG TR-H2+SGTR-H6+RRA	
14	SGTR+SGTR-H2+SPAY 5 + 1 + 4	10	SGTR+SGTR-H2+SPAY	
15	SGTR+SGTR-H4+RRA 5 + 3 + 3	11	SGTR+SGTR-H4+RRA	
16	SG TR+SG TR-H4+SGTR-H5 5 + 3 + 3	11	SGTR+SGTR-H4+SG TR-H5	
17	SGTR+SGTR-H6+RRA 5 + 3 + 3	11	SGTR+SGTR-H6+RRA	
18	SGTR+SPAY 5 + 4	9	SG TR+SPAY	

表 7 SDP-4.3 —— 事故序列 2.2（LOCA）[illegible]

事故序列名称	每一安全功能完全可信的缓解能力：
二次侧快速冲洗（ASG05）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵，同时必须2/3GTG可用。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
失稳停堆法（LOCA-H1）	LOCA事故下操纵员没有误停安注
降温降压操作（LOCA-H2）	操纵员使用二次侧对一回路实施降温降压操作
充排操作（LOCA-H3）	LOCA事故下，操纵员实施一回路实施充排操作
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，3组稳压器安全阀组打开即可。
高压安注再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
中压安注（SIT）	中压安注有3个安注箱及注入管线，对于主回路上的破口，只有两列可用，因此该功能的剩余能力是3。
低压安注直接注入（LPSI）	低压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入
余热排出系统（RRA）	余热排出系统由两个相同列组成，一列运行成功即可。
安全壳喷淋系统有2列。（EAS01）	安全壳喷淋系统有2列，一列运行成功即可，系统是自动启动。
安全壳喷淋再循环（EAS02）	安全壳喷淋系统有2列，一列运行成功即可，系统是自动切换。

编号	选择受影响的功能	基准分	每一受影响的重故序列的剩余缓解能力评价	结果
1	SLOCA+ASG05+EAS01 5 + 2 + 3	10	SLOCA+ASG05+EAS01	
2	SLOCA+ASG05+EAS02 5 + 2 + 3	10	SLOCA+ASG05+EAS02	
3	SLOCA+ASG05+HPR01 5 + 2 + 3	10	SLOCA+ASG05+HPR01 4 + 2 + 3	9
4	SLOCA+ASG05+HPSI 5 + 2 + 3	10	SLOCA+ASG05+HPSI 4 + 2 + 3	9
5	SLOCA+ASG05+LOCA-H1 5 + 2 + 3	10	SLOCA+ASG05+LOCA-H1	
6	SLOCA+ASG05+LOCA-H3 5 + 2 + 2	9	SLOCA+ASG05+LOCA-H3	
7	SLOCA+ASG05+SRV02 5 + 2 + 3	10	SLOCA+ASG05+SRV02	
8	SLOCA+HPSI+LOCA-H2 5 + 3 + 1	9	SLOCA+HPSI+LOCA-H2 4 + 3 + 1	8
9	SLOCA+HPSI+LPR01 5 + 3 + 3	11	SLOCA+HPSI+LPR01 4 + 3 + 3	10
10	SLOCA+HPSI+LPSI 5 + 3 + 3	11	SLOCA+HPSI+LPSI 4 + 3 + 3	10
11	SLOCA+HPSI+RRA+EAS02 5 + 3 + 3 + 3	14	SLOCA+HPSI+RRA+EAS02 4 + 3 + 3 + 3	13
12	SLOCA+HPSI+SIT 5 + 3 + 3	11	SLOCA+HPSI+SIT 4 + 3 + 3	10
13	SLOCA+LOCA-H1 5 + 3	8	SLOCA+LOCA-H1	
14	SLOCA+LOCA-H2+EAS02 5 + 1 + 3	9	SLOCA+LOCA-H2+EAS02	
15	SLOCA+LOCA-H2+HPR01 5 + 1 + 3	9	SLOCA+LOCA-H2+HPR01 4 + 1 + 3	8
16	SLOCA+LPR01 5 + 3	8	SLOCA+LPR01	
17	SLOCA+LPSI 5 + 3	8	SLOCA+LPSI	
18	SLOCA+RRA+EAS02 5 + 3 + 3	11	SLOCA+RRA+EAS02	

表 7 SDP-4.3 —— 事故序列 2.3（SGTR）[illegible]

事故序列名称	每一安全功能完全可信的缓解能力：
二次侧快速冲洗（ASG05）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵，同时必须2/3GTG可用。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
失稳停堆法（LOCA-H1）	LOCA事故下操纵员没有误停安注
降温降压操作（LOCA-H2）	操纵员使用二次侧对一回路实施降温降压操作
充排操作（LOCA-H3）	LOCA事故下，操纵员实施一回路实施充排操作
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，3组稳压器安全阀组打开即可。
高压安注再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
中压安注（SIT）	中压安注有3个安注箱及注入管线，对于主回路上的破口，只有两列可用，因此该功能的剩余能力是3。
低压安注直接注入（LPSI）	低压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入
余热排出系统（RRA）	余热排出系统由两个相同列组成，一列运行成功即可。

编号	选择受影响的功能	基准分	每一受影响的重故序列的剩余缓解能力评价	结果
1	SSGTR1+ASG05 7 + 2	9	SSGTR1+ASG05	
2	SSGTR1+HPSI 7 + 3	10	SSGTR1+HPSI 6 + 3	9
3	SSGTR1+LPSI 7 + 3	10	SSGTR1+LPSI	
4	SSGTR1+RRA 7 + 3	10	SSGTR1+RRA	
5	SSGTR1+SSGTR-H1 7 + 3	10	SSGTR1+SSGTR-H1	

表 7 SDP-4.3 —— 事故序列 2.3（SSGTR-H2）[illegible]

事故序列名称	每一安全功能完全可信的缓解能力：
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
二次侧快速冲洗（ASG05）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵，同时必须2/3GTG可用。
重新投入安注（SSGTRH2）	蒸汽管道小破口叠加10根SGTR事故下重新投入安注
中压安注（SIT）	中压安注有3个安注箱及注入管线，对于主回路上的破口，只有两列可用，因此该功能的剩余能力是3。
低压安注直接注入（LPSI）	低压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入
实施降温降压操作（SSGTRH3）	操纵员对一回路实施降温降压操作
余热排出系统（RRA）	余热排出系统由两个相同列组成，一列运行成功即可。

编号	选择受影响的功能	基准分	每一受影响的重故序列的剩余缓解能力评价	结果
1	SSGTR2+ASG05 8 + 2	10	SSGTR2+ASG05	
2	SSGTR2+HPSI 8 + 3	11	SSGTR2+HPSI 7 + 3	10
3	SSGTR2+LPSI 8 + 3	11	SSGTR2+LPSI	
4	SSGTR2+RRA 8 + 3	11	SSGTR2+RRA	
5	SSGTR2+SIT 8 + 3	11	SSGTR2+SIT	
6	SSGTR2+SSGTR-H2 8 + 1	9	SSGTR2+SSGTR-H2	
7	SSGTR2+SSGTR-H3 8 + 3	11	SSGTR2+SSGTR-H3	

表 7 SDP-4.3 —— 事故序列 2.4（SGTR-H1）[illegible]

事故序列名称	每一安全功能完全可信的缓解能力：
二次侧快速冲洗（ASG05）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是两台电动泵或一台汽动泵，同时必须2/3GTG可用。
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
失稳停堆法（LOCA-H1）	LOCA事故下操纵员没有误停安注
降温降压操作（LOCA-H2）	操纵员使用二次侧对一回路实施降温降压操作
充排操作（LOCA-H3）	LOCA事故下，操纵员实施一回路实施充排操作
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，3组稳压器安全阀组打开即可。
高压安注再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
中压安注（SIT）	中压安注有3个安注箱及注入管线，对于主回路上的破口，只有两列可用，因此该功能的剩余能力是3。
低压安注直接注入（LPSI）	低压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入
余热排出系统（RRA）	余热排出系统由两个相同列组成，一列运行成功即可。
安全壳喷淋系统有2列。（EAS01）	安全壳喷淋系统有2列，一列运行成功即可，系统是自动启动。
安全壳喷淋再循环（EAS02）	安全壳喷淋系统有2列，一列运行成功即可，系统是自动切换。

编号	选择受影响的功能	基准分	每一受影响的重故序列的剩余缓解能力评价	结果
1	SGTR+ASG05+EAS01 7 + 2 + 3	12	SGTR+ASG05+EAS01	
2	SGTR+ASG05+EAS02 7 + 2 + 3	12	SGTR+ASG05+EAS02	
3	SGTR+ASG05+HPR01 7 + 2 + 3	12	SGTR+ASG05+HPR01 6 + 2 + 3	11
4	SGTR+ASG05+HPSI 7 + 2 + 3	12	SGTR+ASG05+HPSI 6 + 2 + 3	11
5	SGTR+ASG05+LOCA-H1 7 + 2 + 3	12	SGTR+ASG05+LOCA-H1	
6	SGTR+ASG05+LOCA-H3 7 + 2 + 2	11	SGTR+ASG05+LOCA-H3	
7	SGTR+ASG05+SRV02 7 + 2 + 3	12	SGTR+ASG05+SRV02	
8	SGTR+HPSI+LOCA-H2 7 + 3 + 1	11	SGTR+HPSI+LOCA-H2 6 + 3 + 1	10
9	SGTR+HPSI+LPR01 7 + 3 + 3	13	SGTR+HPSI+LPR01 6 + 3 + 3	12
10	SGTR+HPSI+LPSI 7 + 3 + 3	13	SGTR+HPSI+LPSI 6 + 3 + 3	12
11	SGTR+HPSI+RRA+EAS02 7 + 3 + 3 + 3	16	SGTR+HPSI+RRA+EAS02 6 + 3 + 3 + 3	15
12	SGTR+HPSI+SIT 7 + 3 + 3	13	SGTR+HPSI+SIT 6 + 3 + 3	12
13	SGTR+LOCA-H1 7 + 3	10	SGTR+LOCA-H1	
14	SGTR+LOCA-H2+EAS02 7 + 1 + 3	11	SGTR+LOCA-H2+EAS02	
15	SGTR+LOCA-H2+HPR01 7 + 1 + 3	11	SGTR+LOCA-H2+HPR01 6 + 1 + 3	10
16	SGTR+LPR01 7 + 3	10	SGTR+LPR01	
17	SGTR+LPSI 7 + 3	10	SGTR+LPSI	
18	SGTR+RRA+EAS02 7 + 3 + 3	13	SGTR+RRA+EAS02	

表 7 SDP-4.3 —— 事故序列 2.5（SSTRANS）[illegible]

事故序列名称	每一安全功能完全可信的缓解能力：
主给水旁路供水（ARE）	主给水旁路有三条，根据成功准则要求，一个旁路向蒸汽发生器供水就满足要求。为了配合供水，还需要1台电动主给水泵或3台凝结水泵供水。
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
充排操作（LMFW-H1）	操纵员实施一回路实施充排操作，启动安注和打开稳压器安全阀
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对F8情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的重故序列的剩余缓解能力评价	结果
1	STRANS+ARE+ASG01+EAS03 3 + 3 + 4 + 3	13	STRANS+ARE+ASG01+EAS03	
2	STRANS+ARE+ASG01+HPR01 3 + 3 + 4 + 3	13	STRANS+ARE+ASG01+HPR01 2 + 3 + 4 + 3	12
3	STRANS+ARE+ASG01+HPSI 3 + 3 + 4 + 3	13	STRANS+ARE+ASG01+HPSI 2 + 3 + 4 + 3	12
4	STRANS+ARE+ASG01+LMFW-H1 3 + 3 + 4 + 3	13	STRANS+ARE+ASG01+LMFW-H1	
5	STRANS+ARE+ASG01+SRV02 3 + 3 + 4 + 3	13	STRANS+ARE+ASG01+SRV02	

表 7 SDP-4.3 —— 事故序列 2.5（TRANS）[illegible]

事故序列名称	每一安全功能完全可信的缓解能力：
主给水旁路供水（ARE）	主给水旁路有三条，根据成功准则要求，一个旁路向蒸汽发生器供水就满足要求。为了配合供水，还需要1台电动主给水泵或3台凝结水泵供水。
辅助给水供水（ASG01）	ASG系统有3列，两列电动泵，一列汽动泵。此功能事件的成功准则是一台泵供水即可。
充排操作（LMFW-H1）	操纵员实施一回路实施充排操作，启动安注和打开稳压器安全阀
高压安注直接注入（HPSI）	高压安注由2列构成，一列从换料水箱取水，并向一回路冷段注入。
稳压器安全阀组打开（SRV02）	由三组稳压器安全阀组，1组稳压器安全阀组打开即可。
高压安注冷段再循环（HPR01）	高压安注由2列构成，一列从地坑取水，并向一回路冷段注入。
安全壳喷淋再循环（EAS03）	安全壳喷淋系统有2列，一列运行成功即可。该功能主要是针对F8情况下的再循环，需要操纵员启动。根据PSA人因分析，有规程指导的启动失效概率为1.7E-3，与两列设备失效等量级。

编号	选择受影响的功能	基准分	每一受影响的重故序列的剩余缓解能力评价	结果
1	TRANS+ARE+ASG01+EAS03 3 + 3 + 4 + 3	13	TRANS+ARE+ASG01+EAS03	
2	TRANS+ARE+ASG01+HPR01 3 + 3 + 4 + 3	13	TRANS+ARE+ASG01+HPR01 1 + 3 + 4 + 3	11
3	TRANS+ARE+ASG01+HPSI 3 + 3 + 4 + 3	13	TRANS+ARE+ASG01+HPSI 1 + 3 + 4 + 3	11
4	TRANS+ARE+ASG01+LMFW-H1 3 + 3 + 4 + 3	13	TRANS+ARE+ASG01+LMFW-H1	
5	TRANS+ARE+ASG01+SRV02 3 + 3 + 4 + 3	13	TRANS+ARE+ASG01+SRV02	

风险重要度计算规则表

SDP计数规则工作表

步骤	操作指令/指示	得分
(1)	输入风险重要序列值等于9的个数。	17
(1)	第（1）步的结果除3，并把所得结果记入下一轮。	5
(1)	输入风险重要序列值等于8的个数。	3
(1)	第（3）步结果与第（2）步结果相加。	8
(1)	第（4）步的结果除3，并把所得结果记入下一轮。	2
(1)	输入风险重要序列值等于7的个数。	2
(1)	第（6）步结果与第（5）步结果相加。	4
(1)	第（7）步的结果除3，并把所得结果记入下一轮。	1
(1)	输入风险重要序列值等于6的个数。	0
(1)	第（9）步结果与第（8）步结果相加。	1
(1)	第（10）步的结果除3，并把所得结果记入下一轮。	
(1)	输入风险重要序列值等于5的个数。	
(1)	第（12）步结果与第（11）步结果相加。	
(1)	第（13）步的结果除3，并把所得结果记入下一轮。	
(1)	输入风险重要序列值等于4的个数。	
(1)	第（15）步结果与第（14）步结果相加。	

- 如果第16步结果大于0，则检查发现项的风险重要性是高安全重要度，用“红色”表征。
- 如果第13步结果大于0，则检查发现项的风险重要性至少是重要的安全重要度，用“黄色”表征。
- 如果第10步结果大于0，则检查发现项的风险重要性至少是中等安全重要度，用“白色”表征。
- 如果第10、13和16步结果都是0，则检查发现项的风险重要性是非常低的安全重要度，用“绿色”表征。

第二阶段评价结果：　绿色　√白色　黄色　红色

计算实例2

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

事件描述：2011年2月12日，运行二处当班值按照计划执行定期试验PT 3LHP 001（柴油发电机组低负荷运行性能试验），发现A列应急柴油发电机启动失败，记录柴油机不可运行的I0，多次重新启动，仍旧失败。 2月13日，经过机械检查，确认为A列空气分配器错位导致进气顺序错乱。调整到正确顺序后柴油机启动成功，消除I0。

3月10日，再次执行3LHP柴油发电机组低负荷试验时，柴油机两次均未成功启动，故障现象与之前空气分配器错位相似。厂家服务人员现场检查后,更换了带来的新的空气分配器并调整到正确顺序，柴油机启动成功。经过设备厂家和电厂的合作调查，最终确认该批次空气分配器产品在制造、安装环节存在缺陷。

WEBSITE http://www.chinansc.cn/

环境保护部核与辐射安全中心
Nuclear and Radiation Safety Center

谢谢！

WEBSITE http://www.chinansc.cn/