DOI:10.3969/j.issn.1001 -4551.2018.05.013

基于 PFMEA 的雷达机电控制系统风险识别与改进研究

徐 俊
(中国电子科技集团公司 第三十八研究所,安徽 合肥 230088)

摘要:针对机电控制系统安全风险识别问题,对雷达机电液一体化控制系统进行了研究,对安全风险识别的原理和流程进行了归纳,提出了一种基于 PFMEA 机电控制系统安全风险识别与改进的方法。结合雷达机电控制系统使用过程,提出了运用 PFMEA 对过程事件进行归纳和识别安全隐患的方法,对事故发生后果的严重程度和可能性分别作了定义,建立了基于过程分解的 PFMEA 风险识别模型,提出了分析实施流程;以天线举升运动为例利用 PFMEA 模型对机电控制系统进行了安全风险分析、识别与改进。研究结果表明:该方法能够快速识别机电控制系统存在的安全风险点,以及从定性和定量的角度去衡量当前机电控制系统所处于的安全水平等级。

关键词:机电控制系统;过程故障模式与影响分析;安全风险
中图分类号:TH39;TN954 **文献标志码**:A **文章编号**:1001 -4551(2018)05 -0512 -05

Risk identification and improvement of radar electromechanical control system based on PFMEA

XU Jun
(The thirty-eighth Institute of China Electronics Technology Group Corporation, Hefei 230088, China)

Abstract: Aiming at the safety risk identification problem of electromechanical control system, the radar electro-mechanical and hydraulic integrated control system was studied, the principle and process of safety risk identification were summarized, and put forward a method about electromechanical control system security risk identification and improvement based on PFMEA. Combined with the process of radar electromechanical control system, the method of using PFMEA to summarize and identify the hidden dangers of process events were put forward, the severity and the possibility of accident consequences were defined, a PFMEA risk identification model based on process decomposition was proposed, and its analysis implementation process was presented. Taking the electromechanical control system to complete the antenna lifting movement as an example, the safety risk analysis, identification and improvement work were carried out by using PFMEA model. The results indicate that this method can quickly identify the safety risk points of the electromechanical control system and measure the safety level of the current electromechanical control system from the qualitative and quantitative view.

Key words: electromechanical control system; process failure modes and effects analysis(PFMEA); safety risk

0 引 言

机电控制系统作为雷达系统工作的重要一部分,其工作的可靠性和安全性直接影响着雷达整机的工作。雷达机电控制系统往往工作在复杂恶劣的外部环境和紧急的任务环境中,因此在研制、生产、使用、保障及处置等全生命周期过程中对产品机电系统的安全性要求也就越来越高[1-3]。

收稿日期:2017 -08 -29
作者简介:徐 俊(1988 -),男,安徽池州人,硕士研究生,工程师,主要从事机电控制、机电系统安全性方面的研究。E-mail:516999682@qq.com

文献[4]中提出运用 FMECA 对雷达机电系统进行系统及全面的可靠性分析,找出薄弱环节,并提出改进措施,有效提高了装备质量。在产品全生命周期过程中,系统性规划、规范化实施安全性工程,可以提高产品的安全性水平,同时还能够有效预防可能发生的事故和减少损失,降低研制和使用风险[5]。

本研究将运用过程故障模式与影响分析方法对雷达机电控制系统使用阶段进行安全风险识别分析[6-7],并针对安全问题风险点提出改进措施。

1　雷达机电液一体化控制系统

雷达机电液一体化控制系统是机动雷达的自动架设撤收控制系统,集机电液一体,包括计算机控制部分、机械执行机构和液压执行机构。在组成上,主要包括控制单元、检测单元、驱动单元和执行机构 4 个部分;从实现功能上,主要是完成雷达装备的自动架设、撤收以及天线的驱动。具体而言,包括支撑腿展开和收回、载车平台调平、天线举升和俯下、天线阵面升降、天线转台的旋转等。

2　PFMEA 风险识别模型及实施流程

PFMEA 是一种基于过程事件分解,由下至上的对过程事件进行归纳分析的方法。本研究主要用于因潜在风险导致事故的危险分析,具体的说,就是识别在过程事件中潜在的危险因素,并对其进行风险等级评估,属于一种定性的分析技术[8]。雷达机电控制系统在完成其相关的功能时,从时间的维度,也是基于过程的步骤或者事件来完成的。通常对机电控制系统使用过程的分析应选择存在安全隐患或重点关注的任务剖面进行 PFMEA 分析。

典型的雷达机电控制系统过程结构如图 1 所示。

过程是由一系列事件按照时间逻辑连接而成的,其中每个复杂的事件可往下分解若干个子事件,这些子事件自然就形成了若干个子过程,最底层的事件定义为基本事件。PFMEA 技术是将 FMECA 技术应用于过程分析的一种分析技术,PFMEA 按照过程的级别自下而上,分析每个级别子过程中的可能事件,以及该事件的故障模式和造成的影响程度。

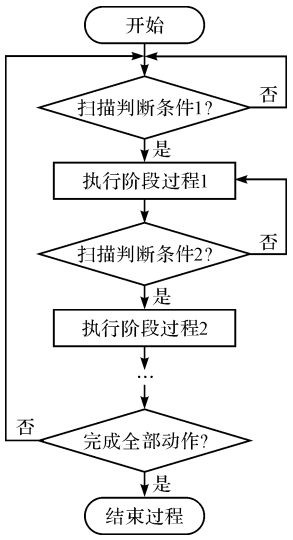

图 1　典型的雷达机电控制系统过程

根据故障模式最终可能造成的功能失效、任务失败、人员伤亡和环境破坏等方面影响程度,对事故发生的可能性和严重程度分别作了定义[9]。

事故严重性等级定义如表 1 所示。

表 1　事故的严重程度

严重性	发生后果	等级
致命或灾难	使整机或系统丧失功能,导致系统或环境重大损坏或造成人身伤亡或很大经济损失的事件	Ⅰ
严重	使系统丧失主要功能,造成较大损坏或经济损失的事件	Ⅱ
一般	导致任务延误或降级,一定的经济损失、人员轻度伤害	Ⅲ
轻微	不足以导致上述 3 类后果的故障,但会导致非计划维修	Ⅳ

事故发生可能性定义如表 2 所示。

表 2　事故发生可能性

发生程度	发生频次	等级
频繁	连续发生($P>10^{-1}$)	A
很可能	经常发生($10^{-1}>P>10^{-2}$)	B
有时	偶尔发生几次($10^{-2}>P>10^{-3}$)	C
很少	极少发生($10^{-3}>P>10^{-6}$)	D
不可能	几乎不发生($P<10^{-6}$)	E

结合对过程结构划分,本研究建立了 PFMEA 风

险识别的结构模型,如图 2 所示。

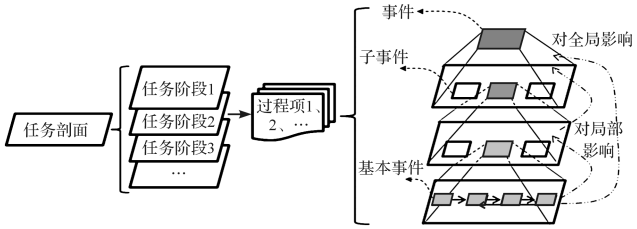

图 2 PFMEA 风险识别过程结构模型

PFMEA 分析实施工作主要依据上述的 PFMEA 风险识别过程结构模型来完成。首先确定分析对象和具体的任务剖面,对具体的阶段和阶段过程进行划分,对具体过程进行分解;在基本事件层面确定故障模式、故障原因以及带来的故障影响,随后确定危险的严重程度和发生可能性程度,建立必要的风险评价矩阵;下一步对已经存在的使用补偿措施进行分析,判断是否可以接受,以进一步决定是否增加设计补偿措施。

PFMEA 采用的是系统性、结构化的分析思路,通常运用列表分析来进行实施[10-11]。针对机电控制系统的分析,需要结合硬件自身和软件实现过程来进行。

典型的 PFMEA 分析实施流程如图 3 所示。

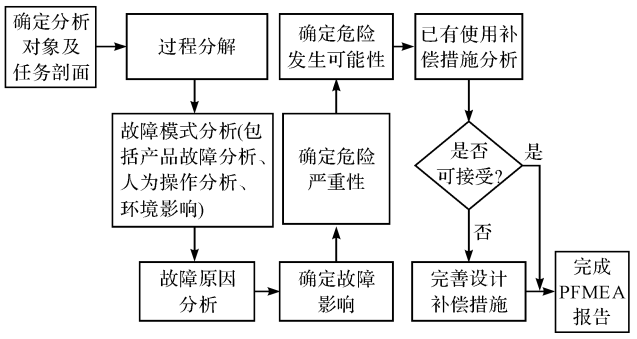

图 3 PFMEA 分析实施流程图

3 实例分析与改进

3.1 实例分析

本研究选取某雷达机电液一体化控制系统为分析对象,任务剖面是机电控制系统完成天线举升运动。由于在天线举升运动过程中,存在控制过程的两个阶段,在过程分解中需要区别对待。

机电控制系统功能分析如表 3 所示。

表 3 机电控制系统功能分析表

硬件	功能	目的
PCC 模块组	接收、分析、输出指令	逻辑控制输出电压
绝对式编码器	输出转轴位置脉冲	检测当前天线角度
24 V 电源	提供电源	给 PCC 和编码器、继电器输出供电
交流接触器	吸合/弹开	给泵站电机供电
继电器组	吸合/弹开	按照 PCC 输出指令输出 24 V
连接器	转接	将输出信号与外接电缆连通

其硬件结构原理图如图 4 所示。

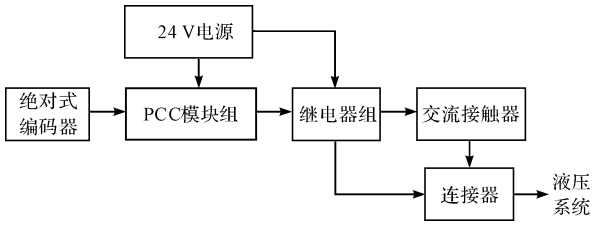

图 4 控制系统硬件结构原理图

在本研究的机电控制系统中,PCC 模块组为逻辑控制核心,举升运动过程中主要依据绝对式编码器反馈的位置脉冲数值做出不同的逻辑判断进而输出给继电器组,最终通过连接器输出至液压系统。本研究以取天线举升运动阶段一过程为例进行 PFMEA 风险识别分析。其中,任务阶段为:机电控制系统完成天线举升运动;目标过程为:天线举升过程第一阶段。

对天线举升运动阶段一过程分解如表 4 所示。

表 4 天线举升阶段一过程

一级过程		二级过程		三级过程	
序号	事件名称	序号	事件名称	序号	事件名称
100	天线举升运动一	110	绝对式编码器启动	111	数值输出范围(612 ~ 2 000)
				112	数值输出连续
		120	泵站启动	121	泵站启动电磁阀打开
		130	电磁阀给电	131	天线举升电磁阀打开
				132	大泵高压电磁阀打开
				133	上撑杆伸出电磁阀打开
				134	中撑杆收回电磁阀打开
				135	下撑杆收回电磁阀打开
				136	下背撑收回电磁阀打开
				137	供油调速阀打开
				138	回油调速阀打开

依据上述过程按照事件的时序关系进行逐步分

析,根据已经发生的故障和预期可能发生的故障,分析每一故障模式的原因以及该类故障模式对局部(三级过程)、上级事件(二级过程)、全过程(一级过程)事件的影响程度,评判故障事件所带来的严重性等级和发生可能性等级,在目前已有的补偿措施前提下,进一步提出相应改进措施。

对机电控制系统完成天线举升运动阶段一过程的 PFMEA 分析结果如表 5(部分节选)所示。

表 5　机电控制系统完成天线举升运动 PFMEA 表

项目代码	基本活动	功能	故障模式	故障原因	局部影响	对上级过程事件的影响	对全过程事件的影响	严重性等级	发生可能性等级	已有补偿措施	建议改进措施
			01 数值输出 <612	01 编码器器件损坏	显示天线角度与实际位置不符	绝对式编码器启动异常	天线会以第一级的油缸速度一直运行,会加快二级和三级油缸的伸出速度,从起点至终点,运动速度处于增长趋势,变缸时天线负载冲击较大	Ⅲ	C	在软件中对数值 < 550 已有互锁报警保护	考虑每套起始数值存在一定差异,底盘受压和正常支撑会影响起始的静态数值,需要进一步验证 550 的数值是否需要改善
111	数值输出范围(612 ~ 2 000)	标识天线运动角度	02 数值输出 >2 300	01 编码器器件损坏	显示天线角度与实际位置不符	绝对式编码器启动异常	天线主油缸举升外,撑杆也主动工作,在正常天线举升一过程中会损坏天线背撑杆件结构	Ⅱ	C	在软件中对数值 > 2 400 已有互锁报警保护	在 2 300 ~ 2 400 数值之间存在风险空挡,对这个范围的大小是否需要调整,做进一步的论证考虑是否需要在这个数值层次增加天线举升接近开关的状态判断以进一步验证编码器数值输出与天线负载实际位置是否一致
			03 数值输出在大于 2 000 小于 2 300 之间	…	…	…	…	…	…	…	…

在上述 PFMEA 结果分析表中,将故障影响严重性等级为列和发生可能性等级为行,建立起本研究实例的风险评价矩阵。在故障严重性和发生可能性等级基础上,风险评价矩阵的应用是从定量的角度去衡量当前处于的安全性水平,其中风险矩阵中评价指数范围从ⅠA ~ ⅣE,最高ⅠA 对应的是灾难性且频繁发生的后果,最低ⅣE 对应的是轻微且几乎不可能发生的后果。风险评价矩阵指数的不同,为后续改进工作优先顺序提供决策依据。建议的评价决策准则一般为:指数ⅠA、ⅠB、ⅠC、ⅡA、ⅡB、ⅢA,这类不可接受,必须立即采取措施;指数ⅠD、ⅡC、ⅡD、ⅢB、ⅢC,这类不希望发生,建议采取必要措施;指数ⅠE、ⅡE、ⅢD、ⅢE、ⅣA、ⅣB,这类考虑实际条件,评审是否可接受;指数ⅣC、ⅣD、ⅣE,这类可接受。

依据风险评价矩阵,本研究实例对机电系统完成天线举升运动阶段一过程风险评价指数主要有ⅡC、ⅡD、ⅢC、ⅢD 这 4 个类别,其中ⅡC、ⅡD 风险点各 1 个、ⅢC 风险点 2 个、ⅢD 风险点 4 个。由分析结果可知:天线举升运动阶段一过程存在的安全风险问题主要集中在器件质量及防护控制、机构状态监测不完善、可视化与安全报警措施设计不足等,具体为:

(1)器件质量及防护控制。在本例中,分析后的关键器件是编码器,其主要影响整个天线举升运动阶段一过程中各个杆件机构的协调动作,因此对于类似编码器同等重要性器件的质量和防护要求会更高。如果编码器容易受到外界干扰或外界高温、低温等恶劣环境影响,会给机构的运动带来巨大危害;

(2)机构状态监测不完善。存在运动机构间的协

调动作,对于开环控制系统而言,在安全性上是无法得到有效保证,比如本课题实例中液压电磁阀在得电后是否工作到指定位置以及对油缸是否按照预定要求方向进行运动,这些都直接影响功能的安全实现;

(3)可视化与安全报警措施设计不足。雷达装备使用中,会要求现场操作人员注意观察,但实际中存在一些关键器件数据输出、过程中关键运动指示对使用人员不可见的状态,或者软件保护检测范围有限以及在关键运动环节存在检测BUG等情况,这对装备健康状态的预判断都是非常不利的。

3.2 改进措施

通过系统分析,结合上述PFMEA分析结果,按照风险评价准则的要求,逐步开展后续改进工作。综合考虑现场实际情况和PFMEA表中的改进建议,确定以下改进工作内容:

(1)重新选型防护等级高的编码器,从抗干扰、防水等方面开展全面改进工作;

(2)确定装配电缆的工艺改进及信号传输要求;

(3)对机电液一体化控制系统开展半闭环或全闭环控制改进研究;

(4)改进控制软件,重新论证安全保护范围及措施;

(5)对关键动作和关键数据增加可视化装置和人机交互界面。

改进工作实施后的情况需要经过必要的验证试验、可靠性试验以及使用过程中实际效果,来进一步证明其有效性。

4 结束语

本研究结合机电控制系统功能实现过程的特点以及FMEA质量分析,提出了基于PFMEA过程分析模型的机电控制系统安全风险识别和改进的方法。

PFMEA方法的运用不仅能够快速识别机电控制系统功能实现过程的安全风险点,还能从定性和定量的角度去衡量当前机电控制系统所处于的安全水平等级。

参考文献(References):

[1] 赵廷弟.安全性设计分析与验证[M].1版.北京:国防工业出版社,2011.

[2] 康 锐,石荣德.FMECA技术及其应用[M].1版.北京:国防工业出版社,2006.

[3] 颜兆林,冉承新,刘敬军.基于PCED的过程控制系统安全分析方法[J].计算机工程,2009,35(22):122-124.

[4] 高红星,李 健.基于FMECA的某型机动雷达可靠性增长[J].电子产品可靠性与环境试验,2006,24(1):52-55.

[5] GJB/Z99-97.系统安全工程手册[S].北京:中国标准出版社,1997.

[6] STIRBU C,ANTON C,STIRBU L, et al. Improved by prediction of the PFMEA using the artificial neural networks in the electrical industry[C].2011 International Conference on Applied Electronics, Pilsen: IEEE Conference Publications, 2011.

[7] STAVROU D I,VENTIKOS N P. Risk evaluation of ship-to-ship transfer of cargo operations by applying PFMEA and FIS [C].2015 Annual Reliability and Maintainability Symposium (RAMS), Palm Harbor: IEEE Conference Publications, 2015.

[8] SHI Zhong, XIE Li-mei, LI Xiao-bing. Research of human error evaluation technique of production system based on PFMEA[C].2015 IEEE 10th Conference on Industrial Electronics and Applications, Auckland: IEEE Conference Publications,2015.

[9] GJB/Z1391-2006.故障模式、影响及危害性分析指南[S].北京:中国标准出版社,2006.

[10] 胡玺良.基于汽车可靠性技术的工艺潜在失效模式及影响分析(PFMEA)研究[D].合肥:合肥工业大学机械工程学院,2007.

[11] 胡 坤.多品种小批量定制生产模式PFMEA技术研究[D].南昌:南昌航空大学经济管理学院,2016.

[编辑:张 豪]

本文引用格式:

徐 俊.基于PFMEA的雷达机电控制系统风险识别与改进研究[J].机电工程,2018,35(5):512-516.

XV Jun. Risk identification and improvement of radar electromechanical control system based on PFMEA[J]. Journal of Mechanical & Electrical Engineering, 2018,35(5):512-516.

《机电工程》杂志:http://www.meem.com.cn