

基于危险分析与风险评价的液压提升机安全设计

彭佑多, 高光辉, 郭迎福, 吴立桃, 李 新

(湖南科技大学机械设备健康维护省重点实验室, 湖南湘潭 411201)

[摘要] 介绍了液压提升机的安全性能要求,对液压提升机进行了危险分析和风险评价,确定了各子系统的危险分值,得到了安全设计中必须高度关注的子系统;进行了各子系统的安全可靠度的预计与分配,并简要分析了子系统的安全设计要点,为液压提升机的安全可靠分析与设计提供了依据。

[关键词] 液压提升机;安全设计;危险分析;风险评价;安全可靠

[中图分类号] TD534.1 [文献标识码] A [文章编号] 1009-1742(2010)02-0070-06

1 前言

矿井提升机担负着沿井筒提升设备、矿石、物料和升降人员的任务,在采矿生产中占有极其重要的地位。矿井生产要求提升设备能长期连续可靠运转并具有高度安全性。液压提升机由复杂的机、电、液复合系统组成,是典型的机电液一体化产品,其安全功能的实现主要依赖于其电控与监测系统、液压驱动系统、液压制动系统、载荷系统、深度指示系统与操作系统等多方协调。以往开展液压提升机设计时考虑安全配套设施较全,但设计方法上没有讲究,基本上未曾进行过安全设计的危险分析和风险评价。

2 对液压提升机的安全性能要求

《矿井提升机和矿用提升绞车安全要求》和《煤矿安全规程》都对矿井提升机和矿用提升绞车有明确的安全要求和规定,液压提升机则应满足防爆、超速、过卷保护、过载过压保护、防坠保护和断绳时防坠器紧急抱紧罐道实现强制停车等安全要求^[1~3]。

2.1 防爆

防爆是煤矿井下提升机最基本的安全要求,液压提升机的主要使用环境是含煤尘和易燃、易爆气

体的煤矿井下或井口,防爆是其最基本的安全功能,液压提升机液压系统为密闭工作回路,具有先天的防爆条件;而液压提升机电气控制系统主要采用隔爆型或安全火花型电气设备,随着电控防爆技术的发展及各种防爆新理论与新元器件的出现,防爆问题在设计上已不是主要问题。

2.2 超速、过卷保护

液压提升机在工作过程中尤其是在下放负载过程中,容易发生跑车超速,速度超过额定最大速度运转时,不仅机械或液压元件如液压马达容易损坏,也是诱发重大事故的安全隐患,因此液压提升机设计中规定,当跑车速度超过额定速度 15% 时,系统必须能自动断电。

提升容器的提升高度超过限定位置(过卷)时,深度指示器顶开安装在其顶部的过卷行程开关,行程开关失电使液压提升机停电抱闸制动。

2.3 高、低压保护

在液压主回路中设置有高低压保护回路,当液压系统工作压力超过正常压力值 1.2~1.25 倍时,高压溢流阀开启,液压油经高压安全阀、单向阀流入主回路的低压侧管道,此时液压系统压力不会继续升高,液压马达带不动过重的负载,提升机自动停机;若辅助补油系统的补油压力过低,低压保护压力

[收稿日期] 2007-07-23

[基金项目] 湖南省教育厅重点科研项目(04A013)

[作者简介] 彭佑多(1964-),男,湖南安化县人,湖南科技大学教授,主要研究方向为矿山机械工程及液压传动与控制;E-mail: ydpeng@hnust.edu.cn

继电器动作,切断电源,提升机也会自动停机,且信号灯亮,报警铃声报警。

2.4 其他安全保护

液压提升机还有齐全的其他安全保护功能,如液压提升机有故障时,不能启动;在运行中发生故障时,提升机中途自动停机,并进行紧急制动,同时信号批示灯亮警示故障发生。闸瓦磨损过大,卷筒一负载系统在减速点未减速,液压系统油箱油温过高,油位过低,都会使液压提升机的主油泵停转,制动闸紧急制动,事故信号灯亮,报警铃报警。紧急制动情况下,司机可操作脚踏制动开关(ES),使液压提升机紧急停车,并断开控制电源。一旦在提升或下降负载时出现断绳现象,防坠器或抓捕器会紧急启动,实现强制停车等。

3 危险分析与风险评价

液压提升机由复杂的机、电、液复合系统组成,是典型的机电液一体化产品,主要由液压驱动系统、液压制动系统、电控监测与报警系统、滚筒载荷系统、深度指示系统与操作系统等组成,如图1所示,其安全功能主要依赖于各子系统的协调得以实现,其高安全可靠也靠各子系统予以保证,当然各种危险及不安全因素也存在于这些子系统之中。

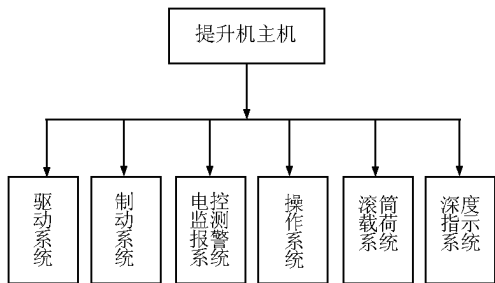


图1 液压提升子系统组成框图

Fig.1 Subsystem structure of hydraulic winder

提升机安全功能的部分或全部失效或不同子系统不安全情况出现时对矿井生产系统都会产生不同

程度的影响,根据后果的严重程度及其出现的概率,通常把提升机安全危险度分成4个等级,如表1所示。

表1 危险等级表^[1,2]

Table 1 Danger grade

危险等级	危险等级分数	危险等级说明	危险状态描述
IV	≥7	致命的	可能成为矿井生产系统安全功能丧失,导致系统或环境重大破坏或造成人身伤亡的潜在原因
III	4~7	严重的	可能成为矿井生产系统安全功能丧失,导致系统或环境重大损坏的潜在原因,可能造成人员的重伤
II	2~4	临界的	可能造成矿井生产系统功能退化,对系统或环境和人员无显著损伤
I	≤2	可忽略的	可能成为矿井生产系统功能退化的原因,对环境和人员无损害

3.1 危险分析

危险分析与评价方法主要有安全检查表法、预先危险分析法、失效模式与效应分析法。危险可操作性研究法、事件树分析法、故障树分析法、原因—后果分析法、危险指数评价法、人的可靠性分析方法、概率风险评价技术、基于可信性的风险分析方法、基于可拓方法的风险评价和模糊风险评价等。

液压提升机已得到较大程度应用,在其寿命期间内因物理性能及预定使用而可能产生的危险、原因及其相应后果等都大量积累并基本掌握,表2是液压提升机各子系统危险分析一览表^[3-5]。

3.2 风险评价

从表2危险分析一览表可知,液压提升机的电控与监测系统、液压驱动系统、液压制动系统、载荷系统、深度指示系统与操作系统各子系统均有可能出现危险情况,但出现的概率不完全相同,产生危险的伤害严重度也不完全相同。表3是各个子系统粗略的定量危险评价^[3-5]。

表 2 危险分析一览表
Table 2 Hazard analysis general view

序号	子系统名称	复杂程序或零部件数量	危险描述	可能性或危险出现概率	可能产生的危险等级或影响
1	电控监测与报警系统	复杂、零部件数量特别多	欠电压运行	绝少可能	II 级
			监测不全或运行不正常	绝少可能	
			部件或系统自动控制和联锁出现故障和保护装置不齐全	极小可能	III 级
			误报警或不报警	极小可能	
			防爆性能低、效果差	绝少可能	IV 级
2	液压驱动系统	复杂、零部件数量多、关键件多	限速装置失灵到达终端位置	可能	III 级
			的速度超过规定值		
			提升速度超过最大速度	可能	
			油路系统渗漏油严重	可能	
			油路系统渗漏油严重	可能	IV 级
3	液压制动系统	非常复杂、零部件数量多、关键件多	安全制动力矩不足或安全制动失效	可能	
			工作制动失效	极小可能	
			制动闸瓦设计摩擦系数不够、接触面积不足或过磨损严重	极小可能	
			安全制动器空行程时间不能保证	极小可能	
			制动盘两侧或制动轮上有降低摩擦系数的介质,如水、油等	非常可能	
4	滚筒载荷系统	复杂、零部件数量多、有关键件	卷筒主要焊缝开裂、主轴内部存在缺陷	绝少可能	IV 级
			钢丝绳安全系数不足	绝少可能	
			超载运行	可能	
			断绳制动器安全可靠度不高	绝少可能	
			提升容器超过正常终端停止位置出现过卷现象	极小可能	III 级
5	深度指示系统	复杂、零部件数量较多	深度指示器有故障或失效	可能	
			司机操纵台位置噪声过大	可能	II 级
6	操作系统	相对简单、零部件数量不多	矿井设备安装处有过量的尘埃和爆炸性气体不能满足防爆要求	极小可能	
			司机操作不规范	可能	
			司机操作失误	极小可能	IV 级

表 3 液压提升机风险评价
Table 3 Risk assessment of hydraulic winder

部件或子系统名称	分值			危险分数 $C \times E \times L$	危险程度及建议
	危险严重度 C	危险出现概率 L	故障(危险)排除难度 E		
液压驱动系统	7	5	7	245	危险,重点设计
液压制动系统	10	7	9	630	高度危险,关键设计
滚筒载荷系统	10	5	7	350	危险,重点设计
深度指示系统	8	7	5	250	危险,重点设计
电控监测与报警系统	9	10	9	810	特别危险,关键设计
操作系统	9	7	7	441	很危险,重点关注

4 安全可靠性设计

液压提升机安全可靠性设计主要包括:a. 明确提升机安全可靠性要求和可靠性指标;b. 进行安全可靠性(失效率)预计和安全可靠性指标分配;c. 子系统或元部件可靠性设计。

安全可靠性预计主要是运用以往的经验、安全故障数据、当前的安全技术水平,尤其是元器件的失效率作为依据,预报所设计提升机系统实际可能达到的安全可靠度,即预报正常完成安全功能的概率;安全可靠性分配是以液压提升机的风险分析与评价结论为依据,将提升机的安全可靠性指标分配给各子系统或单元,确定各单元的安全可靠性定量要求,从而使整机安全可靠性指标得到保证,安全可靠性分配实际上是一个工程决策问题,随着目标函数和约束条件的不同,安全可靠性分配方法也不同,常用的有等同分配法、相对失效率法、AGREE 分配法等。

4.1 安全可靠性预计与分配^[6~10]

提升机各子系统之间、各子系统内部均可视为串联结构,它们的可靠度用乘法法则计算,当子系统的单元数量相当多时,用这种计算方法所得系统安全可靠度很低,甚至出现不能工作的情况。可以证明按乘法法则计算得到的系统安全可靠度是系统安全可靠度的下限,其上限是系统中安全性能最薄弱环节的可靠度。液压提升机安全可靠度预计式为

$$R = R_1 R_2 R_3 \cdots R_n \quad (1)$$

式(1)中, $R_1 \sim R_n$ 分别为各子系统的安全可靠度。一般而言,各子系统的可靠度均服从正态分布,则

$$R = e^{-\lambda t}, R_1 = e^{-\lambda_1 t}, \cdots, R_n = e^{-\lambda_n t} \quad (2)$$

$$\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_n \quad (3)$$

式(2),(3)中, λ 为整机失效率; $\lambda_1 \sim \lambda_n$ 为各子系统失效率。液压提升机的平均无故障时间(mean time between failure, MTBF)为:

$$MTBF = \frac{1}{\lambda} = \frac{1}{\lambda_1 + \lambda_2 + \cdots + \lambda_n} \quad (4)$$

目前矿井使用的液压提升机具有体积小、结构紧凑、安装灵活、操作简单及良好的防爆性能与容积调速和恒扭矩输出特性等优点,广泛应用于矿山井下作提升或下放人员、物料的主要设备。一般而言,液压提升机的 MTBF 多为 2~4 年。

将提升机的安全可靠性指标分配到每一个子系统及每个单元部件,可采用等同分配法、相对失效率法、AGREE 分配法、失效率差值分配法等,文章采用失效率差值分配法。其基本步骤为:

1) 由提升机规定的可靠性指标,计算出允许的总失效率 $\lambda_{允许}$;

2) 由可靠性预计,得出各子系统的预计总失效率 $\lambda_{预计}$;

3) 计算失效率差值: $\lambda_{差值} = \lambda_{预计} - \lambda_{允许}$;

4) 根据各子系统的危险分值大小,实现的可能性及经济性等,将 $\lambda_{差值}$ 分配到各子系统,得到失效率差值分配值;

5) 将各子系统预计的失效率减去失效率差值分配值,得各子系统的失效率分配值;

6) 依据子系统的危险分值大小,对失效率分配值进行再分配,若 $\lambda_{再预计} \leq \lambda_{允许}$,则分配方案可行,否则进行再分配。

以 BYT-2 型液压提升机为例进行安全可靠性预计与分配,从保守出发,取该液压提升机安全可靠性设计指标 MTBF = 20 000 h 计算,则液压提升机的总允许失效率 $\lambda_{允许}$ 为: $\lambda_{允许} = 1/MTBF = 5 \times 10^{-5} h^{-1}$ 。而液压提升机各子系统的预计总失效率 $\lambda_{预计}$ 为: $\lambda_{预计} = \lambda_1 + \lambda_2 + \cdots + \lambda_6 = 34.915 \times 10^{-5} h^{-1}$

根据液压提升机各子系统的危险分值大小、组成元、部件的工作可靠性情况和可靠性预计基本方法,分配各子系统安全失效率预计值(见表4)。失效率差值为: $\lambda_{差值} = \lambda_{预计} - \lambda_{允许} = 29.915 \times 10^{-5} h^{-1}$ 。参照各子系统预计失效率的比例、各子系统的危险分值大小,实现的可能性及经济性等,将 $\lambda_{差值}$ 分配到各子系统,得到失效率差值分配值(见表5)。根据可靠性分配步骤,将各子系统预计的失效率减去失效率差值分配值,得到各部件的失效率分配值(见表6)。 $\lambda_{再预计} = \lambda_1 + \lambda_2 + \cdots + \lambda_6 = 5 \times 10^{-5} h^{-1} = \lambda_{允许}$,此即提升机安全失效率的设计值,其可靠度设计值为 20 000 h。根据以上各子系统失效率分配值,即可进行各子系统的安全可靠性设计。

表4 各子系统安全失效率预计值

Table 4 Safety invalidation ratio value of subsystem

10 ⁻⁵ h ⁻¹					
驱动系统	制动系统	电气系统	操作系统	载荷系统	深度指示系统
2.893 5	7.716	11.574 1	5.787	4.629 6	2.314 8

表5 各子系统失效率差值分配值

Table 5 Distribution value of invalidation ratio margin of subsystem

10^{-5} h^{-1}					
驱动系统	制动系统	电气系统	操作系统	载荷系统	深度指示系统
2.479 1	6.611 1	9.916 5	4.958 3	3.966 6	1.983 3

表6 各子系统失效率分配值

Table 6 Distribution value of invalidation ratio of subsystem

10^{-5} h^{-1}					
驱动系统	制动系统	电气系统	操作系统	载荷系统	深度指示系统
0.414 4	1.104 9	1.657 6	0.828 7	0.663	0.331 5

4.2 子系统安全可靠性设计要点^[11,12]

得到各子系统的安全失效率后,即可进行各子系统的安全可靠性设计。它们的安全可靠性预计和分配方法与整机的方法完全一样,在此就不再重复进行,而只对子系统中相对薄弱的几个环节的安全可靠性设计要点进行分析。

4.2.1 人工操作的安全可靠性

对液压提升机而言,各子系统的安全可靠性在一定程度上受到人的操作安全性影响,因此,必须考虑人的操作安全可靠性,据统计由于人的差错引起的失效占设备失效的10%~15%。人的差错存在于从液压提升机设计到使用操作的全过程中,即包括设计、制造、操作、维修管理等过程的差错,特别是在操作过程中的人为差错有时不能及时纠正,常常引起事故。按人员操作次数考虑人的可靠性时,其可靠度基本方程为

$$R_H = 1 - e/n \quad (5)$$

式(5)中, e 为差错操作次数; n 为完成某项作业而应完成次数。

按连续作用时间来考虑人的可靠度时,可靠度可由式(6)计算:

$$R_H = e^{-\int_0^t e(t) dt} \quad (6)$$

式(6)中, $e(t)$ 为单位时间内人的差错率,统计规律表明,在液压提升机的设计、制造、操作、维修管理过程中操作差错率一般为 $3 \times 10^{-4} \sim 3 \times 10^{-3}$ 。可见,人的操作差错率也是影响提升机安全可靠性的一个重要因素。

4.2.2 液压制动系统薄弱环节可靠度计算

提升机液压制动系统为液压松开、碟形弹簧制

动的常闭式结构,依靠成组对称布置的制动缸的闸瓦抱紧制动盘实现制动。制动盘相对简单,而制动缸中含有的大量机械零部件,是系统安全可靠性的薄弱环节,其中最薄弱的是制动缸中制动弹簧及制动闸瓦,这是制动系统安全可靠性设计重中之重。一般而言,制动弹簧及制动闸瓦的应力与强度均呈正态分布,这时可用联结方程求出可靠度系数,然后利用标准正态分布表求出可靠度。图2所示是制动弹簧及制动闸瓦安全可靠性设计框图。

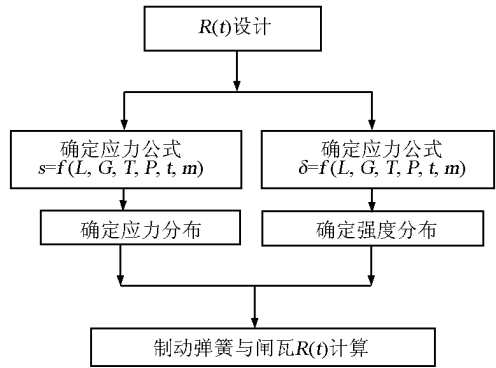


图2 制动弹簧及闸瓦可靠性设计

Fig. 2 Reliability design flow chart

应力的一般表达式为

$$s = f(L, G, T, P, t, m) \quad (7)$$

式(7)中, L 为载荷; G 为几何尺寸; T 为温度; P 为物理性质; t 为时间; m 为其他因素。强度的一般表达式为

$$\delta = f(\sigma_b, \sigma_{-1}, \varepsilon, \beta, k_f, k_t, m) \quad (8)$$

式(8)中, σ_b 为强度极限; σ_{-1} 为持久极限; ε 为尺寸系数; β 为表面质量系数; k_f 为环境系数; k_t 为疲劳应力集中系数; m 为其他因素。

这时应力 s 和强度 δ 的概率密度函数可进一步分别表示为

$$f(s) = \frac{1}{\sigma_s \sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{s - \mu_s}{\sigma_s}\right)^2\right] \quad (9)$$

$$g(\delta) = \frac{1}{\sigma_\delta \sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{\delta - \mu_\delta}{\sigma_\delta}\right)^2\right] \quad (10)$$

式(9),(10)中, μ_s, μ_δ 分别为应力的均值和标准差; σ_s, σ_δ 分别为强度的均值和标准差。据此,可写出可靠度的计算表达式

$$R(t) = \frac{1}{\sqrt{2\pi}} \int_{-\frac{\mu_\delta - \mu_s}{\sqrt{\sigma_\delta^2 + \sigma_s^2}}}^{\infty} e^{-\frac{z^2}{2}} dz \quad (11)$$

式(11)中,随机变量 $z = \frac{\mu_\delta - \mu_s}{\sqrt{\mu_\delta^2 + \mu_s^2}}$,也是标准

正态分布变量,实际上它把应力分布参数、强度分布参数和可靠度三者联结起来,所以称为联结方程或耦合方程。式(11)所表达的可靠度可通过查阅标准正态分布表求得。所以只要掌握强度和应力的均值和标准差则可以计算出提升机制动器的安全可靠度。

4.2.3 提高电控与监测电气系统可靠性的方法

电控与监测电气系统最大的安全是防爆,随着电控防爆与液压防爆技术的发展及各种防爆新理论、新技术与新元件的出现,提升机中的防爆问题已基本得到解决。但电气系统的可靠性对整机安全可靠度影响很大,因此必须确保电气系统的可靠性。常采用以下设计方法以确保其可靠性。

1)降额设计:其目的是减轻元器件的负担,在设计中取元器件的使用应力比其额定值小,降额程度根据元器件的类型和使用情况而定,降额设计的实质是提高电气产品的安全系数。

2)简化设计:在设计中,减少不必要的元件,提高产品的可靠性,简化设计可以从依靠软件功能减少硬件设备、采用新技术和新器件、优选和采用标准组件、压缩电源品种和数量、简化产品功能等几方面入手。

3)冗余设计:包括硬件与软件,当冗余为硬件时称为储备。为保证系统不会因一个元器件失效而不能运行,可采用逻辑技术进行设计,并对电子设备和非电子设备进行逻辑分析。目前由于微电子技术的发展,电子冗余可以做到小型化和微型化,增加的体积与重量有限。

4)提高产品连接部分的可靠度,也即提高接插件或焊接点等的可靠度。

此外还可用电磁兼容设计,进行元器件筛选等办法提高液压提升机电控系统的可靠度。

5 结语

1)矿井提升机的安全可靠度不仅影响整个矿井生产,而且危及人的生命安全。液压提升机应满足防爆、超速、过卷保护、过载过压保护、防坠保护等安全要求。而这些安全功能的实现依赖于电控与监测系统、液压驱动系统、液压制动系统、载荷系统、深度指示系统与操作系统子系统,各种危险及不安全

因素当然也存在于这些子系统之中。因此,对液压提升机开展危险分析与风险评价,并据此进行安全可靠度设计具有重大意义。

2)从危险分析和风险评价所确定的各子系统的危险分值来看,液压提升机的各子系统均有可能出现危险,但出现危险的概率不完全相同,产生危险时的伤害严重度也不完全相同,其中电控与监测系统、液压制动系统的危险分值相对较高,是安全设计的重点和关键。

3)根据各子系统的危险分值大小和可靠性预计基本方法,对各子系统安全失效率进行的预计分配用以指导液压提升机安全可靠度分析和设计,对高安全可靠度液压矿井提升机的进一步研究与开发提供了一定的理论依据,对保障矿井安全生产具有较大的实际意义。

参考文献

- [1] 国家安全生产监督管理总局. 煤矿安全规程[EB/OL]. http://www.chinasafety.gov.cn/zhengcefagui/2004-12/09/content_58351.htm, 2004-12-09
- [2] JB8516-1997. 矿井提升机和矿用提升绞车安全要求[S]. 北京:中国标准出版社,2006
- [3] 彭佑多. 液压提升机的安全功能与安全隐患分析[J]. 中国安全科学, 2001, (4): 25-28
- [4] 周水庭, 黄红武, 盛晓敏, 等. 普通磨床安全设计中的危险分析和风险评价[J]. 湖南大学学报, 2001, 24(8): 54-59
- [5] 盛晓敏, 黄红武, 刘健宁, 等. 机械安全设计方法的研究[J]. 中国机械工程, 2001, 12(12): 1354-1356
- [6] 葛世荣. 矿井提升机可靠性技术研究[M]. 北京:中国矿业大学出版社, 1994
- [7] 苏春. 关于安全系数法和可靠性设计的讨论[J]. 机械科学技术, 1997, 16(1): 35-38
- [8] 肖敏, 孙逸华. 机械的安全设计及其应用[J]. 机床与液压, 2003, 3: 242-243
- [9] 乐滨, 石端伟. 基于可靠性的机械安全系数设计方法的探讨[J]. 武汉大学学报, 2001, 34(2): 48-52
- [10] 杨光. 液压系统安全性设计简述. 机械研究与应用[J]. 2006, 18(1): 11-12
- [11] 孙志礼, 陈良玉. 实用机械可靠性设计理论与方法[M]. 北京:科学出版社, 2003: 271-289
- [12] 王成涛. 现代机械, 设计思想与方法[M]. 上海:上海科学技术文献出版社, 1999: 134-159

(下转 82 页)