数字化人机界面人因可靠性分析方法研究与应用

贾 明,刘燕子,张建波
(深圳中广核工程设计有限公司,广东 深圳 518045)

摘要:为了将人因工程方面有关人的能力和限制的知识应用到人机界面的设计,从而使控制室系统设计达到人-机-环境的最佳匹配,本文研究通过人因可靠性分析方法,结合人因工程设计过程,建立一种适于工程应用的综合性分析方法来识别人机界面中影响人员绩效和容易诱发人因失误的潜在设计缺陷,并采用系统化的方法来优化人机界面设计。结果表明,本文建立的方法具有可操作性强、评价客观等优点,可有效提高核电厂安全性、可靠性和经济性。该方法现已成功应用于在建的CPR1000各项目,具有广阔的应用空间。

关键词:人因可靠性分析;人机界面;人因工程
中图分类号:TM623 **文献标志码**:A **文章编号**:1000-6931(2014)S1-1023-08
doi:10.7538/yzk.2014.48.S1.1023

Study and Application of Human Reliability Analysis for Digital Human-system Interface

JIA Ming, LIU Yan-zi, ZHANG Jian-bo
(*Shenzhen China Nuclear Power Design Co., Ltd., Shenzhen* 518045, *China*)

Abstract: The knowledge of human-orientated abilities and limitations could be used to digital human-system interface (HSI) design by human reliability analysis (HRA) technology. Further, control room system design could achieve the perfect match of man-machine-environment. This research was conducted to establish an integrated HRA method. This method identified HSI potential design flaws which may affect human performance and cause human error. Then a systematic approach was adopted to optimize HSI. It turns out that this method is practical and objective, and effectively improves the safety, reliability and economy of nuclear power plant. This method was applied to CRP1000 projects under construction successfully with great potential.

Key words: human reliability analysis; human-system interface; human factors engineering

控制室是操纵员对机组进行监视和控制的主要场所。控制室的设计直接关系到核电厂的安全、可靠、经济地运行。在以数字化仪控系统为主的核电厂控制室内,人机界面与常规控制

收稿日期:2014-06-30;**修回日期**:2014-09-09
作者简介:贾 明(1983—),男,陕西咸阳人,工程师,硕士,人机与环境工程专业

室相比发生了根本性的变化。相对于常规控制室,数字化控制室信息资源更丰富,信息和操作界面更集中,对操纵员支持帮助手段的开发潜力也更大。当这些大量信息和控制资源在有限显示屏幕上提供给操纵员时,如果人机界面设计不合理,电厂就存在着人因风险。

人因可靠性分析(HRA)技术可将目前已有的人因工程方面有关人的能力和限制的知识应用到人机界面的设计,保证其与整个电厂、系统或设备的运行需求、人员操作任务和工作环境高度协调,从而使控制室设计达到人-机-环境的最佳匹配。

目前对于数字化人机界面的人因可靠性分析和评价缺乏一种综合性的、较为客观的方法,且可靠性分析工作和评价工作并未有效地结合起来。对于人机界面人因可靠性分析工作,现有的多种方法各有利弊,有些方法操作起来较复杂。对于人机界面的评价工作则更是缺乏有效的方法,对人机界面评价的理论、方法尚处于探讨之中。

针对上述情况,通过对人因可靠性分析方法的研究,并结合核电厂数字化控制室的特点及数字化人机界面人因工程设计过程,建立一种适于工程应用的、综合性的分析方法来识别人机界面中影响人员绩效和容易诱发人因失误的潜在设计缺陷,并进一步采用系统化的方法来优化人机接口设计。

1 方法概述

本研究建立了一种综合性人因可靠性分析和评价方法,其分析过程以核电厂事件或事故场景为基础,以各种事件或事故的处理流程为分析单元,针对不同事故的处理过程,分析主控室操纵员执行任务时使用的人机界面的人因可靠性。

在核电厂这样的复杂系统中,对所有风险场景进行一一分析需消耗大量的精力,因此需采用一种筛选原则(如大于某个概率)来选取风险较大的风险场景进行详细分析(采用HCR法[1])。然后针对风险大的场景采用人因失误分析方法(人因可靠性分析方法)进行分析,并识别出可能产生的人因失误,定量计算人因失误发生的概率,识别出需重点考虑的人因失误(采用CREAM法[2])。最后识别出可能诱发人因失误的人机界面或情境环境缺陷(采用HEC法[3]),再根据HEC法识别结果对设计缺陷进行修改优化(采用动态验证法和评审法)。

因此,本研究综合考虑了现有的多种人机界面人因可靠性分析方法和评价方法,选定了HCR+CREAM+HEC三种方法相结合的综合性人因可靠性分析和评价方法。整个分析和评价工作流程如图1所示。

2 应用实例

2.1 基于HCR法的概率风险评价

利用HCR法进行风险场景筛选,从备选的多个核电厂事件或事故场景中筛选出风险较大的进行分析。经过筛选,在众多备选场景中,“误安注”场景的人员不响应失误概率最高,达到了0.44。下面详述计算过程。

采用HCR法构建操纵员的响应失误概率模型$P(t)$:

$$P(t)=\exp\left(-\left(\frac{t/T_{1/2}-\gamma}{\alpha}\right)^{\beta}\right) \quad (1)$$

式中:t为完成任务的可用时间;$T_{1/2}$为操纵员完成任务的中值响应时间;α为尺度参数;β为形状参数;γ为位置参数;$P(t)$为人员的不响应概率。

由于每个运行班组的执行时间可能因各类情况而有所不同,故在使用公式之前需进行修正。在HCR模型中所考虑的关键行为修正因子有训练(K_1)、心理压力(K_2)及人机界面(K_3),用式(2)表示。

$$T_{1/2}=T_{1/2,n}(1+K_1)(1+K_2)(1+K_3) \quad (2)$$

式中,$T_{1/2,n}$为一般状况的执行时间。

在误安注场景下,为分析操纵班组的不响应概率,根据式(1)可知,需对操纵员执行的行为类型、操纵员完成任务的可用时间与实际完成任务的中值时间以及HCR模型的行为形成因子进行评估,结果列于表1。

将K_1、K_2、K_3代入式(2)可得:

$$T_{1/2}=10\times1.843\ 2=18.432\ \text{min}$$

将$\alpha=0.601$、$\beta=0.9$、$\gamma=0.6$、$t=20$ min、$T_{1/2}=18.432$ min代入式(1)可得操纵员的不响应概率$P(t)=0.438\ 4$。

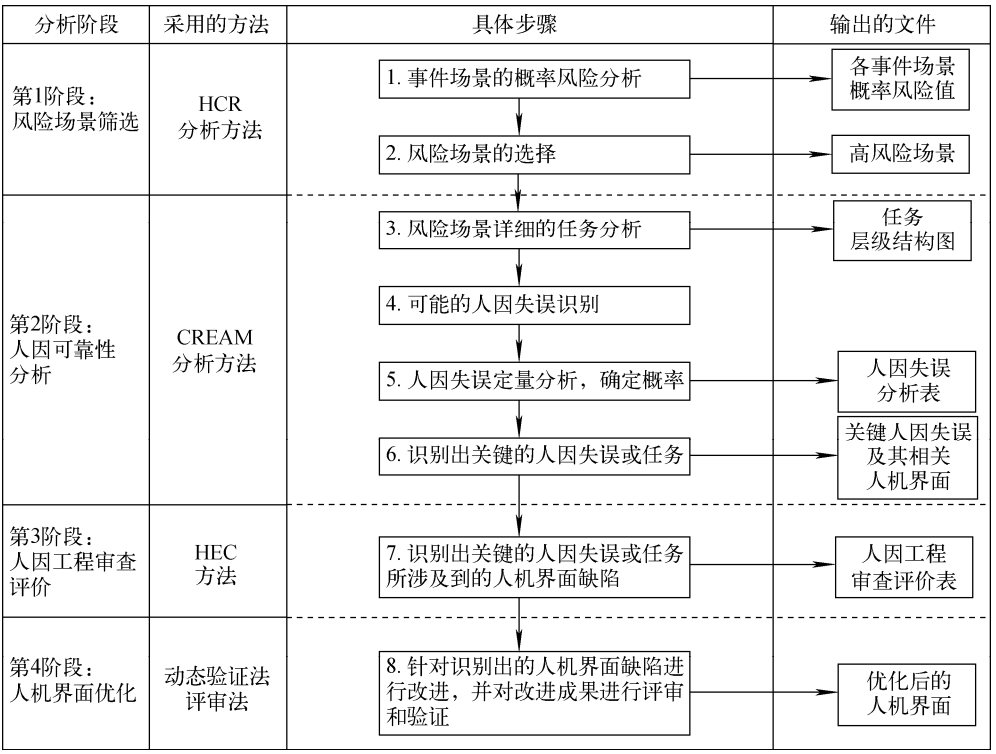

图 1　采用综合性 HRA 法的人机界面分析评价流程

Fig. 1　Human-system interface analysis and evaluation process using integrated HRA method

表 1　收集和评估得到的数据

Table 1　Data obtained by collecting and evaluating

项目	描述	评估结果
行为类型	误安注之后,出现紫色报警,根据初始导向规程进行操作,是受规则和程序支配的,因此评估为规则型行为	规则型行为对应的参数值:$\alpha=0.601$,$\beta=0.9$,$\gamma=0.6$
行为形成因子等级评价	培训情况:在数字化系统中,数字化规程培训一般处于 6 个月到 5 年之内,因此操作经验评价为平均水平	对应的 K_1 等于 0.00
	心理压力:在误安注情境下,出现紫色报警,评估为“潜在应急情景/高负荷工作”	对应的 K_2 等于 0.28
	人机界面:人机界面设计考虑了人因工程问题,但考虑不充分且需要操纵员整合部分信息,因此评价为一般	对应的 K_3 等于 0.44
完成任务的可用时间	在误安注场景下,只要操纵员在停掉安注泵的情况下,则认为事件得到缓解,不会顶开安全阀	经热工水力计算得任务的可用时间为 20 min
实际完成任务的中值时间	与操纵员访谈可知,绩效好的操纵员会在 8 min 完成该任务,绩效不好的会在 13 min 左右完成该任务,平均大约 10 min 左右	假设完成任务的中值时间为 10 min

从分析结果看,误安注情况下,操纵员的行为不响应概率非常高,因此,有必要对误安注场景下的人机界面进行优化。假设通过优化后,人机界面的评价为“优秀”,得到 $K_3=-0.22$。而表 1 中其余参数不变,则得操纵班组不响应概率为 0.137 5。因此,对人机界面进行优化是减少人因失误、提高操纵员绩效的方法之一。

2.2　基于 CREAM 法的人因失误识别

在误安注场景下会产生报警,一回路操纵员执行初始导向规程。下面以初始导向规程第

1页操作单中一回路操纵员行为为例，介绍该方法在人因失误识别中的具体应用。

1）通过层次任务分析，构建事件序列

根据初始导向规程中的第1页操作单和误安注工况条件下操纵员所进行的操作行为，通过分析可知整个操作单任务中共包括9个子任务，如图2所示。要完成任务“确认RCV017VP连接到RCV002BA”，操纵员必须通过以下行为活动才能完成，即：调用RCV002YCD画面；确认RCV017VP处于何种状态（如果没有连接到RCV002BA，则需操作来完成）；操作RCV017VP使其连接到RCV002BA上。因此，子任务1共包括3种具体的行为活动。同理，可分析得到完成其他子任务所需的具体行为活动，整个分析结果如图2所示，得到操作单的层次任务分析（HTA）框图。

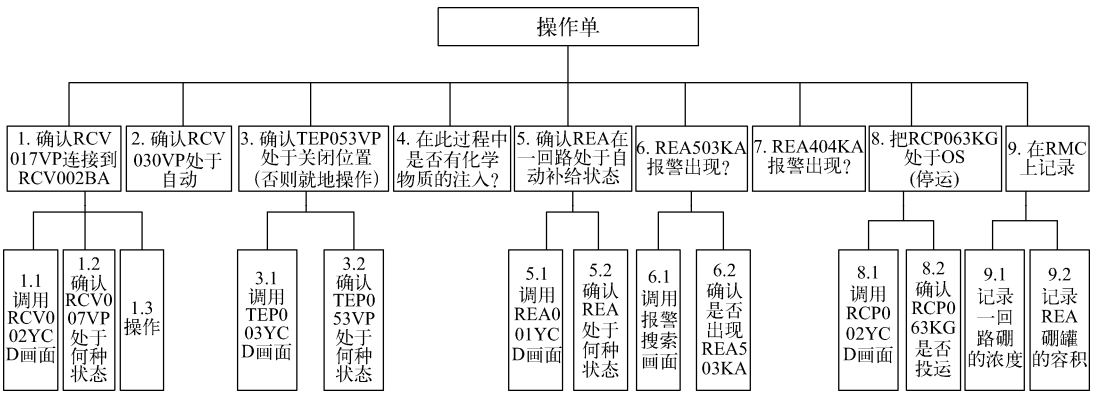

图2 操作单的HTA框图

Fig. 2 HTA diagram of operation sheet

2）确认具体行为活动的认知行为需求

根据具体的行为活动确定认知行为，根据CREAM中的15类行为分类、其具体的描述及该操作单中具体行为的描述，可得到具体行为所对应的主要的认知行为，分析结果列于表2。但是，在某些情况下，可能难以确定事件序列中某些基本子任务（行为活动）的单个认知行为，这时必须判断出最能表征事件序列的最主要的行为。否则必须重新构建事件序列，基本子任务也可再细分。

3）确定认知功能失效

确定具体认知行为之后，可根据表3认知行为与认知功能之间的对应关系，识别出相应的认知功能，如对于活动“1.1 调用RCV画面”，该活动的认知行为为“执行”，那么查表3可得，执行所对应的认知功能为“执行”。确定对应的认知功能后，就可根据情境环境的评价，以及表4基本的认知功能失效分类，评估出最有可能的认知功能失效模式，如对于活动“1.1 调用RCV画面”，可得最可能的失效模式应该为E3，即最有可能的失误即是将RCV画面调用到不适当的屏幕上。另外，针对具体的认知行为，也可通过统计分析得到最可能的认知失误模式，不过需要大量的人力物力。

4）确定失误概率

CREAM法根据众多的HRA法中的数据库，通过综合考虑给出了基本的认知失效概率（即人误概率）和相应的不确定性边界。根据表4可得到基本的失误概率，如E3的基本的失误概率为5.0×10^{-4}。然后考虑共同绩效条件（CPC）的影响权重，对基本失误概率进行修正。例如，针对E3所处的情境环境，分别对9个CPC进行评估，识别他们所处的状态得到9个CPC的评估结果，然后根据表5确定不同的认知功能、不同的CPC、不同状态所对应的权重因子，如组织的充分性所处的状态是“非常有效”，对应的认知功能是执行（E3），因此可得其权重因子为0.8。同理可得其他CPC不同状态对于行为活动1.1所对应的权重因子，从而将权重因子连乘得到综合后的权重因子0.256，并与基本的失误概率相乘，得到修正后的失误概率：

表 2　操作单中人因失误分析和量化结果

Table 2　Human error analysis and quantitative result

子任务	行为活动	认知行为	认知功能	最可能的失误模式	基本失误概率	权重因子	调整后的失误概率	任务失效概率
1. 确认 RCV017VP 连接到 RCV002BA	1.1 调用 RCV 画面	执行	执行	E3 动作目标错误(导航在不适当的屏)	0.000 5	0.256	0.000 128	0.006 14
	1.2 确认	确认	观察解释	O2 错误辨识(读错)	0.007	0.64	0.004 48	
	1.3 操作	执行	执行	E4 动作顺序错误(有很多的操作,可能顺序出错)	0.003	0.512	0.001 536	
2. 确认 RCV030VP 处于自动	2.1 确认	确认	观察解释	O2 错误辨识(读错)	0.007	0.64	0.004 48	0.004 48
3. 确认 TEP053VP 处于关闭位置(否则就地操作)	3.1 调用 TEP 画面	执行	执行	E3 动作目标错误(导航在不适当的屏)	0.000 5	0.256	0.000 128	0.004 61
	3.2 进行确认	确认	观察解释	O2 错误辨识(读错)	0.007	0.64	0.004 48	
4. 在此过程中是否有化学物质的注入?	4.1 操纵员根据机组情况和化学注入(人员是否有通知确定,需要记忆或记录)	评估	解释计划	I3 解释延迟	0.01	0.64	0.006 4	0.006 4
5. 确认 REA 在一回路处于自动补给状态	5.1 配置 REA 画面	执行	执行	E3 动作目标错误(导航在不适当的屏)	0.000 5	0.256	0.000 128	0.004 61
	5.2 确认	确认	观察解释	O2 错误辨识(读错)	0.007	0.64	0.004 48	
6. REA503KA 报警出现?	6.1 搜索 REA403 报警	执行	执行	E3 动作目标错误	0.000 5	3.2	0.001 6	0.007 99
	6.2 确认	评估	解释计划	I3 解释延迟	0.01	0.64	0.006 4	
7. REA404KA 报警出现?	7.1 确认	评估	解释计划	I3 解释延迟	0.01	0.64	0.006 4	0.006 4
8. 把 RCP063KG 处于 OS(停运)	8.1 配置 RCP 画面	执行	执行	E3 动作目标错误(导航在不适当的屏)	0.000 5	0.256	0.000 128	0.004 61
	8.2 判断 063KG 是否处于 OS 状态	确认	观察解释	O2 错误辨识(读错)	0.007	0.64	0.004 48	
9. 在 RMC 上记录	9.1 记录一回路硼的浓度	记录	解释执行	O5 动作遗漏	0.003	0.256	0.000 768	0.002 30
	9.2 记录 REA 硼罐的容积	记录	解释执行	O5 动作遗漏	0.003	0.512	0.001 536	

表 3 认知行为与认知功能间的联系

Table 3 Relationship between cognitive behavioral and cognitive function

行为类型	COCOM 功能			
	观察	解释	计划	执行
协调			√	√
交流				√
比较		√		
诊断		√	√	
评估		√	√	
执行				√
识别		√		
保持			√	√
监控	√	√		
观察	√			
计划			√	
记录		√		√
调整	√			√
扫描	√			
确认	√	√		

$$P_M = 5 \times 10^{-4} \times 0.256 = 0.000\ 128$$

同理可得其他行为活动的失误概率。得到行为活动的失误概率后就可确定子任务的失误概率,例如行为活动 1.1 的失效概率为 0.000 128,行为活动 1.2 的失效概率为 0.004 48,行为活动 1.3 没有处于正确状态,则操作失效的概率为 0.001 536。

因此,整个子任务的成功概率为 $P_S = 0.999\ 872 \times 0.995\ 52 \times 0.998\ 464 = 0.993\ 86$。

整个子任务的失效概率为 $P_F = 1 - P_S = 0.006\ 14$。

同样可算得整个操作单任务失效的概率 $P_{AF} = 0.046\ 46$。

整个操作单所有的分析结果列于表 5。通过上述分析可知,在该事件树中,关键的人因失误依次是 I3 和 O2 等,关键任务排序依次是“REA503KA 报警出现?”、“REA404KA 报警出现?”、“在此过程中是否有化学物质的注入?”等。从而可重点针对这些关键的或重要的人因失误或任务进行分析,对由人机界面诱发的人因失误进行重点审查。

2.3 基于 HEC 法的人机界面评审

结合人因工程的基本设计原理、人机界面设计评审指南及界面设计指南分别对数字化后人机界面的显著变化特征设计人因工程审查数据库,主要包括信息显示方面、数字化规程方

表 4 一般的认知功能失效模式

Table 4 General failure modes of cognitive function

认知功能失效		一般的认知功能失效模式	基本概率
观察失误(O)	O1	观察到错误的目标,对错误的刺激或事物做出响应	1.0×10^{-3}
	O2	由于线索错误或片面的识别,故作出错误的识别	7.0×10^{-3}
	O3	观察错过(即疏忽),忽视了信号或测量值	7.0×10^{-3}
解释失误(I)	I1	诊断错误,诊断要么是错误的要么是不完整的	2.0×10^{-2}
	I2	决策错误,要么没有做出决策要么做出的决策是错误或不完整的	1.0×10^{-2}
	I3	解释延迟,即没有及时做出解释	1.0×10^{-2}
计划失误(P)	P1	优先选择错误,如选择了一个错误目标	1.0×10^{-2}
	P2	制定的计划不充分,要么不完整要么完全错误	1.0×10^{-2}
执行失误(E)	E1	行为执行类型错误,涉及在力度、距离、速度或方向上执行不对	3.0×10^{-3}
	E2	行为执行时间错误,要么太早要么太迟	3.0×10^{-3}
	E3	行为的目标错误(邻近的,相似的或不相关的)	5.0×10^{-4}
	E4	行为执行顺序错误,如反复、跳跃或颠倒	3.0×10^{-3}
	E5	行为错过,没有执行(即疏忽),包括最后一个动作的疏忽	3.0×10^{-3}

表 5　CREAM 法中 CPC 对认知功能影响的权重因子

Table 5　Weight factor of CPC's effect on cognitive function in CREAM method

CPC 名称	等级层次	COCOM 认知功能的权重因子			
		观察	解释	计划	执行
组织的充分性	非常有效	1.0	1.0	0.8	0.8
	有效	1.0	1.0	1.0	1.0
	无效	1.0	1.0	1.2	1.2
	不足	1.0	1.0	2.0	2.0
工作环境	有利的	0.8	0.8	1.0	0.8
	相容的	1.0	1.0	1.0	1.0
	不相容的	2.0	2.0	1.0	2.0
MMI 和操作支持的充分性	支持的	0.5	1.0	1.0	0.5
	充分的	1.0	1.0	1.0	1.0
	可接受的	1.0	1.0	1.0	1.0
	不合适的	5.0	1.0	1.0	5.0
规程/计划的可用性	合适的	0.8	1.0	0.5	0.8
	可接受的	1.0	1.0	1.0	1.0
	不合适的	2.0	1.0	5.0	2.0
需同时响应的目标数量	能力之内的	1.0	1.0	1.0	1.0
	与能力匹配的	1.0	1.0	1.0	1.0
	能力之外的	2.0	2.0	5.0	2.0
可用时间	充分的	0.5	0.5	0.5	0.5
	暂时不足	1.0	1.0	1.0	1.0
	持续不足	5.0	5.0	5.0	5.0
工作时段	白天(可调整的)	1.0	1.0	1.0	1.0
	夜晚(不可调整的)	1.2	1.2	1.2	1.2
培训、准备的充分性	充分,经验丰富	0.8	0.5	0.5	0.8
	充分,有一定的经验	1.0	1.0	1.0	1.0
	不足	2.0	5.0	5.0	2.0
员工的协作质量	非常有效	0.5	0.5	0.5	0.5
	有效	1.0	1.0	1.0	1.0
	无效	1.0	1.0	1.0	1.0
	不足	2.0	2.0	2.0	5.0

面、软控制方面、界面管理方面、报警方面建立较全面系统的人因工程检查清单。然后利用人因工程检查清单结合操纵员的调查和访谈对关键的人因失误及任务所涉及的人机界面进行一一审查,识别人机界面设计的缺陷,并提出一些改进的建议。限于篇幅,在此仅列举部分审查结果供参考(表 6、7)。

2.4　人机界面优化

针对识别出来的设计缺陷,根据设计导则和标准法规要求并结合评审法和动态验证方法对人机界面进行优化改进。人机界面的优化改进是一项复杂的工作,需进行修改、评审和验证,然后再修改、再评审、再验证,如此往复循环直至满意。

表 6 针对具体任务的人因工程审查

Table 6 Human factors engineering review of specific task

事件树	关键的人因失误、任务	所涉及的人机界面	针对任务存在的主要缺陷	建议
操作单	REA503KA 报警是否出现	报警画面 配套画面 规程	如果采用直接在报警屏中搜索 REA503KA，则搜索报警比较繁琐，耽搁操作时间，可能产生解释延迟 如果从配套画面中左边导航框中点击 SOPR500KA 导航按钮，则需要选择导航到什么屏，从众多的报警中去寻找 REA503KA，增加了眼睛的移动距离	在规程页面增加报警导航按钮 在规程页面的某个区域增加该报警的显示
	在此过程中是否有化学物质的注入	规程	需要记忆，增加认知负担，容易记忆错误，或发生混淆。如果需要查看记录，则需要花费时间	如果可能，增加系统自动判断

表 7 操作单关键任务、人因失误所涉及画面的整体审查

Table 7 Human factors engineering review of display related to critical tasks and human errors

事件树	所涉及的人机界面	整体评价
操作单	配套画面	1) 所有数字应该右对齐，如果数字超过 4 位数，则应将其分组，并且每组之间用逗号、小数点或空格分隔开 2) 单位的标注不规范，如 MPa 3) 画面设计密度有些地方大，难以明显区分，如 INTERVALIDATED DATA 4) 字体表达大小写不一致，如 SG LEVEL 5) 就不是以英语为母语的国家来说，外文字母大写对于认读增加了困难 6) 画面迷你图太小，字体太小，曲线太细 7) 对于 SG 对应的曲线区分存在困难
	规程	1) 规程的字体太小，不易于识别 2) 应提示操纵员未完成或遗漏掉的规程步骤
	报警画面	1) 最高优先级的报警应用最显著的编码方式 2) 那些对电厂监视和用户的操作很重要的报警应考虑纳入相关的画面 3) 如果所有报警分为绝对的优先级别，则优先级分类不能超过 4 类

3 结论

本研究综合考虑了现有的多种人机界面人因可靠性分析方法和评价方法，提出了 HCR+CREAM+HEC 相结合的综合性人因可靠性分析方法和评价方法。该方法具有可操作性强、评价客观等优点。现已将该方法成功应用于在建的 CPR1000 各项目，具有广阔的应用空间。

参考文献：

[1] HANNAMAN G W, SPURGIN A J, LUKIC Y D. Human cognitive reliability model for PRA analysis, NUS-4531[R]. California: NUS Corporation, 1984.

[2] HOLLNAGEL E. Cognitive reliability and error analysis method[M]. Oxford, UK: Elsevier Science Ltd., 1998.

[3] JOU Y T, LIN C J. The implementation of a human factors engineering checklist for human-system interfaces upgrade in nuclear power plants [J]. Safety Science, 2009, 47: 1 016-1 025.