(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107065819 B
(45)授权公告日 2019.05.21

(21)申请号 201611240149.2

(22)申请日 2016.12.28

(65)同一申请的已公布的文献号
申请公布号 CN 107065819 A

(43)申请公布日 2017.08.18

(73)专利权人 中国航空工业集团公司西安飞机设计研究所
地址 710089 陕西省西安市阎良区人民东路1号

(72)发明人 黎娜 梅红 戚永灵 张军红

(74)专利代理机构 中国航空专利中心 11008
代理人 杜永保

(51)Int.Cl.
G05B 23/02(2006.01)

(56)对比文件
CN 103970656 A,2014.08.06,
CN 101377683 A,2009.03.04,
CN 1433535 A,2003.07.30,
WO 0109694 A1,2001.02.08,
JP 2011076210 A,2011.04.14,

审查员 张丹

权利要求书1页 说明书2页 附图1页

(54)发明名称

一种结合功能流程图的故障树建立方法

(57)摘要

本发明公开了一种结合功能流程图的故障树建立方法,包括以下步骤:1)根据功能危险分析报告FHA,列出故障树的顶事件;2)对照故障树的顶事件,绘制每个顶事件正常运行时的FFBD图;3)根据FFBD图绘制故障树的功能层;4)对应故障树的功能层,描述可能造成顶事件发生的设备的故障;5)分析设备的故障分析到每个LRU的故障,本层级的分析结束。本发明将基于模型的系统工程的功能流程图(FFBD图)引入故障树绘制过程中,用它来指导故障树的绘制,将基于模型的系统工程的模型同安全性分析的模型进行了对接,解决了基于模型的系统工程的模型与安全性模型割裂的问题,用MBSE的方法论更好的指导安全性的工作。

CN 107065819 B

1.一种结合功能流程图的故障树建立方法,其特征在于,包括以下步骤:

1)根据功能危险分析报告FHA,列出故障树的顶事件;

2)对照故障树的顶事件,绘制每个顶事件正常运行时的FFBD图;

3)根据FFBD图绘制故障树的功能层;

4)对应故障树的功能层,描述可能造成顶事件发生的设备的故障;

5)分析设备的故障分析到每个外场可更换部件LRU的故障,本层级的分析结束。

一种结合功能流程图的故障树建立方法

所属技术领域

[0001] 本发明属于飞机复杂系统的安全性分析技术领域，涉及一种结合功能流程图的故障树建立方法。

背景技术

[0002] 目前我们进行初步安全性分析时，借助故障树分析法，我们的故障树直接从顶事件分析到了设备的失效模式，中间缺少了功能层级，这样将设备与顶层功能之间对应，缺乏与底层功能的对应，不够严谨和严密。

[0003] 本发明将基于模型的系统工程的功能流程图(FFBD图)引入故障树绘制过程中，用它来指导故障树的绘制，将基于模型的系统工程的模型同安全性分析的模型进行了对接，解决了基于模型的系统工程的模型与安全性模型割裂的问题，用MBSE的方法论更好的指导安全性的工作。

发明内容

[0004] 本发明的目的是：本发明为了解决目前故障树缺乏功能层的问题，将基于模型的系统工程的功能流程图(FFBD图)引入故障树绘制过程中，用它来指导故障树功能层的绘制，而且将功能层与设备层进行了对接，从故障树上也可以直观、明了的看到需求分配的关系，这样就将需求分析与安全性从模型上结合起来，填补了目前安全性分析没有涉及功能层这个问题，此外将需求分析模型与安全性模型通过故障树建立了连接关系，解决了基于模型的系统工程的模型与安全性模型割裂的问题。

[0005] 本发明的技术方案是：

[0006] 本发明的优点是：本发明弥补了现有技术的不足，填补了故障树绘制直接从系统级到设备级的空白，使得安全性分析更为严谨和严密。提高了故障树的质量，减少了故障树绘制的迭代次数。故障树直观明了的反映了设备对功能的实现关系。

附图说明：

[0007] 图1为本发明实施例FFBD图；

[0008] 图2为本发明实施例故障树-“失去控制”图；

具体实施方式

[0009] 下面结合具体实施例对本发明做详细叙述。以“失去人工控制”为例：

[0010] 1)功能危险分析报告FHA中“失去人工控制”的功能为I类故障；

[0011] 2)根据功能发生的逻辑顺序和先后次序，绘制“人工控制”正常运行时的FFBD图，如图1所示，首先系统采集驾驶员的操纵指令，同时采集舵面的位置信息，综合两者的信息后，系统计算控制指令，然后根据控制指令驱动作动器对舵面进行控制；

[0012] 3)建立“失去人工控制”故障树，如图2所示，第一步绘制“失去人工控制”的顶事

件，用方框描述“失去人工控制”这个顶事件；

[0013] 3)结合图1，根据FFBD图绘制“失去人工控制”这个故障树的功能层，即“失去人工控制”可能由以下任一故障导致：失去驾驶员指令采集功能，丧失舵面位置信息采集功能，丧失控制指令计算功能，丧失作动器作动功能。采用或门对这一关系进行描述，当失去驾驶员指令采集功能，丧失舵面位置信息采集功能，丧失控制指令计算功能，丧失作动器作动功能任一发生，都会导致失去人工控制这一系统故障的发生。

[0014] 4)对应步骤3)的功能层，失去驾驶员指令采集功能可能是指令传感器全部故障导致，丧失控制指令计算功能可能计算机故障导致，丧失作动器作动功能可能是作动器故障导致，丧失舵面位置信息采集功能可能是舵面位置传感器故障导致，这样就将系统的功能故障与设备故障对应起来，注意当系统有多个功能由同一设备实现时，分析设备的主要功能，不需要对所有功能逐一分析，此外，故障树绘制的颗粒度适应本层级分析需要即可，并不是越细越好；

[0015] 5)再以“指令传感器全部故障”为例，指令传感器有两套：正驾驶员指令和副驾驶员指令，只有当两者指令均全部故障，指令传感器才会全部故障，因此“指令传感器全部故障”向下层分解时，采用与门，正驾驶员指令传感器全部故障和副驾驶员指令传感器全部故障，指令传感器全部故障。本实施例只建立了指令传感器的功能，其它计算机故障\作动器故障\舵面位置传感器故障类似。

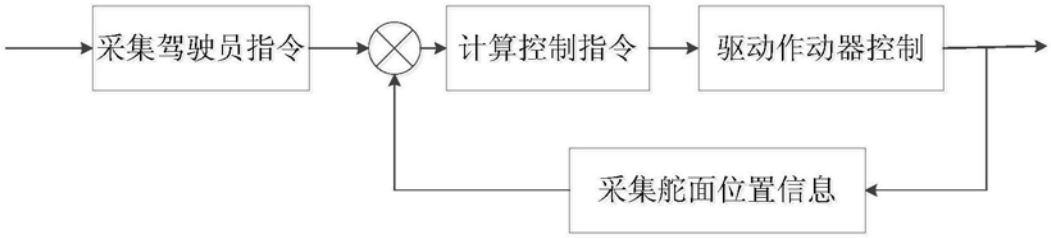
采集驾驶员指令
计算控制指令
驱动作动器控制
采集舵面位置信息

图1

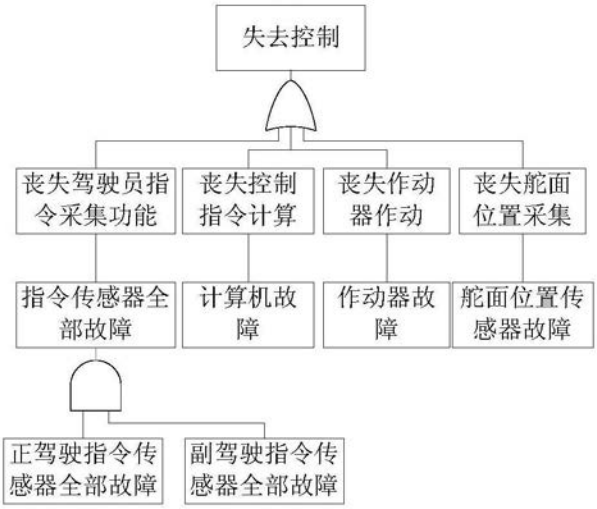
失去控制
丧失驾驶员指令采集功能
丧失控制指令计算
丧失作动器作动
丧失舵面位置采集
指令传感器全部故障
计算机故障
作动器故障
舵面位置传感器故障
正驾驶指令传感器全部故障
副驾驶指令传感器全部故障

图2