文章编号:1006-8244(2019)02-037-07

功能安全硬件指标计算的实践

The practice of hardware metric calculation for functional safety

罗来军 李 兵
(联创汽车电子有限公司,上海市 201206)
Luo Laijun Li Bing
(DIAS Automotive Electronic Systems Co., Ltd, Shanghai 201206)

[摘要]目前在汽车电控系统的开发中,功能安全的重要性越来越高,功能安全标准中硬件度量指标是比较重要的定量评价指标。本文通过实践的经验对硬件指标计算相关的概念进行了举例解释,对硬件指标计算的相关步骤和注意事项进行了说明,并对操作方法给出了一些建议。

[**Abstract**]Recently in the development of automotive electronic control systems, the functional safety of the system becomes more and more important. In the standard of functional safety, the hardware metric is an important quantitative requirement. Based on practical experience, this article gives interpretation of the vocabulary using examples, explanation of the procedure and matters in the calculation procedure, and gives some advice about the execution method.

关键词:功能安全 失效率 失效模式后果及诊断分析 故障树分析 诊断覆盖率

Key words: Functional Safety Failure rate (FIT) FMEDA (Failure Mode, Effect and Diagnostic Analysis) FTA (Fault Tree Analysis) Diagnostic Coverage

中图分类号:TP391.4 **文献标识码**:B

0 引言

目前随着汽车技术的发展,车辆上各种驾驶辅助功能越来越多,无人驾驶的研发现在也在如火如荼地进行。随着这些辅助驾驶和无人驾驶功能的增加,汽车电控系统的功能安全越来越受到重视,2011 年发布的 ISO26262 是汽车领域功能安全的国际标准,在此基础上中国国家标准 GB/T 34590 也于 2017 年发布。

功能安全对系统开发、软件与硬件开发、生产售后、功能安全管理以及安全分析等各个方面都提出了相应的要求,其中对硬件度量指标有具体的量化要求,分别是单点故障度量 SPFM(Single Point Fault Metric),潜伏故障度量 LFM(Latent Fault Metric)和随机硬件失效概率度量 PMHF(Probabilistic Metric for random Hardware Failures)。这三个指标不仅涉及到硬件的设计和分析,也需要考虑整个系统的安全机制,包括相应的软件诊断等。这些安全机制需要在计算硬件指标时进行考虑,才能得到最终的硬件指标计算值。

在硬件度量指标计算过程中,会遇到一些操作的具体问题。本文通过在项目中的具体实践,对硬件指标计算中的相关概念和相关步骤进行了解释,并对分析计算过程给出了一些操作方法的建议。

1 硬件指标计算的准备

硬件度量指标的计算涉及一些概念定义,也需要得到计算所需相关的数据,本章对故障类型、失效率、诊断覆盖率等的含义进行了介绍,并对实践中的具体情况进行了相关说明供参考。

1.1 硬件故障的分类

功能安全标准中将硬件故障进行了如下分类:单点故障、残余故障、多点故障以及安全故障。其中多点故障中三点及以上的故障通常也被认为是安全故障(特殊情况除外),双点故障又细分为可探测的双点、可感知的双点以及潜伏的双点[1,2,3,4]。

作者简介:罗来军(1973-),男,博士,高级工程师,2002 年毕业于上海交通大学车辆工程专业,长期从事汽车底盘电子的控制系统开发工作。
E-mail:luolaijun@dias.com.cn

这样硬件故障的分类变为如下:安全故障、单点故障、残余故障、可探测的双点故障、可感知的双点故障以及潜伏的双点故障。根据故障的时间特性还可以将硬件故障分为瞬时故障和永久故障。以下通过具体实践解释如何理解各个故障,如何对不同部件的故障进行分类。

1.1.1 安全故障

安全故障分为两类,一类情况是该部件和安全无关,那么它的任意故障都是安全故障。比如 PCB 板上用于调试的 LED 灯,它的故障一般不会引起系统输出的变化。

另一类情况是该部件和安全有关,它的一种或几种故障类型也可以是安全故障。比如控制器设计的基本原则之一通常是没有供电时需要保证系统安全,电源处理电路和控制器的功能实现相关,因此和安全相关。但是其中导致控制器无法供电的故障会使得系统进入安全状态,这部分故障就是安全故障。再比如看门狗误触发的故障,该故障也会使得系统进入安全状态,这部分故障也属于安全故障。

需要注意的是这两类安全故障对硬件指标计算的影响是不同的。和安全无关的部件故障失效率不纳入硬件指标的计算公式中,这种安全故障对硬件指标的计算完全没有影响。和安全有关部件的安全故障会纳入硬件指标的计算公式中,这部分安全故障失效率的增加会使得单点故障度量 SPFM 和残余故障度量 LFM 增加,对随机硬件失效概率度量 PMHF 则没有影响。

1.1.2 单点故障

单点故障是指该故障发生后,会直接导致系统违背安全目标,系统中没有任何安全机制来对这种故障进行诊断和处理。对于功能安全等级最高为 ASIL C 和 ASIL D 的系统,功能安全标准规定对此类故障的诊断覆盖率不应低于 90%,否则需增加专用措施。一般情况下,单点故障在 ASIL C 和 ASIL D 系统中不会出现。

1.1.3 残余故障

残余故障是指该故障发生后,也会直接导致系统违背安全目标。系统对于单点故障会采取相应的安全机制来对进行诊断和处理,但是安全机制一般不能完全覆盖单点故障的全部可能性,即诊断覆盖率一般不能达到 100%。功能安全标准对于诊断覆盖率建议了低中高三个等级,分别为 60%、90%、99%。因此单点故障实施安全机制后,一般都会产生相应的残余故障,如采用 99%诊断覆盖率的安全机制时残余故障比例为 1%。

单点故障和残余故障是单点故障度量 SPFM 考察的对象,这两个故障失效率数值的增加会使得 SPFM 降低。因此要尽量避免单点故障,即增加相应的安全机制;同时降低残余故障,即提高安全机制的诊断覆盖率。

单点故障和残余故障也是随机硬件失效概率度量 PMHF 考察的对象,降低这两个故障失效率数值也可以降低随机硬件失效概率度量 PMHF。

1.1.4 可探测的双点故障

首先解释双点故障的含义:如果两个独立的故障同时发生后会使得系统违背安全目标,那么这两个独立的故障都属于双点故障。

目前实践中分析得到的双点故障都是某个故障(称之为故障 X)与其对应的安全机制失效的故障(称之为故障 Y),这两个故障互为双点故障。其中如果没有安全机制,故障 X 会导致系统违背安全目标。安全机制失效的故障 Y 分为两部分,一部分是诊断失效,即无法诊断出故障 X;另一部分为执行失效,即正确诊断后无法将系统切换到安全状态。

可探测的双点故障指的是这两个独立故障被探测到的部分。故障 X 没有被安全机制覆盖的部分属于残余故障,可以直接违背安全目标,不属于双点故障;故障 X 被安全机制覆盖的部分故障会被探测到,同时也会通过指示灯等提示驾驶员并记录故障,因此这部分被覆盖的部分属于可探测的双点故障。如果对安全机制也进行诊断,同时通过指示灯等提示驾驶员并记录故障,那么诊断到的安全机制的故障也属于可探测的双点故障。

1.1.5 可感知的双点故障

可感知的双点故障是指双点故障中没有被探测到,但是可以被驾驶员感知到的故障。假如系统诊断到故障 X 的发生,也采取了安全措施,但是没有对驾驶员进行提醒,驾驶员有可能通过系统性能的改变来感知到有故障发生,那么这种情况应该归属于可感知的双点故障。目前实践中没有遇到可感知的双点故障,一般情况下系统中没有此类故障。

如前所述,故障 X 只包含残余故障和可探测的双点故障,因此它不含可感知的双点故障。如果不对相应的安全机制进行诊断,安全机制发生故障时系统性能一般不会受影响,这种情况下安全机制的故障也无法通过驾驶员感知到,当叠加故障 X 后就会直接违背安全目标,也不属于可感知的双点故障。

1.1.6 潜伏的双点故障

潜伏的双点故障是指双点故障中没有被探测

到,也没有被驾驶员感知到的故障。

如前所述,安全机制的故障被诊断覆盖到的部分也属于可探测的双点故障,另外没有被诊断覆盖的部分则属于潜伏的双点故障。

潜伏的双点故障是潜伏故障指标 LFM 考察的对象,提高对安全机制检测的诊断覆盖率,会增加可探测的双点故障失效率同时降低潜伏的双点故障失效率,进而提高潜伏故障指标 LFM。

潜伏的双点故障也对随机硬件失效概率度量 PMHF 有所贡献,它和对应的双点故障同时发生会使得系统违背安全目标,这两个故障同时发生的概率需要在 PMHF 中进行计算。由于双点故障互相独立,两个故障同时发生的概率等于两个故障单独发生的概率的乘积,因此与残余故障相比,潜伏的双点故障对 PMHF 的贡献通常不大。降低潜伏的双点故障也可以稍稍降低随机硬件失效概率度量 PMHF。

1.1.7 瞬时故障和永久故障

瞬时故障指的是发生后就消失的故障,比如 RAM 数据中的一位数据在外界干扰下由 0 变为 1,之后如果再次对 RAM 数据进行写操作结果仍会是正常的,这种故障就是瞬时故障,瞬时故障通常最迟在下次上电初始化时就会恢复正确状态。

永久故障发生后则不会消失和恢复,比如 RAM 数据中的一个数据位发生故障始终为 1,无法写入 0,发生永久故障后对 RAM 数据进行读写操作都无法修复故障。

需要考虑瞬时故障的一般是集成电路 IC 以及存储单元等。瞬时故障对 SPFM 和 LFM 以及 PMHF 都有影响。由于瞬时故障通常最迟在下次上电初始化时会恢复,它的存在时间最长是一个驾驶周期,在通过 PMHF 计算双点故障时,瞬时故障的影响一般可以忽略。

1.2 失效率 FIT 数值和诊断覆盖率的确定

计算硬件度量指标时需要得到各部件的失效率 FIT(Failures in Time)数值以及相应安全机制的诊断覆盖率数值,本节对这些数值的来源进行说明和建议。

1.2.1 失效率 FIT 数值来源

功能安全标准中对于失效率 FIT 数值的来源规定有三种:业界公认的失效率标准、统计数据以及专家评估[2,4]。

失效率 FIT 数值的单位是每 10^{-9} 小时发生一次故障,功能安全标准对 FIT 数值的置信度有要求,如果通过统计数据来得到 FIT 数值,那么需要庞大的统计数据量才能得到比较精确的结果。如果统计数据量较小,为了提高统计结果的置信度,必然得到比较保守即比较大的 FIT 数值,进而影响后续硬件指标计算的结果。如果投放市场产品的产量比较大,通过对售后故障的统计可以得到相对准确的 FIT 值,这种情况下需要对售后故障件的返回与分析有很好的监控和管理,同时这种方法也并不适用于新开发中采用的新元器件。因此由统计数据得到 FIT 值的方法一般不采用。

专家评估的方法也需要有一定的试验数据做基础同时对评估方法也有要求,这种得到 FIT 数值的方法通常也不采用。

目前汽车行业功能安全硬件指标计算的实践中,FIT 数值的来源通常都是业界公认的失效率标准,其中最常用的是两个:IEC/TR 62380 和 SN 29500,这两个标准得到的 FIT 数值的置信度都可以达到 99%[2,4]。这两个标准用来计算元器件的永久故障,对于瞬态故障可以参考标准 JESD89A,关于瞬态故障的数据建议向供应商索取。

1.2.2 FIT 数值计算所需参数

硬件元器件分为电阻、电容、电感、IC 等类别,其中每个类别又分为不同的类型,比如 SN 29500 标准中将电阻分为 Carbon film, Networks(film circuits), Metal film, Metal-oxide, Wire-wound, Variable 等类型[5]。在通过标准计算 FIT 数值时首先需要确定元器件的具体类型。部分类型还需要了解具体的元器件参数,比如门电路的数量等[5,6],通常需要供应商提供相关参数。

同一个元器件在不同的使用条件和使用环境下,发生失效的概率是不同的,在根据 IEC/TR 62380 以及 SN 29500 计算各个部件的失效率 FIT 数值时,都需要确定相关的环境和条件参数,来计算得到符合实际使用情况的 FIT 值。

在计算失效率 FIT 值时,不同类型元器件的参数是不同的;同一类型元器件在不同标准(IEC/TR 62380 和 SN 29500)中使用的参数也是不同的。在实际应用过程中需要根据器件的类型和选择的标准,确定所需的相关参数,计算得到 FIT 数值。

其中温度参数对于失效率的影响比较大,两个标准中都有温度相关的参数。在 IEC/TR 62380 中温度是作为 Mission Profile 来使用的,Mission Profile 需要定义不同温度所占的时间以及系统开启和关闭的次数等参数。在 SN 29500 里温度是作为平均温度使用的。在确定温度参数时,需要确定元器件所处环境的温度,也要确定元器件在工作过程中

的温升情况。

环境温度可以参考 IEC/TR 62380 里给出的汽车领域的两个 Mission Profile(Motor control 和 Passenger compartment),也可以根据试验数据进行选取。元器件的温升则需要根据元器件的实际功率以及元器件的温度系数等进行计算得到。

1.2.3 失效模式来源

硬件指标计算中需要根据各个元器件的各个故障模式进行分析,因此,在得到元器件的整体失效率后,需要根据故障模式的百分比确定各个故障模式的失效率 FIT 数值。

功能安全标准中对于失效模式及其百分比的来源规定也有三种,和 FIT 数值来源一样:业界公认的失效率标准、统计数据以及专家评估[2,4]。

基于类似的原因,目前功能安全硬件指标计算的实践中,失效模式和百分比的来源通常也是业界公认的标准,其中比较常用的有:IEC/TR 62380、IEC 61709 以及 EN 62601 等。功能安全标准附录中有一些关于失效模式的说明,也可以作为参考。

1.2.4 诊断覆盖率来源

在确定残余故障以及潜伏的双点故障的失效率 FIT 数值时,需要得到相应安全机制的诊断覆盖率。

诊断覆盖率的来源一般是功能安全标准第五部分的附录 D,其中将诊断覆盖率建议了低中高三个等级,覆盖率分别为 60%、90%、99%。标准中对不同安全机制都有所对应的诊断覆盖率的建议[2,4]。

此附录 D 中的诊断覆盖率是建议值,实践中可以根据实际情况对覆盖率进行调整,比如调整为高于 99%等,这种情况下需要对调整进行合理性说明。目前一般是直接采用标准附录 D 的建议。如果安全机制的诊断周期太长,或者诊断效果有所降低等,则需要降低诊断覆盖率。

1.3 硬件度量指标

功能安全标准中关于硬件度量指标分为两个部分:第一部分是硬件架构度量指标,包括单点故障度量 SPFM 和潜伏故障度量 LFM;第二部分是随机硬件失效导致违背安全目标的评估,这个部分可以通过两种方法之一进行评估,方法一就是常用的随机硬件失效概率度量 PMHF,方法二是对可能违背安全目标的每个原因针对不同功能安全等级和不同失效率 FIT 值等级进行诊断覆盖率的评估[2,4]。方法二中需要根据每个失效进行单独评估,没有系统整体的评价指标。

目前关于第二部分随机硬件失效导致违背安全目标的评估中普遍采用的是方法一即 PMHF。这样加上第一部分的两个度量 SPFM 和 LFM,功能安全开发中硬件度量指标一般采用这三个。

功能安全标准对这三个度量指标目标值的选取也定义了两种,一种是标准中根据功能安全等级的推荐值,另一种是从历史项目中计算得到,项目要具备相似性且应用了普遍信任的设计方案。目前实践中普遍采用标准推荐的数值见表 1。

表 1 硬件指标要求

Table 1 Hardware metric requirements

等级	SPFM	LFM	PMHF
ASIL D	> 99%	> 90%	< 10 FIT
ASIL C	> 97%	> 80%	< 100 FIT
ASIL B	> 90%	> 60%	< 100 FIT
ASIL A	-	-	-

2 硬件指标的计算与评价

功能安全的三个硬件指标中,单点故障度量 SPFM 和潜伏故障度量 LFM 需要通过 FMEDA (Failure Mode Effect & Diagnostic Analysis)方法分析计算得到,随机硬件失效概率度量 PMHF 通常通过定量 FTA(Failure Tree Analysis)方法分析计算得到。本章介绍在 FMEDA 和 FTA 分析实践中的相关事项。

2.1 FMEDA 分析计算

FMEDA 是失效模式后果及诊断分析,图 1 为功能安全标准附录里 FMEDA 的示例[2]。图 1 中按照列可以分为三部分,A 部分是各个元器件以及根据标准计算的 FIT 数值和失效模式的百分比,B 部分用来分析各个故障是否可能直接违背安全目标(假设没有任何安全机制),同时根据诊断覆盖率确定单点故障(若有)和残余故障的 FIT 数值,C 部分用来分析各个故障是否和双点故障相关,同时根据诊断覆盖率确定潜伏的双点故障的 FIT 数值。最终根据 A、B、C 三部分汇总分别得到整体的 FIT 数值、单点故障加残余故障的 FIT 数值以及潜伏的双点故障的 FIT 数值,最后根据公式计算得到 SPFM 和 LFM 的指标结果。

计算公式为[2,4]:

$$\mathrm{SPFM}=1-\frac{\sum_{SR,HW}(\lambda_{SPF}+\lambda_{RF})}{\sum_{SR,HW}\lambda},$$

$$\mathrm{LFM}=1-\frac{\sum_{SR,HW}(\lambda_{MPF,\mathrm{latent}})}{\sum_{SR,HW}(\lambda-\lambda_{SPF}-\lambda_{RF})}$$

2.1.1 单点和残余故障的处理方法

图 1 中 B 部分涉及单点故障和残余故障与 SPFM 相关。首先需考虑各个故障在没有任何安全机制时是否可能违背安全目标,如果可能违背,则根据实施的安全机制确定诊断覆盖率。如果需要,可以同时填写多个安全机制。诊断覆盖率根据安全机制按照高中低的原则进行选择,通常不会达到 100%。

Component Name	Failure rate/FIT	Safety-related component to be considered in the calculation?	Failure Mode	Failure rate distribution	Failure mode that has the potential to violate the safety goal in absence of safety mechanisms?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal?	Failure mode coverage wrt. violation of safety goal	Residual or Single-Point Fault failure rate/FIT	Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent?	Failure mode coverage wrt. Latent failures	Latent Multiple-Point Fault failure rate/FIT
R11 note 1, note 6 and note 7	2	YES	open	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			closed	10 %	X		99 %	0,002	X		100 %	0
R12 note 1, note 6 and note 7	2	YES	open	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			closed	10 %	X		99 %	0,002	X		100 %	0
R21 note 2	2	YES	open	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			closed	10 %	X		99 %	0,002	X		100 %	0
R22 note 2	2	YES	open	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			closed	10 %	X		99 %	0,002	X		100 %	0
C11 note 1, note 6 and note 7	2	YES	open	20 %	X	SM2	99 %	0,004	X	SM2	100 %	0
			closed	80 %	X		99 %	0,016	X		100 %	0
C12 note 1, note 6 and note 7	2	YES	open	20 %	X	SM2	99 %	0,004	X	SM2	100 %	0
			closed	80 %	X		99 %	0,016	X		100 %	0
C21	2	YES	open	20 %		SM2				SM2		
			closed	80 %	X		99 %	0,016	X		100 %	0
C22	2	YES	open	20 %		SM2				SM2		
			closed	80 %	X		99 %	0,016	X		100 %	0
I1	4	YES	open	70 %	X	SM2	99 %	0,028	X	SM2	100 %	0
			closed	20 %	X		99 %	0,008	X		100 %	0
			drift 0,5	5 %	X		99 %	0,002	X		100 %	0
			drift 2	5 %								
I2	4	YES	open	70 %	X	SM2	99 %	0,028	X	SM2	100 %	0
			closed	20 %	X		99 %	0,008	X		100 %	0
			drift 0,5	5 %	X		99 %	0,002	X		100 %	0
			drift 2	5 %								
WD	20	YES	Out. Stuck at 1	50 %					X	none	0 %	10
			Out. Stuck at 0	50 %								
T61	5	YES	open circuit	50 %		SM3				SM3		
			short circuit	50 %	X		90 %	0,25	X		100 %	0
R61 note 3 and note 6	2	YES	open	90 %						none		
			closed	10 %					X		0 %	0,2
R62 note 3 and note 6	2	YES	open	90 %						none		
			closed	10 %					X		0 %	0,2
R63	2	NO	open	90 %								
			closed	10 %								
R64 note 1 and note 6	2	YES	open	90 %					X	none	0 %	1,8
			closed	10 %					X		0 %	0,2
I61	5	NO	open	70 %								
			closed	20 %								
C61 note 4 and note 6	2	YES	open						X	none	0 %	0,4
			closed	80 %								
R81	2	NO	open	90 %								
			closed	10 %								
L1	10	NO	open	90 %								
			closed	10 %								
µC	100	YES	All	50 %	X	SM4	90 %	5	X	SM4	100 %	0
			All	50 %								
							Σ	5,48			Σ	12,80

Total failure rate 176
Total Safety Related 157
Total Not Safety Related 19

Single-Point Fault Metric = 1-(5,48/157) = 96,5 %

Latent Fault Metric = 1-(13,99/(157-5,48)) = 91,6 %

图 1 FMEDA 计算示例

Fig. 1 Computational example of FMEDA

2.1.2 潜伏的双点故障的处理方法

图 1 中 C 部分涉及潜伏的多点故障,与 LFM 相关,这部分中的诊断覆盖率有可能达到 100%,即全部覆盖,没有潜伏的多点故障。

对于已经涉及 B 部分的故障,其中在 B 部分被安全机制覆盖的部分通常会对相应故障信息进行记录并且提示驾驶员,因此通常全部为可探测的双点故障,不含有潜伏的双点故障,所以此类故障在 C 部分中的诊断覆盖率可以达到 100%。此类既涉及 B 部分又涉及 C 部分的故障通常为功能实现相关模块的故障。

对于不涉及 B 部分只涉及 C 部分的故障,在 C 部分确定诊断覆盖率时同样根据高中低的原则进行选择,通常不会达到 100%。此类故障一般为安

全机制的故障,比如看门狗和专门用于诊断信号的相关硬件电路等。

如前所述,通常所有涉及 B 部分的故障在 FMEDA 中都和 C 部分相关,同时在 C 部分的诊断覆盖率为 100%即潜伏的双点故障是零。这样的结果和在 C 部分选择无关的结果是一样的。因此在实际操作中,对于涉及 B 部分的相关故障,在 C 部分的双点故障中可以选择无关,这样可以降低一些工作量,同时便于 FMEDA 的检查与维护。如果选择这样操作,需要在 FMEDA 中进行相应的说明。如果出现 B 部分被安全机制覆盖的部分没有全部通知驾驶员的情况,则需要在 C 部分选择双点故障相关,并且确定相应的诊断覆盖率(此时为被驾驶员感知到的部分,通常达不到 100%),目前实践中还没有遇到这种情况。

2.1.3 FMEDA 分析的其他注意事项

FMEDA 分析时应该按照模块对元器件进行分组,便于分析和检查的连贯性和按照模块对结果进行汇总,建议按照硬件设计中的模块对元器件进行分组。

分析某个故障是否可能违背安全目标时需要先考虑没有任何安全机制的情况,如果有多个安全机制,也需要假设这些安全机制全部没有时的情况。

和安全无关的元器件应选取为安全无关,去除这部分零件对 FMEDA 结果的影响。

硬件指标计算中的整体原则之一是保守,根据标准计算得到的 FIT 数值会偏保守,诊断覆盖率为高时覆盖率为 99%也偏保守,在 FMEDA 分析中也应遵循保守的原则。如果分析过程中对某个故障是否可能违背安全目标难以确定,可以根据保守原则选择有可能违背,分析是否属于双点故障时也类似。为了得到比较理想的硬件指标结果,需要对元器件的故障进行仔细分析,减少出于保守原则进行的选择。

2.2 FTA 分析计算

PMHF 的计算中既包含单点故障以及残余故障,也包括双点故障同时发生导致违背安全目标的情况,一般采用定量 FTA 的分析方法进行计算。

FTA 通过各个基本事件进行与门和或门的计算,可以对双点故障同时发生的概率进行计算,得到 PMHF 值。计算过程中,除了需要 FMEDA 计算所需的失效率 FIT 数值和诊断覆盖率之外,还需要 Mission Time 的参数,即系统运行的总时间,该时间通常来自系统设计规范,一般在几千到几万小时。该参数的作用是用来计算双点故障在这段时间内同时发生的概率。

2.2.1 FTA 中单点和残余故障的处理

FTA 里单点故障通常作为基本事件通过几个或门最终连接到顶层事件,即安全目标的违背,这些或门表明这个基本事件单独即可导致顶层事件。

FTA 里残余故障通常由基本事件与相应安全机制通过与门连接到上层事件,基本事件的参数为失效率 FIT 值,安全机制的参数为(1-DC),即没有被诊断覆盖的部分,此参数为与时间无关的固定值。

2.2.2 FTA 中双点故障的处理

如 1.14 节所述,双点故障通常有如下两种:故障 X 与其对应的安全机制同时失效,故障 X 与进入安全状态的路径同时失效,都会使得系统无法进入安全状态。

对于安全机制的失效,一般对于安全机制的检测会在每个驾驶循环进行一次,这就意味着在一个驾驶循环之内,安全机制的故障可能未被探测到。直到下一个驾驶循环,该故障才会被探测到并进行相应的处理。由于一个驾驶循环的时间相对于系统运行总时间很小,这部分可能由可探测的双点故障导致的失效在进行 PMHF 计算时可以忽略。

对于安全机制失效中的瞬时故障,由于瞬时故障最迟在下一个驾驶循环就会恢复,因此潜伏的双点故障中瞬时故障部分也可以进行忽略。

对于进入安全状态的路径失效的故障,如果每次上电时都对安全状态路径的功能进行检测,这部分可能由安全状态路径的故障导致的失效在进行 PMHF 计算时也可以忽略或降低。

因此 PMHF 计算中双点一般可以简化为被安全机制覆盖的功能失效与其对应的安全机制的潜伏的双点故障中永久故障部分。安全机制的实施通常由 MCU 或 IC 实施,不同安全机制对应的潜伏的双点故障 FIT 数值通常也不完全相同,通过对 MCU 或 IC 的详细 FTA 分析可以得到不同安全机制的潜伏的双点故障 FIT 数值。具体实践中通常不对 MCU 及 IC 进行详细的 FTA 分析,通常使用 MCU 及 IC 的 FMEDA 分析中得到的潜伏的双点故障的整体 FIT 数值作为安全机制失效的潜伏的双点故障。

2.2.3 FTA 中残余故障与双点故障的结合

如果没有安全机制时故障 X 的发生会导致系统违背安全目标,那么故障 X 通常既有残余故障部分也有双点故障部分,在 FTA 处理时可以将两部分故障结合起来处理。

例如图 2,左边是各个器件的故障,右边既包含 1%的残余故障比例,也包含由 99%的可探测的双点故障和安全机制的潜伏故障同时发生导致的失效。这样结合处理可以降低 FTA 里的基本事件数量,减少相应的工作量,同时便于 FTA 的检查与维护。

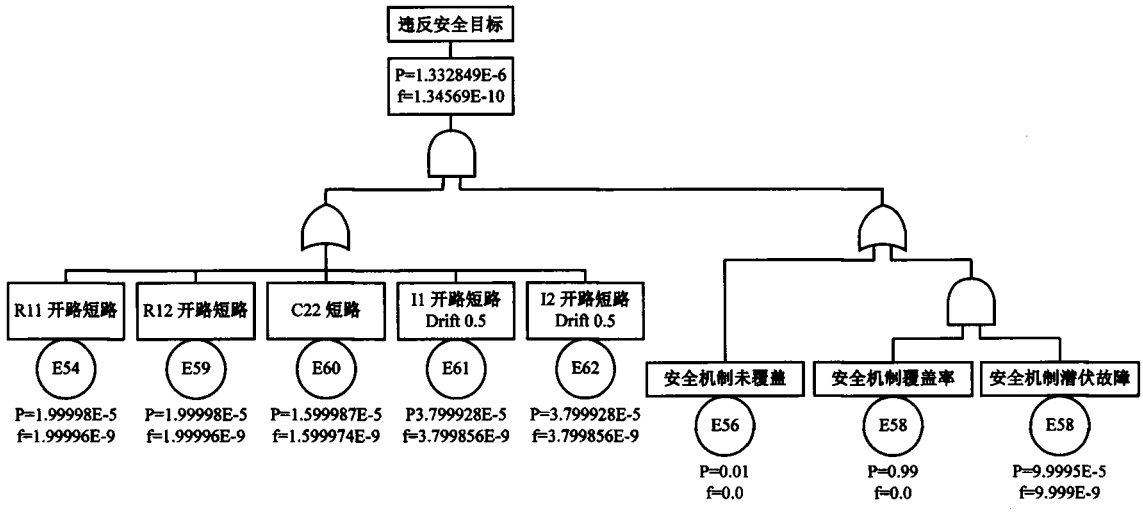

图 2 FTA 示例

Fig. 2 Example of FTA

2.2.4 FTA 分析的其他注意事项

FTA 同样应该按照模块进行树状结构的建立。

FTA 的里基本事件应与 FMEDA 里(除安全故障)的基本事件相同。基本事件的 FIT 失效率数值应与 FMEDA 里的数值相同。

FTA 中同一个基本事件需要放在不同的分支时,需要将这些事件设定为重复事件或重复分支,否则会对计算结果有影响。

2.3 硬件指标评价

2.3.1 硬件指标评价

硬件指标计算完成后,需要对硬件指标进行评价,评价通常是根据功能安全标准的要求进行,即表 1。

FMEDA 计算结果中有单点故障度量 SPFM 和残余故障度量 LFM,也有单点故障加残余故障的 FIT 数值。随机硬件失效概率度量 PMHF 计算的结果应该比 FMEDA 里单点故障加残余故障的数值稍大一些。

2.3.2 硬件指标与设计的关系

为了得到合格的硬件指标,在系统开发中需要对安全机制进行相应设计。

比如对于 ASIL D 等级的电控系统,首先安全机制需要覆盖所有可能违背安全目标的器件,同时尽可能选取诊断覆盖率为高的安全机制。这些安全机制的运行周期也要满足安全需求,通常在运行过程中这些安全机制需要一直工作。

对于安全机制自身的故障,也要尽量进行诊断,降低潜伏的双点故障 FIT 数值。对安全机制进行的诊断通常可以选择在上电时进行一次,不需要,很多情况下有也没办法做到在运行过程中对安全机制进行诊断。

3 结论

本文对功能安全硬件指标计算相关的概念进行了解释,并通过举例说明了相关故障类型与实际系统中元器件的关系。对硬件指标计算的相关步骤进行了解释,并对操作方法给出了一些建议,有助于加深对硬件指标的理解,更好的完成硬件指标计算的工作。最后对硬件指标计算的和系统设计的关系进行了说明。

参 考 文 献

[1] ISO 26262-1:2011, Road vehicles-Functional safety-Part 1: Vocabulary.

[2] ISO 26262-5:2011, Road vehicles-Functional safety-Part 5: Product development at the hardware level.

[3] GB/T34590.1:2017 道路车辆 功能安全 第 1 部分:术语.

[4] GB/T34590.5:2017 道路车辆 功能安全 第 5 部分:产品开发:硬件层面.

[5] SN 29500-4:1999, Failure rates of components, Part 4: Expected values for passive components.

[6] IEC TR 62380:2004, Reliability data handbook-Universal model for reliability prediction of electronics components, PCBs and equipment.