



(12)发明专利申请

(10)申请公布号 CN 107886208 A

(43)申请公布日 2018.04.06

(21)申请号 201611177208.6

(22)申请日 2016.12.19

(71)申请人 比亚迪股份有限公司

地址 518118 广东省深圳市坪山新区比亚迪路3009号

(72)发明人 王发平

其他发明人请求不公开姓名

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201

代理人 张润

(51)Int.Cl.

G06Q 10/06(2012.01)

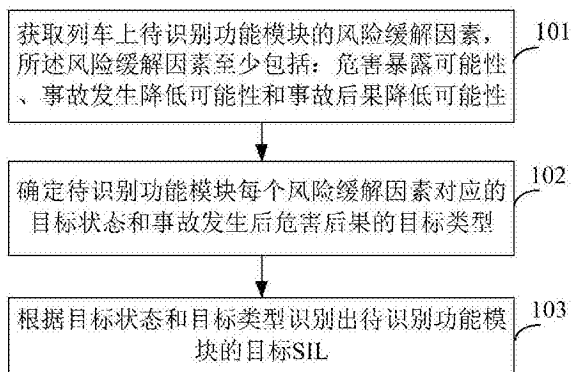
权利要求书4页 说明书17页 附图5页

(54)发明名称

轨道交通信号系统的安全完整性等级识别方法及装置

(57)摘要

本发明提出一种轨道交通信号系统的安全完整性等级识别方法及装置,其中,该方法包括:获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性,确定待识别功能模块每个风险缓解因素对应的目标状态和事故发生后危害后果的目标类型,根据目标状态和目标类型识别出待识别功能模块的目标安全完整性等级。本发明中在确定待识别功能模块的安全完整性等级时,考虑的风险缓解因素更加全面,不仅考虑了事故发生降低可能性,还考虑了事故后果降低可能性,进一步地,结合防护措施来确定最终的危害后果,更加遵循实际情况的考虑,从而能够更加准确地确定待识别功能模块的安全完整性等级,进而提高行车安全。



1. 一种轨道交通信号系统的安全完整性等级识别方法,其特征在于,包括:

获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性;

确定所述待识别功能模块每个风险缓解因素对应的目标状态和危害后果的目标类型;

根据所述目标状态和所述目标类型识别出所述待识别功能模块的目标安全完整性等级。

2. 根据权利要求1所述的轨道交通信号系统的安全完整性等级识别方法,其特征在于,所述根据所述目标状态和所述目标类型识别出所述待识别功能模块的目标安全完整性等级,包括:

将每个所述目标状态进行组合,得到目标排列组合;

获取事故发生后危害后果对应的不同状态下所述目标排列组合对应的所有安全完整性等级;

根据所述目标状态获取所述目标安全完整性等级。

3. 根据权利要求1所述的轨道交通信号系统的安全完整性等级识别方法,其特征在于,所述根据所述目标状态和所述目标类型识别出所述待识别功能模块的目标安全完整性等级,包括:

将每个所述目标状态进行组合,得到目标排列组合;

根据所述目标排列组合和所述目标类型在预设的安全完整性等级分配矩阵中查询,获取到所述目标安全完整性等级。

4. 根据权利要求3所述的轨道交通信号系统的安全完整性等级识别方法,其特征在于,所述获取列车上待识别功能模块的风险缓解因素之前,包括:

基于所有风险缓解因素所包括的状态和事故发生后危害后果对应的类型,构建所述安全完整性等级分配矩阵。

5. 根据权利要求4所述的轨道交通信号系统的安全完整性等级识别方法,其特征在于,所述基于所有风险缓解因素所包括的状态和事故发生后危害后果对应的类型,构建所述安全完整性等级分配矩阵,包括:

获取每个风险缓解因素所包括的状态;

逐次从每个缓解因素中选取一个状态作为目标对象,对所有所述目标对象进行排列组合;

将每个排列组合与事故发生后的危害后果的所有类型进行组合;

获取用户为不同类型下每个排列组合设置的安全完整性等级;

利用不同类型每个排列组合对应的安全完整性等级,构建所述安全完整性等级分配矩阵。

6. 根据权利要求4所述的轨道交通信号系统的安全完整性等级识别方法,其特征在于,所述基于所有风险缓解因素所包括的状态和事故发生后危害后果对应的类型,构建所述安全完整性等级分配矩阵,包括:

为每个风险缓解因素所包括的状态设置第一量值;

为危害后果对应的所有类型设置第二量值;

逐次从每个风险缓解因素中选取一个状态作为目标对象,对所有所述目标对象进行排

列组合；

将每个风险缓解因素中选取的所述目标对象的第一量值相乘，得到每个排列组合的组合量值；

将每个组合量值与危害后果的所有类型的第二量值相乘，得到不同类型下每个排列组合的最终量值；

根据不同类型下每个排列组合的最终量值，确定不同类型下每个排列组合对应的安全完整性等级；

利用不同类型下每个排列组合对应的安全完整性等级，构建所述安全完整性等级分配矩阵。

7. 根据权利要求6所述的轨道交通信号系统的安全完整性等级识别方法，其特征在于，所述根据所述目标排列组合和所述目标类型在预设的安全完整性等级分配矩阵中查询，获取到所述目标安全完整性等级，包括：

将每个所述目标状态对应的第一量值相乘，得到所述目标排列组合的目标组合量值；

在所述安全完整性等级分配矩阵中查询获取各安全完整性等级下所述目标排列组合对应的最终量值；

将所述目标组合量值和所述目标类型的第二量值相乘，得到目标类型下所述目标排列组合的目标最终量值；

从所述目标排列组合对应的所有安全完整性等级中，根据所述目标最终量值确定所述目标安全完整性等级。

8. 根据权利要求1-7任一项所述的轨道交通信号系统的安全完整性等级识别方法，其特征在于，所述确定所述待识别功能模块每个风险缓解因素对应的目标状态和事故发生后的危害后果的目标类型，包括：

对所述待识别功能模块在功能失效的情况下进行风险分析；

根据所述风险分析结果确定所述目标状态和所述目标类型。

9. 一种轨道交通信号系统的安全完整性等级识别装置，其特征在于，包括：

获取模块，用于获取列车上待识别功能模块的风险缓解因素，所述风险缓解因素至少包括：危害暴露可能性、事故发生降低可能性和事故后果降低可能性；

确定模块，用于确定所述待识别功能模块每个风险缓解因素对应的目标状态和事故发生后危害后果的目标类型；

识别模块，用于根据所述目标状态和所述目标类型识别出所述待识别功能模块的目标安全完整性等级。

10. 根据权利要求9所述的轨道交通信号系统的安全完整性等级识别装置，其特征在于，所述识别模块，包括：

第一组合单元，用于将每个所述目标状态进行组合，得到目标排列组合；

获取单元，用于获取事故发生后危害后果对应的不同状态下所述目标排列组合对应的所有安全完整性等级，以及根据所述目标状态获取所述目标安全完整性等级。

11. 根据权利要求10所述的轨道交通信号系统的安全完整性等级识别装置，其特征在于，所述识别模块，包括：

第二组合单元，用于将每个所述目标状态进行组合，得到目标排列组合；

查询单元,用于根据所述目标排列组合和所述目标类型在预设的安全完整性等级分配矩阵中查询,获取到所述目标安全完整性等级。

12.根据权利要求11所述的轨道交通信号系统的安全完整性等级识别装置,其特征在于,还包括:

构建模块,用于基于所有风险缓解因素所包括的状态和事故发生后危害后果对应的类型,构建所述安全完整性等级分配矩阵。

13.根据权利要求12所述的轨道交通信号系统的安全完整性等级识别装置,其特征在于,所述构建模块,具体用于:

获取每个风险缓解因素所包括的状态;

逐次从每个缓解因素中选取一个状态作为目标对象,对所有所述目标对象进行排列组合;

将每个排列组合与事故发生后危害后果对应的所有类型进行组合;

获取用户为不同类型下每个排列组合设置的安全完整性等级;

利用不同类型每个排列组合对应的安全完整性等级,构建所述安全完整性等级分配矩阵。

14.根据权利要求12所述的轨道交通信号系统的安全完整性等级识别装置,其特征在于,所述构建模块,具体用于:

为每个风险缓解因素所包括的状态设置第一量值;

为危害后果对应的所有类型设置第二量值;

逐次从每个风险缓解因素中选取一个状态作为目标对象,对所有所述目标对象进行排列组合;

将每个风险缓解因素中选取的所述目标对象的第一量值相乘,得到每个排列组合的组合量值;

将每个组合量值与危害后果的所有类型的第二量值相乘,得到不同类型下每个排列组合的最终量值;

根据不同类型下每个排列组合的最终量值,确定不同类型下每个排列组合对应的安全完整性等级;

利用不同类型下每个排列组合对应的安全完整性等级,构建所述安全完整性等级分配矩阵。

15.根据权利要求14所述的轨道交通信号系统的安全完整性等级识别装置,其特征在于,所述查询单元,具体用于:

将每个所述目标状态对应的第一量值相乘,得到所述目标排列组合的目标组合量值;

在所述安全完整性等级分配矩阵中查询获取各安全完整性等级下所述目标排列组合对应的最终量值;

将所述目标组合量值和所述目标类型的第二量值相乘,得到目标类型下所述目标排列组合的目标最终量值;

从所述目标排列组合对应的所有安全完整性等级中,根据所述目标最终量值确定所述目标安全完整性等级。

16.根据权利要求9-15任一项所述的轨道交通信号系统的安全完整性等级识别装置,

其特征在于,所述确定模块,具体用于:

对所述待识别功能模块在功能失效的情况下进行风险分析;
根据所述风险分析结果确定所述目标状态和所述目标类型。

轨道交通信号系统的安全完整性等级识别方法及装置

技术领域

[0001] 本发明涉及列车安全领域,尤其涉及一种轨道交通信号系统的安全完整性等级识别方法及装置。

背景技术

[0002] 目前多采用矩阵法或图表法,来分析一个系统中与安全相关的功能模块的安全完整性等级(Safety Integrity Level,简称SIL)。

[0003] 1、矩阵法

[0004] 表1为用于确定功能模块的SIL的矩阵。待识别的功能模块在功能失效的情况下所产生危害的可能性和后果的严重性,矩阵法就是利用头脑风暴的方式,定性确定该装置或者功能模块的SIL。一般情况下,可以将危害发生的可能性分为高、中、低三种类型,危害严重程度分为重大、严重、轻微三种情况,构成一个3×3的矩阵模型,如下1表所示。

[0005]	发生的 可能性	高	2	3*	3*
		中	1	2	3*
		低	NR	1	3
			轻微	严重	重大
			严重程度		

[0006] 表1中NR表示功能模块作为安全设备,*表示判定为SIL3的功能模块自身可能无法产生足够的控制措施降低风险,需要采取其他额外的缓解措施。

[0007] 通过分析该功能模块失效危害发生的可能性和产生的危害严重程度,然后查找SIL矩阵,就可定性为功能模块分配对应的SIL即安全完整性等级。

[0008] 2、图表法

[0009] 现有的图标法中考虑包括后果、处于危险的时间和频率、避开危险的概率和事件发生的频率四个因素,当待识别的功能模块出现功能失效这一事件,采用事件树与矩阵表相结合的方式对事件进行分析,以确定该事件的SIL。图1为现有确定功能模块的SIL的图表法。

[0010] 图1中C表示风险的后果参数,后果参数表示事故发生后后果的严重程度,C₁~C₄为后果参数的等级;F表示暴露参数,暴露参数为事故发生时,人员出现在暴露区域内的概率,F₁~F₂为暴露参数的等级;P表示避免参数,避免参数为事件发生时,避免出现危险的概率,P₁~P₂为避免参数的等级;W表示需求参数,需求参数为无安全防护时事故发生的概率,W₁~W₃需求参数的等级。图1中的矩阵中“——”标识无安全要求;“a”标识无特别安全要求;“1、2、3、4”表示安全完整性等级;“b”表示单个的电气电子器件不够成等级。

[0011] 现有的矩阵法只根据危害的严重性和发生的可能性来定义安全完整性等级,没有考虑风险缓解的因素,有些功能的失效导致危害原始风险等级很高,但系统其他功能可能

会对此危害有防护作用,如果不考虑这些,直接按照上述矩阵分配,可能导致所定义的安全完整性等级过高。而且现有的所定义的最高等级SIL3,主要针对电气、电子和可编程电子系统,应用在工控设备领域,不适用于轨道交通信号系统。

[0012] 现有的图表法虽然考虑了风险缓解因素,但是风险等级应由风险发生的概率和风险后果的严重程度两个维度决定,图表法仅考虑风险发生概率的避免情况,并未考虑后果严重程度降低的情况,直接从原始后果的严重性做事件树分析;其次,由于采用事件树的局限性,对危险暴露时间和避开危险的概率,只有两种情况进行区分不够全面。

[0013] 因此,基于上述矩阵法和图表法为待识别的功能模块确定的SIL,与实际应用中所要求的SIL并不一致,这样就有可能导致轻轨交通信号系统存在安全隐患。

发明内容

[0014] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

[0015] 为此,本发明的一个目的在于提出一种轨道交通信号系统的安全完整性等级识别方法,该方法在确定待识别功能模块的SIL时,考虑的风险缓解因素更加全面,不仅考虑了事故发生降低可能性,还考虑了事故后果降低可能性,进一步地,结合防护措施来确定最终的危害后果,更加遵循实际情况的考虑。

[0016] 本发明的另一个目的在于提出一种轨道交通信号系统的安全完整性等级识别装置。

[0017] 为达到上述目的,本发明第一方面实施例提出的轨道交通信号系统的安全完整性等级识别方法,包括:

[0018] 获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性;

[0019] 确定所述待识别功能模块每个风险缓解因素对应的目标状态和事故发生后危害后果的目标类型;

[0020] 根据所述目标状态和所述目标类型识别出所述待识别功能模块的目标安全完整性等级SIL。

[0021] 本发明第一方面实施例提出的轨道交通信号系统的安全完整性等级识别方法,在确定待识别功能模块的SIL时,考虑更多的风险缓解因素,不仅考虑了事故发生降低可能性,还考虑了事故后果降低可能性,进一步地,结合防护措施来确定最终的危害后果,更加遵循实际情况的考虑,从而能够更加准确地确定待识别功能模块的SIL,进而提高行车安全。

[0022] 为达到上述目的,本发明第二方面实施例提出的轨道交通信号系统的安全完整性等级识别装置,包括:

[0023] 获取模块,用于获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性;

[0024] 确定模块,用于确定所述待识别功能模块每个风险缓解因素对应的目标状态和事故发生后危害后果的目标类型;

[0025] 识别模块,用于根据所述目标状态和所述目标类型识别出所述待识别功能模块的目标安全完整性等级。

[0026] 本发明第二方面实施例提出的轨道交通信号系统的安全完整性等级识别装置,在确定待识别功能模块的SIL时,考虑更多的风险缓解因素,不仅考虑了事故发生降低可能性,还考虑了事故后果降低可能性,进一步地,结合防护措施来确定最终的危害后果,更加遵循实际情况的考虑,从而能够更加准确地确定待识别功能模块的SIL,进而提高行车安全。

[0027] 本发明附加的方面和优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本发明的实践了解到。

附图说明

[0028] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解,其中:

[0029] 图1为现有确定功能模块的SIL的图表法;

[0030] 图2为本发明实施例提供的一种轨道交通信号系统的安全完整性等级识别方法的流程示意图;

[0031] 图3为本发明实施例提供的一种构建SIL分配矩阵的流程示意图;

[0032] 图4为本发明实施例提供的另一种构建SIL分配矩阵的流程示意图;

[0033] 图5为本发明实施例提供的另一种轨道交通信号系统的安全完整性等级识别方法的流程示意图;

[0034] 图6为本发明实施例提供的一种轨道交通信号系统的安全完整性等级识别装置的结构示意图;

[0035] 图7为本发明实施例提供的一种识别模块的结构示意图;

[0036] 图8为本发明实施例提供的另一种识别模块的结构示意图;

[0037] 图9为本发明实施例提供的另一种轨道交通信号系统的安全完整性等级识别装置的结构示意图。

具体实施方式

[0038] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的模块或具有相同或类似功能的模块。下面通过参考附图描述的实施例是示例性的,仅用于解释本发明,而不能理解为对本发明的限制。相反,本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0039] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括一个或者更多个该特征。在本发明的描述中,“多个”的含义是两个或两个以上,除非另有明确具体的限定。

[0040] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为,表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分,并且本发明的优选实施方式的范围包括另外的实现,其中可以不按所示出或讨论的顺序,包括根据所涉及的功能按基本同时的方式或按相反的顺序,来执行功能,这应被本发明

的实施例所属技术领域的技术人员所理解。

[0041] 图2为本发明实施例提供的一种轨道交通信号系统的安全完整性等级识别方法的流程示意图,如图2所示,该轨道交通信号系统的安全完整性等级识别方法包括以下步骤:

[0042] S101、获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性。

[0043] 实际应用中,列车上的与安全相关的设备或者装置,可能会设置有防护措施,以降低当该设备或者装置失效时,这些防护错误能够为列车形成一些风险缓解因素,通过这些风险缓解因素来避免或者降低事故发生的概率。由于与安全相关的设备或者装置设置有防护措施,在该设备或者装置的功能失效后,该防护措施就可以形成一个事故发生降低可能性的风险缓解因素,通过设置的防护能够降低事故发生的可能性。在列车上设置有列车自动运行(Automatic Train Operation,简称ATO)。若ATO出现调速功能失效或发生故障的情况下,列车进行错误的速度调节,可能产生高于要求的速度,此时列车自动防护(Automatic Train Protection,简称ATP)会自动输出制动,不会导致脱轨或碰撞事故发生,可以降低事故发生的可能性,即通过该ATP防护为ATO形成一个事故发生降低可能性的风险缓解因素。

[0044] 当需要分析与安全相关的设备或者装置的SIL时,应该考虑这些风险缓解因素,以准确为与安全相关的设备或者装置分配相应的SIL,只有考虑了较多的风险缓解因素,才能为与安全相关的设备或者装置确定出适配的SIL。本实施例中,获取列车上待识别功能模块的风险缓解因素,其中,风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性。

[0045] S102、确定待识别功能模块每个风险缓解因素对应的目标状态和事故发生后危害后果的目标类型。

[0046] 实际应用中,每个风险缓解因素对应多个状态,不同的状态表示不同的可能性。本实施例中,为危害暴露可能性(Exposure Probability to Hazard)设置三个不同的状态,该危害暴露可能性风险缓解因素可以用字母E表示,三个状态分别表示为E1、E2、E3,用于表示风险承受主体如乘客暴露于危险中的可能。具体如下表2所示:

[0047] 表2

	危害暴露可能性	描述
[0048]	E1	危害发生时, 风险承受主体频繁或永久的暴露于危害中。
	E2	危害发生时, 风险承受主体偶尔或较少的暴露于危害中。
	E3	功能失效危害发生时, 风险承受主体只有极端情况才可能暴露于危害中, 或根本不可能暴露在危害中; 又或者根本不可能发生事故。

[0049] 进一步地,为事故发生降低可能性(Accident Probability Reduction)设置三个不同的状态,该事故发生降低可能性风险缓解因素可以用字母P表示,三个状态分别表示为P1、P2、P3,用于表示功能失效导致危害时,系统有额外的措施防护事故发生,降低事故发生

频率的可能。具体如下表3所示：

[0050] 表3

[0051]	事故发生降低可能性	描述
	P1	危害发生时，没有其他防护措施能够降低事故发生频率。
	P2	危害发生时，存在防护措施能够降低事故发生的频率。
	P3	危害发生时，存在两种或两种以上防护措施能够降低事故发生的频率；或者根本不可能发生事故。

[0052] 进一步地，为事故后果降低可能性 (Consequence Reduction Probability) 设置三个不同的状态，该事故后果降低可能性风险缓解因素可以用字母C表示，三个状态分别表示为C1、C2、C3，用于表示功能失效导致危害时，系统有额外的措施能够降低事故严重性的可能。具体如下表4所示：

[0053] 表4

[0054]	事故后果降低可能性	描述
	C1	危害发生时，没有其他防护措施能够降低事故后果严重性。
	C2	危害发生时，存在防护措施能够降低事故后果严重性。
	C3	危害发生时，存在两种或两种以上防护措施能够降低事故后果严重性；或者根本不可能发生事故。

[0055] 本实施例中，根据轨道交通信号系统特点可以将危害的后果分为灾难性的、严重的、不严重的、无关紧要的四种类型。危害后果分类具体如下表5所示：

[0056] 表5

[0057]

危害后果	描述
灾难性的	死亡事故和/或多人严重受伤
严重的	单一死亡事故和/或严重受伤
不严重的	轻微伤害
无关紧要的	可能造成轻微伤害或不会造成伤害

[0058] 具体地，对待识别功能模块在安全功能失效的情况下进行风险分析，根据风险分析结果确定出待识别功能模块在功能失效的情况下每个风险缓解因素的目标状态和目标类型。本实施例中，目标类型为考虑到待识别功能模块的风险缓解因素后，为其确定的最终

的危害后果对应的类型。

[0059] 例如,针对调速功能即ATO进行风险分析,分析后结果为:若列车上ATO的调速功能失效或发生故障,列车进行错误的速度调节,可能产生高于要求的速度,导致列车脱轨或与其他列车进行碰撞。但是,由于轨道交通信号系统中存在ATP子系统,具有超速防护功能,若ATO的调速功能失效,产生过高的速度时,ATP会输出制动,不会导致脱轨或碰撞事故发生,也就是说,可以降低事故发生的可能性,因此可以确定出ATO的事故降低可能性P的目标状态选择为P2,P2表示即危害发生时,存在防护措施能够降低事故发生的频率。由于列车为一个相对密闭且承载较多人员的交通工具,一旦列车脱轨或与其他列车碰撞的事故后,不能疏散人员或在事故中对人员提供保护,也就是说,虽然ATP的防护措施能够降低事故发生的概率,却无法降低事故后果的严重性,因此可以确定出ATO的事故后果降低可能性C的目标状态选择为C1,即危害发生时,没有其他防护措施能够降低事故后果严重性。由于轨道交通信号系统的行业特点,若发生事故,处于列车中的人员一定会暴露在危害事故中,因此可以确定出ATO的危险暴露可能性E的目标状态选择为E1,即危害发生时,风险承受主体频繁或永久的暴露于危害中。

[0060] 本实施例中,由于考虑到ATO设置有ATP的防护措施,ATO调速功能失效后,ATP可以自动输出制动,使得即使ATO的调速功能失效,并不能导致事故的发生,因此危害后果的目标类型应该确定为“无关紧要”或“不严重。”

[0061] S103、根据目标状态和目标类型识别出待识别功能模块的目标SIL。

[0062] 本实施例中,为每个风险缓解因数所包括的状态进行排列组合,然后用户可以预先设置不同类型下每个排列组合的SIL。具体地,将待识别功能模块每个风险缓解因素对应的目标状态进行组合,得到一个目标排列组合,获取目标排列组合在事故发生后危害后果的不同状态下的所有SIL,然后根据该目标状态获取待识别功能模块的目标SIL。

[0063] 在获取列车上待识别功能模块的风险缓解因素之前,还包括构建SIL分配矩阵的步骤:

[0064] 具体地,基于所有风险缓解因素所包括的状态和事故发生后危害后果对应的类型,构建一个SIL分配矩阵,其中,该SIL分配矩阵中包括每个排列组合在不同状态下的SIL。在确定出目标状态和目标类型后,优选地,就可以根据目标状态和目标类型在预设的SIL分配矩阵中查询,得到待识别功能模块的目标SIL。

[0065] 图3为本发明实施例提供的一种构建SIL分配矩阵的流程示意图。如图3所示,构建SIL分配矩阵过程包括以下步骤:

[0066] S201、获取每个风险缓解因素所包括的状态。

[0067] 关于每个风险缓解因素所包括的状态的介绍,可参见上表2~表4及相关内容的记载,此处不再赘述。

[0068] S202、逐次从每个缓解因素中选取一个状态作为目标对象,选取的所有目标对象进行排列组合。

[0069] 本实施例中,每个风险缓解因素所包括3个状态,分别为E1、E2、E3、P1、P2、P3、C1、C2和C3,逐次从每个风险缓解因素中选取一个状态作为目标状态,对选取的所有目标对象进行排列组合。例如,从E1、E2、E3中选择一个状态作为目标对象,如目标对象可以选择为E2;从P1、P2、P3中选择一个状态作为目标对象,如目标对象可以选择为P1;从C1、C2、C3中选

择一个状态作为目标对象,如目标对象可以选择为C2。从三个风险缓解因素中选取三个目标对象后,则对三个目标对象进行组合,得到E2P1C2。

[0070] 本实施例中,对E1、E2、E3、P1、P2、P3、C1、C2和C3进行排列组合后,可以得到27种组合方式。

[0071] S203、将每个排列组合与事故发生后的危害后果的所有类型进行组合。

[0072] 关于事故发生后的危害后果的所有类型的介绍,可参见上述表5及相关内容的记载,此处不再赘述。

[0073] 将每个排序组合与事故发生后的危害后果的所有类型进行组合,这样每个排列组合对应四个不同类型,例如E2P1C2这个排列组合对应的四个类型分别为灾难性的、严重的、不严重的和无关紧要的。

[0074] S204、获取用户为不同类型下每个排列组合设置的SIL。

[0075] 为不同的类型下每个排序组合设置对应的SIL。例如,灾难性的E2P1C2对应的SIL为SIL 3,严重的E2P1C2对应的SIL为SIL 2,不严重的E2P1C2对应的SIL为SIL 2,无关紧要的E2P1C2对应的SIL为SIL 1。

[0076] S205、利用在不同类型每个排列组合对应的SIL,构建SIL分配矩阵。

[0077] 具体地,可以将EPC组合,即三个风险缓解因素中三个状态的排列组合,作为纵列,事故后果的四种类型作为横行,具体得到的矩阵如下表6所示。

[0078]

EPC 组合	危害后果			
	灾难性的	严重的	不严重的	无关紧要的
E1P1C1	SIL4	SIL4	SIL3	SIL2
E1P2C1、E1P1C2、 E2P1C1	SIL4	SIL3	SIL2	SIL2
E1P3C1、E1P1C3、 E3P1C1、E2P2C1、 E2P1C2、E1P2C2	SIL3	SIL2	SIL2	SIL1
E1P2C3、E1P3C2、 E2P1C3、E2P3C1、 E3P1C2、E3P2C1、 E2P2C2	SIL2	SIL2	SIL1	SIL0
E1P3C3、E3P1C3、 E3P3C1、E2P2C3、 E2P3C2、E3P2C2	SIL2	SIL1	SIL0	SIL0
E2P3C3、E3P2C3、 E3P3C2	SIL1	SIL0	SIL0	SIL0
E3P3C3	SIL0	SIL0	SIL0	SIL0

[0079] 本实施例中的SIL分配矩阵与现有的矩阵法相比,在分配矩阵中引入三个风险缓解因素,全面考虑风险缓解因素能够更加正确的确定待识别功能模块的SIL。与现有的图表法相比,考虑的风险缓解因素更加全面,不只考虑事故发生概率的降低,还考虑了事故后果严重性的降低情况,并对这三个风险缓解因素赋予多个状态,利用所有状态进行多种排列组合,充分考虑系统存在多种防护功能时危害风险等级变化的情况。进一步地,本实施例中提供的SIL分配矩阵中的危害后果同样考虑了风险缓解因素,不是事故后果,而是采取防护措施后最终危害的结果,更加遵循实际情况的考虑。从而能够为待识别功能模块确定出更加精确的SIL。而且与现有图表法比较,本实施例中只采用矩阵方式更加简便,分配过程,只需对照矩阵查表即可,无需绘制事件树。

[0080] 本实施例提供的基于风险缓解因素构建的SIL分配矩阵与现有矩阵法以及现有图表法的区别如下表7所示:

[0081] 表7

[0082]

现有矩阵法	现有图表法	本实施例的 SIL 分配矩阵
无	危害暴露的可能性, 包括两种状态	危害暴露的可能性, 包括三种状态
事故发生的可能性, 不考虑实际是否降低	事故发生的可能性 事故发生降低可能性, 包括两种状态	事故发生降低可能性包括三种状态
事故后果严重程度, 不考虑实际是否降低	事故后果严重程度, 不考虑实际是否降低	事故后果降低可能性包括三种状态
无	无	风险降低后最终危害后果包括四种类型

[0083] 本实施例提供的轨道交通信号系统的安全完整性等级识别方法, 通过获取列车上待识别功能模块的风险缓解因素, 风险缓解因素至少包括: 危害暴露可能性、事故发生降低可能性和事故后果降低可能性, 确定待识别功能模块每个风险缓解因素对应的目标状态和危害后果的目标类型, 根据目标状态和目标类型识别出待识别功能模块的目标SIL。本实施例中, 确定待识别功能模块的SIL时, 考虑的风险缓解因素更加全面, 不仅考虑了事故发生降低可能性, 还考虑了事故后果降低可能性, 进一步地, 结合防护措施来确定最终的危害后果, 更加遵循实际情况的考虑, 从而能够更加准确地确定待识别功能模块的SIL, 进而提高行车安全。

[0084] 图4为本发明实施例提供的另一种构建SIL分配矩阵的流程示意图。如图4所示, 该构建SIL分配矩阵的过程包括以下步骤:

[0085] S301、为每个风险缓解因素所包括的状态设置第一量值。

[0086] 具体地, 在定义每个风险缓解因素所包括的状态时, 为每个状态设置一个第一量值。

[0087] 为危害暴露可能性 (Exposure Probability to Hazard) 的三个不同的状态E1、E2、E3设置第一量值。具体如下表8所示:

[0088] 表8

[0089]

危害暴露的可能性	第一量值	描述
E1	1	危害发生时，风险承受主体频繁或永久的暴露于危害中。
E2	0.1	危害发生时，风险承受主体偶尔或较少的暴露于危害中。
E3	0.01	功能失效危害发生时，风险承受主体只有极端情况才可能暴露于危害中，或根本不可能暴露在危害中；又或者根本不可能发生事故。

[0090] 进一步地，为事故发生降低可能性 (Accident Probability Reduction) 的三个不同的状态P1、P2、P3设置第一量值。具体如下表9所示：

[0091] 表9

[0092]

事故发生降低可能性	第一量值	描述
P1	1	危害发生时，没有其他防护措施能够降低事故发生频率。
P2	0.1	危害发生时，存在防护措施能够降低事故发生的频率。
P3	0.01	危害发生时，存在两种或两种以上防护措施能够降低事故发生的频率；或者根本不可能发生事故。

[0093] 进一步地，为事故后果降低可能性 (Consequence Reduction Probability) 的三个不同的状态C1、C2、C3设置第一量值。具体如下表10所示：

[0094] 表10

[0095]

事故后果降低可能性	第一量值	描述
C1	1	危害发生时，没有其他防护措施能够降低事故后果严重性。
C2	0.1	危害发生时，存在防护措施能够降低事故后果严重性。

[0096]

C3	0.01	危害发生时,存在两种或两种以上防护措施能够降低事故后果严重性;或者根本不可能发生事故。
----	------	---

[0097] S302、为危害后果对应的所有类型设置第二量值。

[0098] 进一步地,为危害后果的分类设置第二量值。具体如下表11所示:

[0099] 表11

[0100]

危害后果	第二量值	描述
灾难性的	1	死亡事故和/或多人严重受伤
严重的	0.1	单一死亡事故和/或严重受伤
不严重的	0.01	轻微伤害
无关紧要的	0.001	可能造成轻微伤害或不会造成伤害

[0101] S303、逐次从每个风险缓解因素中选取一个状态作为目标对象,对所有目标对象进行排列组合。

[0102] 具体过程可参见上述S202中相关内容的记载,此处不再赘述。

[0103] S304、将每个风险缓解因素中选取的目标对象的第一量值相乘,得到每个排列组合的组合量值。

[0104] 本实施例中,可以将每个风险缓解因素中选取的目标对象的第一量值相乘,得到每个排列组合的组合量值。例如,当从三个风险缓解因素中选取的目标对象分别为E2、P1、C2时,则将E2的第一量值、P1的第一量值和C2的第一量值相乘,就可以得到E2P1C2这一排列组合的组合量值为0.01。

[0105] 将E1、E2、E3、P1、P2、P3、C1、C2和C3进行排列组合,共得到27个排列组合,每个组合对应的量值乘积共有7种结果,分别为1、0.1、0.01、0.001、0.0001、0.00001、0.000001。为了表示方便,本实施例中,将7中结果表示为:1、1E-01、1E-02、1E-03、1E-04、1E-05、1E-06。

[0106] S305、将每个组合量值与危害后果的所有类型的第二量值相乘,得到不同类型下每个排列组合的最终量值。

[0107] 进一步地,将每个排列组合的组合量值与危害后果对应的所有类型的第二量值相乘,就可以得到不同类型下每个排列组合的最终量值。例如,排列组合为E2P1C2,该排列组合的组合量值为1E-02,则与危害后果对应的所有类型的第二量值相乘,得到的最终量值分别为:1E-02、1E-03、1E-04、1E-05。其中,1E-02为灾难性的危害后果下E2P1C2的最终量值,1E-03为严重的危害后果下E2P1C2的最终量值,1E-04为不严重的危害后果下E2P1C2的最终量值,1E-05为无关紧要的危害后果下E2P1C2的最终量值。

[0108] 每个EPC排列组合的组合量值作为纵列,事故后果所包括的四种类型第二量值作为横行,构成一个初始的SIL分配矩阵。该矩阵中每个格里的量值即为每个排列组合的最终量值,即为纵列和横行对应量值的乘积,具体如下表12所示:

[0109] 表12

[0110]

量值参数	EPC 组合	危害后果			
		灾难性的 1	严重的 1E-01	不严重的 1E-02	无关紧要的 1E-03
1	E1P1C1	1	1E-01	1E-02	1E-03
1E-01	E1P2C1、E1P1C2、 E2P1C1	1E-01	1E-02	1E-03	1E-04
1E-02	E1P3C1、E1P1C3、 E3P1C1、E2P2C1、 E2P1C2、E1P2C2	1E-02	1E-03	1E-04	1E-05
1E-03	E1P2C3、E1P3C2、 E2P1C3、E2P3C1、 E3P1C2、 E3P2C1、E2P2C2	1E-03	1E-04	1E-05	1E-06
1E-04	E1P3C3、E3P1C3、 E3P3C1、E2P2C3、 E2P3C2、E3P2C2	1E-04	1E-05	1E-06	1E-07
1E-05	E2P3C3、 E3P2C3、E3P3C2	1E-05	1E-06	1E-07	1E-08
1E-06	E3P3C3	1E-06	1E-07	1E-08	1E-09

[0111] S306、根据不同类型下每个排列组合的最终量值,确定不同类型下每个排列组合对应的SIL。

[0112] 在确定出不同类型下每个排列组合的最终量值后,就确定出不同类型下每个排列组合对应的SIL。例如,灾难性的危害后果下E2P1C2的SIL为3,严重的危害后果下E2P1C2的SIL为2,不严重的危害后果下E2P1C2的SIL为2,无关紧要的危害后果下E2P1C2的SIL为1。

[0113] S307、利用不同类型下每个排列组合对应的SIL,构建SIL分配矩阵。

[0114] 在获取到不同类型下每个排列组合对应的SIL,就可以利用不同类型下每个排列组合对应的SIL,构建SIL分配矩阵。本实施例中,结合轨道交通信号系统的实际情况,将最终量值在1E-09到1E-06的待识别功能模块的SIL设置为SIL0,将最终量值在1E-05的待识别功能模块的SIL设置为SIL1,将最终量值在1E-04至1E-03的待识别功能模块的SIL设置为SIL2,将最终量值在1E-02的待识别功能模块的SIL设置为SIL3,将最终量值在1E-01至1的待识别功能模块的SIL设置为SIL4。在上述初始的SIL分配矩阵即表12的基础上,增加不同类型下每个排列组合对应的SIL,然后构建一个SIL分配矩阵如下表13所示:

[0115] 表13

[0116]

量值参数	EPC 组合	危害后果			
		灾难性的 1	严重的 1E-01	不严重的 1E-02	无关紧要的 1E-03
1	E1P1C1	1	1E-01	1E-02	1E-03
		SIL4	SIL4	SIL3	SIL2
1E-01	E1P2C1、E1P1C2、 E2P1C1	1E-01	1E-02	1E-03	1E-04
		SIL4	SIL3	SIL2	SIL2
1E-02	E1P3C1、E1P1C3、 E3P1C1、E2P2C1、 E2P1C2、E1P2C2	1E-02	1E-03	1E-04	1E-05
		SIL3	SIL2	SIL2	SIL1
1E-03	E1P2C3、E1P3C2、 E2P1C3、E2P3C1、 E3P1C2、 E3P2C1、E2P2C2	1E-03	1E-04	1E-05	1E-06
		SIL2	SIL2	SIL1	SIL0
1E-04	E1P3C3、E3P1C3、 E3P3C1、E2P2C3、 E2P3C2、E3P2C2	1E-04	1E-05	1E-06	1E-07
		SIL2	SIL1	SIL0	SIL0
1E-05	E2P3C3、 E3P2C3、E3P3C2	1E-05	1E-06	1E-07	1E-08
		SIL1	SIL0	SIL0	SIL0
1E-06	E3P3C3	1E-06	1E-07	1E-08	1E-09
		SIL0	SIL0	SIL0	SIL0

[0117] 本实施例中,在构建SIL分配矩阵时,不只考虑事故发生概率的降低,还考虑了事故后果严重性的降低情况,即考虑了更多的风险缓解因素,风险缓解因素包括危害暴露可能性、事故发生降低可能性以及事故后果降低可能性等与风险变化相关的因素,并对这三个风险缓解因素设置多个状态,并且其状态分别赋予量值,划分的更加详细,根据风险缓解因素所包括的所有状态,得到排列得到更多的风险组合,并且充分考虑系统存在多种防护功能时,在采取防护措施后最终的危害后果的等级变化的情况。而且本实施例中在SIL分配矩阵中增加SIL4和SIL0,使得为轨道交通信号系统中各功能模块分配SIL时,更加遵循实际情况的考虑,从而能够更加准确地确定待识别功能模块的SIL,进而提高行车安全。

[0118] 图5为本发明实施例提供的另一种轨道交通信号系统的安全完整性等级识别方法

的流程示意图。在上述图4所示的构建SIL分配矩阵的基础上,如图5所示,该轨道交通信号系统的安全完整性等级识别方法包括以下步骤:

[0119] S401、获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性。

[0120] S402、确定待识别功能模块每个风险缓解因素对应的目标状态和事故发生后危害后果的目标类型。

[0121] S403、将每个目标状态进行组合,得到目标排列组合。

[0122] 关于S401~S403的介绍,可参见上述实施例中相关内容的记载,此处不再赘述。

[0123] S404、将每个目标状态对应的第一量值相乘,得到目标排列组合的目标组合量值。

[0124] 在确定出每个目标状态后,就可以却出该目标状态对应的第一量值,将每个状态的第一量值相乘,得到目标排列组合的目标组合量值。例如,每个风险缓解因素对应的目标状态分别为E1、P2和C1,则目标排列组合为E1P2C1,E1的第一量值为1,P2的第一量值为0.1,C1的第一量值为1,则该目标排列组合E1P2C1的目标组合量值为0.1,即 $1E-01$ 。

[0125] S405、在SIL分配矩阵中查询获取各SIL下目标排列组合对应的最终量值。

[0126] 进一步地,在SIL分配矩阵中查询获取到各SIL下目标排序组合对应的最终量值。根据表13所示的SIL分配矩阵,可以得到目标排序组合E1P2C1对应SIL4、SIL3、SIL2,则目标排序组合E1P2C1对应的SIL4的最终量值为 $1E-01$ 、SIL3的最终量值为 $1E-02$ 、SIL2的最终量值为 $1E-03$ 和 $1E-04$ 。

[0127] S406、将目标组合量值和目标类型的第二量值相乘,得到目标类型下目标排列组合的目标最终量值。

[0128] 将目标组合量值再与目标类型的第二量值相乘,则可以得到目标类型下目标排列组合的目标最终量值。例如,目标类型为严重的危害后果,则目标类型的第二量值为0.1,则E1P2C1的目标最终量值为0.01,即 $1E-02$ 。

[0129] S407、从目标排列组合对应的所有SIL中,根据目标最终量值确定目标SIL。

[0130] 在得到目标排列组合的目标最终量值后,就可以从目标排序组合的所有SIL中,根据该目标最终量值确定出该待识别功能模块的目标SIL。由于E1P2C1的目标最终量值为 $1E-02$,则可以确定出目标SIL为SIL3。

[0131] 例如,对ATP超速防护功能进行危害分析,分析结果为若列车超速防护功能失效或发生故障,列车产生高于要求的速度时不能采用制动措施,导致列车脱轨或与其他列车进行碰撞。

[0132] 如果ATP超速防护功能失效,没有其他措施能够避免事故发生,也就是说,无法降低事故发生的可能性,因此可以确定出ATP的事故降低可能性P的目标状态选择为选择P1,即危害发生时,没有其他防护措施能够降低事故发生频率。由于列车为一个相对密闭且承载较多人员的交通工具,一旦列车脱轨或与其他列车碰撞的事故后,不能疏散人员或在事故中对人员提供保护,也就是说,虽然ATP的防护措施能够降低事故发生的概率,却无法降低事故后果的严重性,因此可以确定出ATP的事故后果降低可能性C的目标状态选择为C1,即危害发生时,没有其他防护措施能够降低事故后果严重性。由于轨道交通信号系统的行业特点,若发生事故,处于列车中的人员一定会暴露在危害事故中,因此可以确定出ATP的危险暴露可能性E的目标状态选择为E1,即危害发生时,风险承受主体频繁或永久的暴露于

危害中。

[0133] 由此可得,ATP的目标排列组合为E1P1C1,考虑到ATP超速防护失效后,危害没有任何降低缓解措施,危害会导致事故发生,因此后果应为“灾难性的”或“严重的”,根据以上分析,查找基于风险缓解因素的SIL分配矩阵可知ATP装置的安全完整性等级应为SIL4。

[0134] 根据轨道交通行业标准,ATO装置一般为SIL2的装置,ATP ATP装置为SIL4装置,从而本实施例提供的基于风险缓解因素构建的SIL分配矩阵,能为待识别功能模块分配更加准确的安全完整性等级。

[0135] 本实施例提供的轨道交通信号系统的安全完整性等级识别方法,通过获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性,确定待识别功能模块每个风险缓解因素对应的目标状态和事故发生后的危害后果的目标类型,根据目标状态和目标类型识别出待识别功能模块的目标SIL。本实施例中,确定待识别功能模块的SIL时,考虑的风险缓解因素更加全面,不仅考虑了事故发生降低可能性,还考虑了事故后果降低可能性,进一步地,结合防护措施来确定最终的危害后果,更加遵循实际情况的考虑,从而能够更加准确地为待识别功能模块的SIL,进而提高行车安全。

[0136] 图6为本发明实施例提供的一种轨道交通信号系统的安全完整性等级识别装置的结构示意图。如图6所示,该轨道交通信号系统的安全完整性等级识别装置包括:获取模块11、确定模块12和识别模块13。

[0137] 其中,获取模块11,用于获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性。

[0138] 确定模块12,用于确定所述待识别功能模块每个风险缓解因素对应的目标状态和事故发生后危害后果的目标类型。

[0139] 识别模块13,用于根据所述目标状态和所述目标类型识别出所述待识别功能模块的目标SIL。

[0140] 图7为本发明实施例提供的一种识别模块的结构示意图。如图7所示,该识别模块13包括:第一组合单元131和获取单元132。

[0141] 第一组合单元131,用于将每个所述目标状态进行组合,得到目标排列组合。

[0142] 获取单元132,用于获取事故发生后危害后果对应的不同状态下所述目标排列组合对应的所有SIL,以及根据所述目标状态获取所述目标SIL。

[0143] 图8为本发明实施例提供的另一种识别模块的结构示意图。如图8所示,该识别模块13包括:第二组合单元133和查询单元134。

[0144] 第二组合单元133,用于将每个所述目标状态进行组合,得到目标排列组合。

[0145] 查询单元134,用于根据所述目标排列组合和所述目标类型在预设的SIL分配矩阵中查询,获取到所述目标SIL。

[0146] 本实施例提供的轨道交通信号系统的安全完整性等级识别装置,通过获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性,确定待识别功能模块每个风险缓解因素对应的目标状态和事故发生后的危害后果的目标类型,根据目标状态和目标类型识别出待识别功能模块的目标SIL。本实施例中,确定待识别功能模块的SIL时,考虑的风险缓解因素更加全面,不

仅考虑了事故发生降低可能性,还考虑了事故后果降低可能性,进一步地,结合防护措施来确定最终的危害后果,更加遵循实际情况的考虑,从而能够更加准确地为待识别功能模块的SIL,进而提高行车安全。

[0147] 图9为本发明实施例提供的另一种轨道交通信号系统的安全完整性等级识别装置的结构示意图。如图9所示,该轨道交通信号系统的安全完整性等级识别装置包括上述实施例中的获取模块11、确定模块12和识别模块13,还包括:构建模块14。

[0148] 其中,识别模块13包括:第二组合单元133和查询单元134。

[0149] 构建模块14,用于基于所有风险缓解因素所包括的状态和事故发生后危害后果对应的类型,构建所述SIL分配矩阵。

[0150] 进一步地,构建模块14,具体用于:

[0151] 获取每个风险缓解因素所包括的状态;

[0152] 逐次从每个缓解因素中选取一个状态作为目标对象,对所有所述目标对象进行排列组合;

[0153] 将每个排列组合与事故发生后危害后果对应的所有类型进行组合;

[0154] 获取用户为不同类型下每个排列组合设置的SIL;

[0155] 利用不同类型每个排列组合对应的SIL,构建所述SIL分配矩阵。

[0156] 进一步地,构建模块14,具体用于:

[0157] 为每个风险缓解因素所包括的状态设置第一量值;

[0158] 为危害后果对应的所有类型设置第二量值;

[0159] 逐次从每个风险缓解因素中选取一个状态作为目标对象,对所有所述目标对象进行排列组合;

[0160] 将每个风险缓解因素中选取的所述目标对象的第一量值相乘,得到每个排列组合的组合量值;

[0161] 将每个组合量值与危害后果的所有类型的第二量值相乘,得到不同类型下每个排列组合的最终量值;

[0162] 根据不同类型下每个排列组合的最终量值,确定不同类型下每个排列组合对应的SIL;

[0163] 利用不同类型下每个排列组合对应的SIL,构建所述SIL分配矩阵。

[0164] 进一步地,查询单元134,具体用于:

[0165] 将每个所述目标状态对应的第一量值相乘,得到所述目标排列组合的目标组合量值;

[0166] 在所述SIL分配矩阵中查询获取各SIL下所述目标排列组合对应的最终量值;

[0167] 将所述目标组合量值和所述目标类型的第二量值相乘,得到目标类型下所述目标排列组合的目标最终量值;

[0168] 从所述目标排列组合对应的所有SIL中,根据所述目标最终量值确定所述目标SIL。

[0169] 进一步地,确定模块12,具体用于:

[0170] 对所述待识别功能模块在功能失效的情况下进行风险分析;

[0171] 根据所述风险分析结果确定所述目标状态和所述目标类型。

[0172] 本实施例提供的轨道交通信号系统的安全完整性等级识别装置,通过获取列车上待识别功能模块的风险缓解因素,所述风险缓解因素至少包括:危害暴露可能性、事故发生降低可能性和事故后果降低可能性,确定待识别功能模块每个风险缓解因素对应的目标状态和事故发生后的危害后果的目标类型,根据目标状态和目标类型识别出待识别功能模块的目标SIL。本实施例中,确定待识别功能模块的SIL时,考虑的风险缓解因素更加全面,不仅考虑了事故发生降低可能性,还考虑了事故后果降低可能性,进一步地,结合防护措施来确定最终的危害后果,更加遵循实际情况的考虑,从而能够更加准确地为待识别功能模块的SIL,进而提高行车安全。

[0173] 应当理解,本发明的各部分模块或它们的组合来实现。在上述实施方式中,多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如,如果用硬件来实现,和在另一实施方式中一样,可用本领域公知的下列技术中的任一项或他们的组合来实现:具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路,具有合适的组合逻辑门电路的专用集成电路,可编程门阵列(PGA),现场可编程门阵列(FPGA)等。

[0174] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通程序来指令相关的硬件完成,所述的程序可以存储于一种计算机可读存储介质中,该程序在执行时,包括方法实施例的步骤之一或其组合。

[0175] 此外,在本发明各个实施例中的各功能单元可以集成在一个处理模块中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用,也可以存储在一个计算机可读取存储介质中。

[0176] 上述提到的存储介质可以是只读存储器,磁盘或光盘等。

[0177] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何一个或多个实施例或示例中以合适的方式结合。

[0178] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

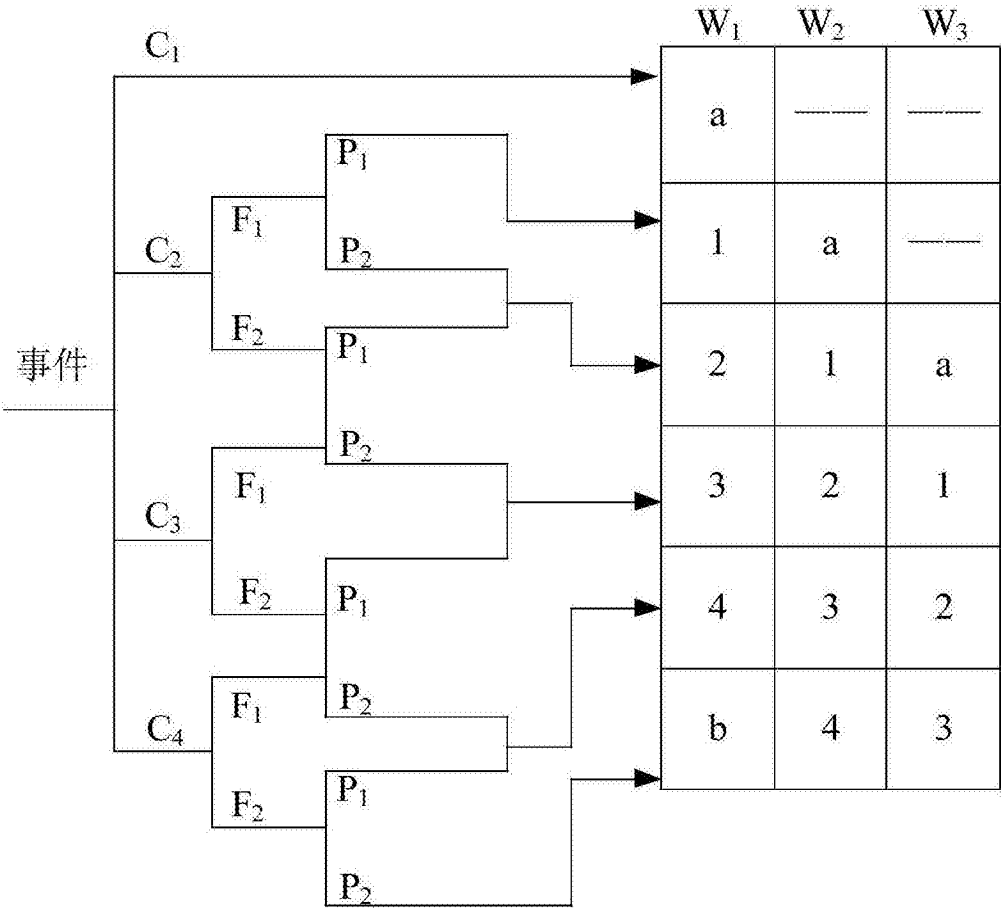


图1

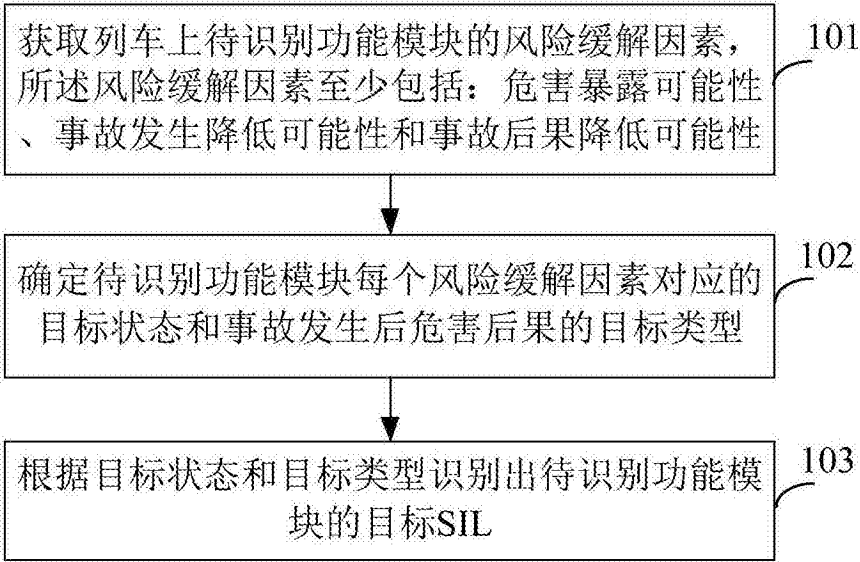


图2

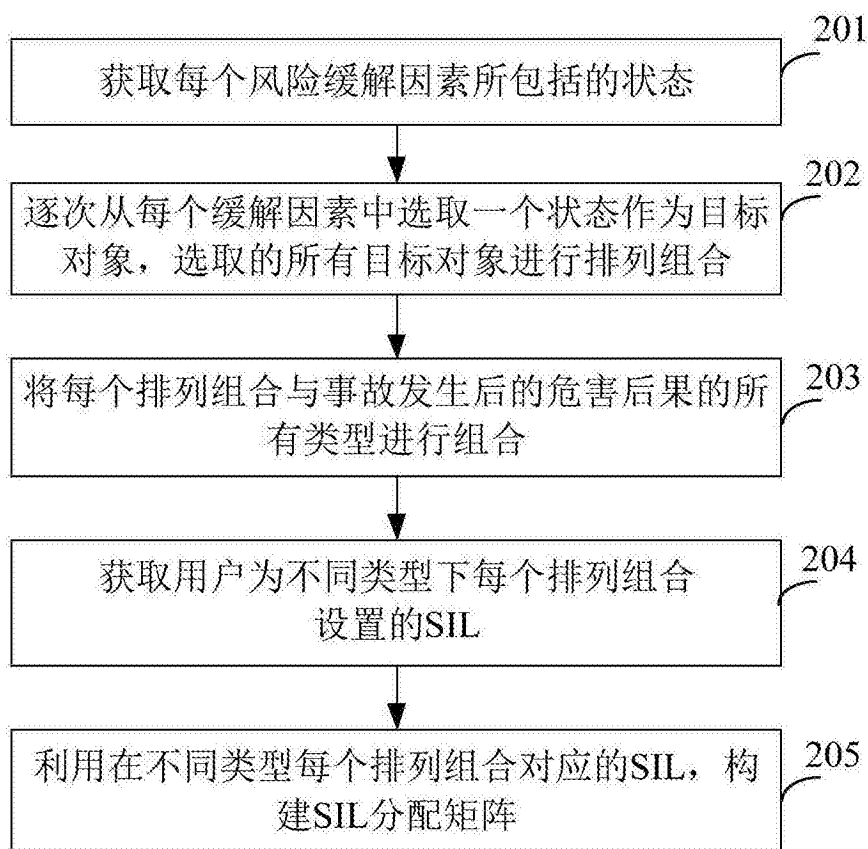


图3

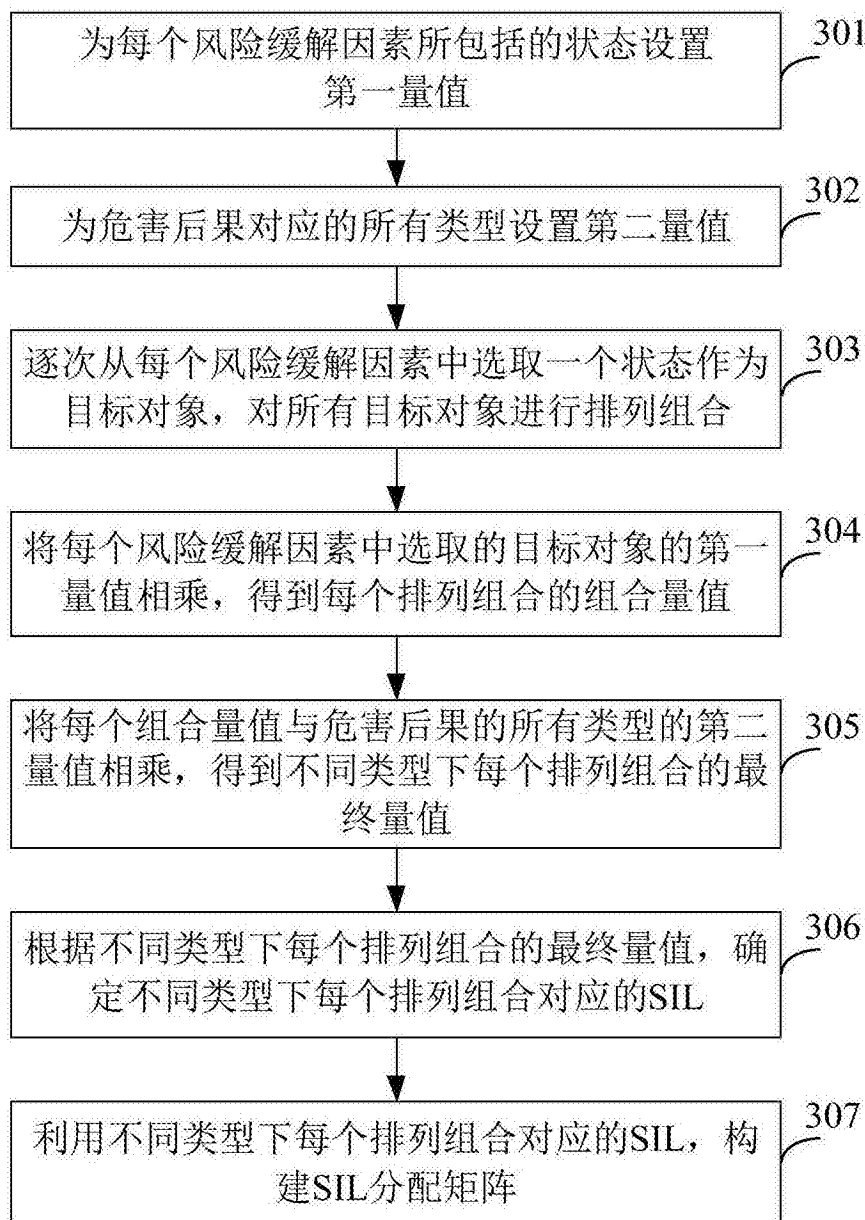


图4

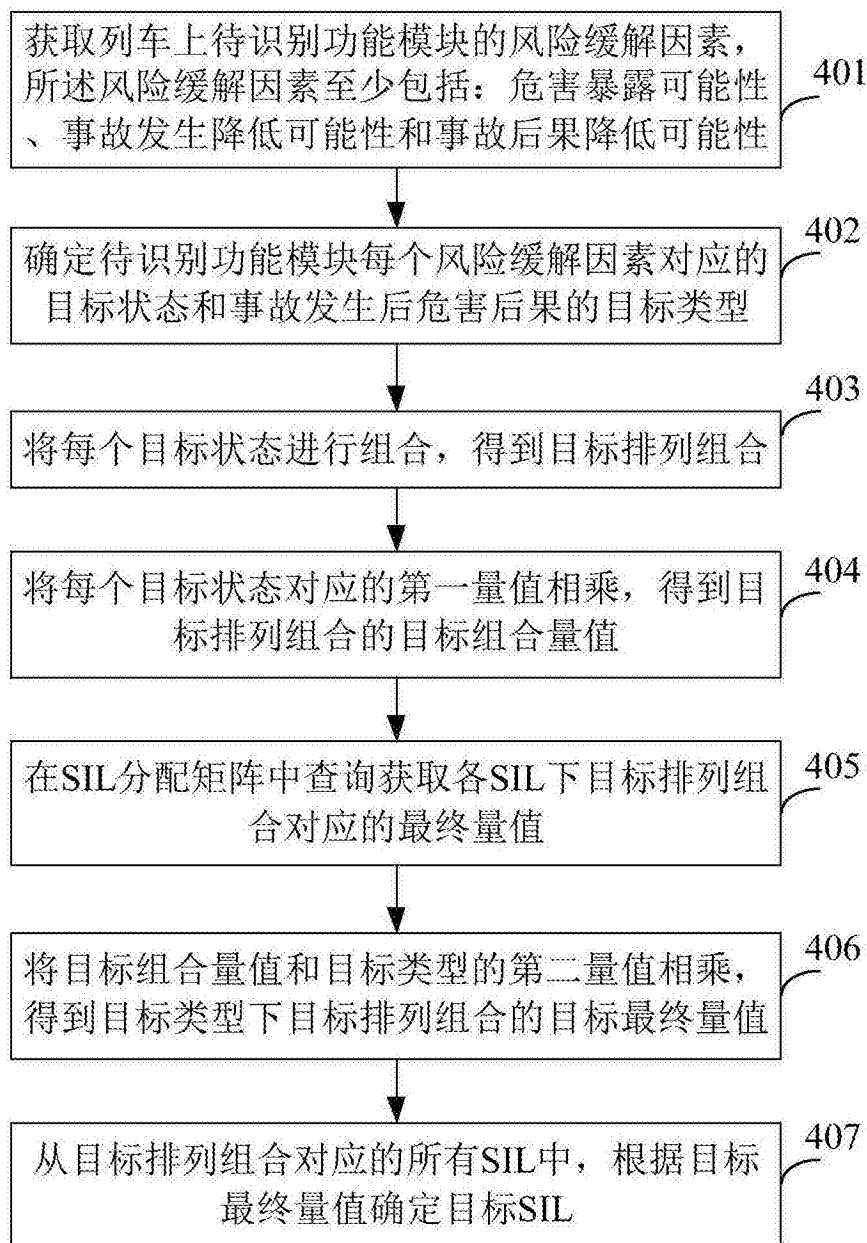


图5

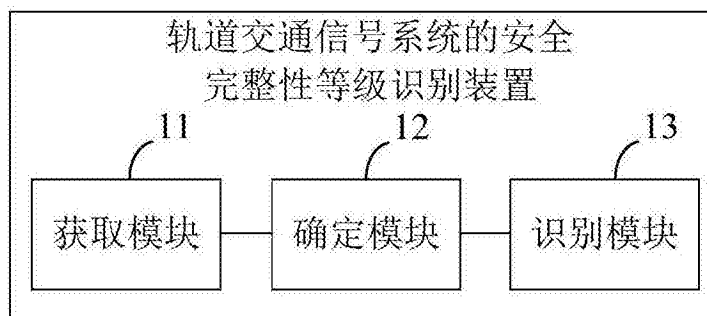


图6

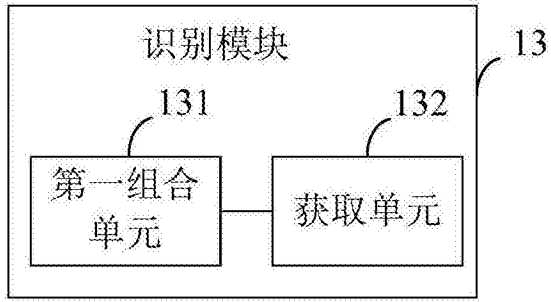


图7

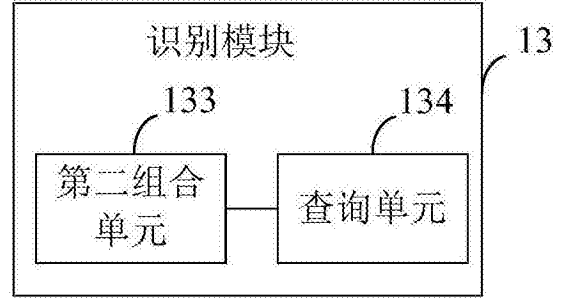


图8

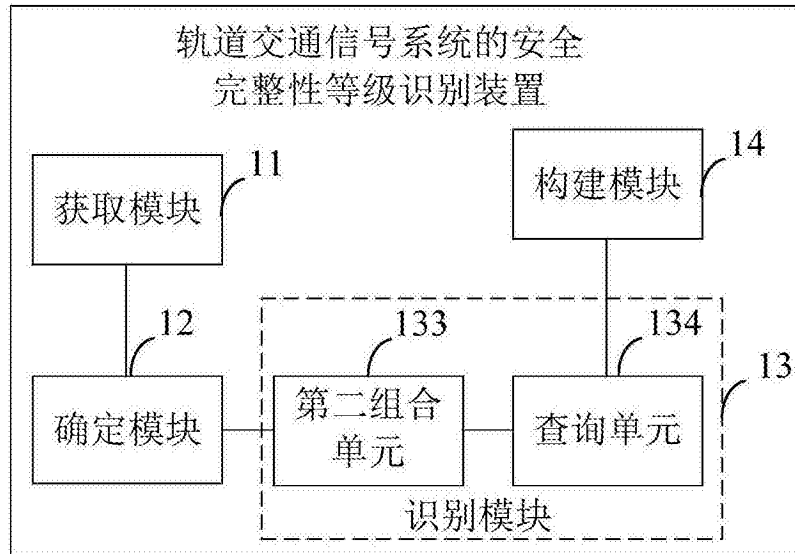


图9