湖南省研究生暑期学校
核电站安全与人因工程系列课程（3）

核电站人因可靠性分析及应用

张　力 教授

南华大学人因研究所

2010年7月

目　录

一、概率安全评价（PSA）中的HRA

1、HRA在PSA中的作用与意义

1）概率安全评价（ PSA）

对来自系统运行各个水平上的损害和其他不期望后果进行辨识，并对相关事件作出定性定量分析、评价、预测的系统安全/风险评估方法。

2）在PSA研究与应用的早期阶段，设计与安全技术能力不如当今，大多数系统失效均与硬件失效相关，因而PSA关注的重点是硬件可靠性对系统安全的贡献。

3）近年来，人因失误已成为对系统安全性影响最大的因素之一：

人机系统：　　70%－90%

核电站:　　国际 55%－85%

国内 70%

系统风险注意焦点之一转向人因失误

4)HRA成为PSA的重要内容

国际原子能机构（IAEA）：

HRA为PSA不可或缺部分；

HRA水平为衡量PSA水平重要指标之一

5)HRA应用于人－机系统PSA也是目前HRA学科研究中心内容之一，是推动该学科发展的主要动力。

2、PSA对HRA的需求分析

为什么历史上几十种HRA方法多数不能在PSA中获得有效应用，甚至有相当数量的HRA方法因不适合PSA而被淘汰、致使夭折？关键是它们未能满足PSA对HRA的本质需求。那么，PSA对HRA的本质需求究竟是什么，应当通过什么途径来实现它。

1）概率安全评价（PSA）的主要功能

PSA是一种工程安全系统评价方法。它用基于事故场景的方法和思路分析研究对象系统，通过综合运用多种安全分析技术，结构化地、系统地鉴别出其可能的后果，计算出各种危险因素导致事故发生的概率，对可降低风险的各种方案进行比较。

2）PSA的基本分析方法

- 基本分析方法：

  找出可能导致事故的各种事件组合(称之为事故序列)，重点考虑初因事件、系统失效和人误等的组合，确定每一组合的发生频度，最后评估其后果 。

- 事故序列建模：事件树与故障树相结合：

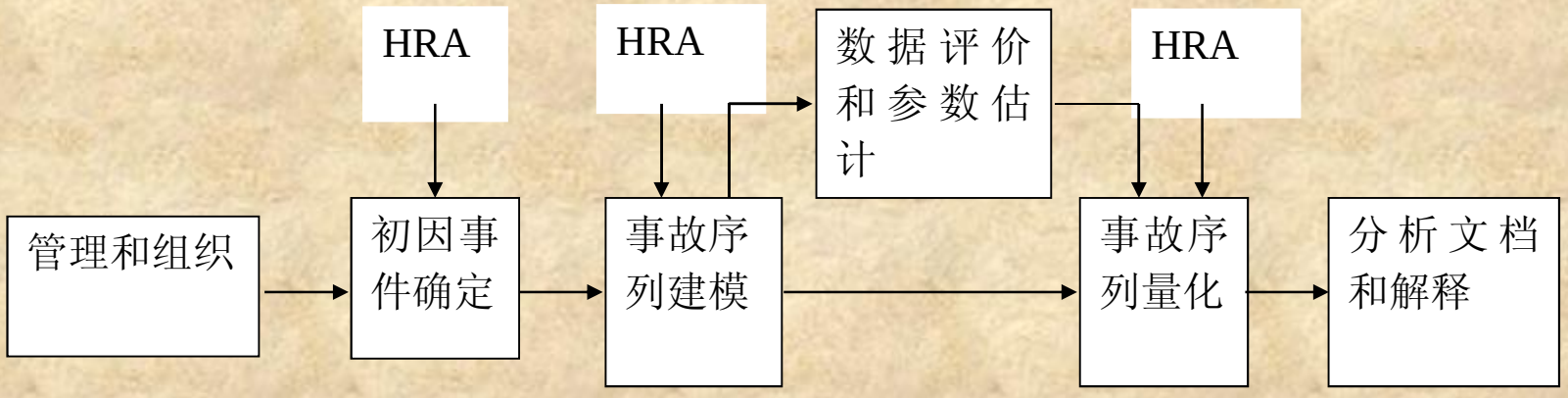
  事件树（ET）描述系统对事故初因事件的响应和事件序列演变过程，进而求得导致系统失效的定性结果（主要事故序列及最小割集组合）和定量结果（系统失效发生频率）；故障树(FT)描述该响应过程中系统的失效模型，进而确定系统失效原因和不可用度 。

3）PSA对HRA的基本需求：

- 在**PSA过程中，需要HRA在初因事件确定、事故序列建模、数据评价和参数估计、事故序列量化等步骤作出支持和贡献。**
  - 在初因事件确定过程，要求寻找和鉴别可能诱发初因事件发生的人员行为和有关因素，以较全面地确定系统潜在的事故源（事故起点）。
  - 在事故序列建模过程，需要分析与初因事件和此后的系统响应有关联的人员行为，包括发生在初因事件之前、之中和之后有关的人的因素，以有助于建立完整的系统事故模型和事故影响的后果模型，特别是系统中事故的传播途径。

- 在数据评价和参数估计方面，需要HRA提供专门技术和数据以支持人员行为的建模。
- 在事故序列量化中，需要对人员行为建模、给出定量分析并最终归并于PSA总体框架中。

pPSA主要程序工作分析：



要求寻找和鉴别可能诱发初因事件发生的人员行为和有关因素，以较全面地确定系统潜在的事故源。

需要分析与初因事件和此后的系统响应有关联的人员行为，包括发生在初因事件之前、之中和之后有关的人的因素，以有助于建立完整的系统事故模型和事故影响的后果模型，特别是系统中事故的传播途径。

4）PSA对HRA的本质需求

在对象系统的PSA模型、系统假设与边界的约束下系统化地辨识系统中潜在的人因事件并给出系统的、客观的定性定量分析与评价。

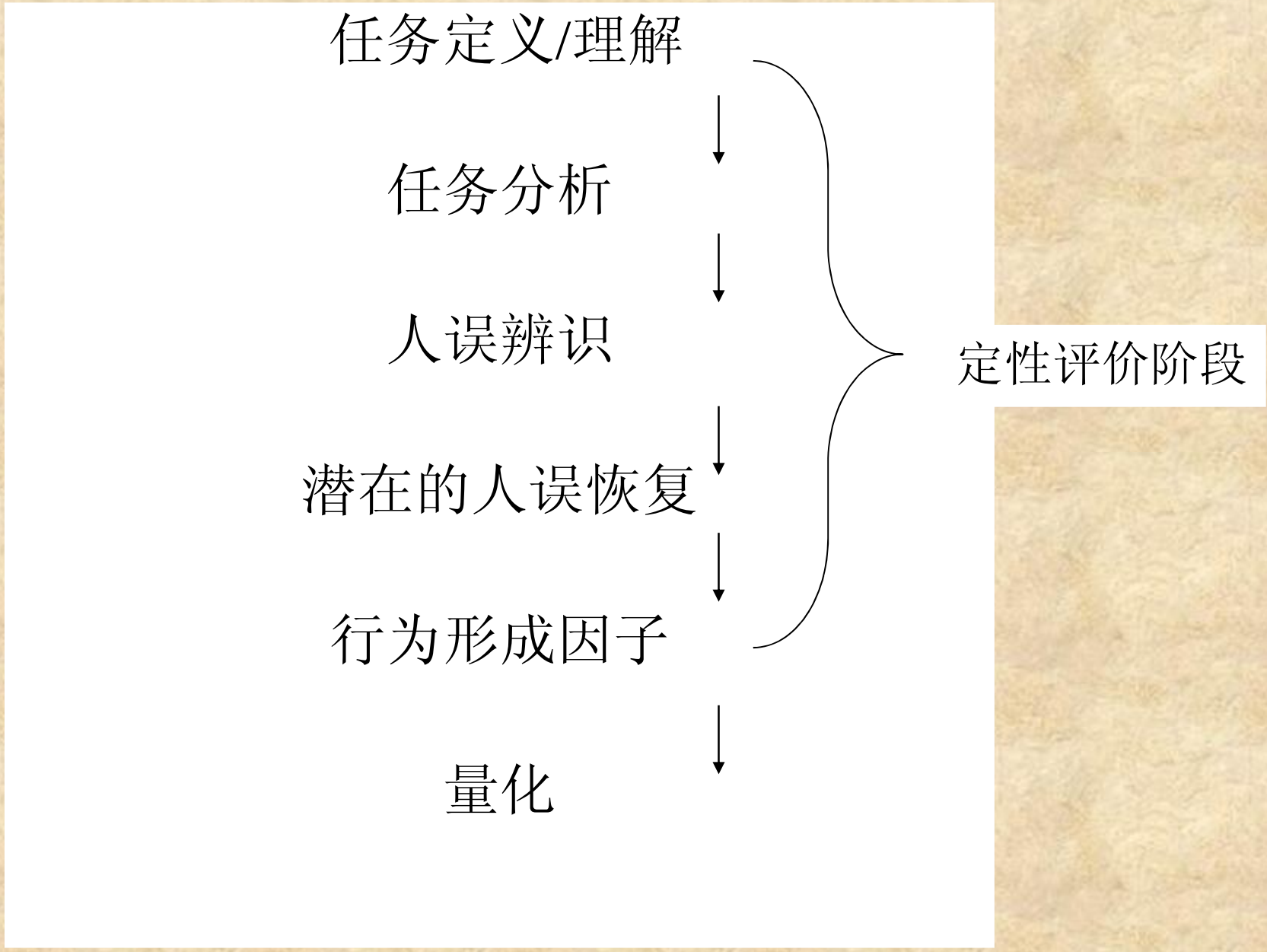
HRA的三个基本目标：

- 辨识什么失误可能发生
- 这些失误发生的概率
- 如何减少失误和/或减轻其影响

3、PSA/HRA人因事件分类(IAEA)

- A类：能导致设备或系统潜在不可用；维护、校验、测试
  事故前人因事件
- B类：由人的行为直接引发或再结合设备失效导致初因事件发生
  激发初因的人因事件
- C类：发生在初因事件之后，在事故处理过程中发生的人因失误事件；诊断、决策、操作事故后人因事件

4、 HRA基本框架



5、PSA中HRA过程范式

七项基本任务：

定义 ⟶ 筛选 ⟶ 定性分析 ⟶ 表征

⟶ 模型集成 ⟶ 量化 ⟶ 建立文件

定义：确保在研究范围内所有不同类型的相关人员行为，
筛选：
定性分析：
表征：
模型集成：描述怎样将重要的人员行为集成到PSA的系统模型中。
量化：
建立文件：

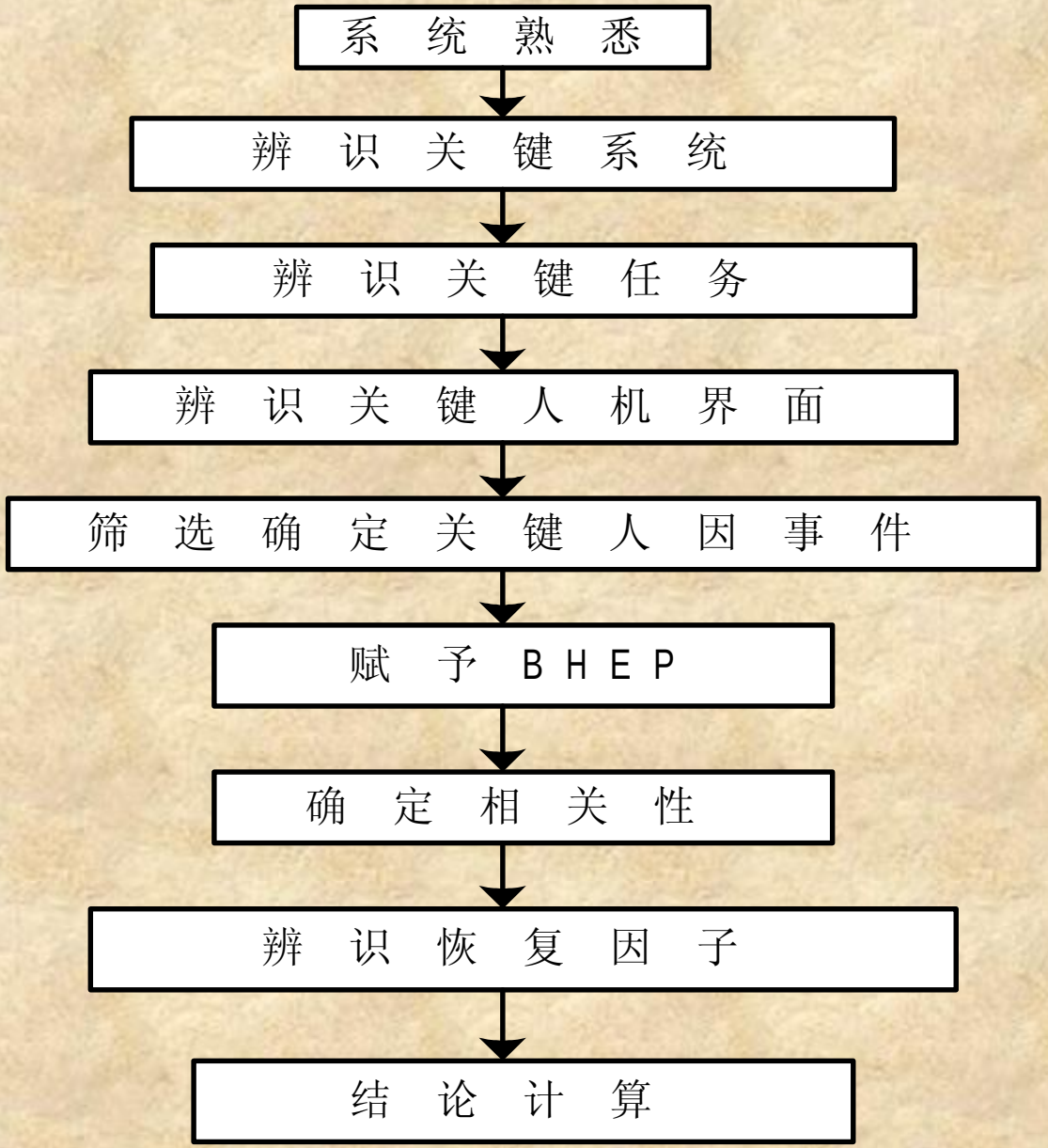
6、HRA 技术程序

- 程序的作用：
  - 规定技术的实施步骤和组织管理
  - 保证该技术的正确应用
- HRA技术程序：
  - 事故前HRA程序
  - 激发初因HRA程序
  - 事故后HRA程序

1）事故前HRA程序

- 事故前（A类）HRA主要分析系统正常运行时，在维护、校验、测试等系统安全相关的仪器、设备工作中，导致设备或系统处于潜在失效状态的人因失误，它们影响到安全系统需要投入运行时的可用性 。

pA类HRA基本程序


系 统 熟 悉
辨 识 关 键 系 统
辨 识 关 键 任 务
辨 识 关 键 人 机 界 面
筛 选 确 定 关 键 人 因 事 件
赋 予 BHEP
确 定 相 关 性
辨 识 恢 复 因 子
结 论 计 算

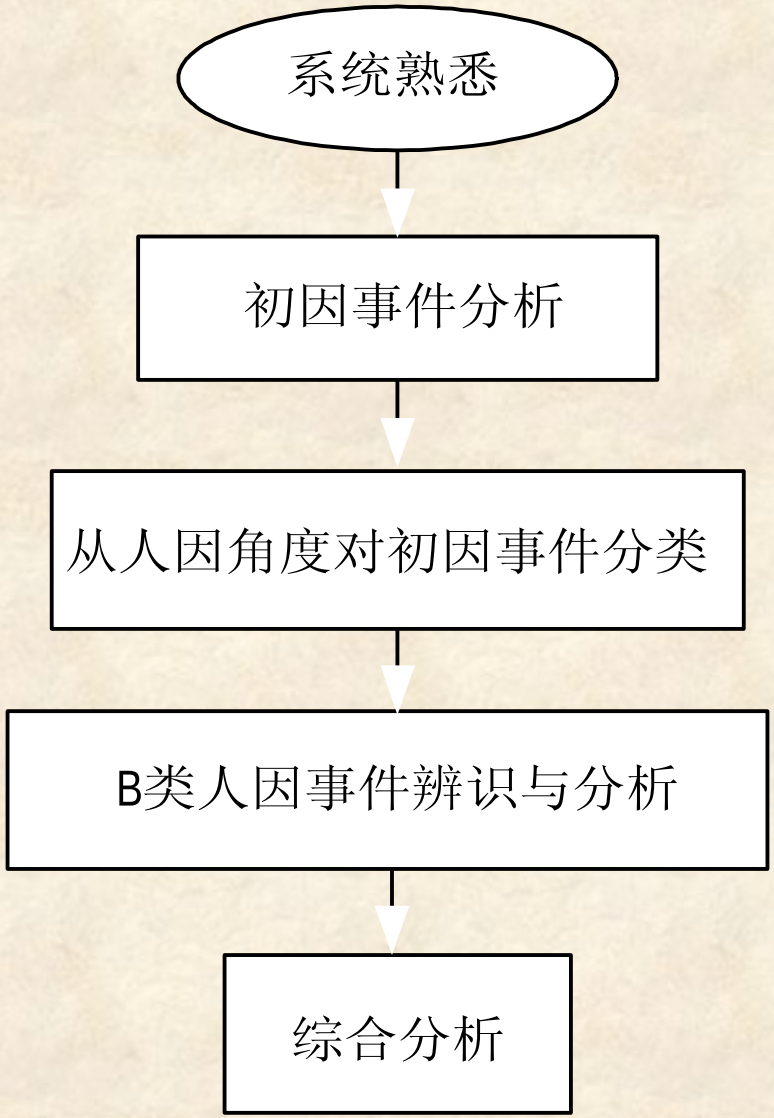
2）激发初因HRA程序

- **B类人因事件定义**
  人因事件本身或再合并设备失效导致事故初因事件；

- **两种主要表达形式**
  在运行、试验过程中由于人员错误操作而导致一个事故序列；
  试验、检修中人因造成设备潜在不可用，当需用该部分设备又未及时采取效措施而引发一个事故序列；

- **特征：兼有A类和C类人因事件特征；**

pB类人因事件分析程序



- B类人误分析应重点审查的工作：
  - 与启、停堆相关的运行和测试工作
  - 定期试验和维护工作以及重新校准备用系统
  - 特别注意激发初因事件后同时使相关的安全系统失效的事件
  - 在审查过程中，对操纵员，试验、检修人员的访谈是非常重要的

pB类人因事件辨识与分析

- 不包含人因事件贡献或可忽略人误影响的初因事件：可确定其中人因的贡献率为0
- 直接构成初因事件的人因事件：其对该初因事件的贡献率为100%，可利用THERP等传统人因分析方法考察该人因事件的发生概率

- 设备（子系统）失效构成的初因事件：
  - 以该初因事件为顶事件，建立该设备失效故障树分析其中人误的影响
  - 重点考察其中可能包含的人误事件及其对初因事件的贡献
- 综合分析：
  - 由于B类人因事件的多样性，采取了不同的分析方法，导致结果可能在水平上存在不一致
  - 敏感性分析，不确定性分析，综合分析

3）事故后HRA程序

- 事故后（C类）人因事件指系统在异常状态下，人与系统发生交互作用过程中的失误，主要是人的诊断、决策等认知行为和诊断后的具体操作行为，它的概率与时间密切相关，而且这类失误往往是难以纠正的错误（mistake）

- C类HRA的主要任务：分析、评价系统人员接受报警信号，感知某项异常事件发生后所采取的任务行为的失误概率

pC类人因事件分析的基本程序

- 基本情况调查： 技术系统、人员组织、管理系统
- 关键工作识别：任务分析 关键HIs ；
- 定性分析：确定重要人因事件序列；
- 定量筛选：确定需详细分析重要人因事件序列；
- 定量评价：人因事件失效概率；
- 综合评价：确认分析没有出现理解偏差，模型及结果合理可接受；

7、HRA规范化文档模式

- 事件背景
- 事件描述
- 事件成功准则
- 提问清单
- 调查、访谈结论
- 事件分析
- 建模与计算
- 系统假设与边界
- 调查访谈记录档案

二、核电站对HRA需求分析

（1）HRA的作用

- ü 辨识与评价人因失误
- ü支持PSA

（2）核电站HRA需求分析

- pHRA的三个基本目标：
- ü 辨识什么失误可能发生
- ü这些失误发生的概率
- ü如何减少失误和/或减轻其影响

（3）完整的HRA过程

- 任务分析：描述运行人员在事故过程中应当做什么；
- 失误分析：确定什么可能会出错；
- 表现形式：以一个逻辑的和量化的结构，确定人与其它硬件、软件和环境事件共同卷入的事件的后果影响；
- 量化：采用适当的模型推算失误的可能性；
- 失误减少：减少人误对风险的影响；
- 质量保证和资料编制：确保该评价是有效的，且能够作为将来设计/运行的一个信息资源。

三、 核电站人因可靠性分析模型

（1）人因失误率预测法（THERP）

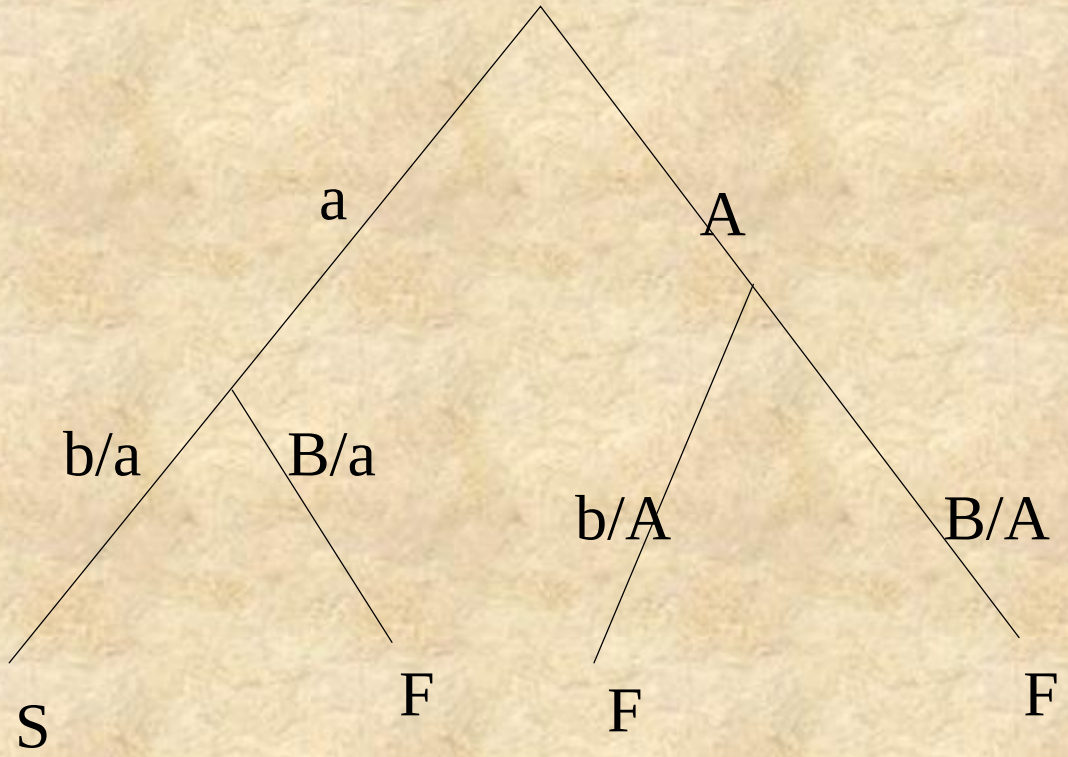


图1 简单的HRA事件树

- 人员作业成功概率:

  $Pr(S)=a' (b/a)$

- 失败概率:

  $Pr(F)=a'(B/a)+A'(b/A)+A'(B/A)$

p 行为形成因子（PSF）修正

$$\mathbf{HEP=BHEP\bullet(PSF)_1(PSF)_2\ \ldots}$$

相关修正

$$1.CD, P(B/A)=1$$

$$2.HD, P(B|A)=\frac{1+P(B)}{2}$$

$$3.MD, P(B|A)=\frac{1+6P(B)}{7}$$

$$4.LD, P(B|A)=\frac{1+19P(B)}{20}$$

$$5.ZD, P(B|A)=P(B)$$

（2）人的认知可靠性预测法（HCR）

1）HCR方法的两个假定

- 所有人员行为类型可分为三类：

  技能型、规则型、知识型；

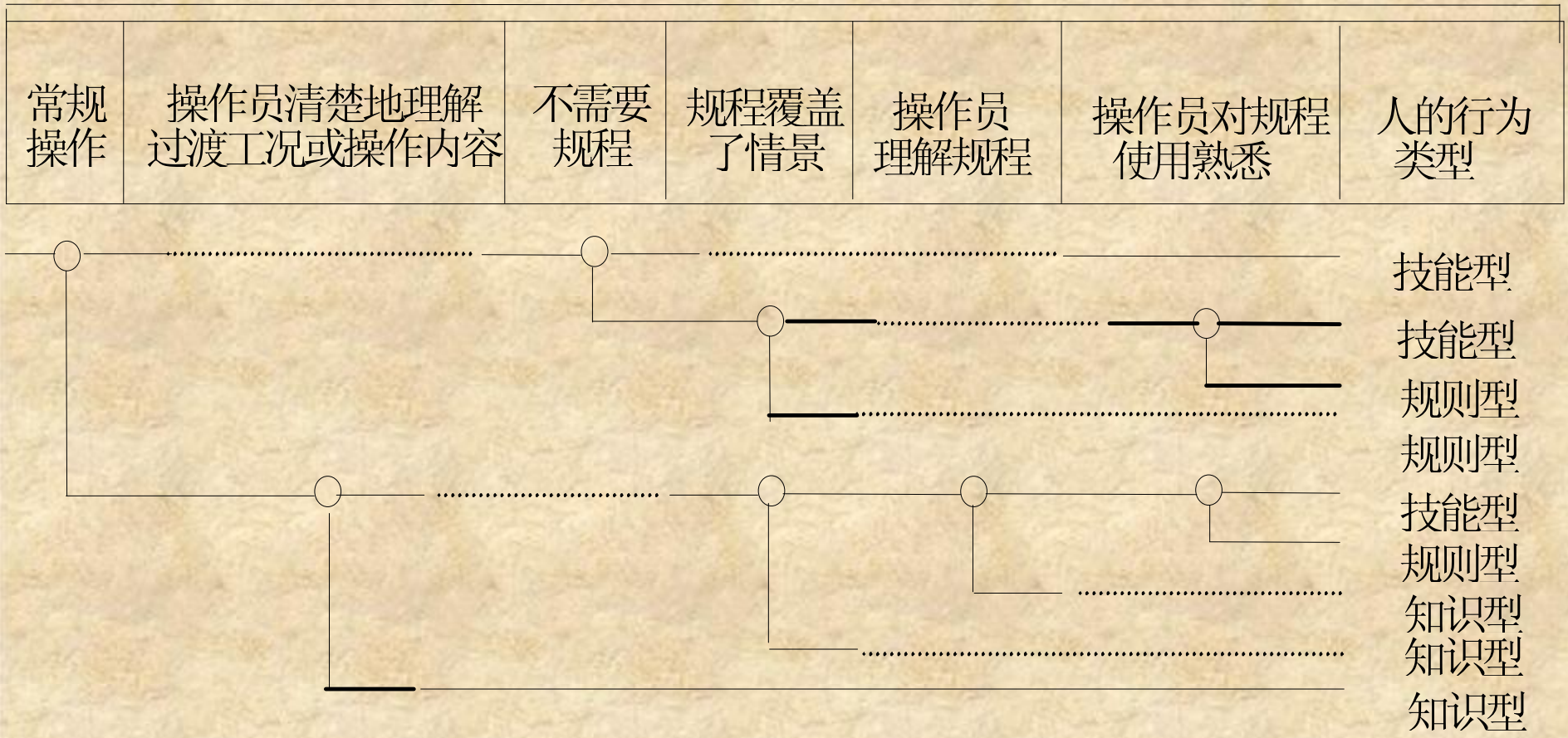


图2 HCR行为类型辨识树

p 每一行为类型的失误概率仅与允许时间t和执行时间$T_{1/2}$的比值有关，且遵从三参数的威布尔分布：

$$p = e^{-\left\{\frac{t/T_{1/2}-g}{a}\right\}^{b}}$$

$T_{1/2} = T_{1/2,n} \times (1+K1) \times (1+K2) \times (1+K3)$

t：允许操纵员进行响应的时间

$T_{1/2}$：操纵员执行时间 $T_{1/2,n}$：一般状况的执行时间

K1：操作经验； K2：心理压力；K3：人机界面；

a、b、g：操作人员行为类型参数

参数a、b、g选取表

行为类型	a	b	g
熟练（SKILL）	**0.407**	**1.2**	**0.7**
规则（RULE）	**0.601**	**0.9**	**0.6**
知识（KNOWLEDGE）	**0.791**	**0.8**	**0.5**

HCR模型的行为形成因子及其取值

操作员经验(K_1)	
1.专家，受过很好训练	-0.22
2.平均训练水平	0.00
3.新手，最小训练水平	0.44
心理压力(K_2)	
1.严重应激情景	0.44
2.潜在应激情景/高工作负荷	0.28
3.最佳应激情况/正常	0.00
4.低度应激/放松情况	0.28
人机界面（K_3）	
1.优秀	-0.22
2.良好	0.00
3.中等（一般）	0.44
4.较差	0.78
5.极差	0.92

（3）THERP+HCR模式

1）THERP、HCR各自解决问题的侧重点：

THERP: 与时间无关的序列动作；

HCR:　与时间密切相关的认知行为；

- 核电站人员的实际行为：认知判断+操作；
- 理想模式： THERP+HCR；

2）THERP＋HCR建模规则

pHRA事件树建模规则：

- ü对于实现同一功能且在同一功能分区的同类型操作行为，视为完全相关的操作。
- ü不考虑操作者对自身行为的恢复。
- ü考虑其他对操作者操作行为有监督作用的人员的恢复。
- ü根据操作界面的状况，考虑操作中有选错与做错两种可能。
- ü对于执行一系列多种类型的操作行为，根据电站条件假设取值。
- ü 对于规程中描述执行A操作，A失效，执行 B，B失效，执行C的动作序列， 仅考虑A 操作的失误，不考虑继续执行B、C操作的恢复。
- ü 一般状况下，不考虑操作人员忽略规程中某一项操作的概率。
- ü 操作失误概率数据主要来源于UREG/CR-1278。

p 相关性原则

一回路操纵员与二回路操纵员之间不考虑对对方操作或指令的监督作用，只考虑值长对两名操纵员操作的监督作用。且操纵员与值长之间的相关度为低。在副值长进行操作时，操纵员与副值长之间的相关度为高。事故后现场技术员也将按操纵员的指令参与有关操作，操纵员与现场技术员之间的相关度为中等。

安全工程师在使用SPI规程期间不对主控室各人员的具体的操作行为有监督作用，而只是按规程对安全参数进行监测。但在RRA连接状态下或无相应规程使用的情况下，则认为安全工程师对主控室内重要的操作有监督作用，且相关度为高。

p 名义HEP修正原则：

ü 在全厂断电、ATWT和执行U规程后所进行的操作失误概率，取其名义值的5倍。

ü 其它事故状况下取名义值的2倍。

ü 通过模拟盘的信号灯、降温速率、阀门开度指示装置、流量显示等多种途径，监督人员可对操作人员的行为进行有效监督，并据此发现操作人员的失误。由于获取该信息的途径较多，因此，监督人员未发现操作人员的操作失误的概率可依据NUREG/CR-1278 取定为3×10^{-3}。

p人员行为类型判断规则：

一般情况依据图2判断，但进入了事故规程或报警后的诊断行为，从保守角度考虑均视为规则型行为。ATWT等情况下无相应规程可用，需要根据个人的经验、知识进行诊断，视为知识型行为。

p事件处理中时间划分规则：

事件处理中允许操纵员响应的时间分为：

ü事件发生到引发可引导操纵员进入该事件处理规程（DEC、A0）或报警卡的报警信号的时间。

ü操纵员利用事故规程进行一系列的诊断，直至作出具体操作行为的诊断时间。

ü有关人员（操纵员、副值长或现场技术员） 完成事件成功准则所要求的操作的执行时间。

p对模型中有关修正因子的确定：

ü安全工程师的诊断行为：

K_1=0（平均培训水平）

K_2=0.44（需进入SPU/U规程，有极高的心理压力）

或K_2＝0.28（执行SPI规程，但不需进入SPU/U规程，有较高的心理压力）

K_3=0（人机界面良好）

ü其他人员：

操作经验：平均培训水平，$K_1=0$

心理应激水平：A工况、全厂断电、ATWT事件状况下，$K_2=0.44$；

其它事故状况，$K_2=0.28$

人机界面：良好，$K_3=0$

3）人因事件分析模式和技术

工程应用的需求：

- 可操作性
- 资料完备性
- 可追溯性

- 事件背景：

刻划事件发生前后系统的状态和为保证系统功能而要求操纵员执行的相应动作以及事件后果。

- 事件描述：

当值人员根据规程对与事故相关的关键系统或设备的状态进行判断以及进行的相应的操作行为和事故演进及处理过程。

- 事件成功准则

为确保事件成功所进行的关键性操作

p 提问清单及调查与访谈记录表

根据对事故进程的理解，列出需要了解或确认的问题，主要包括操纵员、安全工程师对事件进程的理解，运行人员所用规程及规程的易用性，事件进程中所需的操作步骤、条件及关系，操作现场的人-机-环境系统状况，人员间相关性及操作步骤间的相关性，事故可能造成的后果及运行人员对其严重程度的理解（心理压力），允许时间、实际诊断时间、操作时间、一般执行时间等。

- 调查、访谈结论：

  事件的进程、任务分析、人员每一动作的意义、动作目的、成功准则、系统人-机接口的状况、系统状态、运行人员的心理状况以及THERP和HCR模式所需的各类信息和数据

- 事件分析：
  - ü 事件过程分析：根据事件进程将事件划分为几个阶段；
  - ü建模分析：对每一阶段的人员行为进行初步分析，决定采用何种模式计算其失误概率。
- 建模与计算：

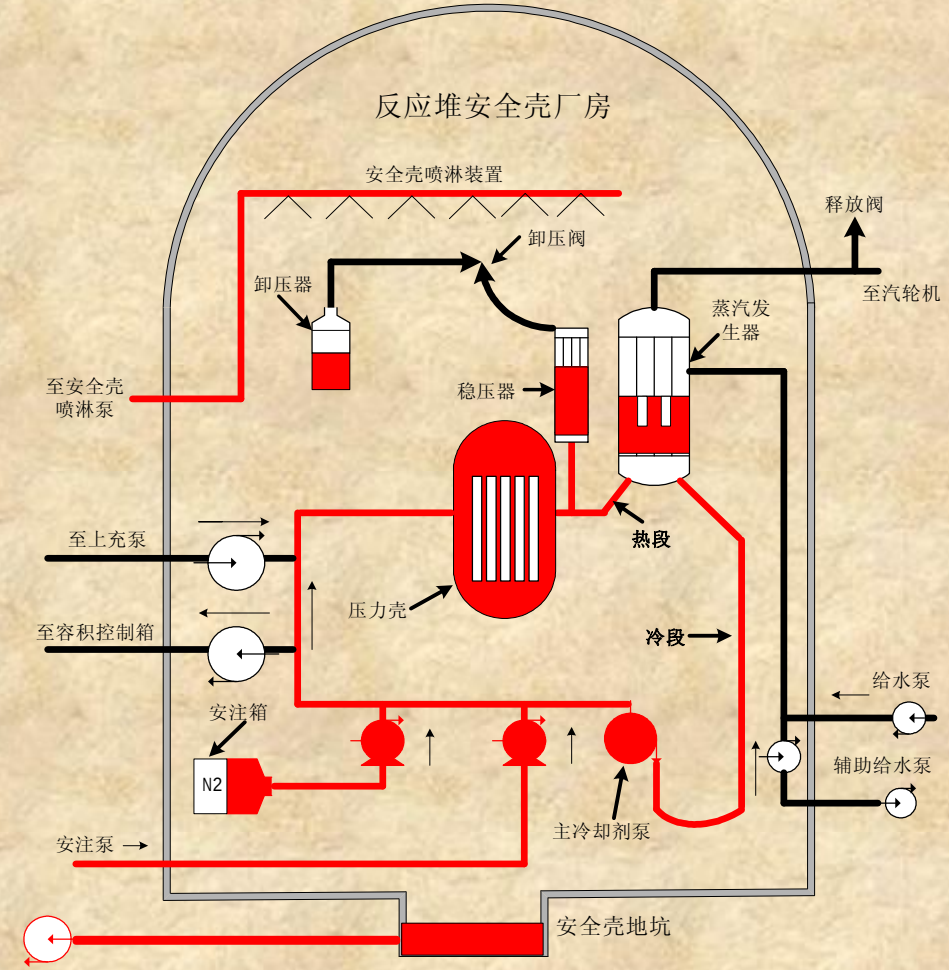
  建模分析 ⟶ 定量分析模型 ⟶ 数学计算

四、HRA在核电站人因失误分析应用实例

（1）系统情况及有关假设

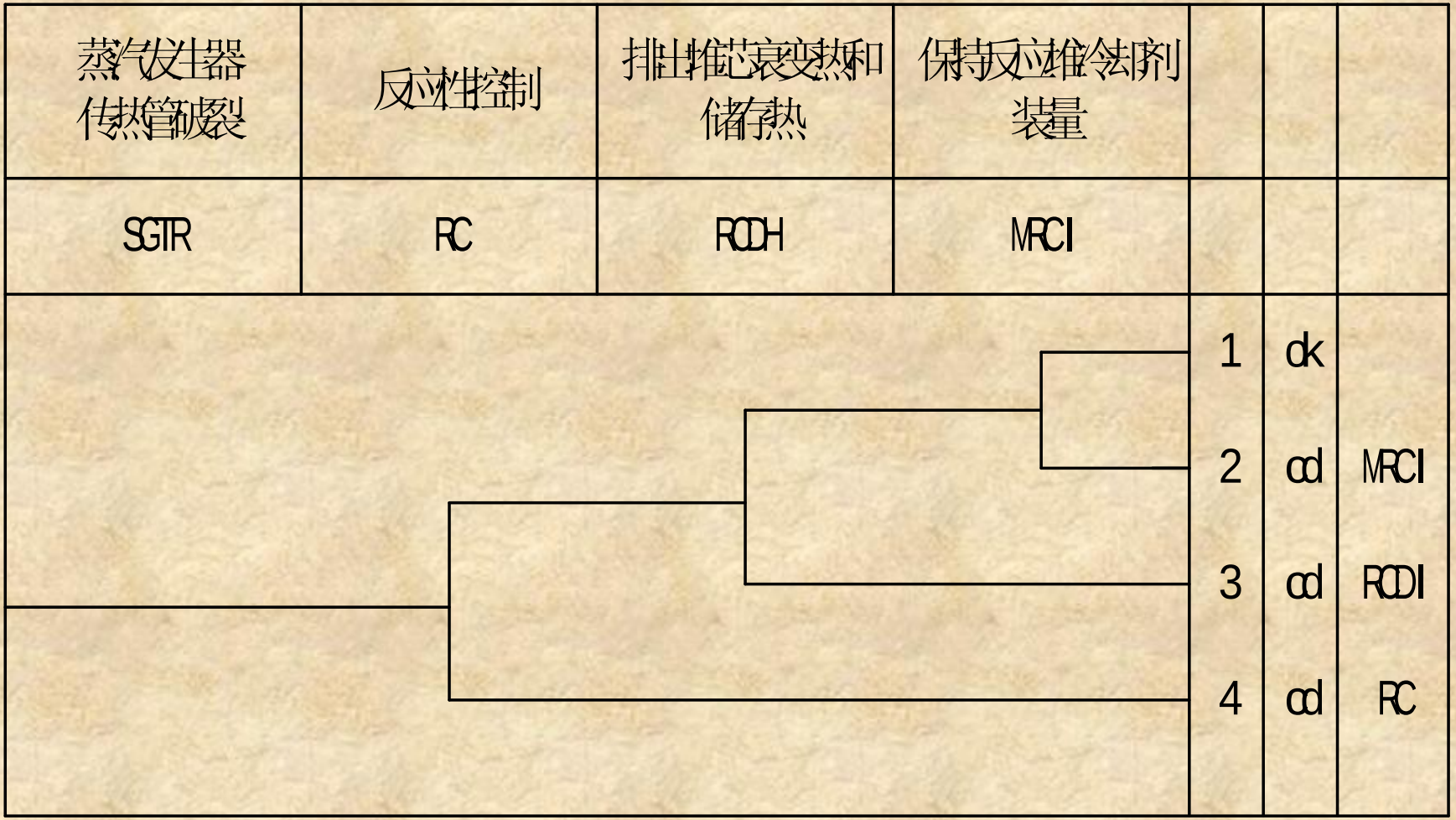
对电站人员配备情况、人员之间的工作关系和紧张情况、规程使用情况等作出统一约定和假设。另外，基于热工水力计算，需给出各事件的有关时间参数。

（2）实例1：SGTR（蒸汽发生器传热管破裂）



核电厂一回路和二回路系统示意图

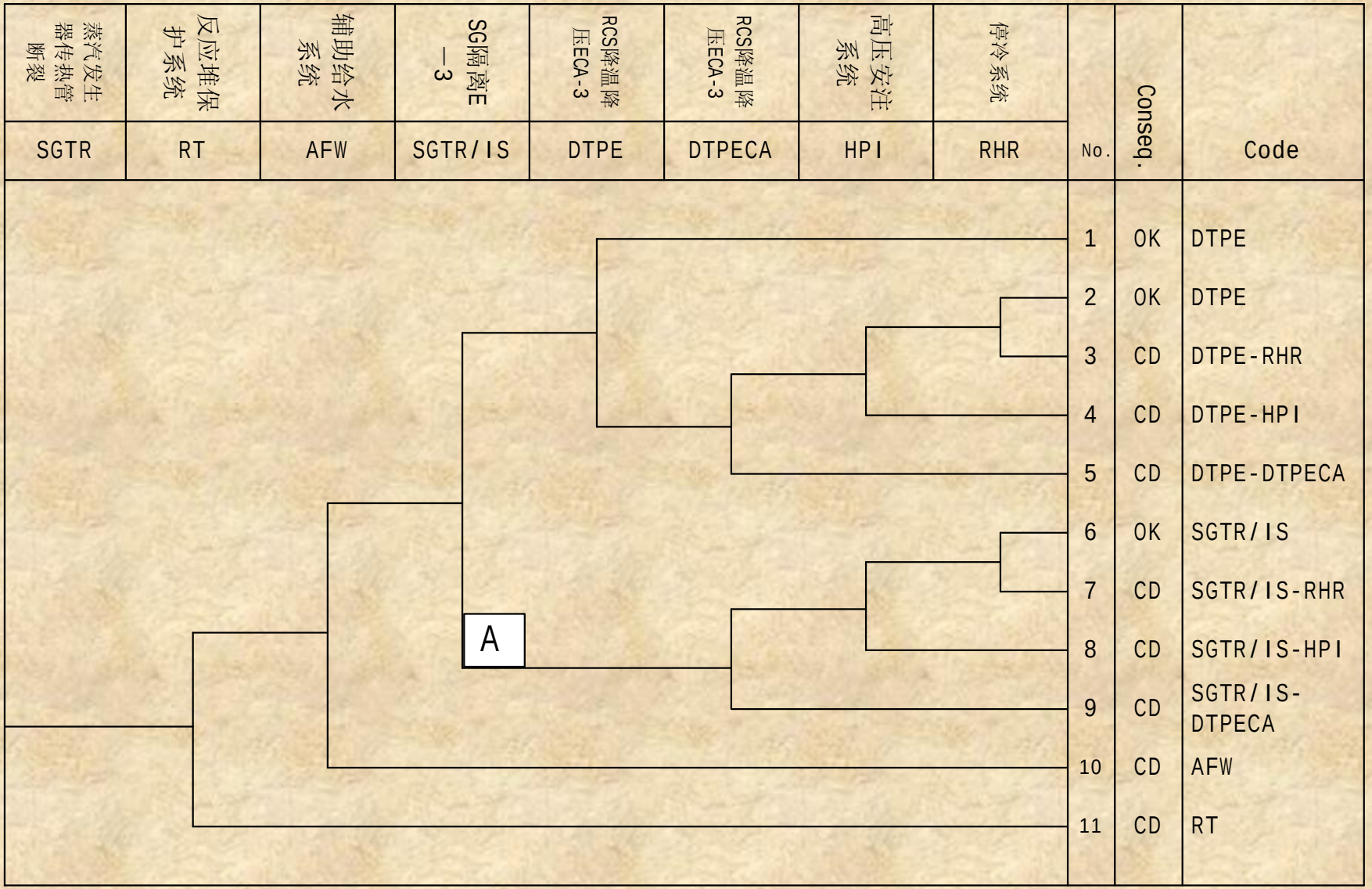
1）事故序列建模：事件树建模与故障树建模



SGTR功能事件树

p 事件树分析

- 电厂响应分析
- 操纵员响应分析
- 事件树题头
- 事件树的展开
- 事件序列： 11个



SGTR事故序列事件树

p 系统故障树分析

SGTR 人因事件在PSA模型中基本位置

2）SGTR人因事件分析

- **SGTR人因事件：**

  蒸汽发生器传热管破裂（SGTR）后，操纵员未能在20分钟内隔离破管蒸汽发生器。

- 事件背景
- 事件描述：

  蒸汽发生器传热管破裂→进入E-0规程执行至23步，蒸汽发生器抽气器排汽放射性N-16高报或蒸汽发生器排污水放射性高报→执行E-3规程至第3步识别破管的蒸汽发生器→关闭破管蒸汽发生器主蒸汽隔离阀隔离破管蒸汽发生器。

- 事件成功准则：

  在20分钟内，操纵员调整蒸汽发生器的大气释放阀开启定值至7.0Mpa,关闭破管蒸汽发生器主蒸汽隔离阀和主给水阀。

3）调查与访谈结论

- 根据热工水力学计算，蒸汽发生器传热管断裂，操纵员在分钟内隔离破管蒸汽发生器；
- 根据系统假设，SGTR引发报警信号的时间T_0为0分钟；
- 根据访谈，完成从进入E_0规程至执行到E_{-3}规程隔离破管蒸汽发生器一般执行时间为4分钟；
- 隔离破管蒸汽发生器的操作包括：
  - ü 调整破管蒸汽发生器的大气释放阀开启设定值至7.0Mpa
  - ü 关闭破管蒸汽发生器的主蒸汽隔离阀及其旁路阀；
  - ü 关闭破管蒸汽发生器的主给水阀（隔离破管蒸汽发生器的给水）

- 隔离破管蒸汽发生器的一般操作时间Ta为2分钟
- 根据系统边界条件和假设，操纵员在此事故处理过程总的人员行为为规则型行为；
- 根据系统假设，操纵员均经过一般水平的培训；
- 根据调查访谈，在此事故状况下，操纵员的心理压力较高；
- 根据系统假设，系统人－机界面状况为一般；
- 反应堆操作员负责隔离破管蒸汽发生器的操作行为，值长对其操作行为的正确性负监督职责，其相关度为中。

4）事件分析

事件分为三个主要阶段：

- 操纵员发现N_{-16}报警信号进入E_{-0}规程（觉察阶段）
- 操纵员由E_0规程进入执行至E_{-3}规程作出需隔离破管SG的诊断（诊断阶段）
- 操纵员按规程指引，隔离破管SG（操作阶段）

5）建模分析

SGTR人因事件属于C类人误行为。响应行动序列失误概率

$$P = P_1 + P_2 + P_3 = p_1 + (1 - p_1)p_2 + (1 - p_1)(1 - p_2)p_3$$

- **根据操纵员培训及事故所触发的报警信号的重要性、明显性，p_1可认为非常小。**
- **操纵员进入E_0规程后，操纵员依次按E_0规程至E_{-3}规程进行操作。根据调查访谈结论，人的行为类别为规则型，其失误概率p_2可用HCR模型计算。**
- **操纵员隔离破管SG，p_3根据HRA人因事件树进行计算**

6）建模与计算

- 察觉失误概率 $p_1 = 1 \times 10^{-4}$

- 诊断失误概率

$$p_2 = e^{-\left\{\frac{\mathrm{Td} / T_{1/2} - g}{h}\right\}^b}$$

T1/2，n = 4s，Ta = 2s，

$$T_d = T_c - T_0 - T_a \times (1 + 0.28) = 20 - 0 - 2 \times 1.28 = 17.44$$

K1=0， K2=0.28，K3=0.44

$$T_{1/2} = T_{1/2,n} \times (1 + K1) \times (1 + K2) \times (1 + K3) = 7.37$$

η=0.601,β=0.9,γ=0.6 (调查访谈结论6)

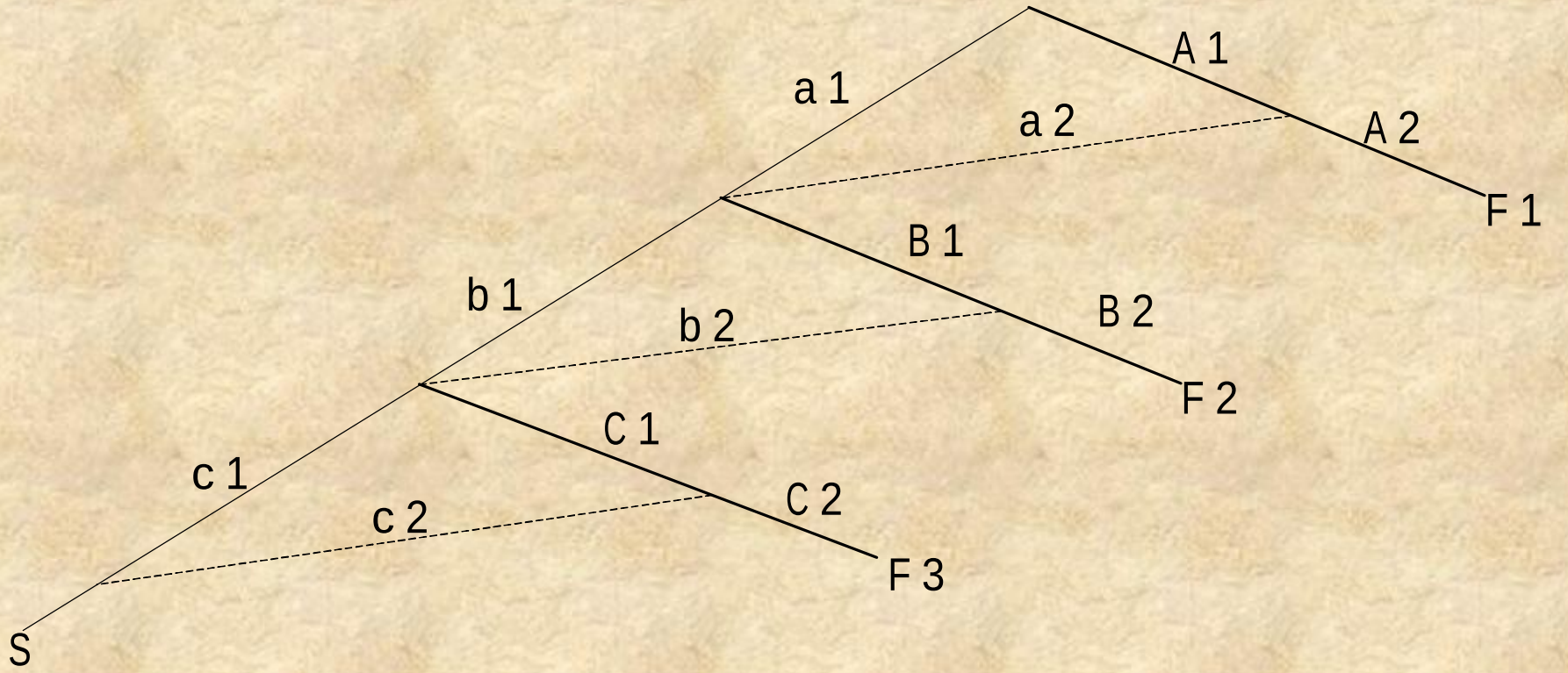
p_2 = 7.140×10^{-2}

7）操作失误概率

操纵员隔离破管SG，需要完成三个重要的序列动作：

- ü 调整大气释放阀至定值7.0Mpa；
- ü 关闭破管SG主蒸汽隔离阀；
- ü 关闭破管SG主给水阀；

操纵员隔离破管蒸汽发生器HRA事件树



$$p_3 = F1 + F2 + F3 = 1.166\times10^{-3} + 4.270\times10^{-4} + 4.268\times10^{-4}$$
$$= 2.020\times10^{-3}$$

- **SGTR整体人因事件失误率为**

$$P = P_1 + P_2 + P_3 = p_1 + (1-p_1)p_2 + (1-p_1)(1-p_2)p_3$$
$$= 1\times10^{-4} + (1-1\times10^{-4})\times7.140\times10^{-2} + (1-1\times10^{-4})(1-7.140\times10^{-2})\times2.020\times10^{-3}$$
$$= 7.347\times10^{-2}$$

（3）HRA 实例2： RRA中破口事件

- 事件名称：

RRA中破口，操纵员未及时投入低压安注且打开GCTa阀。

- 事件背景：

C工况下，RRA系统出现中破口，引起一回路压力下降，安全壳压力因破口漏流而上升，稳压器低水位LOW3或安全壳高压HI-2报警引导操纵员进入A10规程。在A10规程里，要求操纵员在19分钟内完成启动安注以恢复一回路水量，并打开所有可用蒸汽发生器的GCTatm阀。若操作员未成功完成该任务，且值长及STA又未及时纠正，则将导致堆熔。

p 事件描述：

C工况，RRA系统中破口 ——→放射性活度高报警 —→引导操纵员进入DEC规程 —→安全壳高压HI-2信号报警或稳压器低水位LOW3报警 —→操纵员进入A10规程 —→一回路操纵员手动启动RPA058TO、RPB058TO两列低压安注并通知二回路操纵员开启GCT131、132、133VV阀。

p 事件成功准则：

在事故发生19分钟内成功启RPA058TO、RPB058TO两列安注并将蒸汽发生器通大气阀GCT131、132、133VV开至全开。

- 调查与访谈结论
  - ü根据热工水力学计算，操纵员需在T_1=19分钟内完成手动启动两列安注并开启三个GCT阀。
  - ü根据电站基本情况及假设，操纵员经过平均水平训练（有执照且有6个月操作经验）。
  - ü根据电站基本情况及假设，操纵员在C工况下有一定的心理压力，其修正因子取0.28。
  - ü根据热工水力学计算，由事故发生到引发放射性活度高HI_{-2}级报警的时间T_2为1分钟。

ü 根据电站基本情况及假设，操纵员执行DEC规程的时间T_3为4分钟。

ü由于操纵员进入A_{10}规程后所采取的第一个行为就是根据安全壳压力高信号作出投入安注并开启GCTatm阀的诊断，操纵员在A10规程中的执行时间很短，可忽略。

ü一回路操纵员完成手动启动两列安注动作的操作时间为T_4为1分钟，二回路操纵员完成GCTatm阀门的开启时间T_5为1分钟。

ü一回路操纵员与二回路操纵员同时进行各自的操作行为，故事故处理中总操作时间以1分钟计算。

p 事件分析：

1）该事件可分为三个阶段：

ü 操纵员由放射性活度高HI_{-2}级报警进入DEC规程诊断。

ü操纵员由DEC规程引导进入A_{10}规程，并作出手动启动两列安注与开启所有GCT阀的判断。

ü操纵员手动启动两列安注并将GCT阀开至全开。

2）建模分析：

- ü根据报警信号特征及操纵员均经过良好的培训，在此认为操纵员未发现DEC报警并进入DEC规程的概率P_1非常小；
- ü操纵员在执行DEC、A_{10}规程的判断与操作均为基于操作规程的行为，可以用HCR模式计算其失误概率P_2；
- ü一回路操纵员按操作规程开启手动安注按钮的同时，二回路操纵员开启三个GCT阀，其操作行为属于典型的序列操作,其操作失败概率P_3可用THERP方法求出。

3）建模与计算

- 事件失误率$P=P_1+P_2+P_3$
- 根据事件分析中2.1），根据电站基本情况及假定得：

$$P_1=1.00\times10^{-4}$$

$$p = e^{-\left\{\frac{t/T_{1/2}-g}{a}\right\}^{b}}$$

式中,

允许操作员进行诊断的时间

$t=T_1-T_2-T_5'（1+0.28）=19-1-1'1.28=16.72min$

平均诊断时间$T_{1/2,n}=T_3=4min$

$K_1=0$ （平均训练水平）

$K_2=0.28$ （调查访谈结论3）

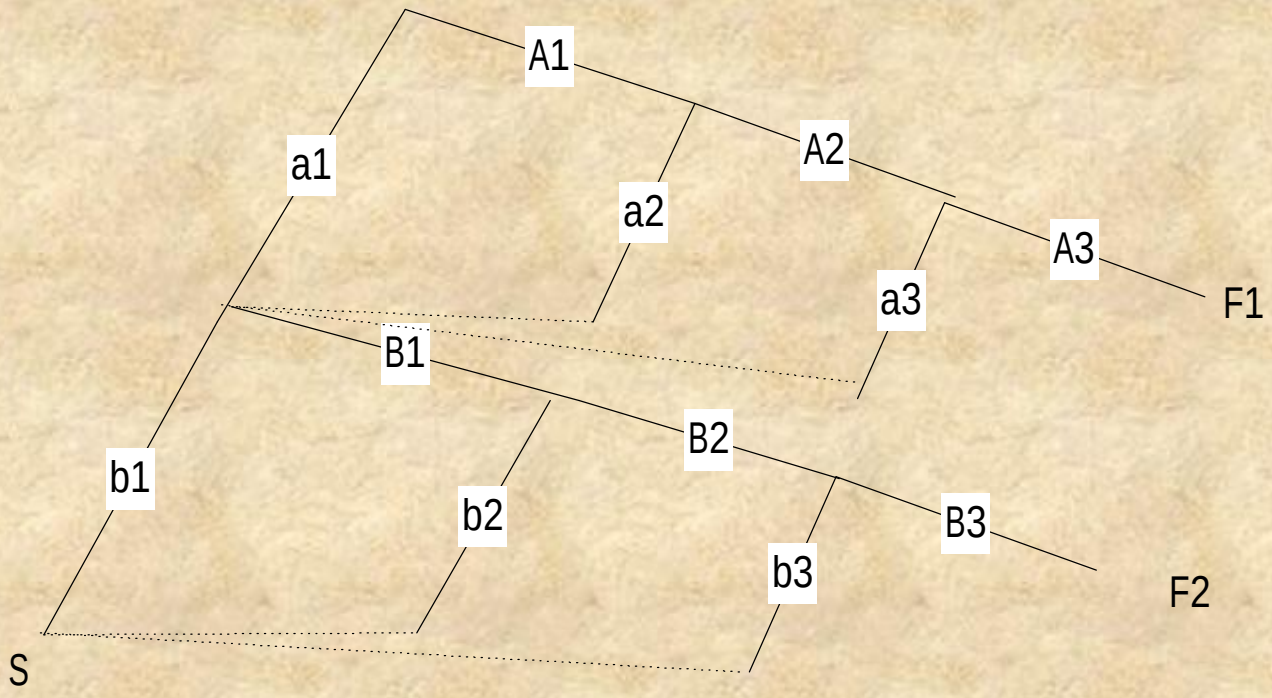
$K_3=0$ （人机界面良好）

$T_{1/2}=T_{1/2,n}'(1+K_1)'(1+K_2)'(1+K_3)=5.12min$

$\alpha=0.601,\beta=0.9,\gamma=0.6$ (规则型)

代入(1)式,得$P_2=2.19'10^{-2}$

ü操纵员启动低压安注和开启GCTatm，其HRA事件树如下图：



其中：

a_1 —操纵员成功完成安注

A_1—操纵员未成功完成安注

b_1—操纵员成功完成GCTa打开

B_1—操纵员未成功完成GCTa打开

a_2—值长成功纠正操纵员的错误完成安注

A_2—值长未成功纠正操纵员的错误并完成安注

b_2—值长成功纠正操纵员的错误并完成GCTa打开

B_2—值长未成功纠正操纵员的错误完成GCTa打开

a_3—安全工程师成功纠正值长失误完成安注

A_3—安全工程师未成功纠正值长失误完成安注

b_3—安全工程师成功纠正值长失误完成GCTa打开

B_3—安全工程师未成功纠正值长失误完成GCTa打开

依据THERP计算公式和基本数据、修正因子及相关性分析等，计算得到：

$A_1=1.2\times10^{-3}$，$A_2=5.57\times10^{-2}$，$A_3=5.03\times10^{-1}$

$B_1=6.0\times10^{-3}$，$B_2=5.57\times10^{-2}$，$B_3=5.03\times10^{-1}$

该事件树的主要失败路径有两条F_1、F_2，它们的失效概率分别为：

$$P_{F1}=P_{A1}\times P_{A2}\times P_{A3}$$
$$=1.2\times10^{-3}\times5.57\times10^{-2}\times5.03\times10^{-1}$$
$$\approx3.37\times10^{-5}$$

$$P_{F2}=P_{a1}\times P_{B1}\times P_{B2}\times P_{B3}=(1-P_{A1})\times P_{B1}\times P_{B2}\times P_{B3}$$
$$=9.998\times10^{-1}\times5.57\times10^{-2}\times5.03\times10^{-1}$$
$$\approx1.69\times10^{-4}$$

总的操作失误率

$$P_3 = P_{F1} + P_{F2}$$

$$= 3.37 \times 10^{-5} + 1.69 \times 10^{-4}$$

$$= 2.02 \times 10^{-4}$$

事件总的失误率

$$P = P_1 + P_2 + P_3$$

$$= 1 \times 10^{-4} + 2.19 \times 10^{-2} + 2.02 \times 10^{-4}$$

$$= 2.22 \times 10^{-2}$$

（４）思考：

- 模型间的接口问题；
- 紧张因子（心理压力因子）选择问题；
- 人因分析资料的可用性问题。

谢谢各位！

请大家提问！