ICS 43.430
CCS T 35

中华人民共和国国家标准

GB/T 34590.10—XXXX
代替 GB/T 34590.10-2017

道路车辆 功能安全
第10部分：指南

Road vehicles—Functional safety—Part10: Guideline

(ISO 26262-10:2018，Road vehicles-Functional safety-Part10: Guideline on ISO 26262,MOD)

（征求意见稿）

（本草案完成时间：2021年4月1日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 III
引言 V
1　范围 7
2　规范性引用文件 7
3　术语、定义和缩略语 7
4　GB/T 34590 中的关键概念 7
4.1　针对汽车系统的功能安全（与 GB/T 20438 的关系） 7
4.2　相关项、系统、要素、组件、硬件元器件和软件单元 9
4.3　故障、错误和失效之间的关系 10
4.4　FTTI 和紧急运行容错时间间隔 11
5　关于安全管理的精选话题 14
5.1　工作成果 14
5.2　认可措施 14
5.3　安全档案的理解 16
6　概念阶段和系统开发 17
6.1　总则 17
6.2　危害分析和风险评估示例 17
6.3　关于可控性分级的论述 18
6.4　外部措施 18
6.5　合并安全目标的示例 19
7　安全过程的要求结构-安全要求的流程和顺序 20
8　关于硬件开发 21
8.1　随机硬件故障的分类 21
8.2　残余失效率和局部单点故障度量评估的示例 25
8.3　关于硬件的进一步解释 35
8.4　PMHF 单位——每小时平均概率 41
9　独立于环境的安全要素 43
9.1　独立于环境的安全要素的开发 43
9.2　使用案例 44
10　在用证明的示例 50
10.1　概述 50
10.2　相关项定义和在用证明候选项的定义 50
10.3　变更分析 50
10.4　在用证明的目标价值 51
11　关于 ASIL 的分解 51
11.1　ASIL 分解的目的 51
11.2　ASIL 分解的描述 51
11.3　ASIL 分解的示例 51

12　带安全相关可用性需求的系统的开发指南 53
12.1　引言 54
12.2　概念阶段指定故障容错时间的说明 54
12.3　硬件设计阶段的可用性考虑 60
12.3.1　随机硬件故障定量分析 60
12.4　软件开发阶段 62
13　关于“所使用软件工具的置信度”的分析 63
14　安全相关的特殊特性指南 64
14.1　总则 64
14.2　安全相关的特殊特性的确定 64
14.3　与安全相关的特殊特性控制措施规范 65
14.4　安全相关的特殊特性的监测 65
附录 A（资料性）　故障树的构建和应用 66
参考文献 68

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

GB/T 34590-XXXX《道路车辆 功能安全》分为以下部分：

——第 1 部分：术语；

——第 2 部分：功能安全管理；

——第 3 部分：概念阶段；

——第 4 部分：产品开发：系统层面；

——第 5 部分：产品开发：硬件层面；

——第 6 部分：产品开发：软件层面；

——第 7 部分：生产、运行、服务和报废；

——第 8 部分：支持过程；

——第 9 部分：以汽车安全完整性等级为导向和以安全为导向的分析；

——第 10 部分：指南；

——第 11 部分：半导体应用指南；

——第 12 部分：摩托车的适用性。

本文件为GB/T 34590-XXXX的第10部分。

本文件代替GB/T 34590.10-2017《道路车辆 功能安全 第10部分：指南》,与GB/T 34590.10-2017相比，除结构调整和编辑性改动外，主要技术变化如下：

——修改了标准适用范围，由“量产乘用车”扩大到“除轻便摩托车外的量产道路车辆”；

——新增了对商用车辆的相关要求和示例、对摩托车的适应性要求等；

——新增了“容错时间间隔和紧急运行容许时间间隔”（见 4.4）；

——新增了“典型的双点失效模式（预期功能以及安全机制）”（见 8.3.2.3）；

——新增了“PMHF 单位——每小时平均概率”（见 8.4）；

——新增了“带安全相关可用性需求的系统的开发指南”（见第 12 章）；

——删除了 2017 版的附录 A。

本文件使用重新起草法修改采用了ISO 26262-10：2018 《道路车辆 功能安全 第10部分：指南》。

本文件与ISO 26262-10：2018的技术性差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：用修改采用国际标准的 GB/T 34590.1-XXXX 代替 ISO 26262-1：2018；

本文件做了下列编辑性修改：

——将国际标准中的“本国际标准”改为“本文件”；

——删除国际标准的前言；

——修改国际标准的引言及其表述。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

本文件起草单位：

本文件主要起草人：

本文件所代替文件的历次版本发布情况为：

——GB/T 34590.10,XXXX 年首次发布。

引　言

ISO 26262是以IEC 61508为基础，为满足道路车辆上电气/电子系统的特定需求而编写。

GB/T 34590修改采用ISO 26262，适用于道路车辆上由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。

安全是道路车辆开发的关键问题之一。汽车功能的开发和集成强化了对功能安全的需求，以及对提供证据证明满足功能安全目标的需求。

随着技术日益复杂、软件和机电一体化应用不断增加，来自系统性失效和随机硬件失效的风险逐渐增加，这些都在功能安全的考虑范畴之内。GB/T 34590通过提供适当的要求和流程来降低风险。

为了实现功能安全，GB/T 34590-XXXX（所有部分）：

a) 提供了一个汽车安全生命周期（开发、生产、运行、服务、报废）的参考，并支持在这些生命周期阶段内对执行的活动进行剪裁；

b) 提供了一种汽车特定的基于风险的分析方法，以确定汽车安全完整性等级（ASIL）；

c) 使用 ASIL 等级来定义 GB/T 34590 中适用的要求，以避免不合理的残余风险；

d) 提出了对于功能安全管理、设计、实现、验证、确认和认可措施的要求；及

e) 提出了客户与供应商之间关系的要求。

GB/T 34590针对的是电气/电子系统的功能安全,通过安全措施(包括安全机制)来实现。它也提供了一个框架，在该框架内可考虑基于其它技术（例如，机械、液压、气压）的安全相关系统。

功能安全的实现受开发过程（例如，包括需求规范、设计、实现、集成、验证、确认和配置）、生产过程、服务过程和管理过程的影响。

安全问题与常规的以功能为导向和以质量为导向的活动及工作成果相互关联。GB/T 34590涉及与安全相关的开发活动和工作成果。

图1为GB/T 34590的整体架构。GB/T 34590基于V模型为产品开发的不同阶段提供参考过程模型：

——阴影”V”表示 GB/T 34590.3-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX、GB/T 34590.6-XXXX、GB/T 34590.7-XXXX 之间的相互关系；

——对于摩托车：

- GB/T 34590.12-XXXX的第8章支持GB/T 34590.3-XXXX；
- GB/T 34590.12-XXXX的第9章和第10章支持GB/T 34590.4-XXXX。

——以“m-n”方式表示的具体章条中，“m”代表特定部分的编号，“n”代表该部分章的编号。

示例：“2-6”代表 GB/T 34590.2-XXXX 的第 6 章。

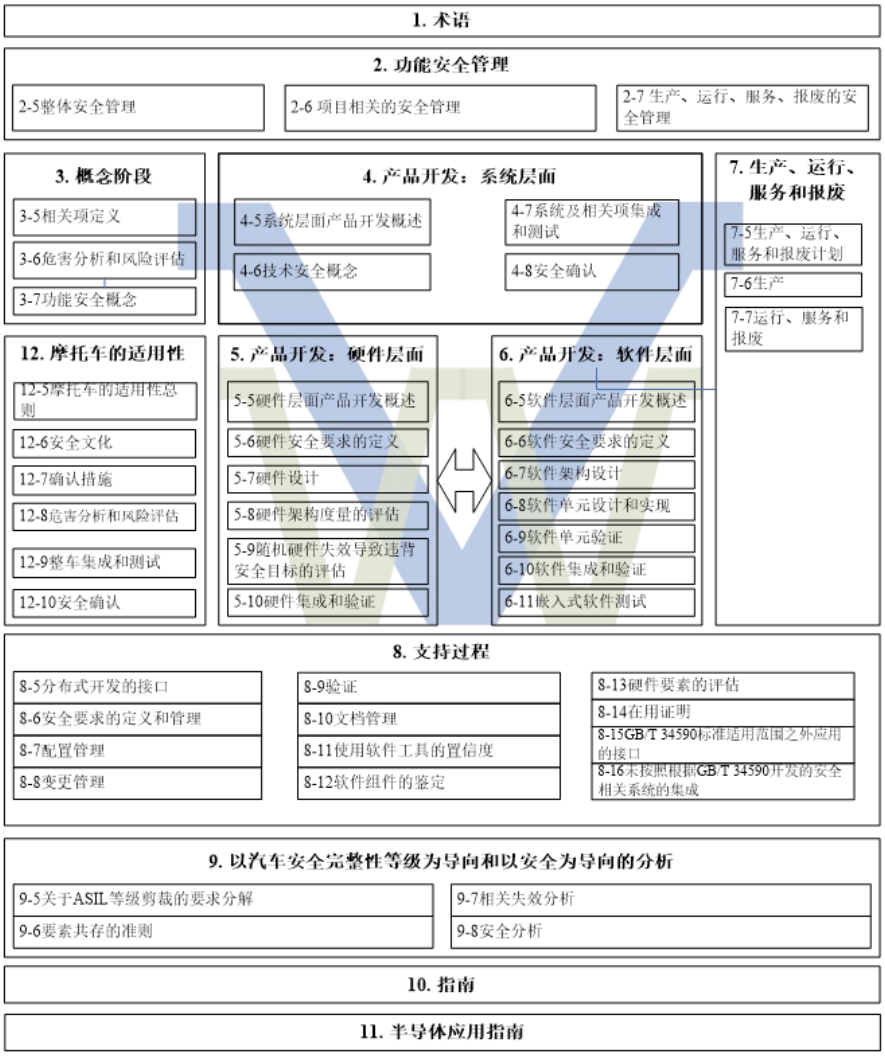


图 1　GB/T 34590-XXXX 概览

道路车辆 功能安全
第10部分：指南

1 范围

GB/T 34590的本部分提供了GB/T 34590的概览，也给出了额外的解释，目的是增强对本文件其它部分的理解。本文件只具有资料性特性，描述了GB/T 34590的一般概念以便于理解。该解释将一般概念扩展到特定的内容。

本文件适用于安装在除轻便摩托车外的量产道路车辆上的包含一个或多个电气/电子系统的与安全相关的系统。

本文件不适用于特殊用途车辆上特定的电气/电子系统，例如，为残疾驾驶者设计的车辆。

注：其他专用的安全标准可作为本文件的补充，反之亦然。

已经完成生产发布的系统及其组件或在本文件发布日期前正在开发的系统及其组件不适用于本文件。对于在本文件发布前完成生产发布的系统及其组件进行变更时，本文件基于这些变更对安全生命周期的活动进行剪裁。未按照本文件开发的系统与按照本文件开发的系统进行集成时，需要按照本文件进行安全生命周期的剪裁。

本文件针对由安全相关的电气/电子系统的功能异常表现而引起的可能的危害，包括这些系统相互作用而引起的可能的危害。本文件不针对与触电、火灾、烟雾、热、辐射、毒性、易燃性、反应性、腐蚀性、能量释放等相关的危害和类似的危害，除非危害是直接由安全相关的电气/电子系统的功能异常表现表现而引起的。

本文件提出了安全相关的电气/电子系统进行功能安全开发的框架，该框架旨在将功能安全活动整合到企业特定的开发框架中。本文件规定了为实现产品功能安全的技术开发要求，也规定了组织应具备相应功能安全能力的开发流程要求。

如果本文件与GB/T 34590其它部分存在不一致时，以GB/T 34590其它部分中定义的要求、建议和信息为准。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34590.1-XXXX 道路车辆 功能安全 第1部分：术语（ISO 26262-1:2018，MOD）

3 术语、定义和缩略语

GB/T 34590.1-XXXX界定的术语、定义和缩略语适用于本文件。

4 GB/T 34590中的关键概念

4.1 针对汽车系统的功能安全（与GB/T 20438的关系）

GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》是关于电气、电子、可编程电子安全相关系统的功能安全通用标准和基础安全标准。这意味着，各工业领域将基于GB/T 20438的要求建立自身的功能安全标准。

在汽车行业，如果直接应用GB/T 20438标准会存在许多问题。其中的一些问题相对应于GB/T 34590系列标准的差异描述如下。

GB/T 20438基于“受控设备”模型，例如具有如下关联控制系统的工业装置：

a) 使用危害分析识别出与受控设备（包括设备控制系统)关联的危害，并对此应用可降低风险的措施。这可通过电气/电子/可编程电子系统、其它技术的安全相关系统（例如：安全阀）、或外部措施（例如：对装置的物理围堵）来实现。GB/T 34590 系列标准基于严重度、暴露概率和可控性，为危害分级提供了规范化的汽车领域的方案。

b) 电气/电子/可编程电子系统可通过完成如下设计的安全功能来降低所分配的风险。这些安全功能可以是独立的保护系统的一部分、也可以被纳入到装置控制中。在汽车系统中，未必都能做出这种区分。车辆的安全依赖于控制系统自身的表现。

GB/T 34590使用了安全目标和安全概念的如下观念：

——通过危害分析和风险评估识别出需要防止、减轻或控制的危害和危害事件；

——每个被评为 ASIL A, B C 或 D 的危害事件与至少一个安全目标关联；

——将汽车安全完整性等级（ASIL）与每个安全目标关联；

——功能安全概念表述了实现安全目标的功能；

——技术安全概念表述了如何在系统层面通过硬件和软件实现安全功能；及

——软件安全要求和硬件安全要求表述了特定的安全要求，这些要求将作为软硬件设计的一部分而被实施。

示例：安全气囊系统：

——其中一个危害是非预期气囊起爆；

——相关的安全目标是气囊只在发生需要气囊起爆的碰撞时起爆；

——功能安全概念可定义冗余的功能来探测车辆是否发生碰撞；

——技术安全概念可定义两个具有不同轴向的独立加速度传感器和两个独立点火回路的实施方案，如果两路均闭合则起爆点火管。

GB/T 20438针对的是单一的或小批量的系统。系统经过制造和测试后安装到装置上，然后执行安全确认。对于大批量销售的系统，如道路车辆，安全确认在量产之前执行。因此GB/T 34590中生命周期活动的次序有所不同。对此，GB/T 34590.7-XXXX提出了对生产的要求。而在GB/T 20438中并未覆盖此部分内容。

GB/T 20438未对管理跨多个组织和供应链的开发提出特定要求。因为汽车系统是由整车厂自身、由整车厂的一个或多个供应商或由整车厂与供应商合作生产的，GB/T 34590包含了明确地解决这个问题的要求，包括开发接口协议(DIA)（见GB/T 34590.8-XXXX，第5章)。

GB/T 20438不包含对危害分级的规范化要求。GB/T 34590则包含了汽车领域危害分级的方案。此方案认为汽车系统的危害并不一定会导致事故。其结果取决于涉险人员是否实际暴露在危害发生的场景下，及相关人员能否采取措施以控制危害的结果。图2给出了此概念的示例，将其应用到了一个对运动中车辆可控性有影响的失效上。

注：此概念仅为了阐述失效的发生和事故之间没有必然的直接关联。尽管此过程中评估的参数与图中状态过渡的可能性相关，但它不是危害分析和风险评估过程的展示。

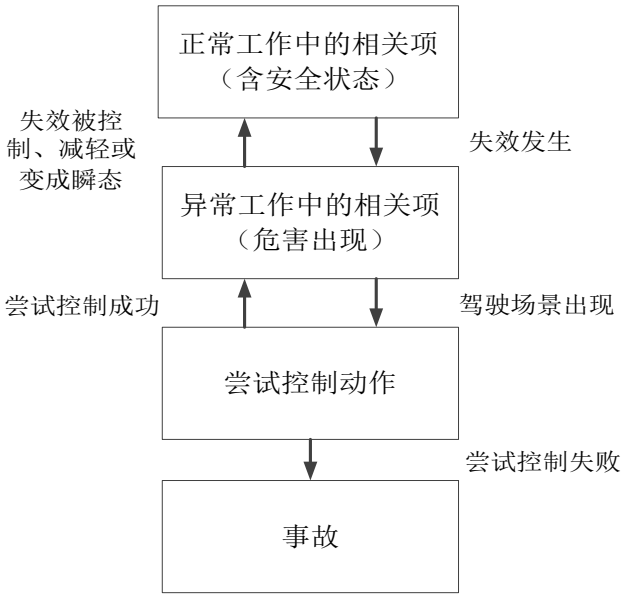


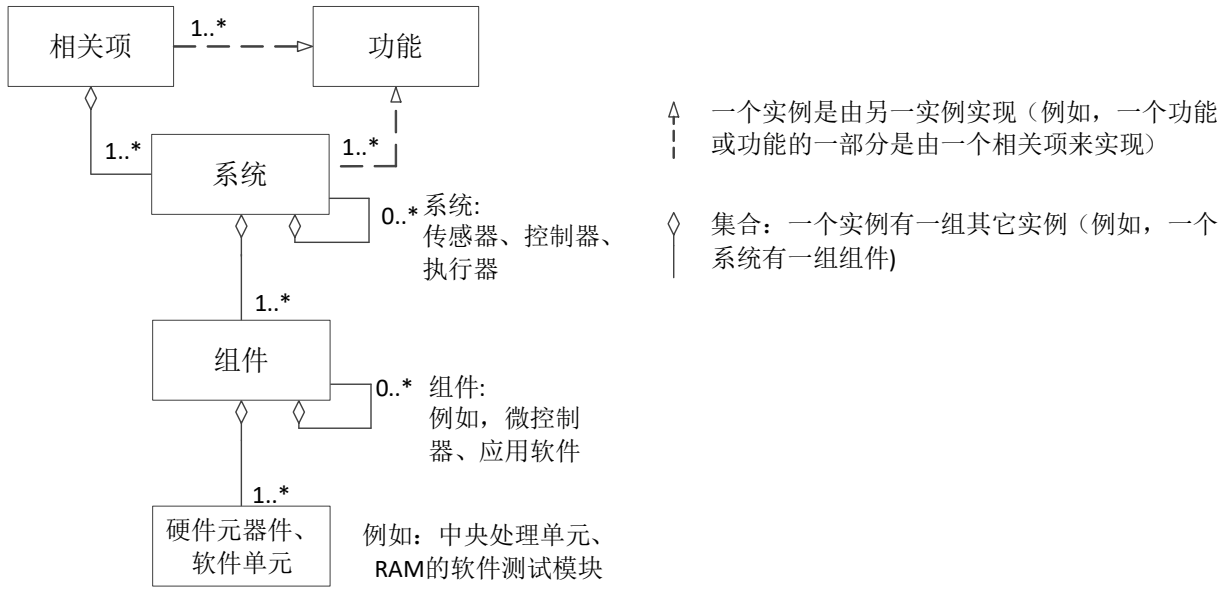
图 2　汽车风险的状态机模型

为符合汽车工业的当前技术水平，对硬件开发（GB/T 34590.5-XXXX）和软件开发（GB/T 34590.6-XXXX）要求进行了调整。对于GB/T 34590中列出的方法给出了特定的目标；为实现这些目标，可应用给出的方法，或应用替代方法，但需提供理由证明替代方法也能实现目标。

为GB/T 34590中的安全要求分配汽车安全完整性等级（ASIL）而不是安全完整性等级（SIL），其主要原因是GB/T 20438中的SIL表述为概率术语（见GB/T 20438.1-2006，表3）。GB/T 20438确认，对于系统安全完整性常常需要定性判断，而对于硬件安全完整性需要量化技术。GB/T 34590中ASIL主要关注在系统、硬件和软件中实现系统安全的要求，但也存在关于符合ASIL随机硬件失效要求的概率目标。

4.2　相关项、系统、要素、组件、硬件元器件和软件单元

GB/T 34590.1-XXXX中定义了相关项、系统、要素、组件、硬件元器件和软件单元。图3展示了系统、要素、组件、硬件元器件和软件单元的关系。图4举例展示了相关项的分解（构成关系）。可分解的要素可被标注为系统或组件。满足系统标准的可分解要素可被标注为系统。组件是非系统层面的、逻辑上和技术上独立的要素。通常，术语“组件”用于仅由元器件和单元组成的要素，但也能用于由更低层面的特定技术领域（例如：电子电气技术，见图4）要素组成的要素。硬件元器件还可以进一步按层次由硬件子元器件和硬件基本子元器件组成。



注1：根据上下文，要素可用于此图表中的系统、组件、硬件元器件和软件单元，按照GB/T 34590-1:XXXX, 3.41

注2：GB/T 34590-1:XXXX, 3.163中定义的系统使至少一个传感器、一个控制器和一个执行器相互关联。该相互关联的传感器和执行器可以被包含在系统内，也可以在系统外部。

注3：*表示可能有N个。

图 3　相关项、系统、组件、硬件元器件和软件单元间的关系

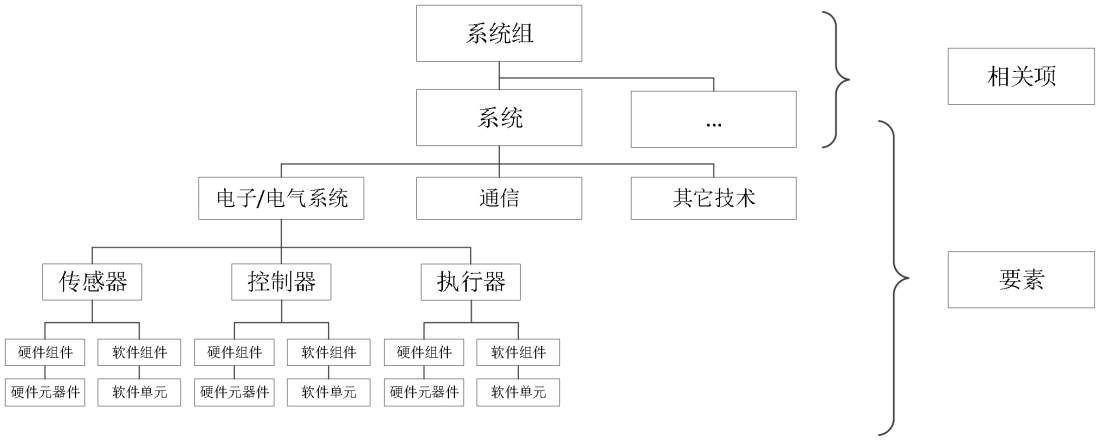


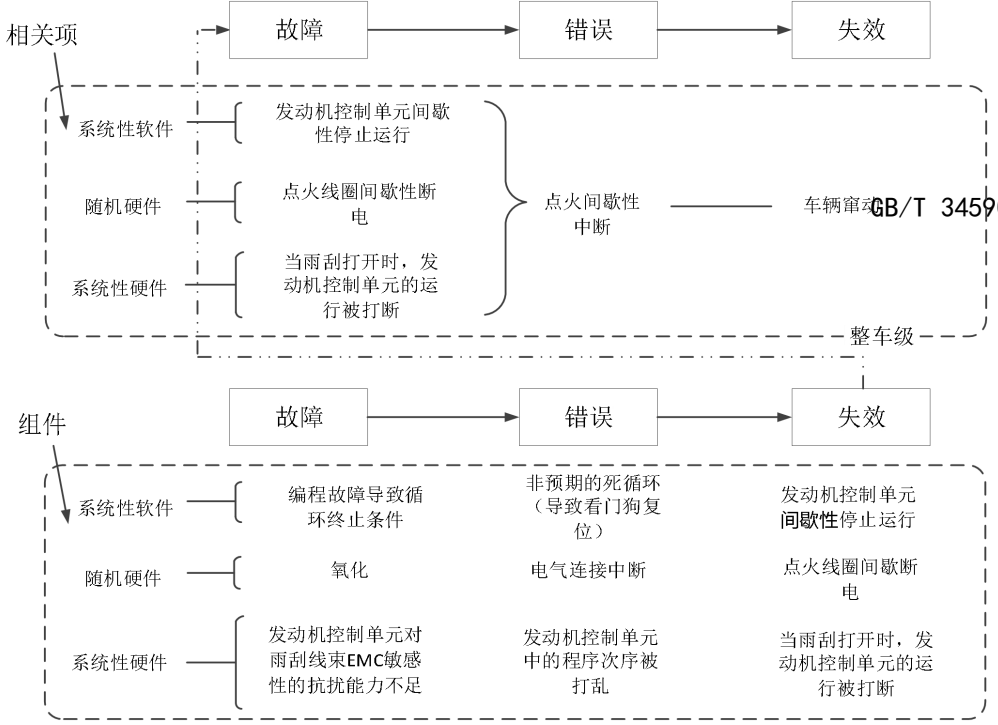
图 4　相关项分解示例

4.3　故障、错误和失效之间的关系

4.3.1　故障到错误并从错误到失效的发展过程

在GB/T 34590.1-XXXX中定义了术语：故障、错误和失效。图5从三个不同类型的原因（系统性软件问题、随机硬件问题和系统性硬件问题）描述了故障到错误并从错误到失效的发展过程。系统故障（见GB/T 34590.1-XXXX, 3.165）起因于设计和规范的问题；软件故障和部分硬件故障是系统性的。在组件层面，每个不同类型的故障会导致不同的失效。然而，组件层面的失效是相关项层面的故障。注意，在此示例中，整车层面不同原因导致的故障可引起相同的失效。如果额外的环境因素使失效叠加了事故场景，相关项层面的部分失效将会是危害（见GB/T 34590.1-XXXX, 3.75）。

示例：当车辆开始穿越十字交叉路口时发生非期望的行为，可能发生碰撞，例如：对危害事件“当车辆开始穿越十



字交叉猛烈窜进行严概率和估（“猛指突然动）。

路口时发生动”的风险重度、暴露可控性的评烈窜动”是的剧烈移

图5 故障导致失效的示例

注1：组件或相关项层级上可能已实施的错误探测和控制没有在图5中描述。

注2：组件的失效是相关项层级的故障(由双点虚线箭头表示)。

4.4 FTTI 和紧急运行容错时间间隔

4.4.1 介绍

GB/T 34590-XXX, 6.4.4.3在注释中指出，FTTI可作为安全目标的一部分被包含在其中。此外，GB/T 34590.4-XXXX 6.4.2.2规定了，在定义每种安全机制的故障处理时间间隔时，应考虑FTTI和紧急运行容错时间间隔。

注：故障处理时间间隔是给定的安全机制的一种特征。故障容错时间间隔（FTTI）相关项的一种特征。

作为概念阶段确定安全目标和功能安全要求流程的一部分，FTTI是基于车辆功能的整车级定义。在产品开发期间需考虑该时间跨度，确定最大故障处理时间间隔，以避免危害事件（例如：在GB/T 34590.1-XXXX 图5中所描述的故障探测时间间隔和故障反应时间间隔的总和）。FTTI是设计安全机制响应时间的必要值。在FTTI内，故障由安全机构控制，可以防止危害事件发生。当故障探测时间间隔和故障反应时间间隔之和比FTTI短时，它可以实现。

当无法在FTTI内达到安全状态时，需定义紧急运行（GB/T 34590.4-XXXX 6.4.2.2)。紧急运行是一种被定义为警告和降级策略的一部分的运行模式。在FTTI结束之前启动紧急运行，并在紧急运行容错时间间隔结束之前，维持直到安全状态为止。为满足安全目标，应在紧急运行容错时间间隔结束之前达到安全状态。

4.4.2 时序模型-控制系统示例

4.4.2.1 控制系统说明

本条将故障探测时间间隔（FDTI)、故障容错时间间隔（FTTI)、故障响应时间间隔（FRTI)、紧急运行容错时间间隔（EOTTI)和诊断测试时间间隔（DTTI)的概念应用于阀门控制系统示例。该系统由阀门、位置传感器、控制器和电机组成。该系统的功能是使用电机将阀门控制到所需的位置。

如果阀门开度超过预期百分比，则可能发生意外流量导致危险事件。作为一种故障响应，电机由一个带有机械弹簧的独立电路断电，机械弹簧将阀门拉到预设的固定开度位置。这个固定开度位置限制了流量，从而使相关项处于安全状态。

4.4.2.2 时序模型在示例控制系统中的应用

在此示例中考虑的特定失效模式是电机故障，它启动阀门达到其最大开度位置。这种情况可能是电机因电源短路或其他电机控制问题造成的。考虑了四种场景。

——场景 1：系统没有任何安全机制避免违反安全目标。

电机中出现短路导致阀门达到其最大位置。因为没有安全机制，一旦超过 FTTI,就会发生危害事件。

——场景 2：系统具备已实施的无紧急运行的安全机制，且 FTTI 内达到了安全状态。

电机中出现短路导致阀门达到其最大位置。已实施的安全机制使阀门电机断电，且机械弹簧在 FTTI 内使阀门返回到低流量位置。安全机制（弹簧）设计为无期限运行，安全状态可以是无限的。

——场景 3：系统具备已实施的可以在 FTTI 内避免危害事件的安全机制，但需要紧急运行来过渡为安全状态。通过限制车辆的运行状态，可以在紧急运行容错时间间隔内达到安全状态。

电机中出现短路导致阀门达到其最大位置。已实施的安全机制使阀门电机断电，且机械弹簧在 FTTI 内使阀门返回到低流量位置。安全机构（弹簧）仅设计为在有限时间内运行，即 EOTTI。在 EOTTI 到期之前，车辆运行状态应受到限制，使得来自阀门的流量不会导致危害事件。

——场景 4：系统具备已实施的可以在 FTTI 内避免危害事件的安全机制，但需要紧急运行来过渡为安全状态。然而，其过渡时间比 EOTTI 长。因此，累积的风险变得无法接受，超出了功能安全概念中指定的目标。

电机中出现短路导致阀门达到最大开度位置。已实施的安全机制使阀门电动机断电，并且机械弹簧在 FTTI 内将阀门返回到低流量位置。安全机制（弹簧）只设计为在有限的时间内运行，即 EOTTI。在这种场景下，车辆运行不受限制，相关项处于比 EOTTI 终止时间长的紧急运行状态，从而导致违背安全目标的不合理风险。

图6展示了与这四种场景相关的时序模型。图6基于GB/T 34590.1-XXXX图4和GB/T 34590.1-XXXX图5。

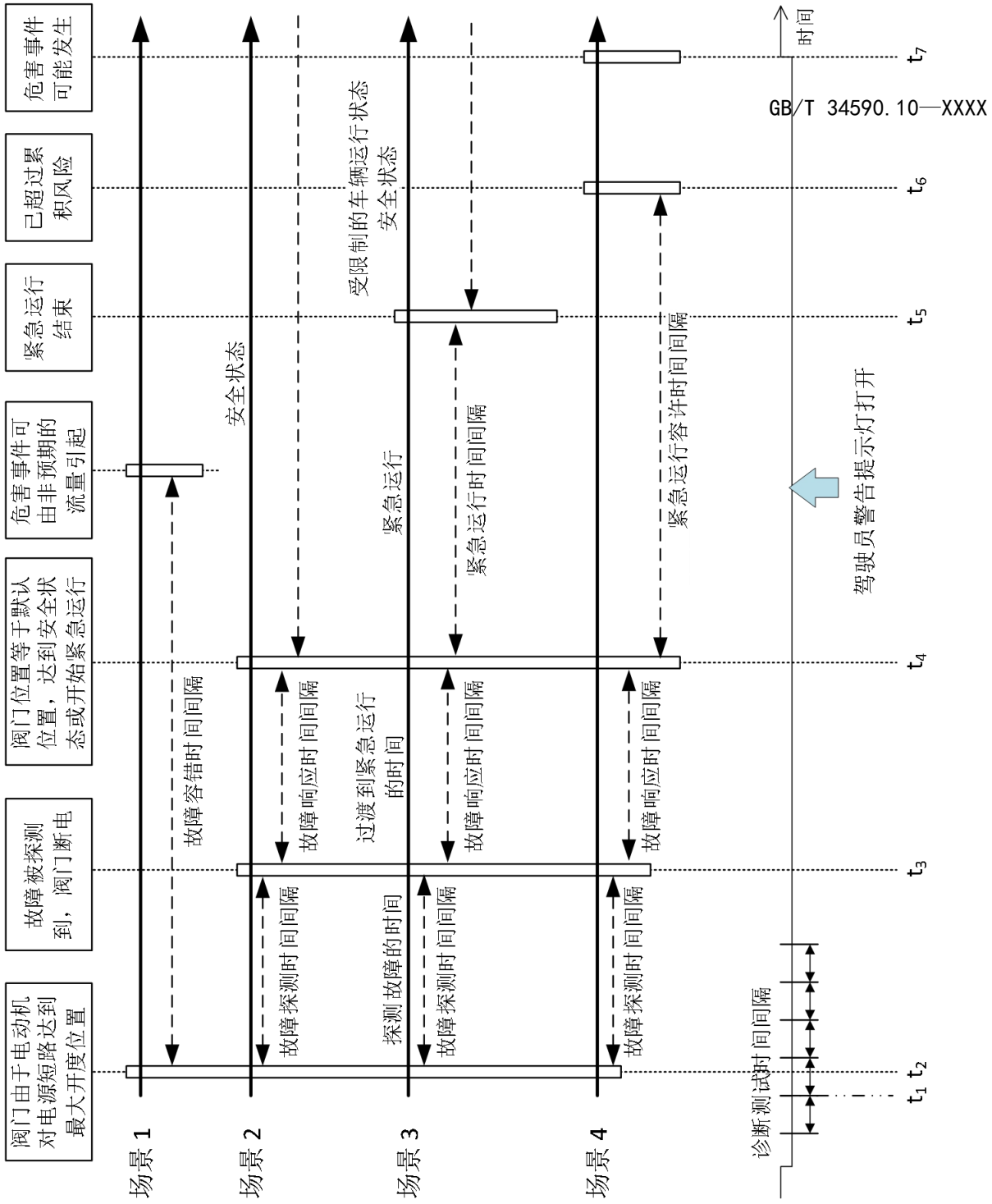


图 6　基于 GB/T 34590-1:XXXX 图 4 的时序模型示例

图 6 包括下列描述的 7 个时间戳：

t1:在故障发生之前诊断测试的时间。

t2:故障发生，故障未被探测。

t3:故障探测（例如，由于错误计数器达到其阈值，见 GB/T 34590.1-XXXX, 3.55 FDTI 示例），故障响应时间间隔开始。

t4:完成到安全状态的过渡（场景 2），紧急运行开始（场景 3 和 4）。

t5:紧急运行结束（场景 3）。

t6:紧急运行的时间限度。

t7:危害事件发生。

4.4.2.3 警告和降级策略

当阀门处于默认位置时，可能产生整车层级的影响。功能安全概念可能还包括在此状态下警告驾驶员的要求。这是警告和降级策略的一部分，由图6上的“驾驶员警告提示灯打开”箭头指示，该箭头可能在t3之后的指定时间内发生。

5 关于安全管理的精选话题

5.1 工作成果

本条描述术语“工作成果”。

工作成果是满足GB/T 34590系列标准的相应要求的结果（见GB/T 34590.1-XXXX）。因此，工作成果可提供符合这些安全要求的证据。

示例：需求规范是可通过需求数据库或文本文件来记录的一种工作成果。可执行模型是能通过可执行建模语言文件表示的一种工作成果（例如，通过使用软件工具达到仿真的目的）。

工作成果的文档（见GB/T 34590.8-XXXX第10章）作为已执行的安全活动、安全要求或相关信息的记录，不局限于任何形式或媒介。

示例：工作成果的文档可通过电子或纸质文件表示，通过单一或系列文档表示。它可以与其它工作成果的文档合并，或与非功能安全直属文档合并。

为避免信息重复，可在文档内或文档间使用交叉引用。

5.2 认可措施

5.2.1 总则

GB/T 34590中定义的工作成果，或作为认可措施的一部分，或作为验证活动的一部分，在后续活动中得到评估。本条描述了验证和认可措施间的差异。

验证活动是GB/T 34590中，为证明工作成果是合适的且遵守相应要求的，提供证据的主要措施。工作成果的验证可包括：

——参照更高层面的安全要求，关于完整性及正确性，对导出的安全要求的规范或实施的验证；或

——测试案例的执行与测试结果的检查，通过检测相关项或其要素，来提供满足已定义的安全要求的证据。

GB/T 34590.3-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX和GB/T 34590.6-XXXX中对验证活动进行了定义。此外，GB/T 34590.8-XXXX第9章定义了有关GB/T 34590系列标准的验证活动的一般要求，GB/T 34590.8-XXXX第6章定义了对安全要求进行验证的进一步细节。

对工作成果的验证，可用如下方法进行：

——评审；

——仿真；

——分析； 或

——测试。

GB/T 34590.2-XXXX中定义了认可措施。执行认可措施用以评估相关项功能安全的实现。

示例：如果在系统架构设计阶段应用 ASIL 分解，则：

——根据技术安全概念（见 GB/T 34590.4-XXXX,6.4.9）对生成的系统架构设计进行验证；及

——按照 GB/T 34590.9-XXXX 第 5 章（关于 ASIL 剪裁的要求分解）对正确实施 ASIL 分解的确认，可作为功能安全评估的一部分，包括：对已经开展的相关失效分析的确认和对声明执行相应冗余安全要求的要素间具备充分独立性的论证。

5.2.2 功能安全评估

如果相关项安全目标的最高ASIL等级是ASIL C或D，则开展功能安全评估以评价相关项是否实现功能安全。在GB/T 34590.2-XXXX中，描述了功能安全评估的某些方面，以及认可措施的其他方面。

功能安全评估的范围在GB/T 34590.2-XXXX，第6章中定义。

对实施功能安全评估的情况，功能安全审核以及认可评审的结果是功能安全评估的输入。负责评估的人员可根据他/她的自由裁量权进行评估，包括如何使用功能安全审核与认可评审的结果。

示例 1：如果功能安全审核的结果令人满意，负责功能安全评估的人员可决定信赖审核结果，而不对功能安全所要求的过程的实施做进一步判断。

示例 2：基于某一特定工作成果的认可评审报告，负责评估的人员可决定实施，或要求对工作成果的某些方面更深入的评审，或可检查是否认可评审充分地考虑了工作成果与相关工作成果之间的相互影响。

注1：负责功能安全评估的人员实施某一特定认可评审是可能的，即认可评审不一定由与负责评估的人员不同的人员实施。

功能安全评估可被重复或更新。

示例 3：因变更管理流程识别出相关项或其要素的变更对相关项的功能安全存在影响（见 GB/T 34590.8-XXXX，第 8 章），而对功能安全评估进行更新。

示例 4：对相关项功能安全建议“有条件接受”或“拒绝”的功能安全评估报告，触发功能安全再评估。在此情况下，重复评估包含对上一次功能安全评估所做建议的跟进，如果适用，还包括对已实施的纠错行动的评价。

如果相关项安全目标的最高ASIL等级是ASIL A或B，功能安全评估可被省略或以不严格的方式执行。然而，即使不执行功能安全评估，仍需执行其它认可措施（见GB/T 34590.2-XXXX，表1）。

在分布式开发的情况下，功能安全评估的范围包括由整车厂和相关项供应链中的供应商生成的工作成果、实施的流程及安全措施（见GB/T 34590.2-XXXX和GB/T 34590.8-XXXX，第5章）。

功能安全评估的目的是评价相关项功能安全的实现，这只能在相关项层面进行。因此，（开发相关项要素的）供应商所作的功能安全评估具有局限性，从本质上它是后续（客户层面）功能安全评估活动的输入。作为相关项开发中的最终客户，整车厂指派人员开展全面的功能安全评估，以判断相关项功能安全的实现。此判断包括对相关项的功能安全提供“接受”、“有条件接受”和“拒绝”的建议。

注2：对于由一级供应商负责包括整车集成的相关项开发的情况，该供应商承担整车厂的上述角色。

实际方法上，分布式开发中的功能安全评估可就此分解为：

——有限范围的功能安全评估，涉及供应链中的供应商。适用的 ASIL 等级是供应商开发的相关项各要素所继承的（相关项各安全目标的）最高 ASIL 等级(见 GB/T 34590.8-XXXX，5.4.5)；及

——最终的功能安全评估，包括对集成的相关项实现功能安全的判断，例如由整车厂开展的评估。适用的 ASIL 等级是安全要求中最高的 ASIL 等级(见 GB/T 34590.2-XXXX)。

示例 5：整车厂开发一个具有 ASIL D 安全目标（SG1）和 ASIL B 安全目标（SG2）的相关项，并将对其开展功能安全评估。存在如下可能情况，某二级供应商或三级供应商只开发了相关项的 ASIL B 要素，即仅继承 SG2 的 ASIL 等级的要素（然而，如果要素共存的标准适用，参考 GB/T 34590.9-XXXX，第 6 章）。关于具有独立 IO 的此要素开发，GB/T 34590，表 1，提供了实施功能安全评估的建议。

与客户和供应商接口有关的功能安全评估的范围、评估的流程（例如：需由供应商提供的工作成果，需由客户评审的工作成果）和评估的执行，在相应开发接口协议中进行了定义（见GB/T 34590.8-XXXX，第5章）。

示例 6：整车厂（客户）与一级供应商之间的开发接口协议（DIA）。一级供应商与二级供应商之间的开发接口协议（DIA）。

在分布式开发的情况下，功能安全评估的可能开展方式是整车厂和供应链中的供应商各自处理所负责的评估活动的如下方面：

——供应商对所开发要素中实施的安全措施进行评审，包括措施对满足相应安全目标或安全要求（由客户提供或由供应商开发）的适当性和有效性，并评估安全措施的实施过程及适用的工作成果。供应商也评估所开发要素对相关项功能安全的潜在影响，例如：对实施的可带来新危害的安全措施的识别；及

——整车厂对集成后的相关项的功能安全进行评估。评估的一部分可基于由一个及以上供应商提供的工作成果或信息，包括功能安全评估报告。

注3：客户可对供应商实施的安全措施及完成的工作成果进行评估。客户也可在供应商处对供应商实施的过程进行评估（见GB/T 34590.8-XXXX，5.4.3.1）。

5.3 安全档案的理解

5.3.1 安全档案的解释

安全档案的目的是提供一个由证据支持的、清晰的、全面的和正当的论据，以证明当运行在预期的环境中时，相关项不存在不合理的风险。

此处提供的指南聚焦于GB/T 34590的范畴。

安全档案有三个主要素：

——安全目标和相关安全要求（相关项或要素的安全目的）；

——安全论证；及

——GB/T 34590 系列标准的工作成果（即，证据）。

图7描述了GB/T 34590系列标准上下文中这三个要素间的关系。

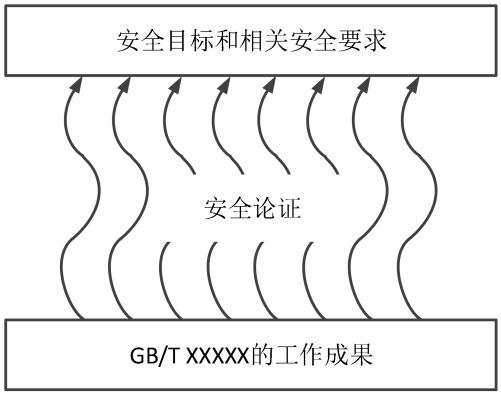


图 7 安全档案（见参考文献[2]）的关键要素

安全论证表达了证据和目标之间的关系。可能展示了许多页的支持证据却没有清晰的解释此证据如何联系到安全目标。论证和证据都是安全档案的决定性要素。没有支持证据的论证是没有事实根据的，因此是不足以令人相信的。没有论证的证据是不清楚的，以致缺乏安全目标如何得到满足的清晰解释。通过开发和展示安全档案报告，表达安全档案。安全档案报告的任务是汇总安全论证，并对记录安全支持证据的报告进行引用（例如：测试报告）。

在其它行业中使用的安全论证，经常是通过叙述性文本的安全案例报告表达的。叙述性文本可描述安全目标是如何被解释、分配和分解的，最终引用证据证明符合较低层面的安全声明。或者，作为一种

辅助，图形化论证符号（如：“声明-论证-证据”和目标结构表示法[2]）可被用以形象化的和明确的展示安全论证的独立要素（要求、声明、证据和背景），同时展示这些要素间存在的关系（即，特定声明如何支持独立要求，证据和为论证定义的假设背景如何支持声明）。

通过直接诉诸实施的相关项的特征（例如：定时看门狗的行为）来证明安全的安全论证通常被称为产品论证。通过诉诸开发和评估过程的特征（例如：采用的设计符号）来证明安全的安全论证通常被称为过程论证。

可使用两种类型的论证，以达到对相关项安全的完整论证，这里，过程论证可被看成是为产品论证中用到的证据提供可信度。

5.3.2 安全档案开发生命周期

安全档案的开发可被视为与安全生命周期内其余开发阶段集成的增量活动。

注：安全计划可包含安全档案增量步骤的计划和安全档案初始版本的计划。

这种方法允许在产品开发的给定节点生成安全档案的中间版本。例如：安全档案的初始版本可在技术安全要求验证后生成；安全档案的中间版本可在系统设计验证后生成；及最终版本可在功能安全评估的最终报告前生成。

安全档案需符合GB/T 34590.2-XXXX,6.4.9中给定的认可评审。

如果相关项被修改，需评估对安全档案的影响，如果必要，需根据修改对安全档案进行更新。

6 概念阶段和系统开发

6.1 总则

本章通过使用简单的示例，为概念阶段提供了危害分析和风险评估的原理概览。

6.2 危害分析和风险评估示例

6.2.1 总则

考虑以控制车载嵌入式能量存储装置的相关项为示例。关于此示例的用途，只有在车辆行驶速度大于等于15km/h时才试图释放储存的能量。如果车速低于15km/h，储存能量的释放会导致过热进而引发装置爆炸。

6.2.2 HARA 示例 1

a) 危害识别

“能够导致爆炸的装置的非预期能量释放”，这一危害被识别。

b) 危害事件

行驶速度低于 15km/h 可认为是所识别危害导致危害事件的驾驶场景。如果在此驾驶条件下相关项发生失效导致非预期能量释放，储能装置可能会爆炸，对车辆乘员造成严重伤害。

c) 对识别出的危害事件分级

爆炸对车辆中的乘员导致危及生命的伤害，存活不确定：危害严重度可被估计为 S3。

车辆行驶速度低于 15km/h。基于对车辆目标市场的交通统计，这一条件在 1%～10%的驾驶时间内发生：此场景的暴露概率可被估计为 E3。

车辆驾驶员或乘客控制相关项失效和装置爆炸的能力被认为是不可能的：可控性可被估计为 C3（难以控制或不可控）。

应用 GB/T 34590.3-XXXX，表 4：ASIL 等级确定为 ASIL C。

6.2.3 HARA 示例 2

本章考虑非预期的能量释放的影响由于设计改进而从本质上被限制的情况。这将导致如下的HARA：

a) 危害识别

“能够导致爆炸的装置的非预期能量释放“作为一种危害，被识别。

b) 危害事件

对于所有驾驶场景，非预期能量释放不会导致危害事件。因此，相关项失效不会引起伤害。

c) 对识别出的危害事件分级

由于相关项的失效不会导致伤害，严重度评为 S0，无需确定可控性，也无需定义安全目标。

6.3 关于可控性分级的论述

如GB/T 34590.3-XXXX，第6章中的解释，可控性代表对驾驶员或其他交通参与者能够避免特定伤害的能力的预估。

在最简单的情况下，只考虑给定危害事件的一个后果，可控性代表了对避免此后果的可能性的预估。然而，也可能存在其它情况。例如，可能有一个严重后果（例如：严重度S2），却很容易避免（例如：可控性C1）；又或者后果的严重度较低（例如：S1），却难以避免（例如：C3）。假设暴露概率等级为E4，下面几组数值是可能的结果，其说明了最高的严重度导致最高的ASIL 等级不是必然成立的。

——E4，S2，C1 => ASIL A；及

——E4，S1，C3 => ASIL B

在此示例中，ASIL B是危害事件的合理分级。

6.4 外部措施

6.4.1 总则

外部措施是独立于且不同于相关项的措施，用于降低或减轻相关项失效造成的风险。

注1：如果外部措施独立于相关项实施的功能，则外部措施可被在HARA中考虑。

注2：外部措施作为一种降低ASIL的技术假设，根据GB/T 34590.3-XXXX，6.4.4.4被确认。

6.4.2 基于车辆的外部措施示例 1

车辆A装备手动变速箱，当熄火后，变速箱能处于任何档位，包括空档。车辆B装备自动变速箱，熄火状态下，维持一个档位啮合且离合器常闭状态。两辆车都有附加相关项，电子驻车制动（EPB）。

对两辆车辆都分析的场景含：

——车辆处于驻车状态（熄火，驾驶员不在）

——车辆位于人口密集的的城市区域的有坡度的路边

——发生涉及电子驻车功能突然丧失的失效

在此场景中，对于车辆A，当熄火时被非预期地置于空档，如果无人看管，将可能溜车。这会导致可控性评估为C3，取决于车辆附近是否有易受伤害的人员，严重度为S2或更高，且暴露概率等级大于E0。依据实际分配的暴露概率等级，得出的ASIL等级在A和C之间或QM。

车辆B一直结合在档位上而不会发生移动，所以不会导致危害。此设计中包含的基于车辆的外部措施有助于消除该场景下的风险，但前提是自动变速器和电子驻车系统能被证明是充分独立的。

6.4.3 基于车辆的外部措施示例 2

车辆A装备动态稳定控制系统和启停功能。车辆B只装备了启停功能。

对两辆车辆都分析的场景包含：

——车辆以中高速行驶（50km/h<v<90km/h）；

——路面平坦、干燥，且在郊区；

——车辆正在接近一个中等曲率的道路；

——车速和道路曲率会产生中高侧向加速度；及

——启停功能中的失效引起发动机非预期熄火，导致在此场景中突然失去驱动力。

作为突然丢失牵引力的后果，车辆会产生横摆力矩，这要求驾驶员调整方向盘以重新控制车辆。在车辆B上执行这个动作可被证明具有更低的可控性，可导致高风险。此风险评级会依赖于分配的暴露概率等级。相比之下，车辆A的动态稳定性控制功能会限制侧向不稳定的影响。结果是，车辆A的可控性等级会更好。因此，由动态稳定性控制提供的基于车辆的外部措施有助于这种情景下风险的降低。然而，仅当能证明所考虑的启停功能失效不会影响动态稳定性控制功能时，才适用这种情况。

注：此示例中使用的危害的深入分析，可在参考文献[6]中找到。

6.5 合并安全目标的示例

6.5.1 介绍

安全目标是相关项的顶层安全要求。它们导出避免危害事件产生不合理风险所需的功能安全要求。按照GB/T 34590.3-XXXX，6.4.4，概念阶段中会确定安全目标。当安全目标相似或涉及不同场景下的相同危害时，它们可以被合并成以原始安全目标的最高ASIL等级为最终ASIL等级的一个安全目标。因为更少的安全目标将被管理，但仍覆盖了所有识别出的危害，所以这能够简化后续的开发活动。

6.5.2 总则

下面示例中展示的相关项、安全目标和ASIL分级仅为了说明安全目标合并的过程。该示例不能反映将GB/T 34590系列标准应用到相似真实项目的情况。特别是，它没有完整表述失效模式识别、场景分析和整车层面的影响评估。

为简单起见，示例只限于两个安全目标的合并，但相同的方法可以扩展到更多初始安全目标的合并。

6.5.3 功能定义

考虑车辆装备了电子驻车制动（EPB）系统。当被驾驶员的特定请求激活时，EPB系统在车辆后轮施加制动力矩以防止驻车时车辆非预期的移动。

6.5.4 应用于不同场景下相同危害的安全目标

6.5.4.1 危害分析和风险评估

为简化示例，只考虑驻车功能的如下失效模式：

——非预期的驻车制动激活。

注：在此上下文中，术语“非预期的激活”是指在没有驾驶员请求的情况下的功能动作。

根据故障发生时的特定场景，此失效模式会导致不同的车辆影响，如表1所示。

表1 由不同场景下相同危害得出的安全目标

失效模式	危害	特定场景	危害事件	可能结果	ASIL	安全目标	安全状态
非预期的驻车制动激活	非预期的减速	高速行驶或转弯或低附路面	高速行驶或转弯或低摩擦路面时非预期的减速	失去车辆稳定性	较高 ASIL等级	当车辆移动时，避免在没有驾驶员请求的情况下激活驻车功能	禁止EPB
非预期的驻车	非预期的	中低速行驶且高	中低速行驶且高	与后车追尾	较低 ASIL	当车辆移动时，避免在	禁止EPB

制动激活	减速	附路面	摩擦路面时非预期的减速		等级	没有驾驶员请求的情况下激活驻车功能	

6.5.4.2 安全目标的阐述

如上所示，相同的安全目标和安全状态适用于两种场景。因此，可定义如下安全目标：

——安全目标：当车辆移动时，避免驻车功能的非预期激活；

——安全状态：禁止 EPB 功能；及

——ASIL：表 1 中确定的较高 ASIL 等级分配给此安全目标。

7 安全过程的要求结构-安全要求的流程和顺序

图8和图9展示了符合GB/T 34590的安全要求开发流程和顺序，并在下面略述。特定章以如下方式表示：“m-n”,m代表部分的数值，n代表章的数值或条的数值。

开展危害分析和风险评估以识别风险并为这些风险定义安全目标。（见GB/T 34590.3-XXXX，第6章）

导出的功能安全概念定义了功能安全要求，以满足安全目标。这些要求定义了相关项将要使用的安全机制和其他的安全措施。此外，对支持这些要求的系统架构要素进行了识别。（见GB/T 34590.3-XXXX，第7章）

导出的技术安全概念定义了技术安全要求和系统设计实现时对系统要素的分配。这些技术安全要求将指明硬件要素和软件要素的分离。（见GB/T 34590.4-XXXX，第6章）

按照技术安全要求进行系统设计开发。技术安全要求的实施可在系统设计规范中进行定义。（见GB/T 34590.4-XXXX，第6章）

最后，按照技术安全要求和系统设计，提供硬件和软件安全要求。（见GB/T 34590.5-XXXX，第6章和见GB/T 34590.6-XXXX，第6章）

图8描述了GB/T 34590硬件要求与设计阶段之间的关系。

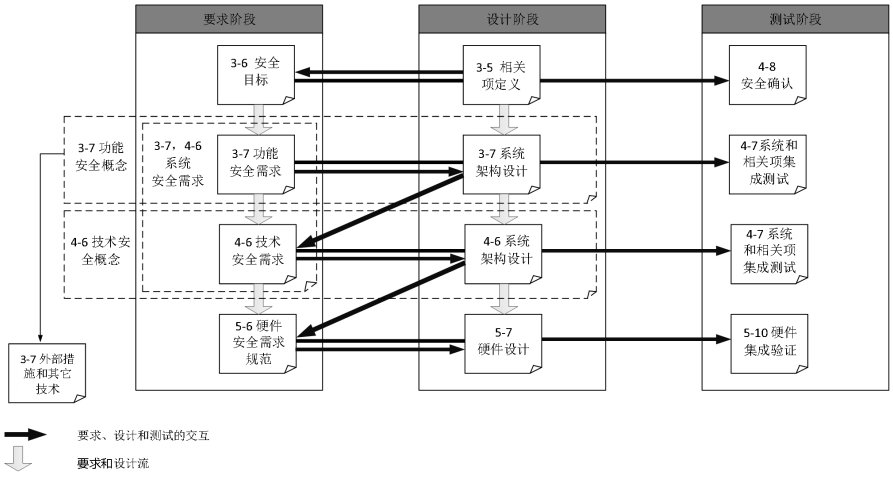


图 8　从概念到硬件的安全要求、设计和测试流

图9说明了GB/T 34590软件要求、设计和测试子阶段之间的关系。

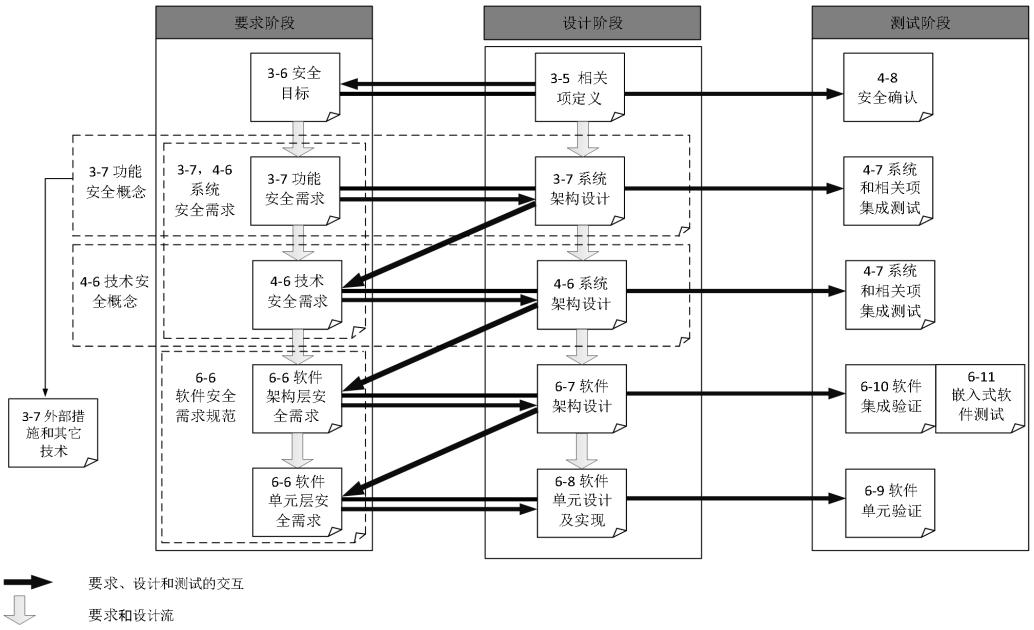


图 9　从概念到软件的安全要求、设计和测试流

——系统设计：

从相关项定义（3-6）到系统架构设计（4-6），不断细化系统设计。

——测试层面间的相关性：

每个层面上的测试规范和测试案例主要取决于相应的要求和设计。它们不取决于其它测试层面的测试规范、测试案例和测试结果。测试规范通常依赖于测试环境。

——测试层面与要求层面的相关性、测试层面与设计层面的相关性：

测试规范和测试案例由相同层面的要求得出，并由相同层面的设计信息所支持。

示例：对于性能测试，设计的信息是必要的。

——软件安全要求验证：

软件安全要求验证阶段(6-11)需要对软硬件进行集成。

——外部措施和其它技术：

外部措施和其他技术在整车层面进行验证。

8　关于硬件开发

8.1　随机硬件故障的分类

8.1.1　总则

一般来说，所考虑的故障组合限定于两个非相关的硬件故障组合，除非基于功能安全概念或技术安全概念的分析显示，n（n>2）点故障是相关的。因此，在大多数情况下，对于给定的安全目标和给定的硬件要素，故障可被归为以下某种类别：

a) 单点故障；
b) 残余故障；
c) 可探测的双点故障；
d) 可感知的双点故障；
e) 潜伏的双点故障；或
f) 安全故障。

下文将给出对于不同故障类别的解释及示例。

8.1.2 单点故障

该故障：

——可直接导致违背安全目标；及

——没有任何安全机制的硬件要素的故障。

示例：一个未被监控的电阻，并且该电阻至少有一种失效模式（例如：开路）有违背安全目标的潜在可能。

注：如果一个硬件元器件有至少一个安全机制（例如：微控制器的看门狗），则该元器件的故障不被归类为单点故障。那些安全机制未预防其违背安全目标的故障被归类为残余故障。

8.1.3 残余故障

该故障或该故障的一部分：

——可直接导致违背安全目标；及

——并且是硬件要素的故障，对于该硬件要素，有至少一个安全机制预防其某些违背安全目标的故障或者该故障的一部分。

示例：如果仅用 RAM 棋盘格检测的安全机制来检查随机存储器(RAM)模块，那么不能探测出某些种类的桥接故障。因这些故障导致的对安全目标的违背不能被安全机制所预防。这些故障即为残余故障。

注：此情况中，安全机制的诊断覆盖率小于100%。

8.1.4 可探测的双点故障

该故障：

——只有与另一个（双点故障有关的）独立硬件故障联合时，才能导致安全目标的违背；及

——并且可以被防止其潜伏的安全机制所探测。

示例 1：被奇偶校验保护的闪存：按照技术安全概念对单个位故障进行探测并触发响应，如：关闭系统并通过警示灯通知驾驶员。

示例 2：被纠错码(ECC)保护的闪存：按照技术安全概念通过测试对这些 ECC 逻辑中的故障进行探测并触发响应，如：通过警示灯通知驾驶员。

对于安全机制通过将相关项恢复至无故障状态以减轻瞬态故障的情况，即使未通知驾驶员故障的存在，此故障也被考虑为可探测的双点故障

示例：在数据提供给 CPU 前，瞬态的位翻转被纠错码(ECC)纠正，并通过写回正确值得到后续纠正。可使用记录来区分间发故障和真正的瞬态故障。

注：双点故障可分为主要双点故障和次要双点故障。即使没有安全机制来控制其故障，主要双点故障本身也不会导致违反安全目标。次要双点故障确实有可能违反安全目标，但安全机制的存在可以减轻违反安全目标的情况。

8.1.5 可感知的双点故障

该故障：

——促使安全目标的违背，但只有与另一个独立硬件故障联合时，才会导致安全目标的违背；及

——并且在规定的时间内会被驾驶员所感知（有或无安全机制探测）。

示例：如果故障后果显著并且会清楚地影响功能，双点故障可被驾驶员感知。

8.1.6 潜伏的双点故障

该故障：

——促使安全目标的违背，但只有与另一个独立硬件故障联合时，才会导致安全目标的违背；及

——不会被安全机制所探测也不被驾驶员感知。直到第二个独立故障发生前，系统始终可以运行且驾驶员也不知道发生了故障。

示例 1：对于被 ECC 保护的闪存：在读取时，ECC 纠正了单个位的永久性故障值，但这不在闪存中纠正也无信号的指示。在此情况中，故障不能导致安全目标的违背（因故障位已得到了纠正），且它不是可探测的（因对单个位故障无信号指示），也不是可感知的（因对应用的功能性无影响）。如果在 ECC 逻辑中发生了额外的故障，它可导致失去对单个位故障的控制，从而导致潜在的安全目标的违背。

示例 2：对于被 ECC 保护的闪存：ECC 逻辑中的永久性单一故障，导致在最大故障处理时间间隔内检测不到 ECC 的不可用性。

8.1.7 安全故障

安全故障可以是以下两类故障中的一种：

a) n > 2 的全部 n 点故障（除非安全概念显示它们与安全目标的违背有关联）；或

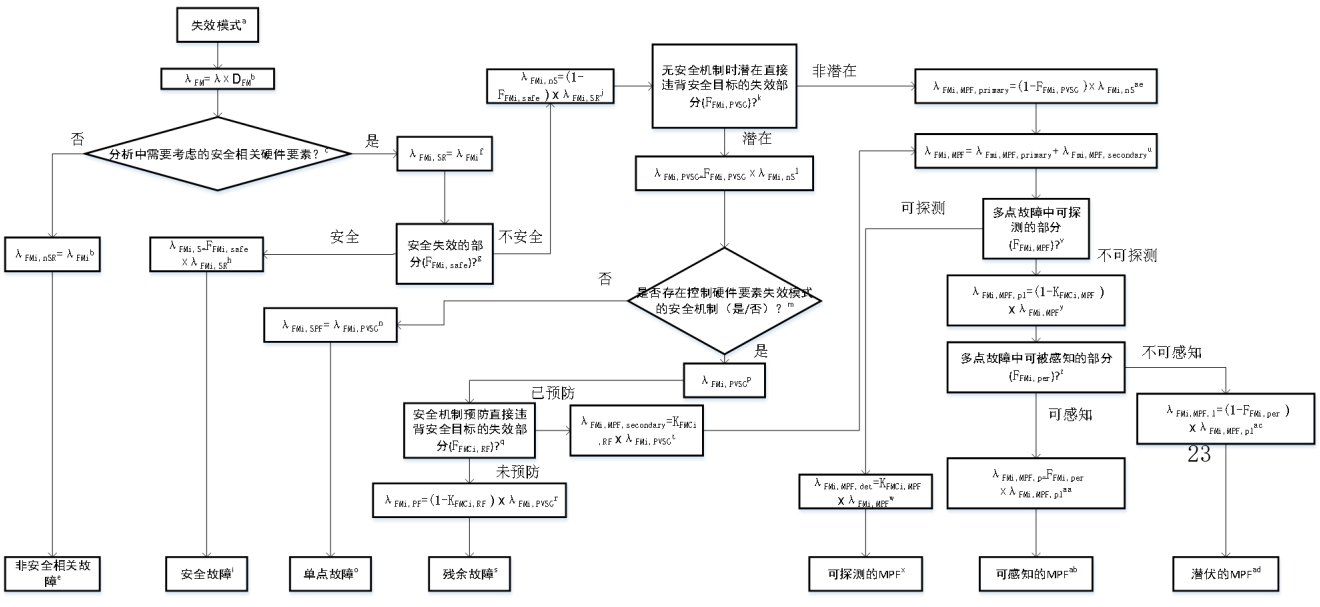
b) 或不会违背安全目标的故障。

示例 1：对于被 ECC 和循环冗余校验(CRC)保护的闪存：被 ECC 纠正的单个位故障不通过信号指示出来。该故障对安全目标的违背得到了 ECC 的预防，但未通过信号指示出来。如果 ECC 逻辑失效，该故障被 CRC 探测到，系统被关闭。只有当闪存中存在单个位故障、ECC 逻辑失效、且 CRC 校验失效时，才能发生对安全目标的违背（n=3）。

示例 2：三个电阻串联以克服短路情况下的单点故障问题，因为需要三个独立的短路才会违背安全目标（n=3），每个独立电阻的短路可被视为安全故障。

8.1.8 故障分类及故障类别贡献率计算的流程图

硬件要素的失效模式可按照GB/T 34590.5-XXXX 图B.1展示的、并使用GB/T 34590.5-XXXX图B.2描述的流程图进行分类。图10展示了考虑基础失效率及不同失效模式（残余和潜伏）覆盖率的多种失效率



计算。

图 10　失效种类的划分和相应失效率的计算

[a] 待分析的失效模式。

[b] λ_{FMi} 是所分析的硬件要素的第 i 个失效模式相关的失效率，其中D_{FMi}为该失效模式的失效模式分布。

[c] 如果所分析的硬件要素的任何失效模式都与安全相关，那么该硬件要素与安全相关。

[d] $\lambda_{FMi,\ nSR}$ 是非安全相关的失效率。

[e] 非安全相关的硬件要素的故障不在单点故障度量或潜伏故障度量之内考虑。

[f] $\lambda_{FMi,\ SR}$ 是安全相关失效率，在单点故障度量和潜伏故障度量中进行考虑。

[g] $F_{FMi,\ safe}$ 是该失效模式中的安全故障部分。安全故障不会显著导致安全目标的违背。对于复杂硬件要素（例如：微控制器），很难给出精确的比例。在此情况下，可假定保守的F_{safe}为 0.5（即 50%）。

[h] $\lambda_{FMi,\ S}$ 是安全故障的失效率。

[i] $\lambda_{FMi,\ S}$ 将增加安全故障的总体比率。

[j] $\lambda_{FMi,\ nS}$ 是非安全失效率，包括单点故障、残余故障和多点故障(n=2)。

[k] $F_{FMi,\ PVSG}$ 是非安全故障中潜在直接违背安全目标的部分（不考虑任何可能存在的防止其发生的安全机制）。违背安全目标不需要额外的独立故障。

[l] $\lambda_{FMi,\ PVSG}$ 是潜在直接违背安全目标的故障的失效率（不考虑任何可能存在的防止其发生的安全机制）。

[m] 判断所考虑的引发失效模式的故障是否为单点故障。若没有实施安全机制以预防所考虑的硬件要素的任何违背安全目标的故障，则这些故障是单点故障。

[n] $\lambda_{FMi,\ SPF}$ 是单点故障失效率。如果控制所考虑的硬件要素失效率的安全机制都不存在，则全部的 $\lambda_{FMi,\ PVSG}$ 都是单点故障。

[o] $\lambda_{FMi,\ SPF}$ 将增加单点故障的总体比率。

[p] 对于所考虑的硬件要素，如果存在至少一个安全机制预防其至少一种违背安全目标的失效模式，那么导致该失效的故障不是单点故障。在后续过程中，$\lambda_{FMi,\ PVSG}$ 被分为残余故障和可探测的、可感知的及潜伏的多点故障。

[q] 安全机制预防了 $\lambda_{FMi,\ PVSG}$ 中的哪部分对安全目标的违背？该部分等于针对残余故障的失效模式覆盖率（也可见 GB/T 34590.5 附录 E 硬件架构度量的计算示例：“单点故障度量”和“潜伏故障度量”）。$K_{FMi,\ RF}$ 是针对残余故障的失效模式覆盖率的缩写。

[r] $\lambda_{FMi,\ RF}$ 是残余故障失效率。

[s] $\lambda_{FMi,\ RF}$ 增加了残余故障的总体比率。

[t] $\lambda_{FMi,\ MPF,\ secondary}$ 是(次要)多点故障失效率，它由安全机制控制的 $\lambda_{FMi,\ PVSG}$ 导致。

[u] $\lambda_{FMi,\ MPF}$ 是由主要多点故障和次要多点故障导出的总体多点故障失效率。

[v] 识别可探测故障和不可探测故障。$K_{FMCi,\ MPF}$ 是针对多点故障的失效模式覆盖率。

[w] $\lambda_{FMi,\ MPF}$ 是多点故障失效率。

注：如果主要和次要多点故障的多点故障覆盖率不同，则可通过以下方式计算可探测的多点故障率：

$$\lambda_{FMi,MPF,det} = \boldsymbol{K}_{FMCi,MPF,primary} \times \lambda_{FMi,MPF,primary} + \lambda_{FMi,MPF,secondary} + \lambda_{FMi,MPF,secondary}$$

[x] $\lambda_{FMi,MPF,det}$ 增加了可探测的多点故障总体比率。

[y] $\lambda_{FMi,MPF,pl}$ 是可感知的或潜伏的多点故障失效率。

注：如果主要和次要多点故障的多点故障覆盖率不同，则可通过以下方式计算可感知的或潜伏的多点故障率：

$$\lambda_{FMi,MPF,p} = F_{FMi,per,primary} \times \left(1 - \boldsymbol{K}_{FMCi,MPF,primary}\right) \times \lambda_{FMi,MPF,primary} + F_{FMi,per,secondary} \times \left(1 - \boldsymbol{K}_{FMCi,MPF,secondary}\right) \times \lambda_{FMi,MPF,secondary}$$

[z] $F_{FMi,per}$ 是多点故障中未被探测但被驾驶员感知的部分。

[aa] $\lambda_{FMi,MPF,p}$ 是可感知的多点故障失效率。

注：如果主要和次要多点故障的可感知部分不同，则可通过以下方式计算可感知的多点故障率：

$$\lambda_{FMi,MPF,p} = F_{FMi,per,primary} \times \left(1 - \boldsymbol{K}_{FMCi,MPF,primary}\right) \times \lambda_{FMi,MPF,primary} + F_{FMi,per,secondary} \times \left(1 - \boldsymbol{K}_{FMCi,MPF,secondary}\right) \times \lambda_{FMi,MPF,secondary}$$

[ab] $\lambda_{FMi,MPF,p}$ 增加了可感知的多点故障的总体比率。

[ac] $\lambda_{FMi,MPF,l}$ 是潜伏多点故障失效率。

注：如果主要和次要多点故障的可感知部分不同，则可通过以下方式计算潜伏多点故障率：

$$\lambda_{FMi,MPF,l} = \left(1 - F_{FMi,per,primary}\right) \times \left(1 - \boldsymbol{K}_{FMCi,MPF,primary}\right) \times \lambda_{FMi,MPF,primary} + \left(1 - F_{FMi,per,secondary}\right) \times \left(1 - \boldsymbol{K}_{FMCi,MPF,secondary}\right) \times \lambda_{FMi,MPF,secondary}$$

[ad] $\lambda_{FMi,MPF,l}$ 增加了潜伏多点故障的总体比率。

[ae] $\lambda_{FMi,MPF,primary}$ 它由导致违背安全目标但不会直接违背安全目标的故障引起（至少需要存在一个其他的非相关故障，它才可能违背安全目标）。

注：只有当相关的诊断覆盖率、故障模式覆盖率或可感知的部分不同时，才可区分对应故障模式是主要还是次要多点故障。

8.1.9 在处理随机硬件失效时，如何考虑与基于软件的安全机制相关的多点故障失效率

尽管在GB/T 34590系列标准中没有对软件和硬件的系统性故障进行量化，但在处理随机硬件失效时，对于支持运行基于软件的安全机制的硬件资源，可计算其随机硬件失效的失效率。

如果那些硬件资源同时用于支持具有直接违背安全目标潜在可能的功能，那么选取反映此情况的失效模式并考虑潜在的相关失效。

8.2 残余失效率和局部单点故障度量评估的示例

8.2.1 总则

本示例阐述了一种评估传感器残余失效率 $\lambda_{RF,\ Sensor}$、单点失效率 λ_{SPF} 和单点故障度量 $M_{SPFM,\ Sensor}$ 实例化方法。在此示例中，测量相同物理量并具有已知误差的两个传感器，一个传感器与另一个传感器的值相比较。应用功能使用传感器A_Master的值，另一个传感器A_Checker的值仅用于确认传感器A_Master的值。

此监控在GB/T 34590.5-XXXX附录D中得到了引用，作为“传感器合理性检查”或“输入比较/表决”。

仅传感器A_Master的故障在本示例中得到了分类和评估，此处不针对传感器A_Checker的故障。

因传感器A_Master有一个已定义的安全机制，将存在的有违背安全目标潜在可能且未被控制的（即：不预防对安全目标的违背）全部故障定义为残余故障。单点失效率 λ_{SPF}（按照定义）等于零。

8.2.2 传感器 A_Master 的技术安全要求

图11中展示了传感器A_Master的安全运行边界，并作为此示例的前提（即：此处不讨论如何从安全目标导出）。它可用下述条款表示：

即

$$\mu_{(SafRelate,A,min)} = Max[C_{PVSG}; v \times (1 + a)]$$

式中：

C_{PVSG}——常值；

$\mu_{(SafRelate,A,min)}$——传感器A_Master的安全下边界；

v——待测量的物理值；

a——常值。

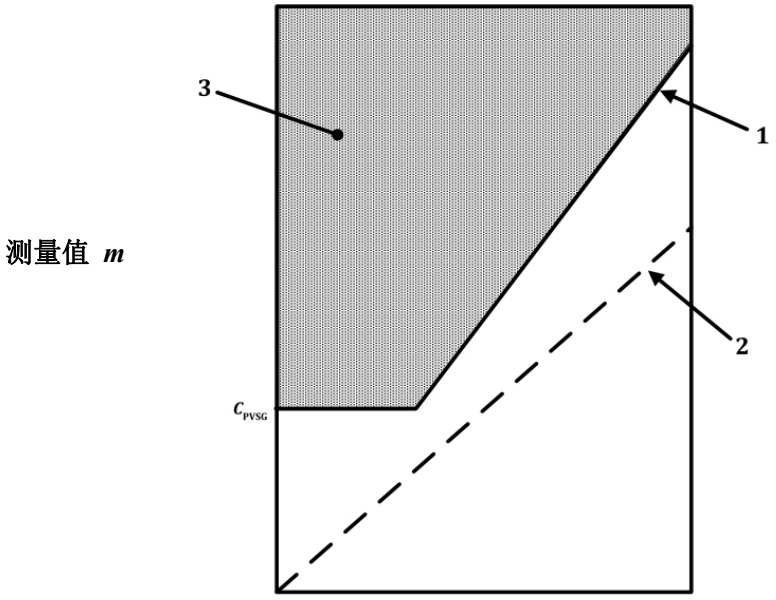
传感器的安全相关失效在如下条件时发生：

$$m_{A,Master} \geq \mu_{(SafRelate,A,min)}$$

式中：

$m_{A,Master}$——传感器A_Master的返回值。

安全要求是在故障容错时间间隔T_{SenA}内探测并控制传感器A_Master的安全相关失效。



说明：

1——传感器A_Master的安全相关下边界$\mu_{(SafRelate,A,min)}$；

2——带有0偏差的理想传感器返回值（作为参考）；

3——具有违背安全目标潜在可能的故障。

图 11　传感器 A_Master 的安全运行边界

图11中，x轴是需要测量的真实物理值v，y轴是传感器A_Master的返回值$m_{A,Master}$。虚线表示作为参考的理想传感器（即：具有0偏差的传感器）返回值。实线表示$\mu_{(SafRelate,A,min)}$。如果传感器A_Master的返回值$\mathrm{m_{A,Master}}$在实线上或高于实线，可能发生安全目标的违背。

8.2.3　安全机制的描述

安全机制的要素是传感器A_Checker和监控硬件，其包含带有嵌入式软件的微控制器。在小于容错时间T_{SenA}的周期内，软件周期性的对比两个传感器的值。通过以下伪码完成评估。

$$\Delta_A = m_{A,Master} - m_{A,Checker}$$

如果$\Delta_A \geq \Delta_{Max}$，那么失效为真。

如果失效为真，那么进入安全状态。

式中：

$m_{A,Master}$——传感器A_Master的返回值；

$m_{A,Checker}$——传感器A_Checker的返回值；

Δ_{Max}——预先定义的作为通过/不通过准则的恒定最大门限值。

假设传感器有如下已知偏差：

$$m_{A,Master} = v \pm C_{A,Master}$$

式中：

$m_{A,Master}$——传感器A_Master的返回值；

$m_{A,Checker}$——传感器A_Checker的返回值；

$C_{A,Master}$——代表传感器A_Master偏差的常值；

$C_{A,Checker}$——代表传感器A_Checker偏差的常值；

v是待测量的物理值。

选取量值Δ_{Max}以探测出传感器A_Master可能违背安全目标的失效。为了避免错误的失效探测，选择Δ_{Max}时考虑每个传感器的偏差及其它偏差的汇总$C_{A,Other}$，例如：在不同时间采样的影响：

$$\Delta_{Max} \geq C_{A,Master} + C_{A,Checker} + C_{A,Other}$$

用这种方法，探测不到失效的最严重情况是：

$$\mu_{(A,Master,wc)} = m_{A,Checker} + \Delta_{Max}$$
$$= \boldsymbol{v} + C_{A,Checker} + \Delta_{Max}$$

式中：

$\mu_{A,Master,wc}$——最恶劣情况的探测门限，即：传感器A_Master探测到的、不作为失效的最大$m_{A,Master}$值；

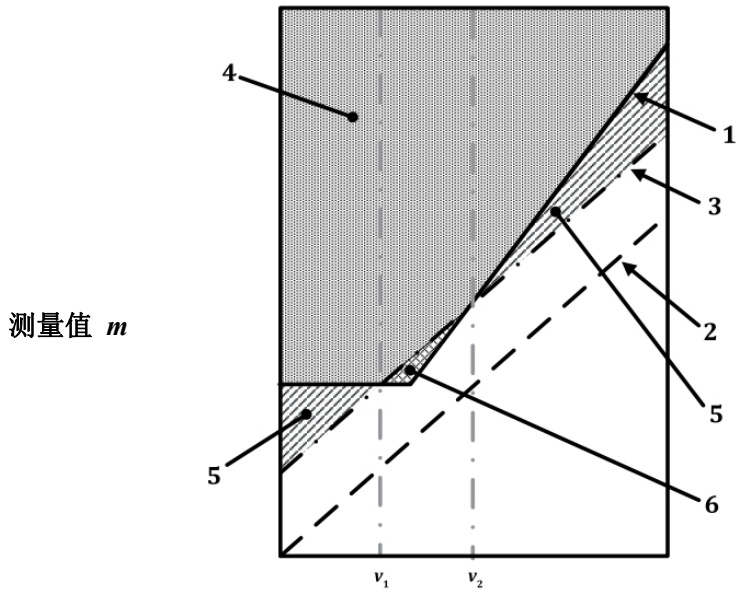
$m_{A,Checker}$——传感器A_Checker的返回值；

Δ_{Max}——预先定义的作为通过/不通过准则的恒定最大门限值；

$\boldsymbol{v}$——待测量的物理值。

将高于或者等于$\mu_{(A,Master,wc)}$的每个$m_{A,Master}$值定义为传感器失效。

取决于偏差值，不同的探测场景是可能的。图12和图13给出了两个可视化示例。



说明：

1——传感器A_Master的安全相关下边界 $\mu_{(SafRel,A,min)}$；

2——带有0偏差的理想传感器返回值（作为参考）；

3——最恶劣情况的探测门限 $\mu_{(A,Master,wc)}$；

4——探测到的双点故障；

5——探测到的不会违背安全目标的故障；

6——残余故障。

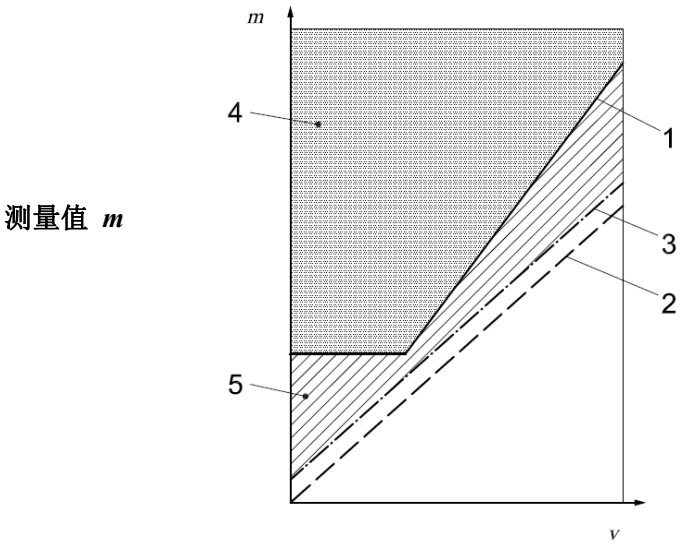
图 12　最恶劣情况探测门限（过高）的示例 1

图12中箭头指示出三个区域。

区域5：“探测到的不会违背安全目标的故障”是因其高于最恶劣情况探测门限 $\mu_{(A,Master,wc)}$，而被安全机制探测出的故障，但因其低于安全相关下边界 $\mu_{(SafRel,A,min)}$，其自身不会导致安全目标的违背。

区域4：“探测到的双点故障”是可导致安全目标违背的故障，但其被安全机制探测并减轻。这些故障同时高于最恶劣情况探测门限 $\mu_{(A,Master,wc)}$，和安全相关下边界 $\mu_{(SafRel,A,min)}$。这些故障的双点属性意味着需要安全机制和传感器同时失效才会导致对安全目标的潜在违背。

区域6：“残余故障”未被安全机制探测且能直接导致安全目标的违背。对应$v \in [v_1,v_2]$的 $\mu_{(SafRel,A,min)} < \mu_{(A,Master,wc)}$区域，位于最恶劣情况探测门限 $\mu_{(A,Master,wc)}$，以下，但高于安全相关下边界 $\mu_{(SafRel,A,min)}$。



说明：

1——传感器A_Master的安全相关下边界 $\mu_{(SafRel,A,min)}$；

2——带有0偏差的理想传感器返回值（作为参考）；

3——最恶劣情况的探测门限 $\mu_{(A,Master,wc)}$；

4——探测到的双点故障；

5——探测到的不会违背安全目标的故障。

图 13　最恶劣情况探测门限（MSPFM, Sensor=100%）的示例 2

在图13的情况，最恶劣情况探测门限 $\mu_{(A,Master,wc)}$始终小于安全相关下边界 $\mu_{(SafRel,A,min)}$。在此情况下，残余失效率为0，且传感器的局部单点故障度量$\mathrm{Min}_{SPFM,Sensor}$等于100%。

8.2.4　对图 12 所述示例 1 的评估

8.2.4.1　总则

在图12的情况，当传感器A_Master的最恶劣情况探测门限 $\mu_{(A,Master,wc)}$高于安全相关下边界 $\mu_{(SafRel,A,min)}$时，存在条件：

对于$v \in [v_1,v_2]$：$\mu_{(SafRel,A,min)} \leq \mu_{(A,Master,wc)}$

为确定在这些条件下的残余失效率 $\lambda_{RF,Sensor}$，和$\mathrm{M}_{\mathrm{SPFM,\,Sensor}}$，进一步的分析是必要的。以下是分析示例。在GB/T 34590.5-XXXX表D.1中，考虑了以下传感器（含信号开关）的故障模式：

——超出范围；

——偏移；

——在范围之内卡滞；

——振荡。

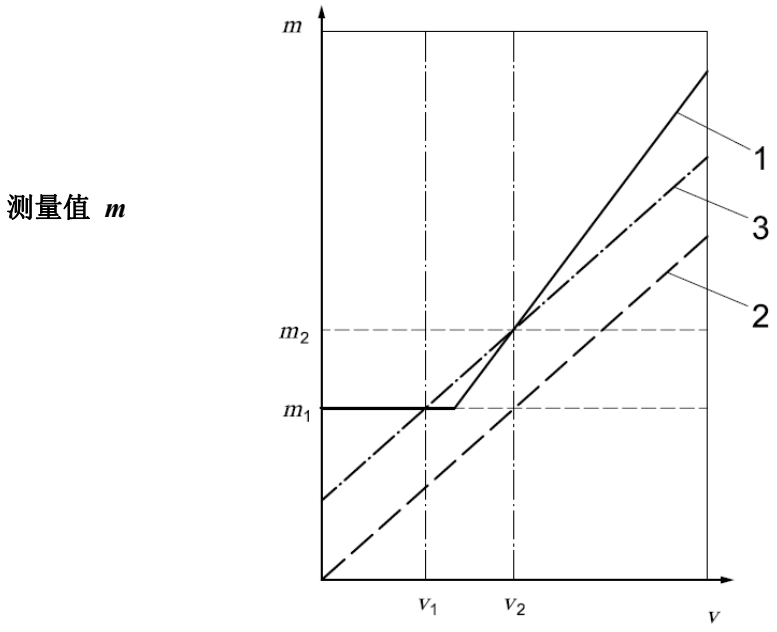
在本示例中，仅评估卡滞在恒定值m（范围内）。对于完整的传感器残余失效率及$M_{SPFM,Sensor}$的评估，全部其它失效模式都需要评估。

分析中，我们区分传感器三种不同的卡滞故障场景（见图14）：

1)　传感器卡滞在值$m > m_2$；

2)　传感器卡滞在值$m > m_1$；及

3) 传感器卡滞在m_1和m_2之间的值 m；



说明：

1——传感器A_Master的安全相关下边界 $\mu_{(SafRel,A,min)}$；

2——带有0偏差的理想传感器返回值（作为参考）；

3——最恶劣情况的探测门限 $\mu_{(A,Master,wc)}$

图 14 卡滞故障场景

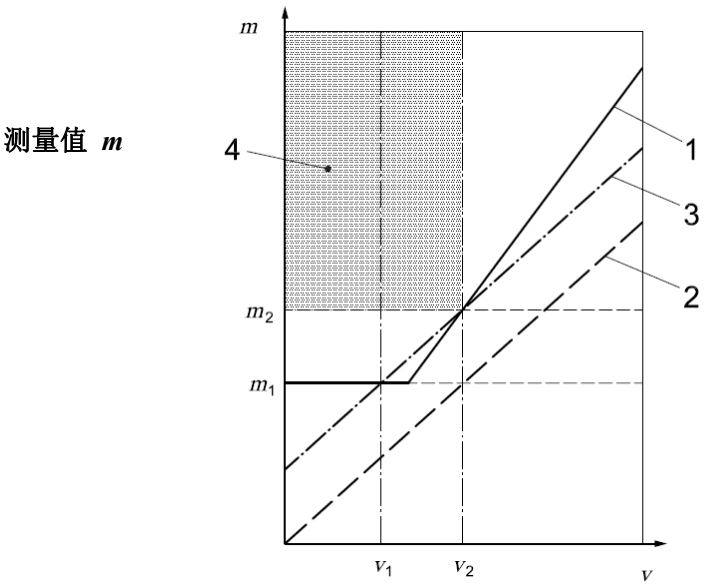
传感器卡滞故障在系统层面的影响取决于当前物理值v，例如：对于物理值$v \le v_2$，卡滞在m_2的故障有违背安全目标的潜在可能。对于值$v > v_2$，此故障没有违背安全目标的潜在可能。在以下分析中，考虑探测门限、物理值v及其分布概率，对故障成为残余故障的可能概率p_{RF}进行分析。

8.2.4.2 案例 1：传感器卡滞在 $m > m_2$值的故障

如果$v \le v_2$，故障有违背安全目标的潜在可能（见图15）。然而，传感器的偏差始终高于最恶劣情况的探测门限 $\mu_{(A,Master,wc)}$，所以安全相关的传感器失效及时得到了探测和控制。每个故障都是可探测的双点故障。在$v \le v_2$的情况下，残余故障率p_{RF}等于0。如果$v > v_2$，故障不总是具有违背安全目标的潜在可能（见图16）。如果该故障具有违背安全目标的潜在可能（图16区域5），它将高于最恶劣情况探测门限并得到及时探测。图16中的区域4和5的故障不会导致安全目标的违背。

这些故障中的一部分位于最恶劣情况探测门限以上并得到探测（图16区域4）。在$v > v_2$的情况下，残余故障率p_{RF}等于0。

如果$v \le v_2$，卡滞在$m > m_2$的故障（图15区域4和图16区域4、5、6）存在违背安全目标的潜在可能，因而它们不能被视为安全故障。因所有的故障在其导致违背安全目标前，都得到了探测和控制，它们是可探测的双点故障；所以，对于卡滞在$m > m_2$的故障的残余故障率$p_{RF_{stuck}@m> m_2}$等于0。



说明：

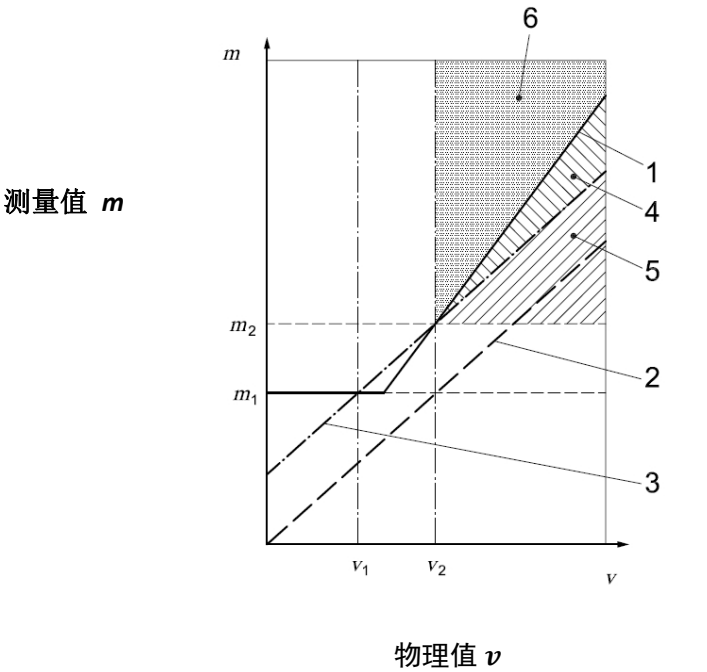
1——传感器A_Master的安全相关下边界 $\mu_{(SafRel,A,min)}$；

2——带有0偏差的理想传感器返回值（作为参考）；

3——最恶劣情况的探测门限 $\mu_{(A,Master,wc)}$；

4——可探测的双点故障。

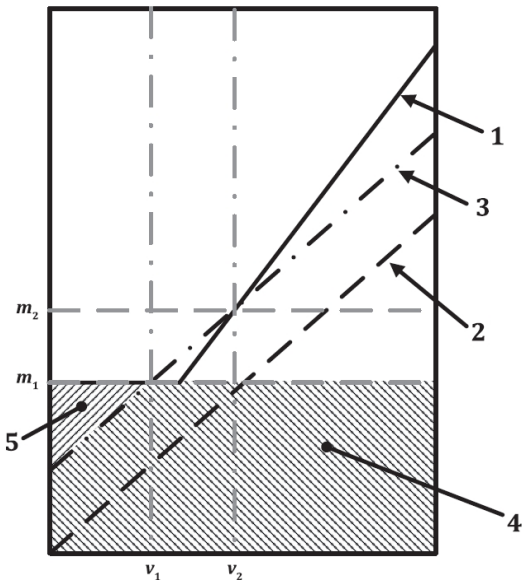
图 15　对卡滞在$m > m_2$且$v \leq v_2$的故障分类



说明：

1——传感器A_Master的安全相关下边界 $\mu_{(SafRel,A,min)}$；

2——带有0偏差的理想传感器返回值（作为参考）；



3——最恶劣情况的探测门限 $\mu_{(A,Master,wc)}$；

4——不具有违背安全目标潜在可能的可探测故障；

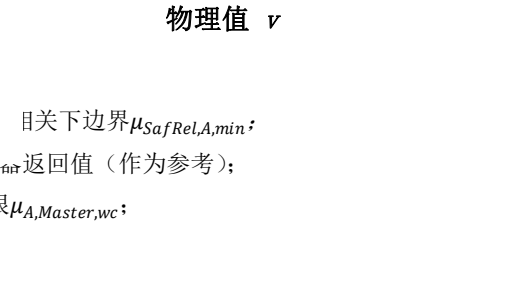
5——不具有违背安全目标潜在可能的不可探测故障；

6——可探测的双点故障。

图 16　对卡滞在$m > m_2$且$v > v_2$的故障分类

8.2.4.3　案例 2：传感器卡滞在值$m < m_1$的故障

图17中可见卡滞在$m < m_1$的故障。因在物理值v的全范围内，这些故障始终位于最恶劣情况探测门限以下，不能导致安全相关的失效，它们是安全故障。所以，对于物理值v全范围内的残余故障，其故障率$p_{RF_{stuck}@m\in[m_1,m_2]}$等于0。



说明：

1——传感器卡滞相关下边界$\mu_{SafRel,A,min}$；

2——带有0偏差的理想传感器返回值（作为参考）；

3——最恶劣情况的探测门限$\mu_{A,Master,wc}$；

4——不可探测的安全故障；

5——可探测的安全故障。

图 17　对卡滞在$m < m_1$的故障分类

8.2.4.4　案例 3：传感器卡滞在值 $m \in [m_1,m_2]$的故障

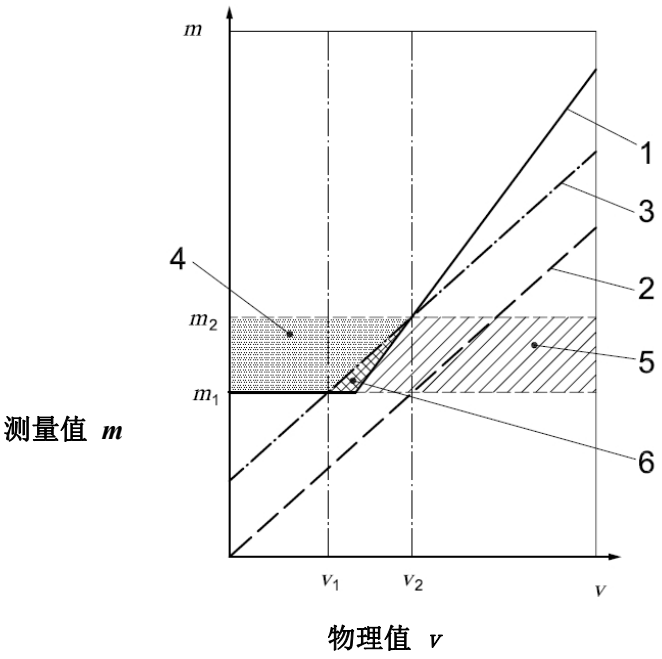
对卡滞在$m \in [m_1,m_2]$的故障，其违背安全目标的潜在可能和对其的探测取决于当前物理值v（见图18），即：违背安全目标的概率取决于故障发生时v的当前值。针对故障发生时v的三个不同区间，对卡滞型残余故障失效率$p_{RF_{stuck}@m\in [m_1,m_2]}$进行评估。

——$v < v_1$；

——$v_1 \le v \le v_2$；及

——$v > v_2$。

针对其中的每个条件，对残余故障率进行单独评估。最终残余故障率的计算，使用这三个故障率的值。



说明：

1——传感器A_Master的安全相关下边界$\mu_{(SafRel,A,min)}$；

2——带有0偏差的理想传感器返回值（作为参考）；

3——最恶劣情况的探测门限$\mu_{(A,Master,wc)}$；

4——可探测的双点故障；

5——不会违背安全目标且不可探测的故障；

6——残余故障。

图 18　对卡滞在 $m \in [m_1,m_2]$的故障分类

取决于v的当前值，故障可以是可探测的双点故障（区域4）、残余故障（区域6）或不具有违背安全目标潜在可能的故障（区域5）。

$$p_{RF_{stuck}@m\in [m_1,m_2]} = p_{RF_{stuck}@m\in [m_1,m_2],v< v_1} \times p_{v< v_1}$$

$$p_{RF_{stuck}@m\in[m_1,m_2],v_1\le v\le v_2}\times p_{v_1\le v\le v_2}$$

$$p_{RF_{stuck}@m\in[m_1,m_2]v>v_2}\times p_{v>v_2}$$

式中：

$p_{RF_{stuck}@m\in[m_1,m_2]}$ ——卡滞在值m（$m\in[m_1,m_2]$）并表现为残余故障的传感器故障率。

$p_{RF_{stuck}@m\in[m_1,m_2],v<v_1}$ ——当故障发生时$v<v_1$、卡滞在值m（$m\in[m_1,m_2]$）并且表现为残余故障的传感器故障率。

$p_{v<v_1}$ ——当故障发生时$v<v_1$的概率。

$p_{RF_{stuck}@m\in[m_1,m_2],v_1\le v\le v_2}$ ——当故障发生时$v_1\le v\le v_2$、卡滞在值m（$m\in[m_1,m_2]$）并且表现为残余故障的传感器故障率。

$p_{v_1\le v\le v_2}$ ——当故障发生时$v_1\le v\le v_2$的概率。

$p_{RF_{stuck}@m\in[m_1,m_2]v>v_2}$ ——当故障发生时$v>v_2$、卡滞在值m（$m\in[m_1,m_2]$）并且表现为残余故障的传感器故障率。

$p_{v>v_2}$ ——当故障发生时$v>v_2$的概率。

$$p_{v<v_1}+p_{v_1\le v\le v_2}+p_{v>v_2}=1$$

如果$v<v_1$，卡滞故障具有违背安全目标的潜在可能，但得到及时的探测，残余故障率$p_{RF_{stuck}@m\in[m_1,m_2],v<v_1}$是0。

如果$v>v_2$，卡滞故障不具有违背安全目标的潜在可能，但未得到探测。因为v值或早或晚介于v_1和v_2之间，则$p_{RF_{stuck}@m\in[m_1,m_2]v>v_2}=p_{RF_{stuck}@m\in[m_1,m_2],v_1\le v\le v_2}$。

如果$v_1\le v\le v_2$，残余故障率$p_{RF_{stuck}@m\in[m_1,m_2],v_1\le v\le v_2}$不为0。

对保持在残余故障区域内足够长的时间并导致潜在违背安全目标的概率的确定并非没有意义。它可基于以下参数：

——物理值 v 及其概率分布的动态表现，例如：温度值更倾向于静态信号，而使用中的电机

——角度位置更倾向于动态信号；

——值v（$v\in[v_1,v_2]$）的概率分布；

——监控软件的响应时间，例如：因过滤次数导致的响应时间。在示例中，单一事件$\Delta_A\ge\Delta_{Max}$足够用于探测传感器的失效并切换到安全状态。然而，作为通用实践，需实施一个错误计数器，进而必须有多于一次的事件以便评估传感器的失效并切换到安全状态。特别是错误计数器的恢复，例如：当探测到非安全相关的事件（此示例中，将是$\Delta_A<\Delta_{Max}$）重置错误计数器，可对监控软件的探测能力产生显著影响，将大大降低其探测能力；及

——安全相关传感器导致潜在违背安全目标所必须的测量偏差次数。同时，也可能关注，必须介于安全相关传感器两个测量偏差内的有效测量次数，以便不再违背安全目标。

如果不具备每个影响参数的准确细节，使用专家判断和工程实践（例如：对未知的概率分布使用一个等效分布）得出保守估计是合理的。

基于已评估的不同概率$p_{RF_{stuck}@m>m_2}$、$p_{RF_{stuck}@m<m_1}$和$p_{RF_{stuck}@m\in[m_1,m_2]}$，可计算传感器残余卡滞故障率$p_{RF_{stuck}@m}$：

$$p_{RF_{stuck}@m}=p_{RF_{stuck}@m<m_1}\times p_{m<m_1}+p_{RF_{stuck}@m\in[m_1,m_2]}\times p_{m_1\le m\le m_2}+$$

$$m<m_1 p_{RF_{stuck}@m>m_2}\times p_{m>m_2}$$

式中：

$p_{m<m_1}$ ——卡滞在$m<m_1$的故障率。

$p_{m_1\le m\le m_2}$ ——卡滞在$m_1\le m\le m_2$的故障率。

$p_{m>m_2}$ ——卡滞在$m>m_2$的故障率。

$$p_{m<m_1}+p_{m_1\le m\le m_2}+p_{m>m_2}=1$$

8.2.4.5 最终残余失效率评估

如果对每个相关失效模式FM_i按照上述方法进行评估，表现为残余故障的传感器总体故障率$p_{RF,Sensor}$可按如下进行计算：

$$p_{RF,Sensor} = \sum_i p_{FM,i} \times p_{RF,FM,i}$$

式中：

$p_{FM,i}$ —— 失效模式FM_i的概率。

$p_{RF,FM,i}$——失效模式FM_i表现为残余故障的概率。

$$\sum_i p_{FM,i} = 1$$

伴随此概率，残余失效率$\lambda_{RF,Sensor}$可被评估为：

$$\lambda_{\mathrm{RF,Sensor}} = p_{RF,Sensor} \times \lambda_{\mathrm{Sensor}}$$

由此得出$M_{SPFM,Sensor}$：

$$M_{SPFM,Sensor} = 1 - {}^{\lambda_{\mathrm{RF,Sensor}}}/_{\lambda_{\mathrm{Sensor}}} = 1 - p_{RF,Sensor}$$

8.2.4.6 $SPFM_{Sensor}$的提升

降低传感器残余失效率的有效方法是减小Δ_{Max}的值。在下述条件中，减小Δ_{Max}不会显著增加误探测：

——公差的概率分布可能显示预估的最恶劣情况是极其不可能的。因此，误报警概率足够低而可接受。

——系统的重新设计可得到改善的公差值。

注意，在此示例中，仅评估了传感器的故障，而非传感器存在路径中发生的故障。对于可导致两个传感器同时功能异常或可同时篡改两个传感器值的共享硬件资源（例如：微控制器的数模转换器ADC）的功能异常，进行单独评估。此外，完成如GB/T 34590.9-XXXX第7章（相关失效分析）中给出的相关失效分析。

8.3 关于硬件的进一步解释

8.3.1 在 GB/T 34590 的应用范畴内如何处理微控制器

微控制器是车辆现代电子电气系统所必需的组件。可作为独立于环境的安全要素进行开发（见第9章SEooC）。

对其复杂性的处理，是通过在恰当的抽象层面（即，从概念阶段框图到产品开发阶段连线和布局层面）开展针对微控制器元器件/子器件的定性和定量联合分析实现的。

GB/T 34590.11描述了对如何在GB/T 34590范畴内处理微控制器的包括不详尽示例清单在内的指导。

其描述了计算微控制器失效率的方法，包括如何考虑永久故障和瞬态故障。

它包含如下示例：

——相关失效分析；

——在微控制器设计过程中对系统性失效的避免；

——对微控制器安全机制的验证；及

——在系统层面对微控制器独立分析的考虑。

8.3.2 安全分析方法

8.3.2.1 总则

附录A给出了分析系统故障模式的技术方法，包括归纳分析和演绎分析。

8.3.2.2 随机硬件失效概率度量(PMHF)的计算中对暴露持续时间的考量

如GB/T 34590.5-XXXX，9.4.2.4中描述的，定量分析为GB/T 34590.5-XXXX，9.4.2.1要求的目标值得到满足提供了证据。如GB/T XXXXX.5-XXXX，9.4.2.4中给出的，在双点故障情况下，此定量分析考虑暴露持续时间。在此示例中，n=2以上的失效场景被认为是安全的，不被包括在计算中。

基于GB/T XXXXX.5-XXXX，9.4.2.4中的注2，暴露持续时间开始于故障发生时。

它包括：

——每个安全机制相关的多点故障探测时间间隔，或当故障不被驾驶员所知（潜伏故障） 时，车辆的生命周期；

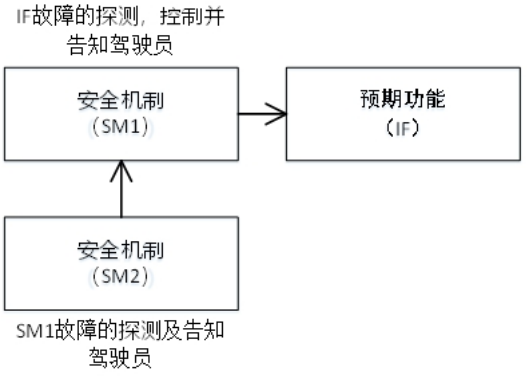
——一次行程的最长时间（驾驶员被要求以安全方式停车的情况）；及

——出现警示到车辆进入车间得到维修前的平均时间间隔（驾驶员被警示修理车辆的情况）。

8.3.2.3 典型的双点失效模式（预期功能以及安全机制）

以下示例展示了考虑暴露持续时间的可能方法。在此示例中，假定预期功能（任务块“IF”）得到安全机制“SM”的监控。

架构假设如图19所示。该示例假设，预期功能IF的故障由安全机制SM1探测和减轻。SM1还负责将IF的故障状态告知驾驶员。此外，安全机制SM1中的故障由另一个安全机制SM2探测，该安全机制SM2负责减轻SM1的故障并且将SM1的故障状态告知驾驶员。



说明：

→ 箭头起始点的安全机制探测箭头指向点的组件故障

图 19 系统架构设计示例

图19展示了由预期功能（IF）和用于探测IF失效的安全机制（SM1）构成的典型双点失效路径。假设SM1和IF的所有失效都是独立的，则IF和SM1组合导致的双点失效需要考虑：

——故障发生的顺序；

——探测和控制第一个故障的概率；

——已探测故障告知驾驶员的概率；及

——告知驾驶员后到开始修理的时间。

从以上考虑，如表2所示，可以列出四种双点失效的情况。

表 2 示例架构中的双点失效模式

	第一个故障: SM1 → 第二个故障： IF	第一个故障: IF → 第二个故障： SM1
不能告知驾驶员	模式 1	模式 3

	SM1 中的故障已被 SM2 减轻但没有告知驾驶员。故障的暴露持续时间为是整车的生命周期，为最坏情况下的暴露持续时间。 或 SM1 中的故障没有被 SM2 减轻。故障的暴露持续时间为是整车的生命周期，为最坏情况下的暴露持续时间。	IF 中的故障已经被 SM1 减轻但没有告知驾驶员。故障的暴露持续时间为是整车的生命周期，为最坏情况下的暴露持续时间。
能告知驾驶员	模式 2 SM1 中的故障已经被 SM2 减轻并且告知驾驶员。故障的暴露持续时间为驾驶员将车辆送去修理所需要的预期时间。	模式 4 IF 中的故障已经被 SM1 减轻并且告知驾驶员。故障的暴露持续时间为驾驶员将车辆送去修理所需要的预计时间。

8.3.2.4 计算公式

本章节中的公式参照了表2所列模式及GB/T 34590.5-XXXX,9.4.2.4的内容.

$$M_{PMHF} = \lambda_{SPF} + \lambda_{RF}$$
$$+ 0.5 \times \lambda_{SM1,DPF,latent} \times \lambda_{IF,DPF} \times T_{lifetime} \quad \text{模式1}$$
$$+ \lambda_{SM1,DPF,detected} \times \lambda_{IF,DPF} \times T_{service} \quad \text{模式2}$$
$$+ 0.5 \times \lambda_{IF,DPF,latent} \times \lambda_{SM1,DPF} \times T_{lifetime} \quad \text{模式3}$$
$$+ \lambda_{IF,DPF,detected} \times \lambda_{SM1,DPF} \times T_{service} \quad \text{模式4}$$

式中：

M_{PMHF} ——使用 GB/T 34590-5:XXXX, 9.4.2.2 确定的 PMHF 值；

λ_{SPF} ——单点失效率；

λ_{RF} ——残余失效率；

$\lambda_{IF,DPF}$ ——IF 的双点失效率；

$\lambda_{IF,DPF,detected}$ ——IF 被探测并告知驾驶员的双点失效率；

$\lambda_{IF,DPF,latent}$ ——IF 的潜伏双点失效率（被减轻但没有告知驾驶员）；

$\lambda_{SM1,DPF}$ ——SM1 的双点失效率；

$\lambda_{SM1,DPF,detected}$ ——SM1 被探测并告知驾驶员的双点失效率；

$\lambda_{SM1,DPF,latent}$ ——SM1 的潜伏双点失效率；

$T_{lifetime}$ ——整车生命周期；

$T_{service}$ ——驾驶员被告知后送修的预计时间。

注1：在此示例中，由于所有硬件要素由安全机制监控，故单点失效率为零（λSPF = 0）。

注2：在模式1和模式3中，双点失效中的单个故障发生顺序是很重要的。在模式1中，SM1的潜伏双点故障在IF的双点故障之前发生。在模式3中，IF的潜伏双点故障在SM1的双点故障之前发生。

如在8.1.8中的定义，不同的双点失效率能如下进行计算：

$$\lambda_{IF,DPF} = \lambda_{IF,DPF,primary} + \lambda_{IF,DPF,secondary}$$
$$\lambda_{IF,DPF,primary} = \left(1 - F_{IF,safe}\right) \times \left(1 - F_{IF,PVSG}\right) \times \lambda_{IF}$$
$$\lambda_{IF,DPF,\text{secondary}} = \left(1 - F_{IF,safe}\right) \times F_{IF,PVSG} \times K_{FMC,SM1,RF} \times \lambda_{IF}$$
$$\lambda_{IF,DPF,detected} = \lambda_{IF,DPF,\text{detected},primary} + \lambda_{IF,DPF,\text{detected},secondary}$$

$$\lambda_{IF,DPF,\text{detected},primary} = \lambda_{IF,DPF,primary} \times K_{FMC1,SM1,MPF}$$
$$= \left(1 - F_{IF,safe}\right) \times \left(1 - F_{IF,PVSG}\right) \times K_{FMC1,SM1,MPF} \times \lambda_{IF}$$
$$\lambda_{IF,DPF,\text{detected},secondary} = \lambda_{IF,DPF,secondary} \times K_{FMC2,SM1,MPF}$$
$$= \left(1 - F_{IF,safe}\right) \times F_{IF,PVSG} \times K_{FMC1,SM1,RF} \times K_{FMC2,SM1,MPF} \times \lambda_{IF}$$
$$\lambda_{IF,DPF,latent} = \lambda_{IF,DPF,\text{latent},primary} + \lambda_{IF,DPF,\text{latent},secondary}$$
$$\lambda_{IF,DPF,\text{latent},primary} = \lambda_{IF,DPF,primary} \times \left(1 - K_{FMC1,SM1,MPF}\right)$$
$$= \left(1 - F_{IF,safe}\right) \times \left(1 - F_{IF,PVSG}\right) \times \left(1 - K_{FMC1,SM1,MPF}\right) \times \lambda_{IF}$$
$$\lambda_{IF,DPF,\text{latent},secondary} = \lambda_{IF,DPF,secondary} \times \left(1 - K_{FMC2,SM1,MPF}\right)$$
$$= \left(1 - F_{IF,safe}\right) \times F_{IF,PVSG} \times K_{FMC,SM1,RF} \times \left(1 - K_{FMC2,SM1,MPF}\right) \times \lambda_{IF}$$
$$\lambda_{SM1,DPF} = \lambda_{SM1,DPF,primary} + \lambda_{SM1,DPF,secondary}$$
$$\lambda_{SM1,DPF,primary} = \left(1 - F_{SM1,safe}\right) \times \left(1 - F_{SM1,PVSG}\right) \times \lambda_{SM1}$$
$$\lambda_{SM1,DPF,\text{secondary}} = \left(1 - F_{SM1,safe}\right) \times F_{SM1,PVSG} \times K_{FMC,SM2,RF} \times \lambda_{SM1}$$
$$\lambda_{SM1,DPF,detected} = \lambda_{SM1,DPF,\text{detected},primary} + \lambda_{SM1,DPF,\text{detected},secondary}$$
$$\lambda_{SM1,DPF,\text{detected},primary} = \lambda_{SM1,DPF,primary} \times K_{FMC1,SM2,MPF}$$
$$= \left(1 - F_{SM1,safe}\right) \times \left(1 - F_{SM1,PVSG}\right) \times K_{FMC1,SM2,MPF} \times \lambda_{SM1}$$
$$\lambda_{SM1,DPF,\text{detected},secondary} = \lambda_{SM1,DPF,secondary} \times K_{FMC2,SM2,MPF}$$
$$= \left(1 - F_{SM1,safe}\right) \times F_{SM1,PVSG} \times K_{FMC,SM2,RF} \times K_{FMC2,SM2,MPF} \times \lambda_{SM1}$$
$$\lambda_{SM1,DPF,latent} = \lambda_{SM1,DPF,\text{latent},primary} + \lambda_{SM1,DPF,\text{latent},secondary}$$
$$\lambda_{SM1,DPF,\text{latent},primary} = \lambda_{SM1,DPF,primary} \times \left(1 - K_{FMC1,SM2,MPF}\right)$$
$$= \left(1 - F_{SM1,safe}\right) \times \left(1 - F_{SM1,PVSG}\right) \times \left(1 - K_{FMC1,SM2,MPF}\right) \times \lambda_{SM1}$$
$$\lambda_{SM1,DPF,\text{latent},secondary} = \lambda_{SM1,DPF,secondary} \times \left(1 - K_{FMC2,SM2,MPF}\right)$$
$$= \left(1 - F_{SM1,safe}\right) \times F_{SM1,PVSG} \times K_{FMC,SM1,RF} \times \left(1 - K_{FMC2,SM2,MPF}\right) \times \lambda_{SM1}$$

式中：

λ_{IF} ——IF 的失效率；

λ_{SM1} ——SM1 的失效率；

$F_{IF,safe}$ ——IF 安全故障的概率；

$F_{SM1,safe}$ ——SM1 安全故障的概率；

$F_{IF,PVSG}$ ——在缺乏安全机制的情况下，IF 的故障有可能直接违反安全目标的概率；

$F_{SM1,PVSG}$ ——在缺乏安全机制的情况下，SM1 的故障有可能直接违反安全目标的概率；

注：某些安全机制自身的失效可能会导致安全目标的违反，例如，ECC可以通过错误的纠正从而损坏正确的值。

$K_{FMC,SM1,RF}$ ——SM1 对 IF 残余故障的诊断覆盖率；

$K_{FMC1,SM1,MPF}$ ——多点故障中先发生 SM1 对 IF 故障的可探测并且可感知的诊断覆盖率；

$K_{FMC2,SM1,MPF}$ ——多点故障中后发生 SM1 对 IF 故障的可探测并且可感知的诊断覆盖率；

$K_{FMC,SM2,RF}$ ——SM2 对 SM1 残余故障的诊断覆盖率；

$K_{FMC1,SM2,MPF}$ ——多点故障中先发生 SM2 对 SM1 故障的可探测并且可感知的诊断覆盖率；

$K_{FMC2,SM2,MPF}$ ——多点故障中后发生 SM2 对 SM1 故障的可探测并且可感知的诊断覆盖率；

表 3　图 19 示例架构的失效率示例

违反安全目标的失效模式诊断覆盖率	残余或单点故障失效率(e^{-9}/h)	双点故障失效率(e^{-9}/h)	描述	阻止失效模式成为潜在故障的探测方法或安全机制 SM(S)	对于潜在失效的失效模式覆盖率	潜在多点故障失效率(e^{-9}/h)	描述	可探测多点故障失效率(e^{-9}/h)	描述
0.9	2.0	18.0	$\lambda_{IF,DPF,lsecondary}$	SM1	0.8	3.6	$\lambda_{IF,DPF,latent,secondary}$	14.4	$\lambda_{IF,DPF,detected,secondary}$
0	15.0								
		15.0	$\lambda_{IF,DPF,primary}$	SM1	0.7	4.5	$\lambda_{IF,DPF,latent,primary}$	10.5	$\lambda_{IF,DPF,detected,primary}$
0.8	1.5	6.0	$\lambda_{SM1,DPF,secondary}$	SM2	0.6	2.4	$\lambda_{SM1,DPF,latent,secondary}$	3.6	$\lambda_{SM1,DPF,detected,secondary}$
		10.0	$\lambda_{SM1,DPF,primary}$	SM2	0.4	6.0	$\lambda_{SM1,DPF,latent,primary}$	4.0	$\lambda_{SM1,DPF,detected,primary}$
		7.5	$\lambda_{SM1,DPF,primary}$	无	—	7.5	$\lambda_{SM1,DPF,latent,primary}$		$\lambda_{SM1,DPF,detected,primary}$

组件名	失效率（e^{-9}/h）	失效模式	失效模式分布	安全机制缺失导致失效模式有可能违反安全目标	安全机制SM(S)阻止失效模式违反安全目标
IF	100	安全	0.5		
		FM A	0.2	X	SM1
		FM B	0.15	X	无
		FM C	0.15		
SM1	50	安全	0.5		
		FM D	0.15	X	SM2
		FM E	0.2		
		FM F	0.15		

示例：根据双点故障率计算公式，8.3.2.4 中的M_{PMHF}可根据表 3 中的值进行如下计算得到：

$\lambda_{IF,DPF}$ = 33e^{-9}/h

$\lambda_{IF,DPF,detected}$ = 24.9e^{-9}/h

$\lambda_{IF,DPF,latented}$ = 8.1e^{-9}/h

$\lambda_{SM1,DPF}$ = 23.5e^{-9}/h

$\lambda_{SM1,DPF,detected}$= 7.6e^{-9}/h

$\lambda_{SM1,DPF,latent}$ = 15.9e^{-9}/h

M_{PMHF} = 18.5e^{-9}/h + 0.5 × 15.9e^{-9}/h × 33e^{-9}/h × 10000 h + 7.6e^{-9}/h × 33e^{-9}/h × 20h + 0.5 × 8.1e^{-9}/h × 23.5e-9/h × 10000 h + 24.9e^{-9}/h × 23.5e^{-9}/h × 20 h = 18.504e^{-9}/h

在示例中做出假设：

$F_{IF,safe}$ = 0（IF 无安全故障），

$F_{SM1,safe}$ = 0（SM1 无安全故障），

$F_{IF,PVSM}$ = 1（安全机制缺失的情况下，IF 存在唯一故障有可能违反安全目标），及

$F_{SM1,PVSG}$ = 0（安全机制缺失的情况下，IF 不存在故障有可能违反安全目标），

双点失效率可按如下进行计算：

$\lambda_{IF,DPF} = K_{FMC,SM1,RF} \times \lambda_{IF}$

$\lambda_{IF,DPF,detected} = K_{FMC,SM1,RF} \times K_{FMC2,SM1,RF} \times \lambda_{IF}$

$\lambda_{IF,DPF,latent} = K_{FMC,SM1,RF} \times \left(1 - K_{FMC2,SM1,RF}\right) \times \lambda_{IF}$

$\lambda_{SM1,DPF} = \lambda_{SM1}$

$\lambda_{SM1,DPF,detected} = K_{FMC1,SM2,MPF} \times \lambda_{SM1}$

$\lambda_{SM1,DPF,latent} = \left(1 - K_{FMC1,SM2,MPF}\right) \times \lambda_{SM1}$

本章的公式假设了一个指数失效率模型和一阶近似解。例如：$T_{lifetime} \times \lambda_{SM1}$和$T_{lifetime} \times \lambda_{IF}$都很小（通常小于 0.1）。

在以下情况下评估$T_{service}$的贡献：通过对M_{PMHF}进行计算，以验证 PMHF 的目标值是否可以按照所考虑的硬件设计假设来达到：

a) 如果 PMHF 的目标值高于或等于$\lambda_{SPF} + \lambda_{RF} + \lambda_{SM1,DPF} \times \lambda_{IF,DPF} \times T_{lifetime}$，PMHF 的目标值可以独立于$T_{service}$来达到。

注：当所有的双点故障都假定为潜伏故障用于计算时，$M_{PMHF} = \lambda_{SPF} + \lambda_{RF} + \lambda_{SM1,DPF} \times \lambda_{IF,DPF} \times T_{lifetime}$。

b) 如果 PMHF 的目标值低于$\lambda_{SPF} + \lambda_{RF} + \left(\lambda_{SM1,DPF,latent} \times \lambda_{IF,DPF} + \lambda_{IF,DPF,latent} \times \lambda_{SM1,DPF}\right) \times 0.5_{SM1,DPF} \times T_{lifetime}$，PMHF 的目标值不能独立于$T_{service}$来达到。

注：当$T_{service}$被假定等于0用于计算时，$M_{PMHF} = \lambda_{SPF} + \lambda_{RF} + \left(\lambda_{SM1,DPF,latent} \times \lambda_{IF,DPF} + \lambda_{IF,DPF,latent} \times \lambda_{SM1,DPF}\right) \times 0.5 \times T_{lifetime}$。

c) 如果 PMHF 的目标值低于$\lambda_{SPF} + \lambda_{RF} + \lambda_{SM1,DPF} \times \lambda_{IF,DPF} \times T_{lifetime}$并且高于或等于$\lambda_{SPF} + \lambda_{RF} + \left(\lambda_{SM1,DPF,latent} \times \lambda_{IF,DPF} + \lambda_{IF,DPF,latent} \times \lambda_{SM1,DPF}\right) \times 0.5 \times T_{lifetime}$，若$T_{service}$满足下式，则可以达到 PMHF 的目标值：

$$T_{service} \leq \frac{\left(PMHF \text{ 目标值} - \lambda_{SPF} - \lambda_{RF} - \left(\lambda_{SM1,DPF,latent} \times \lambda_{IF,DPF} + \lambda_{IF,DPF,latent} \times \lambda_{SMI,SPF}\right) \times 0.5 \times T_{lifetime}\right)}{\left(\lambda_{SM1,DPF,detected} \times \lambda_{IF,DPF} + \lambda_{IF,DPF,detected} \times \lambda_{SMI,SPF}\right)}$$

注：这个公式在12.3.1.2中使用。

8.4 PMHF 单位——每小时平均概率

可靠性分析通常提供单个组件或者零件的失效率。功能安全需要考虑安全机制提供的故障探测、控制和通知功能的影响。因此，即使采用与可靠性分析相同的单位（1/h），其意义也不相同。

GB/T 34590.5-XXXX, 9.4.2.1给出了PMHF计算的单位，即相关项在整个运行生命周期内每小时的平均概率。该条的注1指出，即使共享相同的单元，在相关项整个运行生命周期内的失效率和每小时平均失效概率也是不同的值。

PMHF的计算用于确定由于相关项的随机硬件失效导致的违背安全目标的风险相对于指定的ASIL是否足够低。PMHF不会显示出随机硬件失效发生的频率。即使硬件元器件的失效率很高，由于良好的硬件架构设计（包括安全机制），PMHF可能会很低。

PMHF由单点故障(8.1.2)、残余故障(8.1.3)、可探测或可感知的双点故障(8.1.4和8.1.5)和潜在故障(8.1.6)组成。相关项中的各类故障在运行生命周期内的每小时平均概率，对PMHF的组成是不同的。

下面给出了关于相关项单点故障在运行生命周期内每小时平均失效概率的推导：

$$Prob(T \leq t) = F(t) = 1 - R(t), t \geq 0$$

式中：

$Prob(T \leq t)$ ——当 $T \leq t$ 时，失效发生的概率；

$F(t)$ ——失效分布；

t ——时间；

T ——失效发生的时间；

$R(t)$ ——随时间变化的系统可靠性；

F(t)表示为：

$$\mathrm{F(t)} = \int_0^t f(\tau) \times d\tau$$

式中 f(t)为失效密度函数。

瞬时失效率λ(t)为：

$$\lambda(\mathrm{t}) = \lim_{\Delta t \to 0} \left[\frac{R(t)-R(t+\Delta t)}{\Delta t \times R(t)}\right] = \frac{f(t)}{R(t)} = \frac{f(t)}{1-F(t)}$$

一般认为，失效率为常数，失效密度函数为指数分布。

因此，$\mathrm{F(t)} = 1 - e^{-\lambda t}$，式中 λ 为失效率。

那么，运行生命周期内（$\mathrm{T_{lifetime}}$）每小时平均失效概率（根据 GB/T 34590-5）为：

$$\frac{\mathrm{Prob}(T \le T_{\mathrm{lifetime}})}{T_{\mathrm{lifetime}}} = \frac{1 - e^{-\lambda \times T_{\mathrm{lifetime}}}}{T_{\mathrm{lifetime}}}$$

如果$\lambda \times T_{\mathrm{lifetime}} \ll 1$，那么 $1 - e^{-\lambda \times T_{\mathrm{lifetime}}} \cong \lambda \times T_{\mathrm{lifetime}}$。

因此，相关项在运行生命周期内每小时平均失效概率可以简化为：

$$\frac{\mathrm{Prob}(T \le T_{\mathrm{lifetime}})}{T_{\mathrm{lifetime}}} = \lambda$$

因此，对于单点故障，相关项在运行生命周期内每小时平均失效概率与失效率相等。考虑到安全机制探测和处理故障的比例，相关项在运行生命周期内残余故障与此类似。

如果考虑多点故障，则考虑GB/T 34590.5-XXXX，9.4.2.4中规定的暴露持续时间。如果多点故障可被探测或被感知，则暴露持续时间等于故障发生后维持工作的时间跨度。在这种情况下，运行时间内每小时的平均概率取决于失效率和暴露持续时间，与整车生命周期无关。如果多点故障仍然是潜在的，那么在运行生命周期内每小时平均失效概率取决于运行生命周期。这些可以用8.3.2.4中的数学公式表示。

示例：一个系统有两个独立的组件，A 和 B，提供了系统冗余。两个组件必须不能违反安全目标，且任何一个组件的故障不可被自身探测和感知，即 A 和 B 组件的所有故障都是潜在双点故障，两者均为指数失效分布：

$F_A(t) = \int_0^t \lambda_A \times e^{-\lambda_A \times \tau} d\tau = 1 - e^{-\lambda_A \times \tau}$；及

$F_B(t) = \int \lambda_B \times e^{-\lambda_B \times \tau} d\tau = 1 - e^{-\lambda_B \times \tau}$

式中λ_A和λ_B分别是组件A和B的失效率，并且$\lambda_A = \lambda_B$ = 3e-6/h。

图20显示了组件A和组件B的多点失效的失效分布F(t)，生命周期可达10000小时（黑色实线）。该失效分布的时间导数f(t)除以相应的可靠性R(t)，即为该多点失效的瞬时失效率。由于f(t)随时间增加而R(t)保持非常接近1.0，因此瞬时故障率随时间增加。

灰色的点线和虚线的斜率分别表示5000小时内和8000小时内的平均失效率。注意，每小时平均概率并不等于恒定的失效率。点划线和实灰线的斜率分别表示在5000 h和8000 h时的失效密度函数f(t)。在这个示例中，由于R(t)非常接近1.0，所以这个失效密度非常接近瞬时失效率。

假设$\lambda_A \times T_{\mathrm{lifetime}}$和$\lambda_B \times T_{\mathrm{lifetime}}$很小，在整车生命周期内违反安全目标的概率(F (t))大约为：

$$F(T_{\mathrm{lifetime}}) \approx (\lambda_A \times T_{\mathrm{lifetime}}) \times (\lambda_B \times T_{\mathrm{lifetime}})$$

因此，在相关项的运行生命周期内每小时的平均概率为:

$$F(T_{\mathrm{lifetime}})/T_{\mathrm{lifetime}} \approx \lambda_A \times \lambda_B \times T_{\mathrm{lifetime}}$$

对应的瞬时失效率大约为：

$$\lambda(T_{\text{lifetime}}) = \frac{\frac{dF}{dt}(T_{\text{lifetime}})}{1 - F(T_{\text{lifetime}})} = \frac{f(T_{\text{lifetime}})}{R(T_{\text{lifetime}})} \approx 2 \times \lambda_A \times \lambda_B \times T_{\text{lifetime}}$$

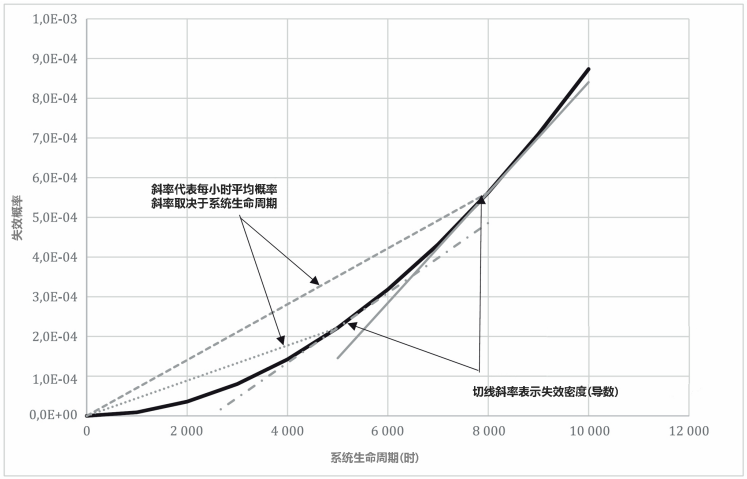


图 20　失效率分布示例

总之，该示例说明了GB/T 34590-5中定义的PMHF计算的主要目的。在相关项的运行生命周期内，违反安全目标的概率被确定后并除以相关项的运行生命周期。该结果表示为每小时的平均概率，这类评估很典型(例：IEC 61508采用了相同的单元)，而不是失效率。

系统失效率是一个与时间相关的函数，评估时可能会变得非常复杂，特别是在系统设计中包含冗余的情况下。这个示例在最简单的冗余架构上说明了这种复杂性。此外，对这种函数的解释对于非专业人士来说并不明显，而概率是一个容易理解的量。

注：GB/T 34590.5对如何确定运行生命周期没有给出指导。相关项所有者有责任指定要使用的运行生命周期。

9　独立于环境的安全要素

9.1　独立于环境的安全要素的开发

汽车工业为不同的客户和不同的应用开发通用的要素。这些通用的产品是在不同的组织中独立开发出来的。在这种情况下，先做出关于需求以及设计的假定，这些假定包括了通过更高设计层级以及要素外部设计而得到的分配到要素的安全要求。

这样开发出来的要素可以当作是独立于环境的安全要素（SEooC）。SEooC是与安全相关的要素，它不是为了一个特定相关项而开发的。这意味着它不是在一个特定车辆环境中开发出来的。

SEooC可以是系统，系统组合，子系统，软件组件，硬件组件或者零部件。SEooC的示例包括系统控制器，ECU，微控制器，执行通信协议的软件，或者AUTOSAR软件组件。

SEooC不可以是一个相关项，因为相关项总是需要用于批量生产的整车环境。如果SEooC是一个系统，而该系统不是在整车环境中开发的，那么它就不是一个相关项。

对比SEooC与GB/T 34590.8-XXXX第12章中鉴定的软件组件和GB/T 34590.8-XXXX第13章中评估的硬件要素，其区别在于：

——SEooC 是按照 GB/T 34590 基于假设开发的。若在集成 SEooC 过程中可以证实该 SEooC 的假设的有效性，则它可用于多个不同的相关项。

——软件组件的鉴定和硬件要素的评估表述了按照 GB/T 34590 开发的相关项对于已有软件组件或硬件要素的使用。这些组件和要素不是为了复用性设计的，也不是按照 ISO26262 系列标准开发的。

针对软件开发，表4描述了不同软件组件的鉴定、独立于环境的安全要素和在用证明的预期使用。针对硬件开发，可以构建一个等价表。

表 4　软件组件的分类

软件组件的分类	GB/T 34590.6 在相关项的环境中	GB/T 34590.8-XXXX 第12 章软件组件的鉴定	GB/T 34590.6 作为独立于环境的安全要素	GB/T 34590.8-XXXX 第14 章在用证明的论据
全新开发	适用	不适用	适用	不适用
带变更的复用	适用	不适用	适用	适用 [a]
不带变更的复用	不适用	适用	适用 （如果最初作为SEooC来开发）	适用
[a] 见GB/T 34590.8-XXXX,14.4.4。				

当开发一个SEooC时，可根据GB/T 34590-XXXX，6.4.5.7对所应用的安全活动进行裁剪。这种对于SEooC开发的裁剪并不意味着安全生命周期中的任何一个步骤都可被省略。即使在SEooC的开发中某些步骤推迟了，它们也会在相关项开发中完成的。

SEooC的ASIL能力标明了该SEooC遵从指定了ASIL等级的安全要求的能力。所以，它定义了应用于该SEooC开发的GB/T 34590的需求。

因此，SEooC是基于假设而开发的；假设了一个既定的功能以及包含外部接口的使用环境。这些假定是以一种阐述相关项父级的方式而建立的，故后期SEooC可在多个不同但却相似的相关项中使用。

在实际相关项的环境中集成SEooC时，证实这些假设的有效性。

一个相关项可能包含多个SEooC，而各SEooC之间的接口是直接互相连接的。这种情况下，对其中一个SEooC假设的有效性证实需要考虑与其互连的SEooC。

如果在SEooC集成到相关项的过程中无法证实该SEooC在开发过程所做的假设的有效性，则可以按照GB/T 34590.8-XXXX第8章对该SEooC或相关项进行更改。

9.2　使用案例

9.2.1　概述

SEooC的开发包括对产品开发的相应阶段做出前提条件的假设，例如对于一个软件组件，它是软件架构设计的一部分，相应的阶段是GB/T 34590.8-XXXX第7章。无须对所有的前提条件做假设。

图21表示了假设与SEooC开发之间的关系。一个SEooC的开发可以从需求和设计的某个层级开始。每个单独的要求和设计的先决条件都预定义为“假设”状态。

对SEooC需求（由假设的高级别需求和假设的该SEooC外部设计而派生出来的）的正确实施将在SEooC开发过程中得到验证。

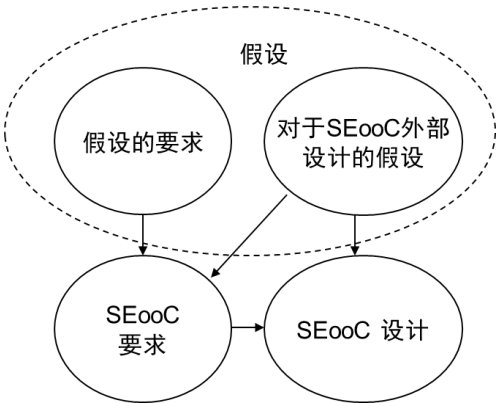


图 21　假设与 SEooC 开发之间的关系

这些需求和假设的确认在相关项的开发过程中进行确认。

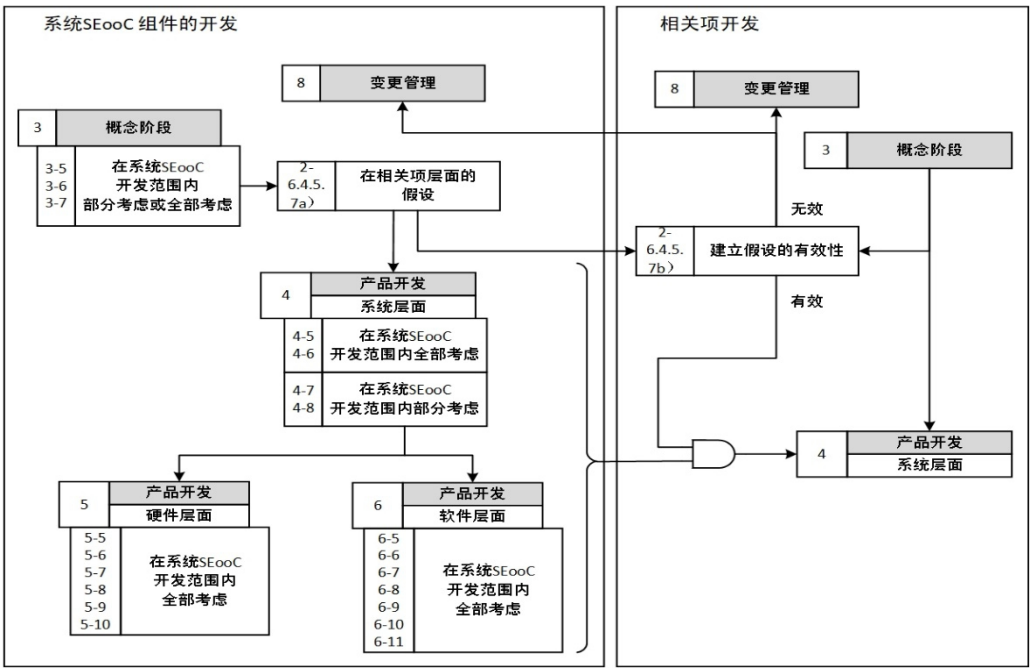
类似的，确认活动表明了一个已经开发好的SEooC，在任何层面，是符合其使用环境需求的。例如，当使用一个独立于环境而开发的软件组件，对软件规范的确认能证明其满足软件架构设计规范中的需求。在SEooC开发完成，并且相关项开发达到安全要素需求形成的阶段，可以产出该确认报告。

下面给出了SEooC的一些典型示例，即系统，硬件组件和软件组件。

9.2.2　开发一个作为 SEooC 的系统

本节用于说明一个可被不同整车制造商所集成的新的E/E系统中，如何应用SEooC概念的裁剪工作。

为了说明，系统包含的功能不仅有在特定整车条件下的功能激活，还允许在适当的驾驶员要求下功能停止。过程流如图22所示。



注1：有必要依据SEooC的确切特性，对需求做额外的裁剪。

注2：依据SEooC的确切特性，第三部分和第四部分的一些需求可能不适用，所以只做了部分考虑。

注3：尽管不能给出所有的GB/T 34590章条，但这并不意味着它们是不适用的。

图 22　SEooC 系统开发

步骤1a：对SEooC范围的定义

基于假设，SEooC的开发者定义SEooC的目的、功能以及外部接口。

对SEooC范围的这些假设，可举例如下：

——系统是针对总质量不超过 1800kg 的车辆而设计的

——系统是针对前轮驱动车辆而设计的。

——系统是针对不超过 32%的道路坡度而设计的。

——系统有对外部系统的接口，用于获取所需的车辆信息。

——功能性要求：

- 系统在某些车辆状况下应驾驶员的请求而激活功能；
- 系统应驾驶员的请求而解除功能。

步骤 1b：对SEooC安全需求的假设

为了识别SEooC的技术安全要求，开发一个SEooC需要对与SEooC功能相关的相关项定义、相关项的安全目标、以及相应的功能安全需求做出假设。

对分配到SEooC的功能安全需求假设，可举例如下：

——系统在高车速时不会激活功能（ASIL x）。

——系统不会在没有检测到驾驶员请求的时候解除功能（ASIL y）。

为了达到所假设的安全目标，可定义针对背景的特定假设。

对于SEooC环境的假设，可举例如下：

——有一个外部源，可以提供具有所需 ASIL 等级的信息，使得系统能检测到适当的车辆状况（ASIL x）。

——有一个外部源，可以提供关于驾驶员请求的信息，且该信息达到所需的 ASIL 等级（ASIL y）。

步骤2：SEooC的开发

当技术安全要求由相关项假定的功能安全需求导出后，则SEooC遵循GB/T 34590的要求来开发。

步骤3：工作成果

在SEooC开发的最后阶段，可得到用于展示所导出的技术安全要求已全部得到满足的工作成果。然后，将工作成果中的所有必要信息，包括SEooC的安全要求以及对于环境的假设，提供给相关项的集成者。

步骤4：SEooC集成到相关项

在相关项开发中，定义安全目标和功能安全要求。相关项的功能安全要求与SEooC所假设的功能安全要求是匹配的，以证明假设的有效性。

如果发生某个SEooC的假设不匹配，要开展从影响分析开始的变更管理活动，如GB/T 34590.8-XXXX，第8章（变更管理）所述。可能的结果包括：

——根据安全目标的达成情况，差异是可接受的，没有行动要做；

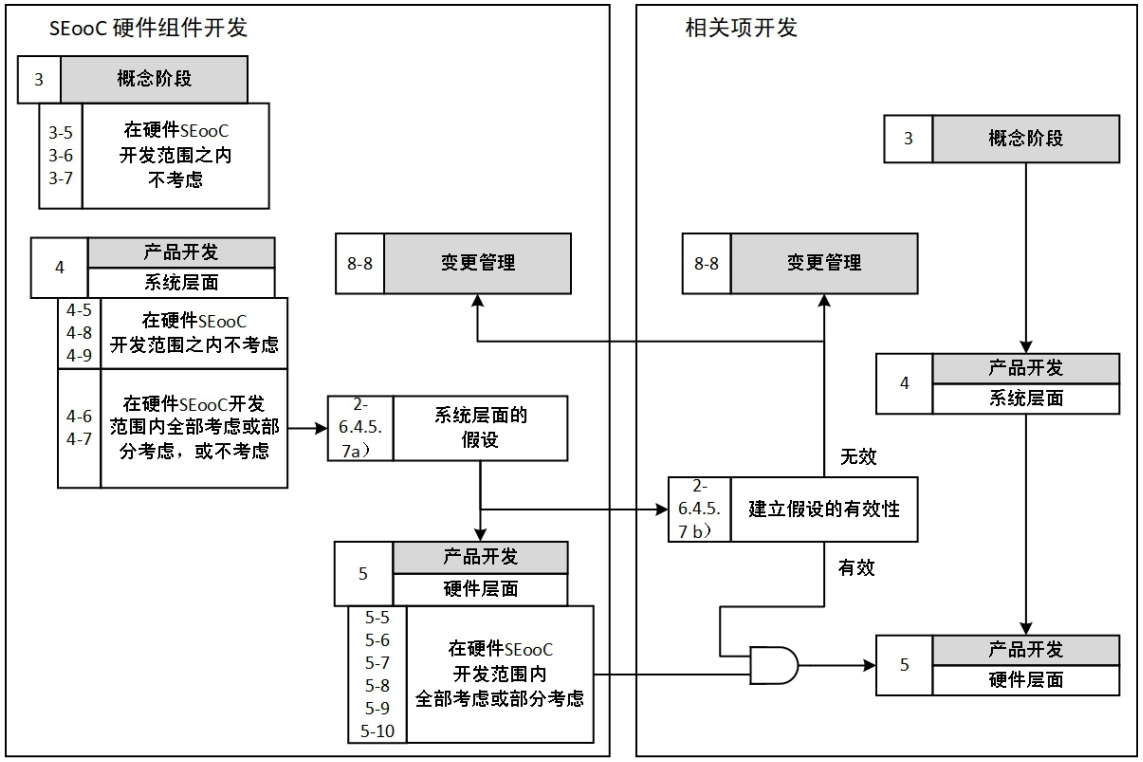
——差异影响到了安全目标的完成，需有一个相关项定义或者功能安全概念的必要的变更；

——差异影响到了安全目标，需有一个对于 SEooC 组件的变更（包括组件的一个可能的变更）。

9.2.3 开发一个作为独立于环境的安全要素的硬件组件

9.2.3.1 概述

本节使用微处理器（MCU）作为SEooC的硬件示例。流程图如图23所示。



注1：依据SEooC的确切性质，一些对需求的额外剪裁是必须的。例如根据随机硬件失效调整违反某个安全目标概率的目标值。

注2：依据SEooC的确切性质，第五部分的一些要求将不适用，因此只做了部分的考虑。

注3：尽管不能给出所有的GB/T 34590章条，但这并不意味着它们是不适用的。

图 23　SEooC 硬件组件开发

9.2.3.2　步骤 1：系统层面的假设

开发一个作为SEooC的微处理器（MCU）（如图23），首先是依据GB/T 34590.2-XXXX, 6.4.5.7对系统层面属性和需求的假设。

基于一些参考应用的分析，本阶段可以分解成两个子步骤（1a和1b）。需求的假设要考虑硬件产品开发（GB/T 34590.5-XXXX，表A.1）的前提条件。示例如下。

9.2.3.3　步骤 1a：对于技术安全要求的假设

下面是对于MCU示例的一些假设的技术安全要求的例子：

对于技术安全要求（步骤1a）的假设：

a)　通过在硬件方面的安全机制来减轻 CPU 指令存储器的失效，至少满足分配到硬件元器件层面的单点故障度量（也可是“要求的诊断覆盖率”）的目标值（例如 90%）。

b)　MCU 对于违反一个安全目标的总体可能性的贡献不能超过相关 ASIL 所允许可能性的 10%。

c)　复位时， MCU 实施一个已定义为所有 I/O 驱动输出到低状态的安全状态。

d)　任何与正在处理的功能相关的安全机制要在小于 10 ms（所分配到的部分故障允许时间间隔）内完成。

e)　有一个存储保护单元用以隔离不同 ASIL 的软件任务。

在这一步，建立起了ASIL能力。

9.2.3.4 步骤 1b：系统层级设计的假设

一些系统层级设计假设的例子，对SEooC的外部：

a) 系统将在 MCU 的供电上实施安全机制以检测过压失效模式和欠压失效模式。
b) 将在 MCU 外部实施一个窗口看门狗安全机制以检测 MCU 的时序失效或者程序顺序失效。
c) 将实施一个软件测试以检测 MCU（SM4）的 EDC 安全机制中的潜伏故障。
d) 在上电时会执行一个基于软件的测试（SM2）以确认对 CPU 程序顺序的逻辑监控（SM1）中不存在潜伏故障。
e) 在安全相关的操作中不使用 MCU 的调试接口。因此，调试逻辑中的任何故障将被视为安全故障。

9.2.3.5 步骤 2：硬件开发的执行

基于这些决定（假设的技术安全要求以及与SEooC外部设计相关的假设），根据GB/T 34590.5-XXXX进行SEooC的开发（步骤2），并准备每一项适用的工作成果。例如，考虑对于SEooC的假设，包括在假设的技术安全要求中发现的任何FIT率目标，完成对于由随机硬件失效引起的安全目标违反的评估（见GB/T 34590.5-XXXX，9.5.1的工作成果）。基于SEooC的假设，根据GB/T 34590.9-XXXX进行安全分析和MCU内部的相关失效分析。

9.2.3.6 步骤 3：工作成果

在MCU产品开发的最后（步骤3），将工作成果中的必要信息提供给系统集成者；这包括以下文档：假设的要求，与SEooC外部设计相关的假设以及适用的GB/T 34590工作成果（例如，针对由随机硬件失效而违反安全目标的可能性的报告）。

9.2.3.7 步骤 4：将 SEooC 集成到相关项

当作为SEooC开发的MCU在相关项硬件产品开发阶段的环境中予以考虑时，所有关于SEooC的假设，包括假设的技术安全要求和针对SEooC外部设计的假设，都需要建立有效性（步骤4）。有可能会出现SEooC假设和系统要求之间的不匹配。例如，相关项的开发者可以决定不实施假设的外部组件。由此，SEooC开发者所做的因随机硬件失效而导致的违反安全目标的评估就与相关项不一致了。

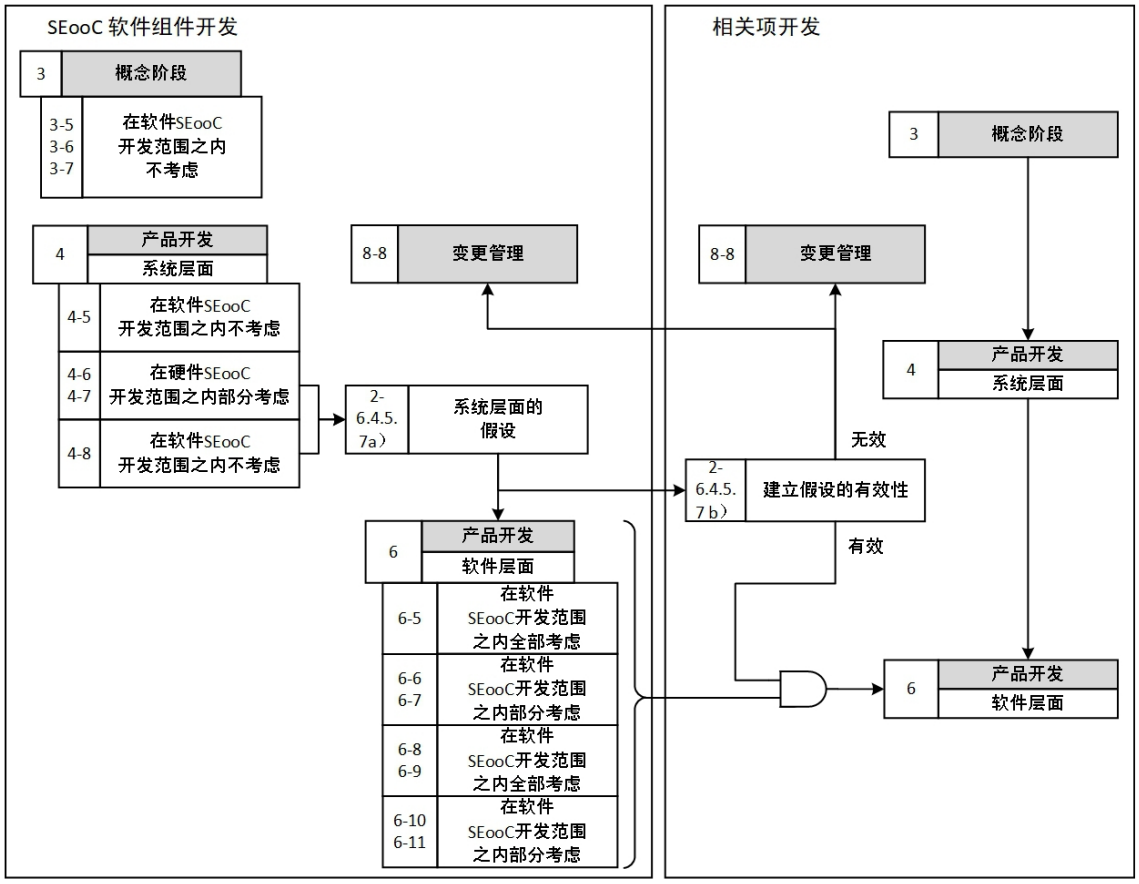
如果发生某个SEooC的假设不匹配，要开展从影响分析开始的变更管理活动，如GB/T 34590.8-XXXX，第8章（变更管理）所述。可能的结果包括：

——根据安全目标的达成情况，差异是可接受的，没有行动要做。
——差异影响到了安全目标的完成，要有一个对相关项定义或者功能安全概念的必要的变更。
——差异影响到了安全目标的完成，要有一个对 SEooC 组件的变更（可能包括组件的一个变更）。
——差异影响到了安全目标，由此重新计算安全度量，但是这个重新计算的度量表明设计是满足系统目标的，所以无须更改。

9.2.4 开发一个作为独立于环境的安全要素的软件组件

9.2.4.1 概述

本章说明了将SEooC概念应用于一个新的中/低层软件组件。流程图如图24所示。



注1：依据SEooC的确切性质，一些对额外的需求剪裁是必须的。

注2：依据SEooC的确切性质，GB/T 34590.6的一些要求将不适用，因此只考虑部分要求。

注3：尽管没有列出GB/T 34590的所有章节，但这并不意味着它们是不适用的。

图 24　SEooC 软件组件开发

9.2.4.2　步骤 1a：对于作为 SEooC 的软件组件范围的假设

本步骤用于明确与软件组件的目的、边界、目标环境、功能及特性相关的假设。

这些假设的例子可包括：

——集成软件组件到一个给定的软件层级架构中。

——由软件组件引起的任何潜在干扰是在其（应用）环境中监测和处理的。

——软件组件按假设的软件功能要求中的定义提供功能。

9.2.4.3　步骤 1b：对于软件组件安全要求的假设

步骤1b用于假设潜在影响软件组件的更高层级的软件要求，以便导出软件安全需求。例如，如果假设一组给定的由软件组件计算得到的数据是具备高完整性（ASIL x），那么由此得到的分配到SEooC的软件安全要求可以是：

——软件组件探测可导致违背安全目标的输入数据的任何损坏（ASIL x）；

——基于假设的技术安全要求，软件组件对需要被告知的错误状态进行指示（ASIL x）；

——对于任何探测到的错误条件，返回一个带有故障状态的默认值（ASIL x）；及

——软件组件返回经 CRC 编码的下列结果，以及返回一个状态（ASIL x）。

9.2.4.4 步骤 2： 软件组件的开发

一旦针对软件组件的必要假设得到清晰的规定，根据SEooC的ASIL能力（在本示例中为ASIL x），按照GB/T 34590.6-XXXX的要求，进行SEooC的开发。完成所有适用的工作成果，包括与假设的软件安全要求的验证相关的工作成果，以用于不同环境中的进一步集成。

9.2.4.5 步骤 3：全新特定环境下的软件组件的集成

软件组件与其它软件组件在全新特定环境下进行集成之前，检查SEooC所做的全部假设在该环境下的有效性。这包括假设的带ASIL能力的软件安全要求，和所有关于软件组件的目的，边界，目标环境、功能及特性的假设（见9.2.4.2和9.2.4.3）

如果发生某个SEooC的假设与该新环境不匹配，要开展从影响分析开始的变更管理活动，根据GB/T 34590.8-XXXX，第8章，启动影响分析。影响分析的可能结果包括：

——根据软件架构设计层面所适用的安全要求的达成情况，差异是可接受的，无需执行进一步的活动。

——差异影响到了软件架构设计层面所适用的安全要求的达成，可以根据 GB/T 34590.8-XXXX，第 8 章，对这些要求做必要的变更。

——差异影响到了软件架构设计层面所适用的安全要求的达成情况，需要根据 GB/T 34590.8-XXXX，第 8 章对 SEooC 组件进行变更（包括可能的组件变更）；

注：当一个软件组件集成到特定的软件架构设计中，导致分配不同ASIL等级的软件安全相关要素的共存，那么需如GB/T 34590.9-XXXX，第6章所描述的，满足要素共存的准则，或者作为选择的，低ASIL等级的要素升级到高ASIL等级。

10 在用证明的示例

10.1 概述

本章所描述的相关项及其要求是一个示例。这里给出了安全目标、其ASIL等级和后续要求，以说明GB/T 34590.8-XXXX，第14章（在用证明）所定义的在用证明。本示例不反映GB/T 34590.8-XXXX对于类似的现实案例的应用。

10.2 相关项定义和在用证明候选项的定义

整车制造商想在新车上集成一个新的功能。例如：实施该功能的相关项由一些传感器，一个ECU（含功能所需的完整软硬件），以及一个执行器组成。

整车制造商把功能的异常动作评定为ASIL C等级。相应的安全目标派生出一个分配到ECU的ASIL C等级的功能安全要求。

ECU的供应商提议沿用一个已经在使用的ECU。

分析ECU之前使用和它将要在新应用中使用的区别。分析表明，需要通过更改标定数据来修改软件以实施新的功能，但是ECU的硬件可以沿用，不做改动。供应商想用ECU硬件的在用证明来代替符合GB/T 34590.5-XXXX要求的说明。因此，该ECU的硬件就是在用证明的候选项。

10.3 变更分析

为了建立在用证明的可信度，供应商对在用证明的候选项开展变更分析。

该分析表明，从ECU的量产开始，没有引入对在用证明候选项的安全行为产生影响的变更。

此外，分析表明在用证明候选项的先前应用与预期应用之间的差异没有安全影响：

——候选项边界在规范限制之内；

——先前的集成环境需要相同的技术表现；及

——候选项边界的原因和影响在先前和未来的集成环境中是相同的。

10.4 在用证明的目标价值

为了证实在用证明的有效性，供应商预估了在用证明候选项已经在现场使用的累计小时数。供应商也分析了售后期间任何与安全相关事件的现场数据，即，有关新的相关项中候选项的预期用途，已报告的任何潜在导致或促使违背安全目标或安全要求的事件。

基于搭载在用证明候选项的量产车辆的数量、车辆量产日期、及在该细分市场中车辆典型使用数据（每年驾驶小时数），对维修历史的持久性进行预测。

维修历史是基于搭载在用证明候选项的不同车辆的现场返修数据：

——保修索赔；

——现场缺陷分析；或

——从整车制造商处返回的缺陷零件。

在相关项硬件开发之初，这些分析表明现场没有发生安全相关的事件。预测的总体累计驾驶小时数小于ASIL C的在用证明的确定目标，但是满足GB/T XXXXX.8-XXXX，14.4.5.2.5定义的临时服务期限。

由此结论如下：

——ECU 硬件的临时在用证明可继续被相关项开发所采信。

——继续进行现场观察以获取一个确定的在用证明的状态（见 GB/T 34590.8-XXXX，14.4.5.2.5 和 GB/T 34590.8-XXXX，14.4.5.2.6）。

11 关于 ASIL 的分解

11.1 ASIL 分解的目的

ASIL 分解的目的是针对系统性失效，应用多个充分独立的要素以满足安全目标。

11.2 ASIL 分解的描述

ASIL分解是指将冗余的安全要求分配到充分独立的相关项要素上。此处，冗余不一定是传统的模块化冗余（见GB/T 34590.1-XXXX，2.94）。

示例：ECU 的主处理器可被一个冗余的监控处理器所监控，即使监控处理器不能实现分配到 ECU 的功能要求，主处理器和监控处理器均能独立的启动已定义的安全状态。

ASIL分解仅对系统性失效有意义，也就是说，它是降低这些失效可能性的方法和途径。ASIL分解不会改变对硬件架构度量的评估要求，也不会改变对随机硬件失效导致违背安全目标的评估要求（见GB/T 34590.9-XXXX，5.4.5）。

示例：对于 ASIL B（D）分解的案例，在硬件架构度量评估中，不允许将 ASIL D 的目标分解成对于每个硬件要素的 ASIL B 目标。如 GB/T 34590.5-XXXX,8.2 所述，可以将目标值分配到硬件要素，但是这些目标是基于在相关项的整体硬件层面开始的分析而逐项分配的。安全目标的目标度量是应用到相关项层面的。

在这样一个分解后的架构里，只有当两个要素同时违背了分解后的安全要求，才会违背相关的安全目标。

在GB/T 34590.9-XXXX,第5章（关于ASIL裁剪的要求分解）中描述了GB/T 34590中所允许的分解。

11.3 ASIL 分解的示例

11.3.1 总则

本章中描述的相关项及其要求均为示例。安全目标及其ASIL等级和后续要求，仅为了说明ASIL分解过程而设计的。本示例不能反映GB/T 34590在类似的现实示例上的应用情况。

11.3.2 相关项定义

以具有一个执行器的系统为示例（见图25），驾驶员通过使用仪表板上的开关来触发此执行器。执行器在车速为零时提供舒适功能，但是如果在超过15km/h时激活会导致危害。

相关项的初始架构如下：

——由一个专门的 ECU（本示例中称之为“AC ECU”）读取仪表板开关的输入，该 ECU 通过一个专门的电源线为执行器供电。

——搭载本相关项的车辆同时也带有一个能提供车速的 ECU（本示例中称之为“VS ECU”）。假定此 ECU 能按照 ASILC 的要求提供车速超过 15km/h 的信息。

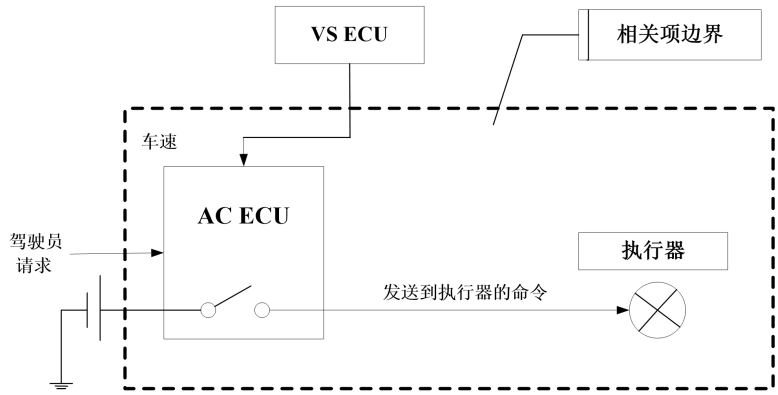


图 25　相关项边界

11.3.3 危害分析和风险评估

本分析中考虑的危害事件是在车速超过15km/h时激活执行器，无论此时是否存在驾驶员请求。

本危害事件的ASIL分级为ASIL C。

11.3.4 相关的安全目标

安全目标1：避免在车速超过15km/h时激活执行器：ASIL C。

11.3.5 系统架构设计

下面列出了初步架构要素的目的：

——VS ECU 为 AC ECU 提供车速。

——AC ECU 监控驾驶员请求，检测车速是否小于或等于 15km/h，若是，则发送命令到执行器。

——执行器通电后就被激活。

11.3.6 功能安全概念

11.3.6.1 总则

本功能安全概念的示例仅用于说明ASIL分解，该示例并不完整，未包括全部的功能安全要求。

——要求 A1：VS ECU 发出准确的车速信息给 AC ECU。➔ASIL C

——要求 A2：当车速超过 15km/h 时，AC ECU 不能给执行器供电。➔ASIL C

——要求 A3：执行器只有在得到 AC ECU 的供电之后才能被激活。➔ASIL C

11.3.6.2 演化后的相关项安全概念

开发者可以选择引入一个冗余的要素，在这里是一个安全开关，如图26所示。通过引入这个冗余的要素， AC ECU可根据ASIL分解的结果，按照等同于或者低于ASIL C的一个ASIL等级来进行开发。

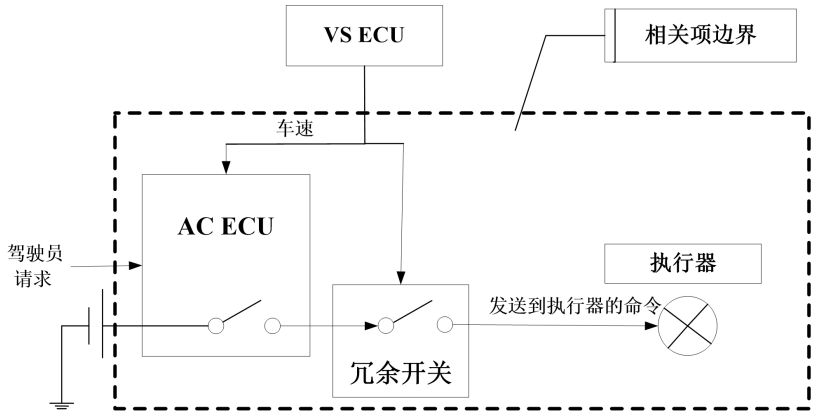


图 26 相关项设计的第二次迭代

这些要素的目标（演化后的架构）：

——VS ECU 控制单元提供车速给 AC ECU。

——AC ECU 监控驾驶员请求，检测车速是否小于或等于 15km/h，若是，则发送命令到执行器。

——冗余开关位于 AC ECU 和执行器之间的供电线路上。当车速小于或者等于 15km/h 时，开关闭合；当车速大于 15km/h 时，开关打开。开关的这种操作与供电线的状态无关（开关本身的供电是独立的）。

——执行器通电后才可被激活。

功能安全要求：

——要求 B1： VS ECU 发出准确的车速信息给 AC ECU。➔ASIL C

——或者：避免不正确的传输车速低于或者等于 15 km/h 的信息。➔ASIL C

——要求 B2：当车速超过 15km/h 时，AC ECU 不能给执行器供电。➔ASIL X（C）（见表 5）

——要求 B3： VS ECU 发送准确的车速信息给冗余开关。➔ASIL C

——要求 B4： 在车速大于 15km/h 时，冗余开关处于打开状态。➔ASIL Y（C） （见表 5）

——要求 B5：执行器只有当 AC ECU 给出供电并且冗余开关闭合时才工作。➔ASIL C

为了允许ASIL分解，如果必要，开发者需增加一个独立性要求：

——要求 B6： 说明 AC ECU 和冗余开关之间的充分独立性。➔ASIL C

初始要求A2被都符合安全目标的冗余要求B2和B4替代，因此可应用ASIL分解。

表 5 可能的分解

	要求 B2：ASIL X（C）	要求 B4：ASIL Y（C）
可能1	ASIL C（C） 要求	QM（C） 要求
可能2	ASIL B（C） 要求	ASIL A（C） 要求
可能3	ASIL A（C） 要求	ASIL B（C） 要求
可能4	QM（C） 要求	ASIL C（C） 要求

12 带安全相关可用性需求的系统的开发指南

12.1 引言

对于许多E/E系统，功能的缺失不会导致危害，因此，当系统内部发生故障时，可以通过关闭功能来达到安全状态。然而，在某些情况下，HARA可以表明某些功能的丢失会导致危害事件，这可能导致指定安全相关可用性需求的安全目标。

“故障容错”一词在本章中是有限制意义的。在本章中，术语“故障容错”仅在以下情况下使用：特定的功能是预期的功能或预期功能的一个子集即出现一个或多个错误时提供的功能（见GB/T 34590.1-XXXX，3.60）。此术语不适用于：用于关闭系统的特定功能；通过关闭特定功能可以直接进入安全状态的功能。

注1：有多种措施可确保足够的可用性，包括容错、故障避免和故障预测，其中容错是指在属于指定故障集的故障发生后至少在有限时间内实现特定功能的能力。故障避免是指减少故障发生的措施，而故障预测是指在导致失效发生之前发现故障或功能降级的能力。

注2：在故障容错的情况下，并不是所有可以想象到的故障都能被容忍。需要申明可容忍的故障集合（例如，ECC具有单个bit错误纠正和双bit错误检测功能时的单bit错误）。

12.2 概念阶段指定故障容错时间的说明

12.2.1 总则

在定义容错时，概念阶段将考虑以下内容：

a) 功能可用性与安全相关时的车辆运行状态；
b) 故障是可以容忍的；
c) 故障发生后对危害事件的预防；
d) 故障发生后的响应操作；
e) 故障发生后可以达到的安全状态；
f) 对故障容错项的 ASIL 分解；及
g) 其他项的安全要求。

12.2.2 功能可用性与安全相关时的车辆运行状态

相关项的功能丢失是否会导致危险事件取决于车辆的运行状态。例如，在特定的车辆运行状态下（例如在高速行驶时转向），功能的丢失可能会导致危险事件，而在另一种车辆运行状态下（例如在零车速时转向），则可能不会发生危险事件。如果车辆处于特定车辆运行状态，某一功能的丢失不会导致危险事件，则认为功能的可用性与安全无关。

满足安全相关可用性要求的措施是基于与其他相关项之间的可能交互、包含其他技术的系统架构（如机械备份）和安全分析的结果。如果采取故障容错措施，则适用12.2.3和12.2.4。

注：如果车辆的运行状态是由其他相关项维持的，则需要考虑这些相关项可能带来的新的或变更的危害，并在必要时重新进行HARA评估。

示例：系统 X 是一个没有机械备份的 E/E 系统。当在乡村公路上高速行驶时，突然失去功能是很难控制的，并可能导致 ASIL 级别的危险事件。在非常低的速度下，通过应用足够独立且可用的系统 Y 的不同的功能，可以很容易地控制其功能的突然丢失，从而产生 C0 的可控性评级。

所以，在车辆运行状态为“相关项处于高车速的正常操作模式”时，其功能的可用性被考虑为安全相关的。而在车辆运行状态为“相关项处于低车速的正常操作模式”时，其功能的可用性并不认为是安全相关的。

12.2.3 故障后危害事件的预防

12.2.3.1 从故障发生到完成故障响应的允许时间间隔

作为安全需求的一部分，最大故障处理时间间隔要与故障容错时间间隔相一致。

12.2.3.2 故障响应后要保持的功能和性能

故障的情况下会导致失去预期的功能或预期功能的一个子集,且功能丢失会导致危险事件,需要定义故障发生后的功能和性能状态，以实现到安全状态的过渡、安全状态之间的过渡或安全状态的保持。

注：这些功能和性能需要在紧急操作或安全状态下提供。

示例：只有当相关项输出性能低于其指定的最大输出的50%时，才会发生危险事件。该相关项由两个系统组成，每个系统都能够提供50%的最大指定输出。如果一个系统发生故障，可以通过关闭故障系统，而另一个系统则保持最高50%的指定输出来防止危险事件的发生。

12.2.4 故障响应后的运行

12.2.4.1 紧急运行

在紧急运行期间，即使该相关项的ASIL能力低于可能的危害的ASIL等级，该相关项仍然没有不合理的风险。为了解决这种情况，该状态下的运行时间会被限制，因此不太可能发生导致违背安全目标的附加故障。

注1：根据12.3.1，从下一次故障的可能性中定义和验证了紧急运行容许时间间隔。

注2：已定义并验证向紧急运行的过渡是安全的。

12.2.4.2 故障容错相关项的安全状态

在故障容错行为的情况下，通常选择以下两个安全状态之一：

a) 出于安全原因，特定功能不再被需要的车辆运行状态。在这种情况下，特定功能被永久关闭，因此在该相关项修复之前不再提供。或者

b) 可能的车辆运行状态受到限制，以使在受限的车辆运行状态下可能发生的危害事件的ASIL等级等于或低于剩余系统的ASIL能力。在这种情况下，由剩余系统提供的受限运行状态下的特定功能本身可以被解释为一个相关项，并且可以不受时间限制地运行。修复该相关项后，可能的车辆运行状态将恢复为不受限。

注1：对可能的车辆运行状态的限制会影响可能的危害事件的E，C和S参数。

示例1：限制车速可以降低严重度，并可以提高危害事件的可控性，从而导致ASIL等级低于无限制情况下的等级。

注2：在此HARA评估中的暴露概率E不考虑故障的发生。

注3：该ASIL等级可用于：

——限制相关项的ASIL分解（12.2.6）。

——为构成相关项的各个冗余组件指定安全要求。这包括在丢失一个冗余组件的情况下确定其余系统的ASIL能力。

注4：如果某相关项的安全目标是在出现故障时保持全部功能或降级功能，则可以扩展HARA以涵盖受限车辆运行状态的功能。

注5：如果在发生故障之后车辆的运行状态没有改变（例如，车辆在无警告情况下无限制运行），则ASIL与从无故障的车辆运行状态中得出的相同（适用于原始HARA）。

注6：实施可能的车辆运行状态限制的安全机制继承了安全目标的原始ASIL。如果在其他相关项的功能支持下达到或维持了安全状态，则将这些状态确定为对这些相关项的安全要求。

示例 2：在没有故障的情况下，该项目的安全目标的 ASIL 为“D”，可控性= C3，严重度= S3 和暴露概率= E4，并且如果在功能降级的运行状态下，则可控性得到改善，例如，对于 C2，则此运行状态下的 ASIL 要求为 ASIL C：S3，E4，C2。

示例 3：存在故障的线控系统将车辆运行限制为低速行驶，其中大多数驾驶员可以通过另一个系统防止碰撞。这可以提高可控性，并且还可以降低车速限制状态下的严重度。

注7：一旦达到安全状态并通知了驾驶员，则根据《维也纳道路交通公约》[17]，任何修理均由车主/驾驶员负责。

12.2.4.3 紧急运行时间间隔

对于故障容忍相关项，一旦故障发生，故障容忍相关项将保持特定的功能。相关项根据12.2.3.2进入安全状态。在过渡到安全状态期间，整车级的故障响应生效（例如： 限制车速到30km/h）。但是，在完成整车级故障响应之前，紧急运行时间间隔内因为另一个故障导致的可能危险事件没有被减轻。

为了将风险降到最低，紧急运行时间间隔限制在安全概念中定义的紧急运行容忍时间间隔内。

注1：定义紧急运行容忍时间间隔时，需考虑以下：

——物理系统限制

——其他对于在紧急运行时使用的硬件和软件的安全需求，如果有要求；以及

——剩余系统以常见方式发生故障的可能性

注2：对于随机硬件故障，GB/T 34590.5-XXXX, 9.4.2.4 e） 通过将紧急运行时间间隔作为暴露持续时间来保证硬件架构减轻随机硬件故障的有效性。

注3：保证紧急运行时间间隔不超过紧急运行容忍时间间隔不总是汽车制造商的责任，也可以是汽车驾驶员的责任。

示例：一个前照灯灯泡烧坏。该失效被探测到并且驾驶员被通知该失效。驾驶员有责任在合理的时间内维修前照灯。

12.2.5 故障容错相关项示例

12.2.5.1 说明

该示例用于描述与故障容错系统行为相关的可能的事件流。将说明各种故障时间间隔符号的应用。

12.2.5.2 假设

对于该相关项的危害分析与风险评估表明特定功能的严重丧失超过时间X会导致一个危险事件。该危险事件的ASIL等级与功能丧失时的车速有关。

在这个示例中，对于危害分析与风险评估，假设运行场景的暴露度不因车速而变化。因此，安全目标是在最坏情况的条件下形成的。

该示例中的安全目标表述如下：

——避免特定功能的严重丧失超过时间 X（故障容错时间间隔）（ASILD）

注：特定功能的严重丧失意味着该功能的输出性能低于最低要求的性能级别。

12.2.5.3 示例的策略

为实现12.2.5.2中假设的安全目标，可以考虑以下两种策略：

——策略 1：相关项在发生故障后保持特定的功能。该功能持续运行至相关项得到修复。在修复前，车辆运行状态不受限制。在这种情况下，应在允许的时间间隔内（即紧急运行容错时间间隔）修复该相关项。

——策略 2：相关项在发生故障后保持特定的功能。该功能将保持在受限的车辆运行状态下，没有时间限制。在这种情况下，车辆状态在允许的时间间隔内（即紧急运行容错时间间隔）达到受限的车辆运行状态。

12.2.5.4 相关项的系统架构描述

以下是示例的相关项描述：

——该相关项包括两个充分独立的通道，通道 A 和通道 B。

——通道 A 提供标称功能。

——通道 B 是一个备份系统。它的性能高于安全操作所必需的最低性能级别。该功能的充分性根据 ISO 26262-4：2018 第 8 章进行验证。

——如果通道 A 发生故障导致功能严重丧失，则通道 B 在时间 x 内被激活，以防止违背安全目标。

——当考虑系统性故障时，通道 A 和通道 B 均可单独满足 ASIL D 的安全要求。

——当考虑随机硬件故障时（例如，≤ 1%的随机硬件故障可导致功能严重丧失），通道 A 和通道 B 的组合可满足 ASIL D 的安全要求。

注：可能存在其它安全目标对相关项的要素提出额外的安全要求。本次讨论不考虑这些问题。

示例考虑了通道B能力上不同的两种策略：

策略1：在紧急运行容错时间间隔内修复

——通道 B 本身不满足 ASIL D 等级的随机硬件故障的安全要求。

——当探测到通道 A 丢失时，通知驾驶员，并要求驾驶员在紧急操作容许时间间隔内修复该相关项。紧急运行时间间隔内故障发生的概率应作为 PMHF 计算的一部分考虑，也可以通过 12.3 中的方法来确保。

策略2：不受时间限制的受限操作

——通道 B 本身不满足 ASIL D 随机硬件故障的安全要求。它只能满足在 ASIL A 随机硬件故障的安全要求，即它关于该安全目标只有 ASIL A 的能力。它仅通过故障预防措施来实现这一点。

——引用 ASIL 等级依赖于车速的相关项的危害分析和风险评估。在本例中，假定 ASIL 等级为：

- 如果最大车速不受限制，则等级为ASIL D；
- 如果最大车速被限制为v_4，则等级为ASIL C；
- 如果最大车速被限制为v_3，则等级为ASIL B；
- 如果最大车速被限制为v_2，则等级为ASIL A；
- 如果最大车速被限制为v_1，则等级为QM；
- 如果最大车速被限制为v_0，则不会发生危害。

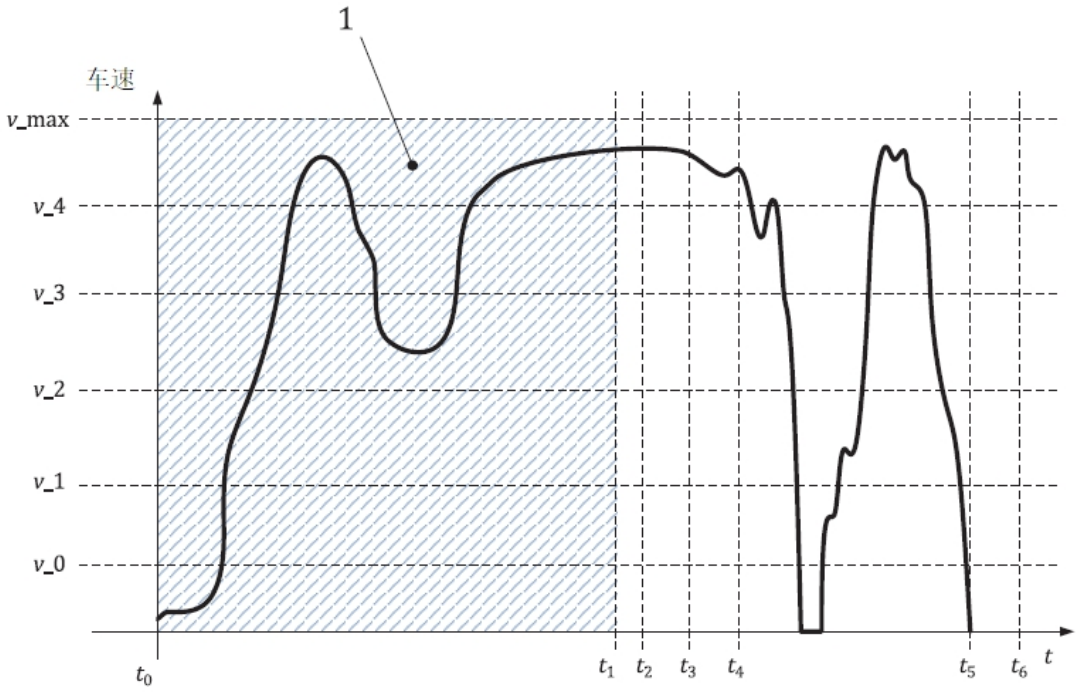
注：由于可能的车辆运行状态不受限制（即车速 > v_4），因此该安全目标被定为ASIL D。但是，对于特定的驾驶情况（如车速 < v_2），要么不会发生某些危险，要么S、C和E等级与最坏情况假设不同。这个整体结果降低了该危害的ASIL要求。在本例中，危险仅当车速较高时定为ASIL D。如果车速等于或小于v_2，则认为比车速更高时具有更好的可控性和更低的严重度，并且由于特定功能的严重丧失而导致的危害被定为ASIL A。

——通过其它相关项将车速降低到 v_2 以下，此功能是对 ASIL D 等级的相关项的额外安全要求。这是在策略 2 中实施通道 B 的先决条件。

12.2.5.5 本示例的事件流

图27和28的示例分别描述了，适用策略1和策略2的容错系统来处理安全相关可用性需求的场景下的FTTI、故障探测和故障响应时间、紧急运行和安全状态的概念。

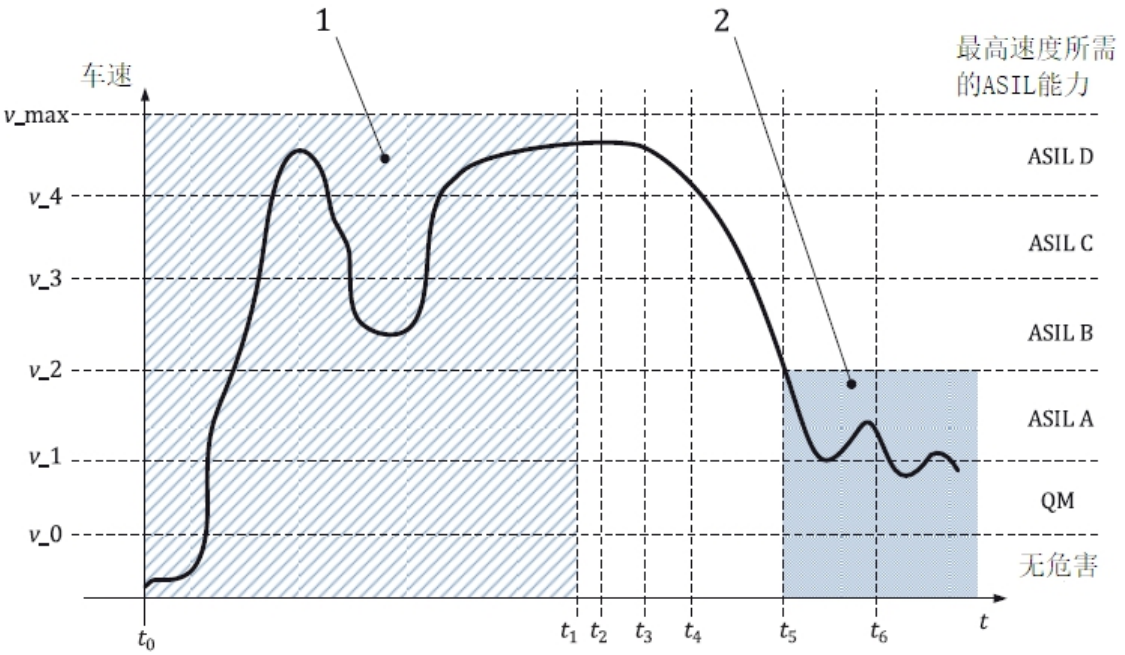
在这些图中，使用了相同的时间尺度来阐明两种策略之间的差异。



说明：

1——相关项处于具备/须 ASILD 等级能力的正常工作模式下。

图 27　策略 1 的车速历史示例



说明：

1——相关项处于具备ASILD等级能力的正常工作模式下；

2——相关项处于具备ASIL A等级能力的故障模式下。

图 28　策略 2 的车速历史示例

图27和图28从t1到t6的事件为：

——t1：故障表现其为特定功能严重丧失的时刻

通道 A 中的故障表现其为通道 A 的丧失，从而导致特定功能严重丧失。该功能的丧失发生在车速 ＞v_4 时，可能导致 ASIL D 等级的危害。

——t2：探测到故障的时刻;

在这两种策略中，所定义功能的显著失效都会被安全机制诊断到。

注：t1和t2之间的时间跨度也称为故障诊断时间间隔。

——t3：相关项完成其运行模式切换，故障响应时间间隔结束的时刻；

作为失效的响应，通道 B 被激活，提供所需的功能。由于所需的功能是在小于 x 的时间内提供的，即 t1＜t3＜t1＋x，因此可以防止危害。

在策略 1 中，故障的发生会通过报警和降级策略中定义的方式被告知到驾驶员。

在策略 2 中，从此时开始减速到 v_2。

注：降低车辆速度到v_2的安全要求是ASIL D等级。因此，降低和保持车辆速度到v_2的功能需要达到ASIL D等级的能力。

——t4：容错时间间隔结束的时刻；

t4 = t1 + x，时间 x 对应 FTTI。如果所定义功能的显著失效持续到 t4 或持续更长时间，则可能发生 ASIL D 级危害。两种策略多会发生。

——t5：相关项达到安全状态的时刻，定义 t5-t3 为紧急运行时间间隔;

在策略 1 中，相关项在 t5 被修复。维修前，车辆运行状态不受限制。根据警告和降级策略，在一次行程结束时或在几个驾驶循环后会到达 t5。

在策略 2 中，此时车速达到 vvehicle ＜ v_2。在这种状态下，所定义功能的显著失效（例如，由于通道 B 的故障）只会导致 ASIL A 的危害。由于剩余有效的安全措施可以支持 ASIL A 的安全目标，即通道 B 对于该安全目标拥有 ASIL A 的能力，因此可以认为该项目的运行状态不存在不合理的风险。

注：t3与t5之间的时间间隔，即紧急运行时间间隔，也可以认为是不存在不合理的风险，不是因为其实现了风险的降低，而是因为相关项在这种车辆运行状态下所工作的时间是有限的。

——t6： 达到安全状态最大允许时间间隔的时刻，t6-t3 定义为紧急运行容错时间间隔;

定义从 t3 到达到安全状态的时间间隔为紧急运行容错时间间隔。紧急运行容错时间间隔为 t3 + y。

在策略 1 中，t6 是相关项得到修复的预期时刻。

在策略 2 中，t6 是车辆速度被限制到车速 ＜ v_2 的目标时刻。

注：对于可用性是非安全相关的相关项，要求其在t4前达到安全状态。

12.2.6　故障容错相关项的 ASIL 分解

ASIL分解的基本思想是将ASIL X的初始安全需求分解为ASIL Y1（X）和ASIL Y2（X）的冗余安全需求组合。目标风险的降低是通过分解的冗余安全需求的组合来实现的，而不是单独通过其中一个来实现的。该方法也适用于通过冗余实现安全需求分解的故障容错相关项。因此，对ISO 26262-9：2018第五章 没有附加的限制。

注：故障容错相关项需证明具有充分的独立性（见GB/T 34590.9-XXXX, 5.4.3）

如果ASIL分解是应用于故障容错相关项中的冗余要素,那么设计方案就需要同时考虑ASIL分解的结果和相关项进入非冗余状态时的危害分析和风险评估的结果，参考12.2.4.2 b）。

定义冗余安全要求的ASIL等级需要考虑：

——丧失冗余后，维持相关项运行所需的最低 ASIL 等级;及

——通过对初始安全需求分解得出的 ASIL 等级。

示例：一个相关项具备 ASIL D 等级的安全目标为“应避免丧失 60%以上输出能力的时间超过 X”。 该相关项由两个独立的组件实现，各组件提供所需输出的 50%。这两个输出相加（图 29）。各组件均具备充分的能力将预期的输出维持在 40%以上，并且有足够的能力保持对危害的控制和预防。

当其中一个组件发生故障，由于其性能受限并独立于剩余组件，所以车辆将以降级模式运行。因为车辆性能受其他相关项的限制，并且降级模式下的异常会被ASIL D等级的初始运行模式所减轻以满足初始的安全目标，所以危害分析和风险评估确定了降级模式下的运行为ASIL B等级。

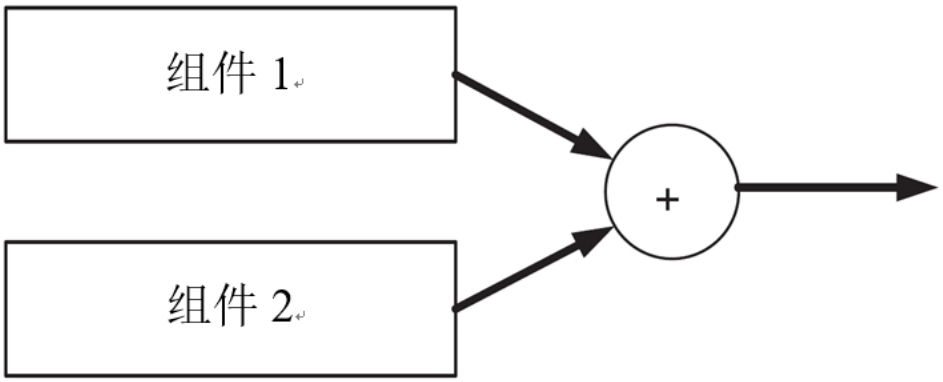


图 29　由两个独立组件相加所组成的故障容错相关项

GB/T 34590.9-XXXX， 5.4.9，允许按照下列之一对两个由独立组件实现的需求进行ASIL分解::

a)　ASIL C（D） 和 ASIL A（D）；

b)　ASIL B（D） 和 ASIL B（D）；或

c)　ASIL D（D） 和 QM（D）。

但是，对于一个将相关项的安全目标的ASIL等级限制为ASIL B的设计方案，当车辆性能受限时，每个组件的ASIL能力最小为ASIL B，对于该设计方案最合适的分解方案为b） ASIL B（D）和ASIL B（D）。选项a）和c）是不合适的，除非其他部分的ASIL等级至少提高到ASIL B [即 ASIL C（D）和ASIL B（D）或ASIL D（D）和ASIL B（D）]。

12.3　硬件设计阶段的可用性考虑

12.3.1　随机硬件故障定量分析

12.3.1.1　紧急运行容错时间间隔的计算方法

对于使用冗余实现容错的系统，一旦系统完成对第一个故障的故障响应，系统就处于无冗余的运行模式。如果采用这种运行模式的系统的ASIL能力不满足车辆运行状态的ASIL要求，则限制允许车辆维持在该运行状态下的时间，以减少发生第二次故障的风险。这是一个可能会决定紧急运行容错时间间隔的因素，该时间间隔的基本原理通过GB/T 34590.5-XXXX第9章的定量分析得到了确认。

如果采用GB/T 34590.5-XXXX,9.4.2的方法来确定随机硬件故障的度量，则需用依据紧急运行容错时间间隔（Teotti）的PMHF预估量来满足PMHF目标。或者，可以用PMHF来为Teotti计算一个极限，这个极限是关于一个组件的后续随机硬件故障导致违背安全目标的风险。

注：由于PMHF值本身没有绝对意义（见GB/T 34590.5-XXXX, 9.4.2.2，注1），使用它来计算Teotti是一种选择。也可以选择其他定量或定性方法。

也可以通过将Teotti视为故障发生或冗余丢失后的相关项状态属性来限制它。在这种状态下，Teotti的适当性是通过比较车辆预期使用情况下违背安全目标的概率度量（PMHF×Tlifetime）和在没有冗余的情况下违反安全目标的概率度量来决定的。式（1）给出了一个公式例子 （做一阶近似）：

$$T_{\text{eotti}} \leq T_{\text{lifetime}} \times \lambda_{\text{target}} / \lambda_{degr}$$

式中：

λ_{target} —— 故障发生或冗余丢失后对应相关项ASIL等级的目标PMHF（根据GB/T 34590.5-XXXX, 9.4.2.2推导）。没有降级模式或紧急运行的任何说明，则使用初始的ASIL；

λ_{degr} —— 对于故障发生或冗余丢失后的相关项状态，在紧急运行容错时间间隔内，导致违背安全目标的故障每小时发生的平均概率。

具体公式取决于系统架构和详细设计。

12.3.1.2 示例-带备用机制的动态冗余架构

图30为一个带有备用机制的动态冗余架构，用于演示Teotti的计算。

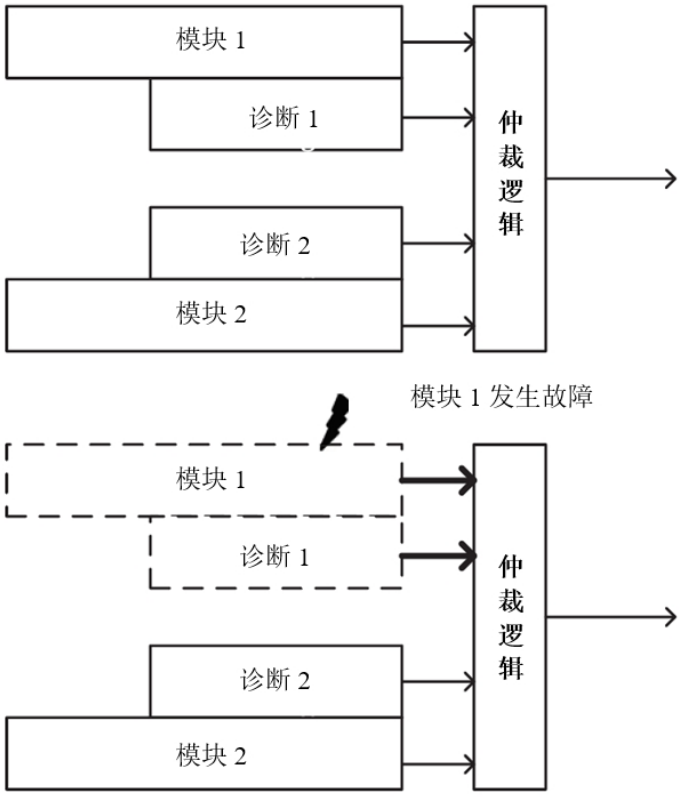


图30 示例——带备用机制的动态冗余架构

这种情况类似于8.3.2.2中以模块1为IF（预期功能），模块2为SM1（安全机制1）的例子。PMHF的公式与8.3.2.4中给出的公式相同，用Teotti代替Tservice。对于该系统，Teotti现在可以计算为式（2）：

$$T_{\text{eotti}} \leq \left(M_{\text{PMHF}} - \lambda_{\text{SPF}} - \lambda_{\text{RF}} - 0.5 \times \lambda_{\text{SM1,DPF,latent}} \times \lambda_{\text{IF,DPF}} \times T_{\text{lifetime}} - 0.5 \times \lambda_{\text{IF,DPF,latent}} \times \lambda_{\text{SM1,DPF}} \times T_{\text{lifetime}}\right) / \left(\lambda_{\text{SM1,DPF,detected}} \times \lambda_{\text{IF,DPF}} + \lambda_{\text{IF,DPF,detected}} \times \lambda_{\text{SM1,DPF}}\right) \quad (2)$$

将 $\lambda_{\text{target}} = M_{\text{PMHF}}$ and $\lambda_{\text{degr}} = \lambda_{\text{SM1,DPF}}$ 公式1可得

$$T_{\text{eotti}} \leq T_{\text{lifetime}} \times M_{\text{PMHF}} / \lambda_{\text{SM1,DPF}} \quad (3)$$

表6比较了在Tlifetime =10000h时，两个公式对两组故障率计算出的结果。对于第一种方案，式（3）为限制因子，Teotti≤167 h，对于第二种方案，式（2）为限制因子，Teotti≤31 h。

紧急运行容错时间间隔是功能安全要求的一部分。在这个例子中，通过参照12.3.1.1中描述的两种方法，式2和式3，证实了ETTOI的适用性，式（2）给出了给定PMHF目标的紧急运行容错时间间隔的余量、要素失效率和潜在诊断试验时间间隔。另一方面，式（3）计算出Teotti的一个额外限制，在故障发生或冗余丢失后，作为相关项状态的一个属性。

表 6　公式（2）和（3）的示例参数

λ（h-1）	方案1	方案2
IF,DPF	6.0E-6	6.0E-6
IF,DPF,DETECTED	5.4E-6	5.4E-6
IF,DPF,LATENT	6.0E-7	6.0E-7
SM1,DPF	6.0E-6	6.0E-6
SM1,DPF,DETECTED	5.4E-6	5.4E-6
SM1,DPF,LATENT	6.0E-7	6.0E-7
Results		
Equation （2）	772 h	31 h
Equation （3）	167 h	167 h

注1：GB/T 34590.5-XXXX, 9.4.2.4给出了车辆行驶的平均持续时间可以被认为等于1小时。

示例：为了允许系统在故障发生后进行 10 次行驶或启动循环操作，紧急运行容错时间间隔需要大于或等于 10 小时。

注2：如果基于PMHF计算得到的Teotti受到太大限制，则可以通过处理剩余失效率等其他参数来放宽Teotti的限制。

12.3.1.3　无 PMHF 值时紧急运行容错时间间隔计算

如果采用GB/T 34590.5-XXXX ，9.4.3的方法，那么GB/T 34590.5-XXXX 9.4.3.13提供的标准适用。

12.3.1.4　过渡到安全状态后的需求分配

如果一个相关项在达到没有时间限制的安全状态后，仍然具有某些特定功能，则需对剩余安全措施的ASIL能力进行评估。采取GB/T 34590.5-XXXX的相关章节，包括第8章和第9章。

注：注：对于系统性故障，故障避免措施被理解为开发的一部分。如果这些措施的有效性是量化的，那么这些措施可以考虑定量的安全分析（即GB/T 34590.5-XXXX第8章的硬件架构度量，和第9章的 PMHF或EEC）。

12.4　软件开发阶段

12.4.1　软件故障的避免和容错

与软件安全相关的可用性需求可以通过两种方法来解决：故障避免(12.4.2)和故障容错(12.4.3)。

12.4.2　软件故障避免

故障避免的方法旨在减少系统性故障的总体发生。通过使用GB/T 34590.6-XXXX开发软件要素可以实现必要的故障避免。

12.4.3 软件故障容错

故障容错技术试图在软件出现系统性故障的情况下保持相关项的运行。GB/T 34590.6-XXXX,7.4.12,注2和注3中提到了一些故障容错机制。

13 关于“所使用软件工具的置信度”的分析

GB/T 34590.8-XXXX第11章中描述的确定软件工具使用置信度的过程分为两个步骤：

第一步：工具使用案例的评估

工具鉴定的要求是基于“工具影响”（TI）和“工具误差探测”（TD） 等级的确定。TI表示特定软件工具功能异常可引入或不能探测开发中安全相关项或要素中错误的可能性。TD表示用于防止软件工具功能异常并产生相应错误输出的措施的置信度,或用于探测软件工具存在功能异常并已产生相应错误输出的措施的置信度。TI和TD用于确定“工具置信度水平”（TCL）。

TI和TD是根据预期软件工具的特定用例确定的。用例的评估可以独立于特定工具本身来完成。

第二步：软件工具的鉴定

如果工具置信度水平在第一步的结果是TCL2或TCL3，那么鉴定措施是确保，用户可以依赖软件工具的正确功能，以及软件工具是适合用来支持GB/T34590系列标准所要求的活动或任务。在这种情况下，建议采取下列四种鉴定方法中的至少一种：

——使用中积累置信度；

——工具开发流程评估；

——软件工具确认；

——按照安全标准开发。

该鉴定方法适用于特定的软件工具及其版本和环境。因此，ISO 26262-8：2018, 11.4.6.2，描述了：

——软件工具的唯一识别码和版本号（a）；及

——软件工具被鉴定的配置和环境（d）。

工具鉴定通常会导致很高的工作量，特别是在频繁更改工具或其版本的情况下（例如，在更新、补丁等情况下），因为工具需要为每个新版本重新鉴定。重新鉴定也适用于可能对工具输出产生影响的工具环境的变化（例如操作系统或常用的软件库）。

工具鉴定的另一种选择是通过在使用软件工具的产品开发过程中引入额外的措施来增加检测错误工具输出的可能性。这将把工具错误探测等级降低到TD1。在这种情况下，流程如图31所示：

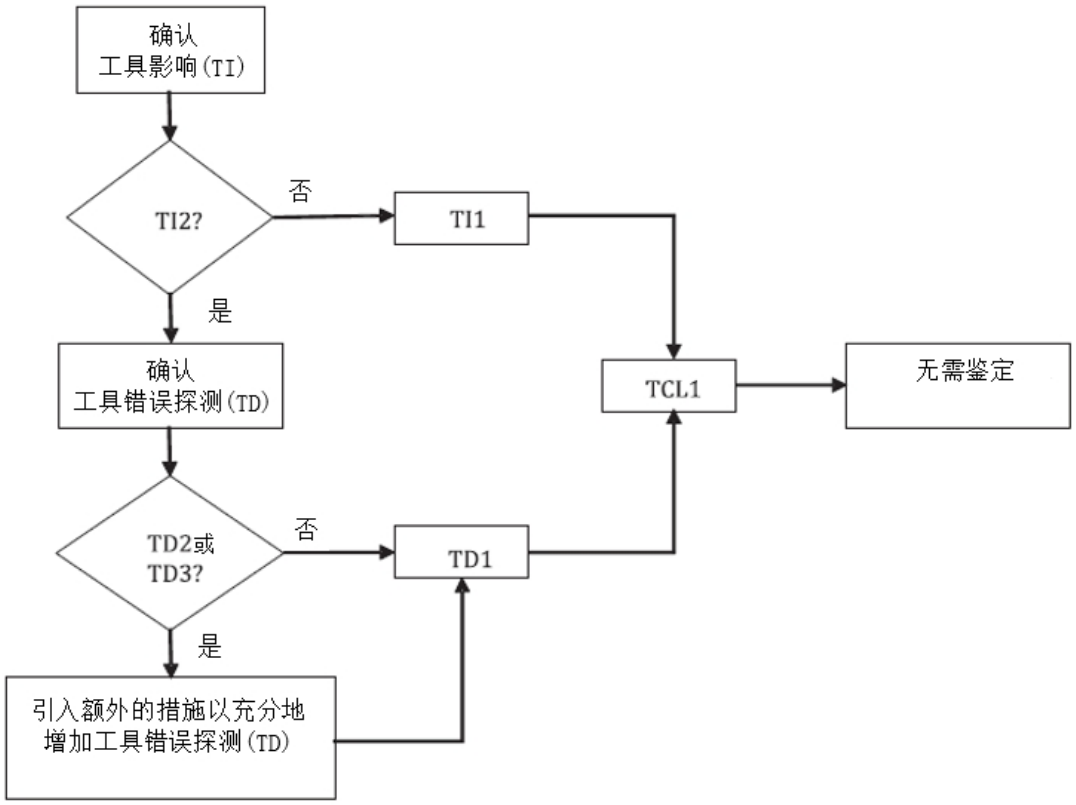


图 30　为达到 TCL1 工具级别的工具鉴定流程图

这个替代方案不需要对特定的软件工具进行鉴定（第二步），它只基于工具的用例，并且可以独立于特定的工具、工具版本和它的环境来执行。

这种方法可能导致更多的初始和正在进行的开发工作,因为需要引入额外的措施来增加工具错误探测（例如，检查工具输出、额外的测试步骤、使用后续工具进行检查等）。然而，这通常可以减少工具鉴定工作，因为后续的鉴定步骤可以省略，在理想情况下，这个程序只一次就完成。

只要用例保持不变，工具置信度水平就是有效的。对于额外的用例，第一步中的等级需被更新（影响分析），这可能导致需要进一步的措施来增加工具错误探测。

14　安全相关的特殊特性指南

14.1　总则

本章节对从产品开发阶段的安全相关特性的鉴别到生产阶段的监控提供指导。

特殊特性管理是一种已建立的程序，以确保生产的产品或其要素提供客户所需的安全和质量水平。因此，GB/T 34590中的通用方法与已建立的汽车质量管理体系中定义的方法兼容（见GB/T 34590.2，5.4.5）。GB/T 34590特别关注汽车产品中与安全相关的电气、电子和软件要素。

根据GB/T 34590.7，在产品的生产过程中，为了达到产品的功能安全，需要符合所有与安全相关的相关项或要素的特殊特性。

注：特殊特性可为产品特性或制造工艺参数。

安全相关的特殊特性的管理包括：

——在开发过程中对其身份的确定；

——生产计划期间用于控制它们的措施的规范；及

——监测其在生产期间的执行情况。

与安全相关的特殊特性在GB/T 34590.4-XXXX，6.4.8.1和GB/T 34590.5-XXXX，7.4.5.1中都有被规定，并且在所有这三个阶段都可追溯。此外，还检查了每个识别出的安全相关的特殊特性都得到了适当的规划和控制。功能安全评估可用于提供证据，证明在开发阶段适当的安全相关特殊特性已被确定。生产能力评估是用来提供证据，证明生产能够满足与安全相关的特殊特性。

注：不同组织之间可以交换相关的安全相关特殊特性，例如：客户和供应商，以确保可追溯性。

14.2 安全相关的特殊特性的确定

与安全相关的特殊特性在产品开发和生产计划期间都会被确定。为了能确定特殊特性对相关项或要素的安全影响，可根据GB/T 34590-9的安全分析报告中获取。

注1：生产计划在开发过程中启动。

注2：并非所有的特殊特性都与安全有关。

安全相关的特殊特性可以在系统级、硬件级和软件级中被确定，用于生产。

示例 1：在系统 FMEA 期间，电机旋转变压器偏移量的校准被认为是制造过程中的安全要求，一个动作被指定为在生产下线测试期间为了满足与安全相关的特殊特性，包括存储标定数据和测试结果。过程控制方案规定了电机校准是一种与安全相关的特殊特性。

示例 2：在组件 FMEA 期间，两个相邻引脚之间的最小间距以确保电气绝缘被认为是制造期间组件 FMEA 的一个安全要求。一个动作被指定为在硬件组件的生产过程中要满足的安全相关的特殊特性，包括电气参数的测试，一个动作被指定为在装配图上放置一个特殊特性的符号。

示例 3：在过程 FMEA 中，正确选择嵌入式软件（包括用于下载到 ECU 的标定数据）被识别为安全相关特殊特性，将在 ECU 下线烧写中通过比较校验和来满足该特性。

示例 4：在过程 FMEA 中，生产过程中沉积的焊膏量被识别为安全相关的特殊特性，将在 PCB 生产时满足该特性，包括通过视觉系统的控制。

14.3 与安全相关的特殊特性控制措施规范

一旦确定了安全相关的特殊特性，就规定了在生产过程中控制这些特性的准则和要求，以确保相关项或要素的功能安全。

通常，控制与安全相关的特殊特性的准则和措施的规范包括：

——可接受的参数范围；

示例：可接受的电流和电压范围。

——评估或测量技术，包括测试 ID；

示例：自动光学检验、下线测试和电路测试。

——控制策略；及

注：样本的控制可基于统计学或以一定频率应用于所有样本。在这种情况下，控制的样本大小和频率被指定。这些要求可以提供给外部（如供应商）或内部生产团队。

——验收准则。

示例：焊接修补的宽度的可接受容忍度。

14.4 安全相关的特殊特性的监测

安全相关的特殊特性（包括来自客户和供应商的特性）的控制计划和实施的证据，可以记录在GB/T 34590.7-XXXX，6.5.1和6.5.2的工作成果中。

附 录 A
（资料性）
故障树的构建和应用

A.1 总则

分析相关项和要素的故障和失效时，最常用的两种技术是FTA和FMEA。FMEA通常以归纳（自下而上，见图 A.1）的方式执行，重点关注系统的各个部分、如何失效以及这些失效对系统的影响。FTA通常以演绎（自上而下，见图 A.2）的方式执行，从非预期的系统行为到确定导致该行为的可能原因。FTA包含覆盖了所有可能导致违反某个危害事件的多个故障和事件或情况的组合，而FMEA考虑每个单一故障的影响。

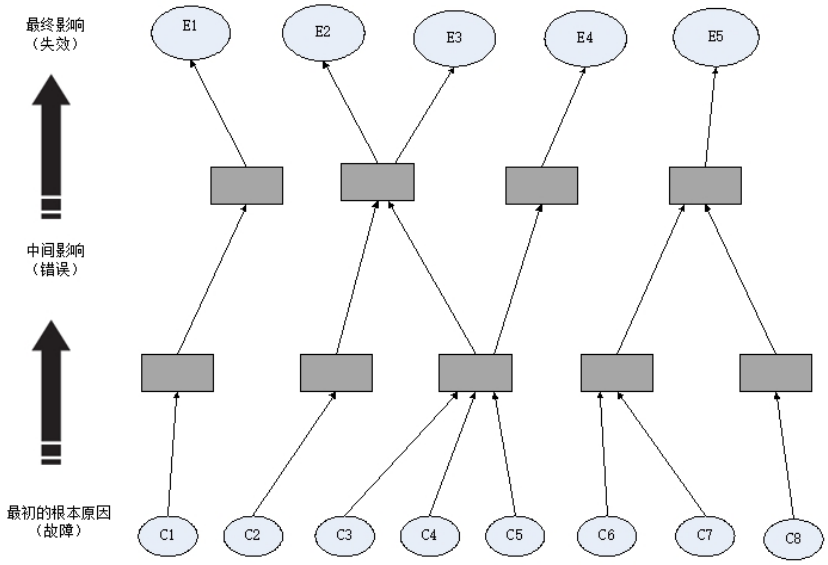


图 A.1 FMEA 图解，自下而上的方法

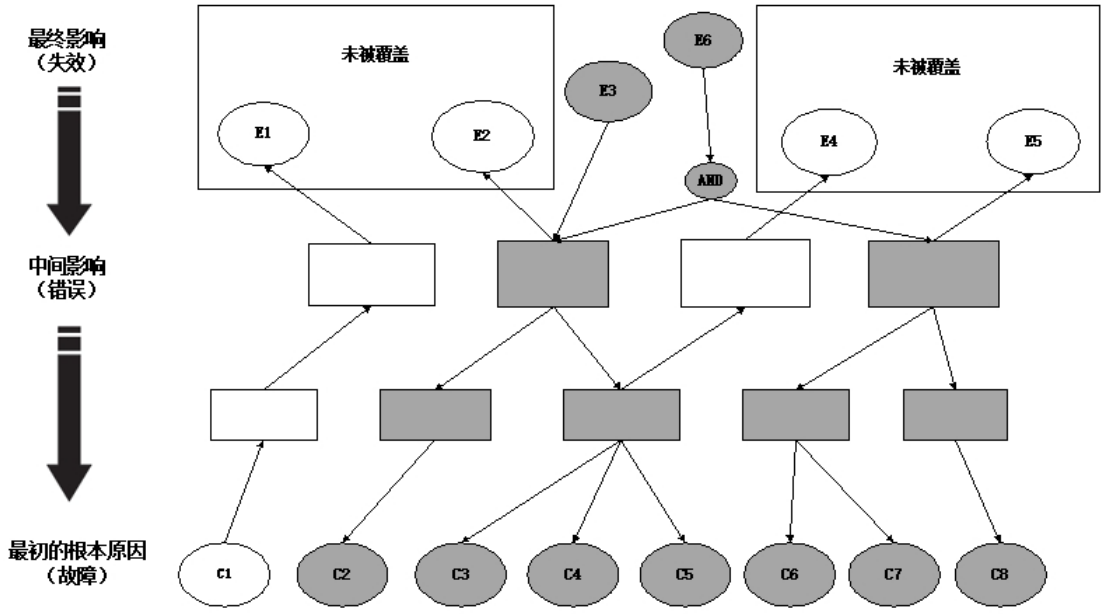


图 A.2 FTA 图解，自上而下的方法

这些方法是互补的，如GB/T 34590.5-XXXX，7.4.3.1表2所述：“分析的详细程度与设计的详细程度是相称的。在某些情况下，这两种方法都可以在不同的细节层面上执行。”图A.1和图A.2的“Cx”既可代表硬件组件也可代表软件组件。一种典型的分析方法是使用FTA把危害分析到组件层面。然后使用FMEA自下而上的分析所有组件的失效模式，以确定它们的失效模式和安全机制来完成故障树的底层事件，期望通过这种方法来避免因为FTA模型和FMEA重叠导致的重复工作。由此更倾向于将一系列的系统元器件的FMEA结果做为底事件失效率提供给故障树模型。

注1：如GB/T 34590.9-XXXX, 7.4.2所述，因不存在统一的且充分可信的方法来量化相关失效，对相关失效诱因的预估是定性的。

注2：FMEA示例标准包括JEP131A[3]和SAE J1739[4]，以及FTA IEC 61025[5]。

A.2 FTA 与 FMEA 的结合

系统是由许多零部件和子零部件组成的。可将FTA和FMEA相结合，以提供具有自上而下和自下而上方法合理平衡的安全分析。如图A.3展示了将FTA和FMEA相结合的可能方法。在此图中，底事件是由在更低的抽象层面（例如：子元器件、元器件或组件层面）上执行的不同FMEAs（在本示例中以FMEA A-E标示）中得出的。在本示例中，底事件1和2是FMEA D中发现的故障影响，而故障树中没有使用来自FMEA B的故障影响。

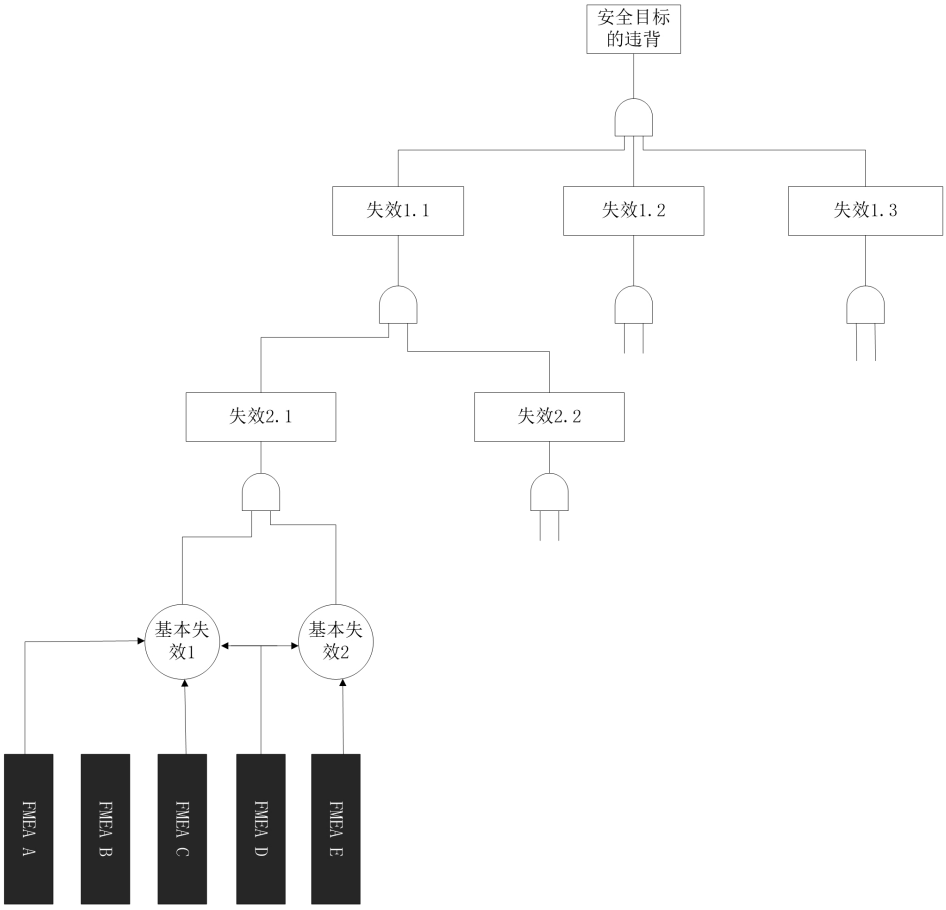


图 A.3 FTA 和 FMEA 相结合的图解

参 考 文 献

[1] GB/T 20438-2017 (所有部分)电气/电子/可编程电子安全相关系统的功能安全.

[2] GSN COMMUNITY STANDARD VERSION 1, November 2011.

[3] JEDEC - JEP131A (May 2005), Potential Failure Mode and Effects Analysis (FMEA).

[4] SAE-J1739_200901, Potential Failure Mode and Effects Analysis in Design (Design FMEA) and

Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process

FMEA) and Effects Analysis for Machinery (Machinery FMEA).

[5] IEC 61025, ed. 2.0 — Procedures and Symbols for FTA.

[6] SAE J2980, Considerations for ISO 26262 ASIL Hazard Classification.

[7] ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of Functional Safety.

[8] ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase.

[9] ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the

system level.

[10] ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the

hardware level.

[11] ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the

software level

[12] ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning

[13] ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes

[14] ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL) oriented and safety-oriented analyses

[15] ISO 26262-11:2018, Road vehicles — Functional safety — Part 11: Guideline on application of ISO 26262 to semiconductors

[16] ISO 26262-12:2018, Road vehicles — Functional safety — Part 12: Adaptation of ISO 26262 for motorcycles

[17] Convention on Road Traffic. Done at Vienna on 8 November 1968 including amendment 1,

Economic Commission for Europe, Inland Transportation Committee, [viewed 2018-09-25]

Available at: https://www.unece.org/fileadmin/DAM/trans/conventn/crt1968e.pdf