

# 2000 m 多用途深海环境模拟装置 的可靠性分析

沈国鉴 胡勇 殷俊 易宏

(船舶及海洋工程系)

**摘要** 本文对 2000 m 压力球系统进行了可靠性分析。通过定性分析和定量计算求得了该系统几个重要的可靠性指标。根据文章得出的结论对原设计作了评价,提出了改进设计,并就如何应用可靠性分析理论来解决实际工程设计问题,特别是对复杂故障树的简化方面进行了探索。

**关键词** 可靠性,故障树,可靠寿命,最小割集,结构函数

## 0 引言

2000 m 多用途深海环境模拟装置系上海交通大学水下工程研究所深潜实验室的主要试验设备。1982年自行设计并投入试用。当时设计者虽从多方面考虑了系统的安全性,但未从可靠性理论的角度对系统可靠性进行分析。由于该装置是在高压(最大压力为 200 个大气压)条件下工作,它的可靠性对试验装置的操作者和试件的安全都是至关重要的。本文旨在探索一种合适的可靠性分析方法对这一设计进行评价。经可靠性分析后得出的结论,对改进设计和指导操作者今后的工作都具有一定的实际意义。

## 1 功能分析和故障树的建立

### 1.1 系统的组成和功能

图 1 为 2000 m 多用途深海环境模拟装置的工作原理图。装置通过一个高压水泵向压力球内打水,在球内产生高压,以模拟深海环境,用来做动压试验和静压试验。

由图 1 可见,装置主要由高压水泵、压力球、蓄压器和排水系统四部分组成。高压水泵用来向压力球内打水以产生压力。压力球为试验时承放试件的容器。动态试验时,由于试件的伸缩等运动引起体积的变化,球内压力也将随之变化。为使球内压力恒定,专门设置一个重锤式蓄压器。在此蓄压器上加上一数量砝码(重锤),即可得到试验所需的压力。蓄压器与压力球通过连通器相连。当压力球内压力发生变化时,可通过蓄压器活塞的上下运动

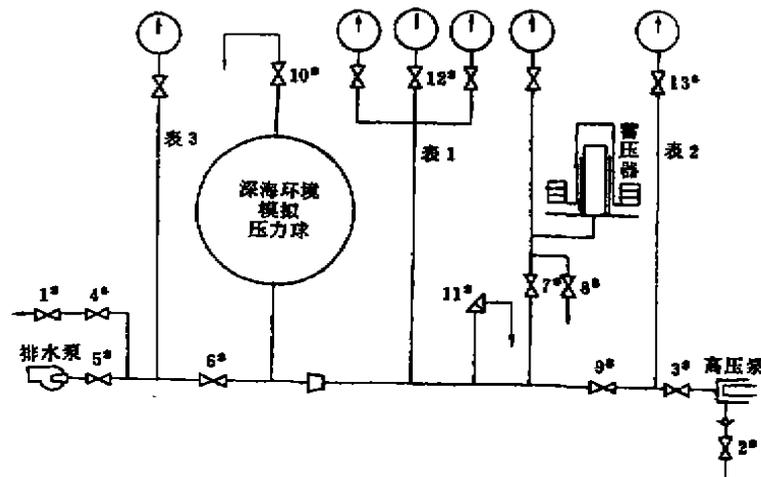


图 1 工作原理图

来保证球内压力恒定。排水系统由 5 号、6 号两个截止阀及排水泵组成。当做完试验或发生紧急情况需要排水时，可以打开这两个阀门，启动排水泵排水。

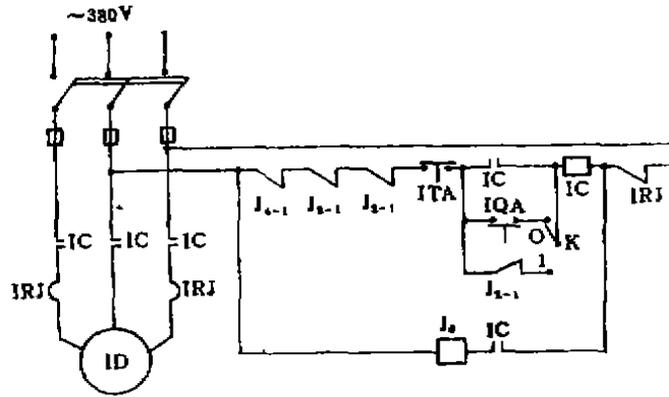
11号安全阀是为了防止压力过大使压力球破裂而设置的。当球内压力超过压力球最大承载压力时，11号阀门自动跳开。压力表 1 用来监视压力球内的压力。表 2 的作用是控制高压泵的启动与关闭。它连接一个压力开关，当压力到达预定值时，压力开关闭合，通过一个高压控制电路使泵停转。阀门 7、8、9 都是截止阀。当做动压试验时，7 号阀门打开，8 号阀门关闭。当做静压试验时，7 号阀门关闭，蓄压器不起作用。10 号阀门是排气阀。在往压力球内注水时，将它打开可以放走空气。压力表 3 是监视排水管的低压表。

图 2 为高压控制电路图。控制电路主要由线路接触器，各中间继电器以及它们的触点  $J_{1-1}$ 、 $J_{3-1}$ 、 $J_{4-1}$ ，热继电器 IRJ，保险丝和各种按钮开关组成。为了对压力球内水压实行自动控制，设置了一道低压(12 V)中间继电器电路(见图 2 b)。当压力达到规定的高压时，压力开关  $HJ_2$  闭合，低压电路通电， $J_3$  继电器开始动作，带动高压(380 V)电路中继电器的触点  $J_{3-1}$  动作(见图 2 a)，高压电路的旁路中的线路接触器 IC 断电，使高压水泵电路中的线路接触器 IC 线圈断开，高压泵即停止转动。

## 1.2 故障树的建立

对于所研究的系统来说，有两种危险情况：一是压力球内的试件被压坏，二是压力球破裂。因而，我们选择以上两种危险性故障为故障树顶事件。由于该系统可以做动压、静压两种形式的试验，所以把故障树分为静压试验故障树分支和动压试验故障树分支。

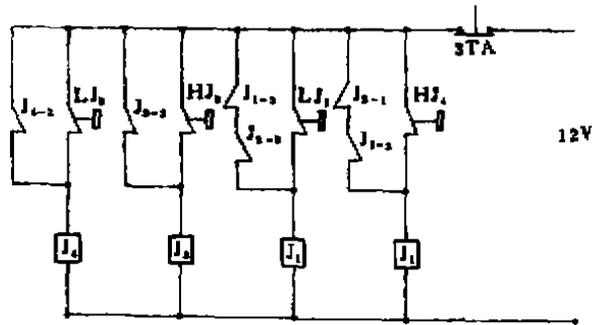
图 3 为 2000 m 压力球系统的总故障树。在建树时，考虑到了问题的边界条件，并假定压力球系统中高压水泵、低压水泵及其所有的管道都不失效。



2-a

符号说明：

- |             |                                |
|-------------|--------------------------------|
| ID——高压泵电动机； | IRJ——热继电器；                     |
| IQA——启动按钮；  | J <sub>0</sub> ——中间继电器(380 V)； |
| ITA——停止按钮；  | K——手动自动转换器(0手动；1自动)。           |
| IC——线路接触器；  |                                |



2-b

符号说明：

- J<sub>1</sub>-J<sub>4</sub>——中间继电器(12 V)  
 3TA——复位按钮  
 HJ<sub>1</sub>-HJ<sub>2</sub>——高位压力继电器(DXB-113)  
 LJ<sub>1</sub>-LJ<sub>2</sub>——低位压力继电器(DXB-113)

图 2 高压控制电路图

## 2 系统的可靠性分析

由于顶事件属“系统出现危险性故障”，本文所要求的系统可靠度将是指在规定条件下和规定时间内系统不出现危险性故障的概率。这就是说，即使系统在工作时发生故障，甚至妨碍系统的正常工作，但只要不出现危险性故障，仍认为本系统是可靠的。

本文所讨论的系统应是一个可维修系统，但区别于一般可维修系统的是，本系统的故障不允许发生。因此不能按一般可维修系统的 MTBF 来讨论它的平均寿命，而应该讨论它的可靠寿命  $T_r$ 。当使用期大于  $T_r$  时就应该进行维修。

对于可靠性分析来说还必须求元器件的重要度。这对于系统设计、使用和维修来说都是重要的参数。本文将主要分析关键重要度。它在数学上的意义是，某部件故障概率的变化率所引起的系统故障概率的变化率。

### 2.1 系统可靠度的计算

对于图 3 所示的复杂故障树进行定性、定量分析是较为困难的，本文将对之进行必要的简化。考虑到存在大量的重复事件，可把一个单独的故障树模块作为一个准底事件，把它拿出来进行单独计算，而在总故障树中则用一个“准底事件”来代替，这样可以简化计算。文章在“高压控制电路故障”及“高压时系统压力控制失灵”两处作了这种简化，把这两个故障树模块分割出来，单独地枚举最小割集和计算概率。图 4 为高压控制电路故障树模块及其简图。图 5 为高压时系统压力控制失灵模块故障树及其简图。

对以上两处作了简化后，故障树还是显得很大、很繁。为了进一步简化，我们把一些逻辑重复事件在分析最小割集前去掉。在总故障树中，有两处含有“报警装置失灵”，从逻辑上看可以去掉一个故障树分支。在“动压试验时系统出现危险性故障”中，有两处出现“蓄压器未能按要求动作”，从逻辑上看也可去掉一处。

经过上述两个步骤，总故障树已得到大大简化。图 6 就是处理后总故障树及其简图。下面将对这个总故障树，以及两个分离出来的故障树模块进行分析，得出它们的最小割集 (MCS)，从而进行定量计算。

#### 2.1.1 高压控制电路故障模块的 MCS 及结构函数

用 Fussell-Vesely 法可算出该模块的五个最小割集： $\{x_{16}\}$ ， $\{x_{18}\}$ ， $\{x_{17}\}$ ， $\{x_{10}\}$ ， $\{x_{15}\}$ 。因此，模块的结构函数可表示为

$$\phi_1 = x_{15} + x_{16} + x_{17} + x_{18} + x_{19} \quad (1)$$

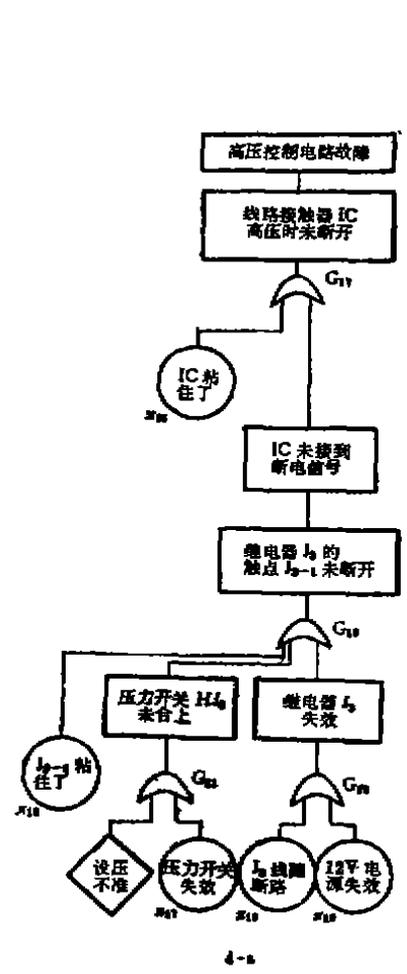
#### 2.1.2 高压时系统压力控制失灵模块的 MCS 及结构函数

用 F-V 方法可得出本模块的七个最小割集，即  $\{x_4, x_9, x_{11}\}$ ， $\{x_4, x_5, x_7\}$ ， $\{x_4, x_5, x_8\}$ ， $\{x_4, x_6, x_7\}$ ， $\{x_4, x_6, x_8\}$ ， $\{x_4, x_7, x_9\}$ ， $\{x_4, x_8, x_9\}$ 。因而，模块的结构函数可表示为

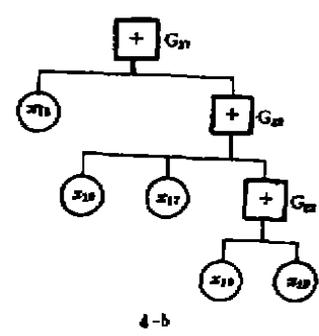
$$\phi_2 = x_4 x_9 x_{11} + x_4 x_5 x_7 + x_4 x_5 x_8 + x_4 x_6 x_7 + x_4 x_6 x_8 + x_4 x_7 x_9 + x_4 x_8 x_9 \quad (2)$$

#### 2.1.3 处理后总故障树的最小割集和结构函数

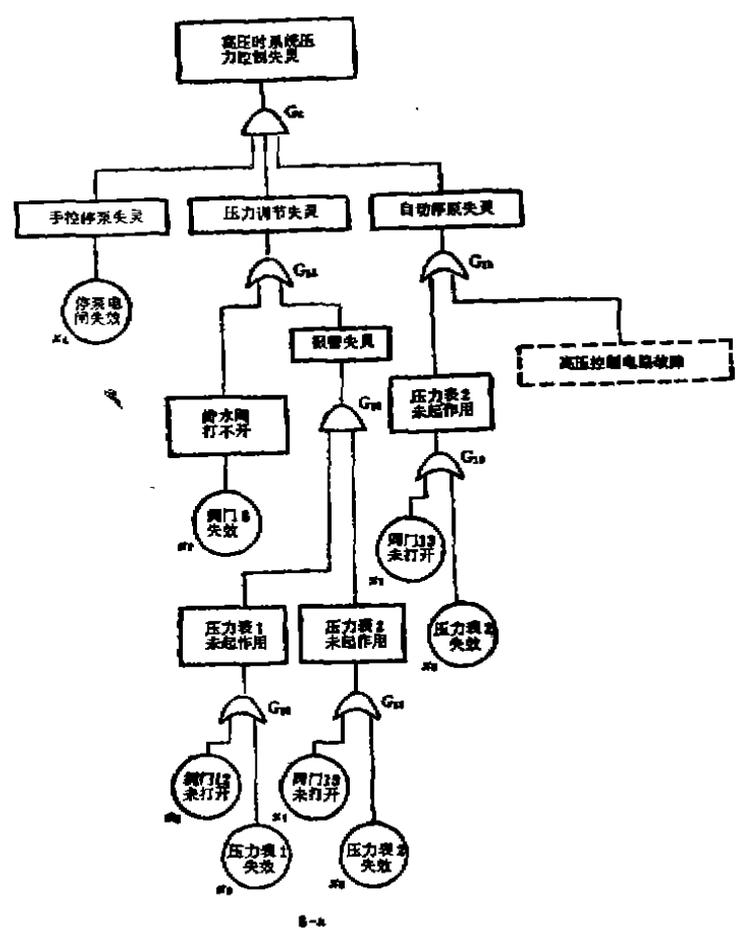
用 F-V 法可求出处理后总故障树的五个最小割集，即  $\{x_1\}$ ， $\{x_{12}\}$ ， $\{x_{13}\}$ ， $\{x_{20}\}$ ， $\{x_2 x_3\}$ 。因此，总故障树的结构函数可表示为



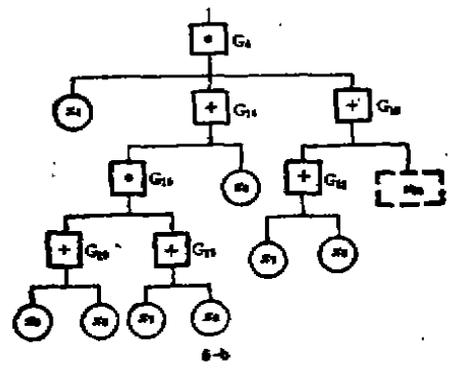
4-a



4-b



5-a



5-b

图 4 高压控制电路故障模块故障树及其简图

图 5 高压时系统压力控制失灵模块故障树及其简图

$$\phi = x_1 + x_{12} + x_{13} + x_{20} + x_2 x_3 \quad (3)$$

当求得系统的结构函数后，就可以进行定量计算，以求出顶事件发生的概率。

一般情况下，最小割集之间是不独立的，本文采用不论最小割集之间是否独立，都可以进行精确计算的容斥定理求顶事件的发生概率（即系统的不可靠度）。

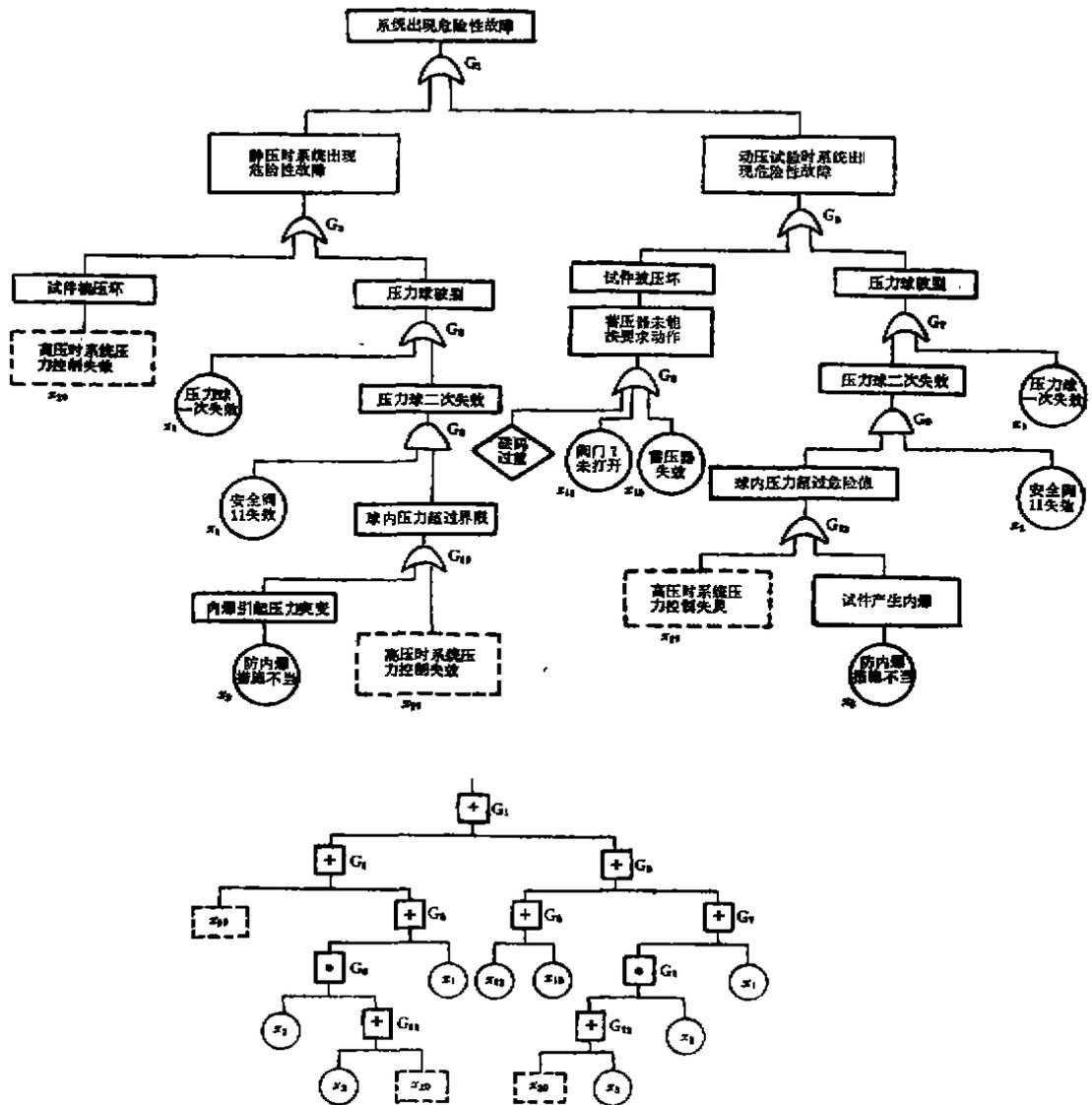


图 6 处理后总故障树及其简图

由容斥定理表达的系统不可靠度  $Q_s$  为

$$Q_s = \sum_{i=1}^k (-1)^{i-1} \sum_{1 \leq j_1 < \dots < j_{i-1} \leq k} Q(\prod_{l=1}^{i-1} M_{j_l}) \quad (4)$$

式中： $M$ 为最小割集， $k$ 为系统具有的最小割集数。

2.1.4 高压控制电路故障的发生概率  $Q_{11}$

计算是在电子计算机上进行的。输入数据为： $N, Q_{15}, Q_{16}, Q_{17}, Q_{18}, Q_{19}$ 。其中， $N$ 表示系统具有的最小割集数， $Q_{15} \sim Q_{19}$ 表示对应底事件的发生概率，也就是对应各个部件的不可靠度值。这些不可靠度值是根据文献[2]查得的失效率数据按指数规律换算而得的。换算中取总工作时间为3000h。这是根据该压力球系统原设计要求使用1000次，每次平均工作时间为3h而定的，上述6个输入数据依次为：5,  $1.49887 \times 10^{-3}$ ,  $7.47194 \times 10^{-3}$ ,

$4.48989 \times 10^{-3}$ ,  $5.99819 \times 10^{-3}$ ,  $4.48989 \times 10^{-3}$ .

输出结果为:  $Q_{11} = 1.842808 \times 10^{-2}$ .

### 2.1.5 高压时系统压力控制失灵的发生概率 $Q_{20}$

将  $Q_{11}$  作为准底事件  $x_{11}$  的发生概率和别的有关底事件发生概率一起输入计算机, 输入数据及格式从略, 输出结果为:  $Q_{20} = 1.675181 \times 10^{-5}$ .

### 2.1.6 总故障树的顶事件发生概率 $Q$

将  $Q_{20}$  作为准底事件  $x_{20}$  的发生概率和别的有关数据一起输入计算机, 输出结果为:  $Q = 0.3633486$ , 故系统的可靠度 (即系统不发生危险性故障的概率) 为:  $R_s = 1 - Q = 0.6366514$ .

2.1.7 用上述方法计算不同总工作时间时系统的可靠度, 得到了如图 7 所示的近似指数分布的可靠度曲线。

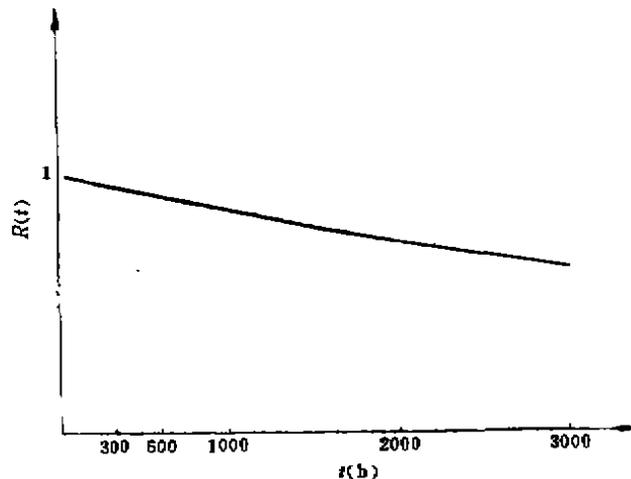


图 7 可靠性函数曲线

## 2.2 系统可靠寿命 $T_r$

设系统可靠度  $R(t) \geq 0.95$  时系统足够可靠, 则系统可靠性下降到  $R(t) = 0.95$  时的寿命时间  $T_r = T_{0.95}$  即为系统的可靠寿命, 从图 7 所示的  $R(t) \sim t$  曲线中可以看到: 当  $R(t) = 0.95$  时,  $T_{0.95} \approx 300$ h, 即系统的可靠寿命为 300h.

## 2.3 重要度 $w$

本文讨论重要度的目的是要找出重要度大的关键部件, 以改进设计, 提高系统的可靠度。

表 1 为不同工作时间时的关键重要度  $w$ , 其中  $x_{20}$  代表“高压时系统压力控制失灵”这个准底事件, 讨论时将它作为一个整体来求其重要度。

## 2.4 改进设计

从表 1 可以看出, 虽然随着时间的变化各基本事件 (各部件) 的重要度略有不同, 但它们之间的相对关系基本上不随时间而变化, 如系统工作 3000h 时, 它们的关键重要度顺序

表 1 2000m 压力球系统部件重要度( $w$ )

元 件	时间(h)					
	60	150	300	600	1500	3000
$x_1$	0.0033	0.00328	0.00325	0.00317	0.00296	0.00263
$x_2$	1.32E-5	1.31E-6	1.3E-5	1.27E-6	1.18E-5	1.05E-5
$x_3$	1.32E-6	1.31E-5	1.3E-5	1.27E-5	1.18E-5	1.05E-5
$x_{12}$	1.1E-3	4.38E-4	2.16E-4	1.058E-4	3.948E-5	1.75E-5
$x_{10}$	0.996	0.991	0.9960	0.9960	0.9960	0.9950
$x_{20}$	1.58E-8	9.67E-8	3.8E-7	1.475E-6	8.47E-6	2.87E-5

为:  $x_{12} > x_1 > x_{20} > x_{10} > x_2 = x_3$ ; 系统工作 60 h, 150 h, 300 h, 1500 h, 它们的关键重要度顺序为:  $x_{12} > x_1 > x_{10} > x_2 = x_3 > x_{20}$ 。

由此可知, 蓄压器的一次失效的重要度  $x_{12}$  与其他部件相比是个相当大的量。这说明蓄压器的可靠度的变化对系统可靠度变化的影响亦相当大。因此, 要改进系统的设计, 提高系统的可靠度, 着眼点应放在提高蓄压器的可靠度上。蓄压器的失效模式是重锤与套筒之间卡死, 使重锤不可自由地上下移动, 导致压力球内的压力升高。因此我们建议在蓄压器管路上连接一个安全阀。工作时将安全阀的压力调到预定值。当蓄压器卡死后, 压力一旦超过预定值就将跳闸, 切断总电源而停止试验。

## 2.5 改进设计后的系统可靠度与改进设计前的系统可靠度

由表 2 可知, 改进后的系统可靠度有了极大的提高。

表 2 2000m 压力球系统改进前后的可靠度比较

工作时间(h)	改进前系统可靠度	改进后系统可靠度
60	0.991	0.9999688
150	0.978	0.999908
300	0.956	0.999813
600	0.914	0.9995855
1500	0.788	0.998632
3000	0.637	0.996304

## 3 分析与结论

(1) 从所求得系统可靠度看, 原系统工作 300 h 的可靠度为 0.956。2000 m 压力球系统至今已累计工作约 100 h。从使用要求看, 现在的可靠度是令人满意的。

(2) 原系统设计的要求为工作 1000 次, 每次 3 h 而不发生危险性故障。从本文的分析结果看, 若不进行维修, 工作到 3000 h 时, 系统可靠度只有 0.637, 这是相当危险的。

(3) 通过对系统的可靠性分析并改进设计后系统可靠度大幅度提高。工作 3000 h 时可靠度由原来的 0.637 提高到 0.996304, 不发生危险性故障的安全性有了足够的保证。

(4) 应该指出, 2000m 压力球系统做静压试验时, 蓄压器是不用的。但我们在计算部件

失效概率时, 假定系统工作时间与部件工作时间是相同的, 即一旦系统工作, 不论是动压试验还是静压试验, 都认为蓄压器参加了工作。这样求得的系统可靠度是偏小的。另外, 在计算部件失效概率时, 只考虑了工作时间增加使部件失效概率增大, 而未考虑部件不工作时的自然老化, 使之失效概率的增大。而这使计算的系统可靠度增大。

致谢: 深潜实验室曹智裕同志在本文撰写过程中给予了合作和帮助, 在此表示衷心的感谢。

### 参 考 文 献

- [1] 黄秀章等. 2000m多用途深海环境模拟装置的压力球设计, 深海环境模拟压力筒论文集, 1985
- [2] 梅启智等. 系统可靠性工程基础, 科学出版社, 1987

## Reliability Analysis of Multi-purpose 2000 m Deepsea Environment Simulation Equipment

*Shen Guojian Hu Yong Yin Jun Yi Hong*

**Abstract** This paper describes a reliability analysis on a Multi-purpose 2000m Deepsea Environment Simulation Equipment. It presents some important reliability parameters of the system, an evaluation on the original design and an improved plan by analysing and calculation.

It also has practical significance for the exploration of research on how to use reliability theory to solve engineering problems, especially in the simplification of the fault tree.

**Key words** reliability, fault tree, Qpercentile life, minimum cut set (MCS), structure function