ICS 43.430
CCS T 35

中华人民共和国国家标准

GB/T 34590.9—XXXX
代替 GB/T 34590.9-2017

道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和安全为导向的分析

Road vehicles—Functional safety—Part1:Automotive Safety Integrity Level(ASIL)-oriented and safety-oriented analyses

(ISO 26262-9:2018，MOD)

（征求意见稿）

（本草案完成时间：2021年4月1日）

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

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。

本部分为GB/T 34590-XXXX的第9部分。

本文件代替GB/T 34590.9-2017《道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和安全为导向的分析》,与GB/T 34590.9-2017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；
——修改了关于 ASIL 等级剪裁的要求分解目的（见 5.1）；
——修改了关于 ASIL 等级剪裁的要求分解总则（见 5.2）；
——修改了初始安全需求应分解为冗余安全需求的内容（见 5.4.3）；
——修改了每个分解初始安全要求自身应符合初始安全要求的内容（见 5.4.4）；
——删除了“如果不能通过将要素关闭来阻止对初始安全要求的违背，则应展示执行分解后安全要求的充分独立要素具备足够的可用性”内容（见 2017 版的 5.4.8）；
——修改了要素共存准则的总则内容（见 6.2）；
——删除了“应用本章之前应将安全要求分配给要素的子要素”内容（见 2017 版的 6.4.2）；
——修改了如果同一要素中存在执行不同 ASIL 等级要求的内容（见 6.4.4）；
——修改了相关失效分析的目的（见 7.1）；
——修改了相关失效分析的总则（见 7.2）；
——修改了相关失效分析的前提条件（见 7.3.1）；
——修改了“维修错误”为“服务错误”（见 7.4.4 e））；
——增加了“老化和磨损”（见 7.4.4 i））；
——增加了相关失效分析的细节程度和严格程度的内容（见 7.4.8）；
——增加了相关失效分析的验证依据条款（见 7.4.9）；
——增加了相关失效分析验证报告（见 7.5.2）；
——修改了安全分析目的内容（见 8.1）；
——修改了安全分析的要求和建议内容（见 8.4.1）；
——增加了安全分析验证报告（见 8.5.2）；

——增加了附录 B 要素共存和要求分解的架构示例（见附录 B）；
——增加了附录 C 识别相关失效的框架（见附录 C）。
本文件使用重新起草法修改采用了ISO 26262-9：2018 《道路车辆 功能安全 第9部分：术语》。
本文件与ISO 26262-9：2018的技术性差异及其原因如下：
——关于规范性引用文件，本部分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；
- 用修改采用国际标准的GB/T 34590.2-XXXX代替ISO 26262-2：2018；
- 用修改采用国际标准的GB/T 34590.1-XXXX代替ISO 26262-3：2018；
- 用修改采用国际标准的GB/T 34590.4-XXXX代替ISO 26262-4：2018；
- 用修改采用国际标准的GB/T 34590.1-XXXX代替ISO 26262-5：2018；
- 用修改采用国际标准的GB/T 34590.6-XXXX代替ISO 26262-6：2018；
- 用修改采用国际标准的GB/T 34590.7-XXXX代替ISO 26262-7：2018；
- 用修改采用国际标准的GB/T 34590.8-XXXX代替ISO 26262-8：2018；

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 34590.9-2017 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。

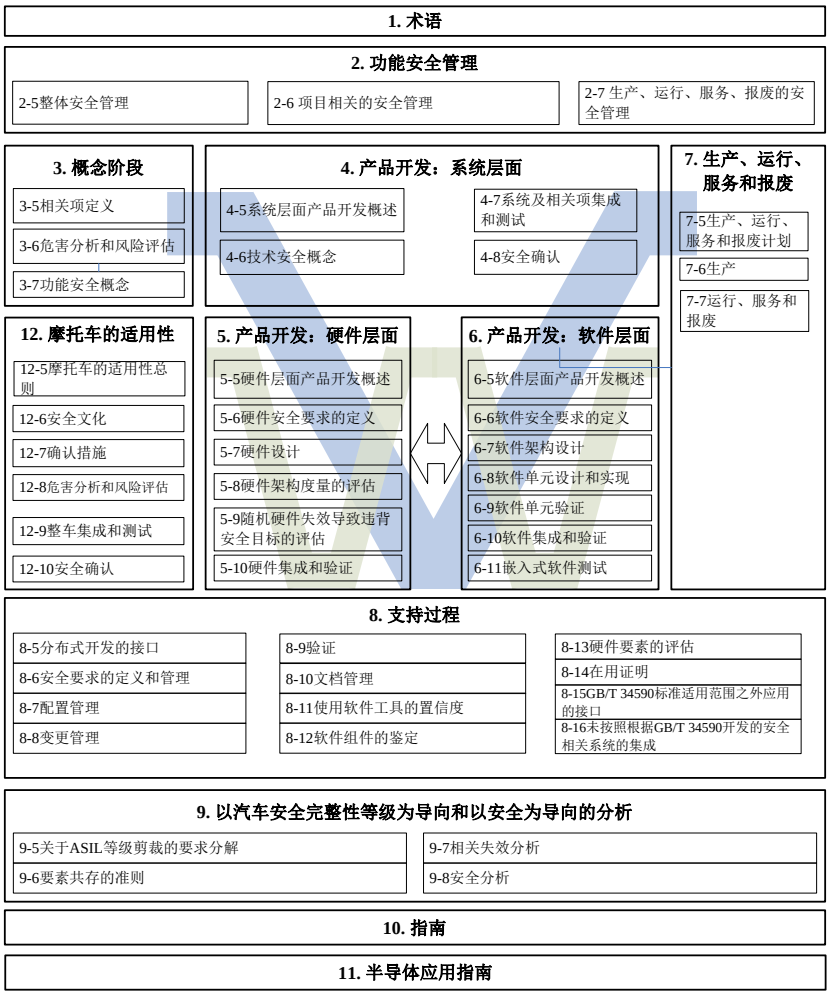


图1　GB/T 34590-XXXX 概览

道路车辆 功能安全
第9部分：以汽车安全完整性等级为导向和安全为导向的分析

1 范围

GB/T 34590的本部分规定了以汽车安全完整性等级为导向和以安全为导向的分析的要求，包括：

——关于ASIL剪裁的要求分解；

——要素共存的准则；

——相关失效分析；及

——安全分析。

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裁剪。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裁剪。

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。

本文件不针对电气/电子系统的标称性能。

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-XXXX（所有部分） 道路车辆 功能安全（ISO 26262:2018，MOD）

3 术语、定义和缩略语

GB/T 34590.1 界定的术语、定义和缩略语适用于本文件。

4 要求

4.1 目的

本章规定了：

a) 如何符合 GB/T 34590-XXXX；

如何解释 GB/T 34590-XXXX 所使用的表格；及

如何解释各章条基于不同的 ASIL 等级的适用性。

4.2 一般要求

如声明满足GB/T 34590-XXXX的要求时，应满足每一个要求，除非有下列情况之一：

a) 按照 GB/T 34590.2-XXXX 的要求，安全活动的剪裁已经实施并表明这些要求不适用；或

不满足要求的理由存在且是可接受的，并且按照 GB/T 34590.2-XXXX 的要求对该理由进行了评估。

标有“注”或“示例”的信息仅用于辅助理解或阐明相关要求，不应作为要求本身且不具备完备性。

将安全活动的结果作为工作成果。应具备上一阶段工作成果作为“前提条件”的信息。如果章条的某些要求是依照ASIL定义的或可剪裁的，某些工作成果可不作为前提条件。

“支持信息”是可供参考的信息，但在某些情况下，GB/T 34590-XXXX不要求其作为上一阶段的工作成果，并且可以是由不同于负责功能安全活动的人员或组织等外部资源提供的信息。

4.3 表的诠释

本文件中的表是规范性或资料性取决于上下文。在满足相关要求时，表中列出的不同方法有助于置信度水平。表中的每个方法是：

a) 一个连续的条目（在最左侧列以顺序号标明，如 1、2、3）；或

一个选择的条目（在最左侧列以数字后加字母标明，如 2a、2b、2c）。

对于连续的条目，高度推荐和推荐的方法按照ASIL等级推荐予以使用。高度推荐或推荐的方法允许用未列入表中的其它方法替代,此种情况下，应给出满足相关要求的理由。如果可以给出不选择所有条目也能符合相应要求的理由，则不需要对缺省方法做进一步解释。

对于选择性的条目，应按照指定的ASIL等级对这些方法进行适当的组合，而与这些方法在表中是否列出无关。如果所列出的方法对于一个ASIL等级来说具有不同的推荐等级，宜采用具有较高推荐等级的方法。应给出选择组合方法或选择单一方法满足相应要求的理由。

注：在表中所列出方法的理由是充分的。但是，这并不意味着有倾向性或对未列到表中的方法表示反对。

对于每种方法，应用相关方法的推荐等级取决于ASIL等级，分类如下：

——“++”表示对于指定的 ASIL 等级，高度推荐该方法；

——“+” 表示对于指定的 ASIL 等级，推荐该方法；

——“o” 表示对于指定的 ASIL 等级，不推荐也不反对该方法。

4.4 基于 ASIL 等级的要求和建议

若无其它说明，对于ASIL A、 B、 C和D等级，应满足每一章条的要求或建议。这些要求和建议参照安全目标的ASIL等级。如果在项目开发的早期对ASIL等级完成了分解，按照GB/T XXXXX-9第5章的要求，应遵循分解后的ASIL等级。

如果GB/T 34590-XXXX中ASIL等级在括号中给出，则对于该ASIL等级，相应的章条应被认为是推荐而非要求。这里的括号与ASIL等级分解无关。

4.5 摩托车的适用性

对于适用于GB/T 34590.12要求的摩托车的相关项或要素，GB/T 34590.12的要求替代本部分和GB/T 34590.2的相应要求。

4.6 卡车、客车、挂车和半挂车的适用性

对卡车、客车、挂车和半挂车的特殊规定以（T&B）来表示。

5 关于ASIL等级剪裁的要求分解

5.1 目的

本章的目的是，如果使用了ASIL等级分解，则：

a) 确保安全求在下一个更细层面上分解成冗余的安全要求，并将这些要求分配给了充分独立的设计要素；及

根据允许的ASIL等级分解方案应用ASIL等级分解。

注：本章中所提到的独立性是指技术独立性，而不是组织独立性（参见GB/T 34590.1-XXXX 的3.78）。

5.2 总则

所开发相关项的安全目标的ASIL等级贯穿整个相关项的开发。从安全目标开始，在各开发阶段得出并细化安全要求。作为安全目标的一个属性，ASIL等级由后续每个安全要求来继承。 安全要求被分配给架构要素，从分配给系统架构设计要素的功能安全要求开始，最终得出分配给硬件和/或软件要素的安全要求。

ASIL等级分解是在概念和各个开发阶段进行ASIL等级剪裁的一种方法。在安全要求分配过程中，可从包括存在充分独立的架构要素的架构决策中获得益处，这提供了以下机会：

——通过这些独立的架构要素冗余实现安全要求；及

——分配一个可能更低的ASIL等级给这些（或其中一部分）分解后的安全要求。

如果架构要素不是充分独立的，则冗余要求和架构要素继承初始的ASIL等级。

ASIL等级分解是一种ASIL等级剪裁方法，可用于相关项或要素的功能安全要求、技术安全要求、硬件安全要求或软件安全要求。

通常，ASIL等级分解允许将安全要求的ASIL等级在多个用来确保同一安全目标的同一安全要求的要素间进行分配。在特定条件下，允许在预期功能及其相应的安全机制间进行ASIL等级分解（参见5.4.7）。

针对随机硬件失效的要求，包括硬件架构度量的评估和由于随机硬件失效导致违背安全目标的评估（参见GB/T 34590.5-XXXX，第8章和第9章），在ASIL等级分解后仍保持不变。

附录B给出了一个架构分解的示例。

5.3 本章的输入

5.3.1 前提条件

应具备下列信息：

——ASIL等级分解所在整车、系统、硬件或软件层面的安全要求，按照GB/T 34590.3-XXXX 的7.5.1、GB/T 34590.4-XXXX 的6.5.1、GB/T 34590.5-XXXX 的6.5.1或GB/T 34590.6-XXXX 的6.5.1；及

——ASIL等级分解所在整车、系统、硬件或软件层面的架构信息，按照GB/T 34590.3-XXXX 的7.5.1、GB/T 34590.4-XXXX 的6.5.3、GB/T 34590.5-XXXX 的7.5.1或GB/T 34590.6-XXXX 的7.5.1。

5.3.2 支持信息

可考虑下列信息：

——相关项定义（参见GB/T 34590.3-XXXX 的5.5.1）；及

——包含在危害分析和风险评估报告中的安全目标（参见GB/T 34590.3-XXXX 的6.5.1）。

5.4 要求和建议

5.4.1 如果应用 ASIL 等级分解，应满足本章的所有要求。

5.4.2 进行 ASIL 等级分解时，应分别考虑每一个初始的安全要求。

注：对不同初始安全要求的ASIL等级分解，可能导致将几个安全要求分配给相同的独立要素。

5.4.3 初始安全要求应分解为冗余安全要求，并由充分独立要素实现。如果相关失效分析（参见第 7 章）没有找到导致违反初始安全要求的合理原因，或者根据初始安全要求的 ASIL 等级，所识别的相关失效的每个原因都被充分的安全措施控制，则这些要素具有充分的独立性。

注1：一条被分解的要求可能是几个初始安全要求分解的结果。

注2：使用同构冗余来实现分解的要求（例如，通过复制的设备或复制的软件）并不能解决硬件和软件系统性失效。除非相关失效的分析（参见第7章）提供了充分的独立性证据（参见GB/T 34590.1-XXXX的3.78）或存在潜在共因可进入安全状态的证据，否则不允许ASIL等级的降低。因此，在没有针对特定系统应用背景的相关失效分析的支持下，单靠同构冗余通常不足以降低ASIL等级。

注3：ASIL等级分解通常不适用于在多通道架构设计中确保通道选择或通道切换的要素。

5.4.4 每个分解后的安全要求自身应符合初始安全要求。

注1：此要求通过定义提供了冗余。

注2：如果将分解后的安全要求分配给安全机制，则应在评估分解后的要求是否符合初始安全要求时，考虑该安全机制的有效性。

示例：分配给指定 ECU 的 ASIL D 要求，可能被轻易的分解为分配给 ECU 中简单看门狗的 ASIL D 要求和该 ECU 微处理器的 QM 安全要求。然而，这个简单的看门狗不足以覆盖 ASIL D 要求的微处理器的失效模式。在这种情况下，该看门狗不能有效地满足初始的安全要求。

5.4.5 按照 GB/T 34590.5，对硬件架构度量的评估要求和对由于随机硬件失效导致违背安全目标的评估要求应在 ASIL 等级分解后保持不变。

5.4.6 如果在软件层面应用 ASIL 等级分解，应在系统层面对实施分解后要求的要素间的充分独立性进行验证。如果有必要，应在软件层面、硬件层面或系统层面采取额外的措施来实现充分的独立性。

5.4.7 如果对初始安全要求的 ASIL 等级分解导致将分解后的要求分配给预期功能及相关安全机制，则：

a) 相关安全机制宜被分配分解后的较高 ASIL 等级；及

注1：通常，与预期功能相比，安全机制具备较低的复杂度和更小的规模。

安全要求应被分配给预期功能，并按照相应分解后的 ASIL 等级实现。

注2：如果选择了分解方案 ASILx(x) +QM(x)，则 QM(x)意味着质量管理体系足以实现预期功能要素安全要求的开发。

5.4.8 对安全要求应用 ASIL 等级分解时：

a) 应按照 5.4.9 应用 ASIL 等级分解；

ASIL 等级分解的应用可多一次（在这种情况下，中间的需求分配步骤可以省略）；及

应通过在括号中给出安全目标的 ASIL 等级，对每个分解后的 ASIL 等级做标注。

示例：如果一个 ASIL D 的要求分解成一个 ASIL C 的要求和一个 ASIL A 的要求，则应标注成“ASIL C(D)”和“ASIL A(D)”。如果 ASIL C(D)的要求进一步分解成一个 ASIL B 的要求和一个 ASIL A 的要求，则应使用安全目标的 ASIL 等级将其标注为“ASIL B(D)”和“ASIL A(D)”。

5.4.9 应按照分解前的 ASIL 等级选择下列分解方案中的一种（如图 2 所示）。也可使用得出较高 ASIL 等级的分解方案。

注1：从所选分解方案的一个层面到相邻较低层面的步骤定义了ASIL等级的一个分解。

a) 应按照下列之一对一个 ASIL D 的要求进行分解：

1) 一个 ASIL C(D)的要求和一个 ASIL A(D)的要求；或

2) 一个 ASIL B(D)的要求和一个 ASIL B(D)的要求；或

3) 一个 ASIL D(D)的要求和一个 QM(D)的要求。

应按照下列之一对一个 ASIL C 的要求进行分解：

4) 一个 ASIL B(C) 的要求和一个 ASIL A(C)的要求；或

5) 一个 ASIL C(C) 的要求和一个 QM(C)的要求。

应按照下列之一对一个 ASIL B 的要求进行分解：

6) 一个 ASIL A(B)的要求和一个 ASIL A(B)的要求；或

7) 一个 ASIL B(B)的要求和一个 QM(B)的要求。

如果需要，ASIL A 只应被分解为一个 ASIL A(A)的要求和一个 QM(A)的要求。

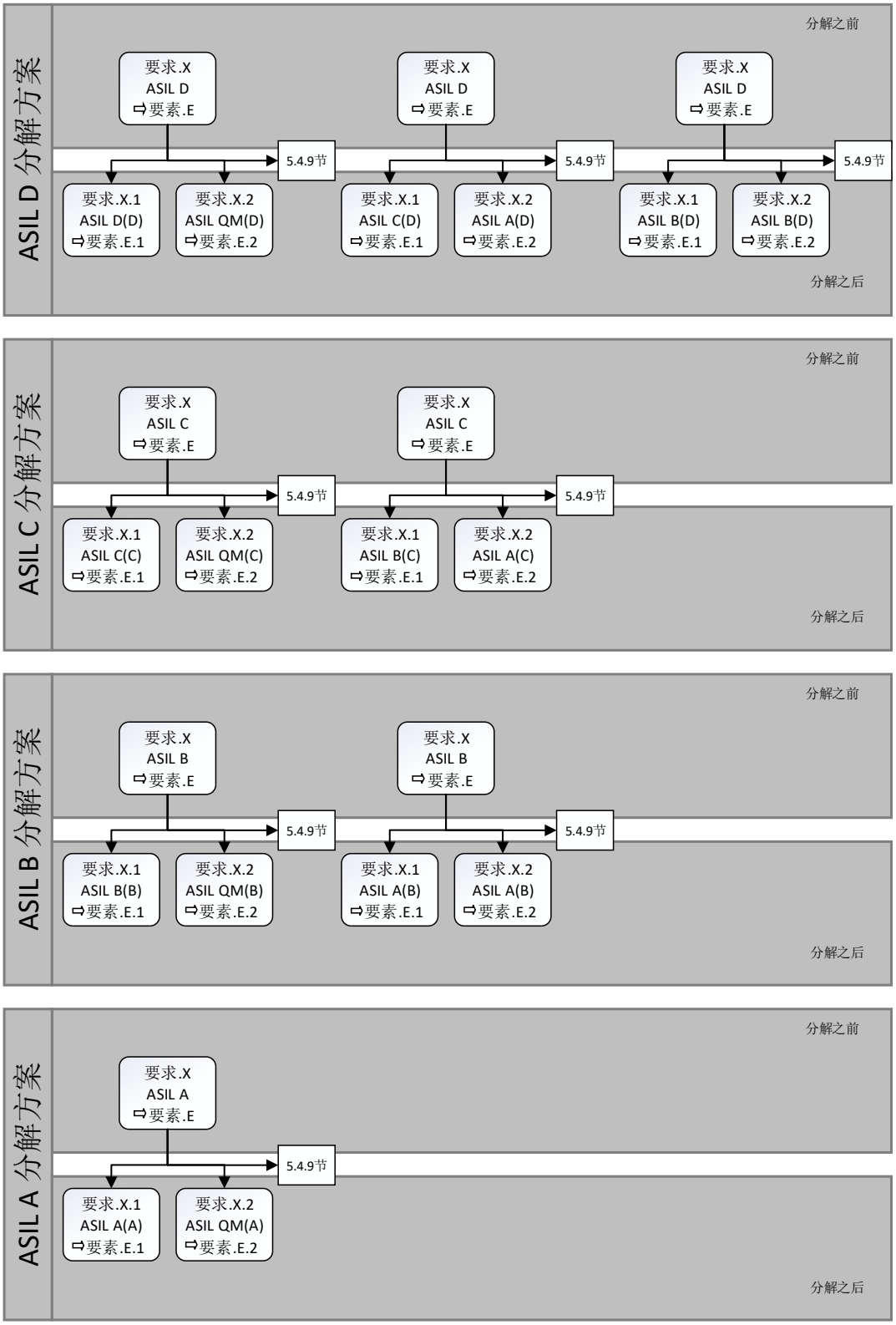


图2　ASIL 等级分解方案

要点：要求X ASIL D→要素.E表示具有ASIL D属性的要求X被分配给要素E。

示例：5.4.7 中描述的案例，即：QM 分配给预期功能、与初始 ASIL 等级相同的 ASIL 等级分配给相关安全机制，如

最左列所示。

注2：每个分解步骤最上面框内的值代表分解前的ASIL等级。

注3：构架要素E.1和E.2充分独立，符合5.4.3。

5.4.10 当使用 5.4.9 中给出的任何分解方案时，应具备分解后要素充分独立性的证据（参见 5.4.3）。

5.4.11 应至少按照 GB/T 34590.4 和 GB/T 34590.6 中（分解后的）ASIL 等级要求，在系统层面和软件层面开发分解后的要素。应至少按照 GB/T 34590.5 中（分解后的）ASIL 等级要求，在硬件层面开发分解后的要素，但硬件架构度量的评估和因随机硬件失效导致违背安全目标的评估除外（参见 5.4.5）。

5.4.12 在应用了分解的设计过程的每个层面， 对分解后的要素的相关集成活动及后续活动，包括验证和认可措施，应按照分解前的 ASIL 等级的要求开展。

5.5 工作成果

5.5.1 架构信息的更新，由 5.4 得出。

5.5.2 作为安全要求和要素的属性的 ASIL 等级更新，由 5.4 得出。

6 要素共存的准则

6.1 目的

本章提供了以下子要素在同一要素内共存的准则:

a) 安全相关的子要素与非安全相关的子要素;及

分配了不同 ASIL 等级的安全相关子要素。

6.2 总则

通常，当某个要素由几个子要素组成时，按照适用于该要素的最高ASIL等级（即分配给要素的安全要求的最高ASIL等级）的相应措施开发每个子要素。

在未分配ASIL等级或分配了不同ASIL等级的子要素共存情况下，或与安全无关的子要素和与安全相关的子要素共存情况下，避免将要素的ASIL等级分配给全部子要素可能是有益的。为达到该目的，本章为确定不同ASIL等级的子要素是否能在同一要素下共存提供了指导。本章以要素中各个子要素与其余子要素间的干扰分析为基础。

在本章的上下文中，干扰是从未分配ASIL等级的子要素或分配了较低ASIL等级的子要素，到分配了较高ASIL等级的子要素之间存在级联失效，从而导致违背了要素的安全要求（参见GB/T 34590.1-XXXX的3.65）。

当确定要素中子要素的ASIL等级时，应关注级联失效的相关失效分析（参见第7章），此分析为免于干扰提供了依据。

6.3 本章的输入

6.3.1 前提条件

应具备下列信息：

——开展分析所在系统、硬件或软件层面的安全要求，按照 GB/T 34590.3-XXXX 的 7.5.1、 GB/T 34590.4-XXXX 的 6.5.1、GB/T 34590.5-XXXX 的 6.5.1 或 GB/T 34590.6-XXXX 的 6.5.1；

——开展分析所在系统、硬件或软件层面的要素架构信息，按照 GB/T 34590.3-XXXX 的 7.5.1、GB/T 34590.4-XXXX 的 6.5.3、GB/T 34590.5-XXXX 的 7.5.1 或 GB/T 34590.6-XXXX 的 7.5.1；及

——将安全要求分配给所考虑的要素和子要素。

6.3.2 支持信息

无。

6.4 要求和建议

6.4.1 本章适用于设计过程中任何改进步骤，并行于架构要素和子要素的安全要求分配。

注：按照GB/T 34590.4、GB/T 34590.5或GB/T 34590.6，通常在系统设计、硬件设计或软件架构设计时考虑共存准则。

6.4.2 分析要素时应考虑下列内容：

a) 分配到要素的每个安全要求；及

要素包含的每个子要素。

6.4.3 如果非安全相关的子要素和安全相关子要素共同存在于同一要素中,如果能证明非安全相关的子要素不直接或间接地违背分配给该要素的任何安全要求,即:非安全子要素不干扰要素中安全相关的任何子要素,则应仅视其为非安全相关的子要素。

注1：这意味着从该子要素到安全相关子要素的级联失效是不存在的。

注2：可通过设计措施获得，诸如考虑软件的数据流和控制流，或硬件的输入/输出信号及控制线。

否则,在不具备免于干扰证据的情况下,应将共存安全相关子要素的最高ASIL等级分配给该子要素。

6.4.4 如果同一要素中存在执行不同 ASIL 等级要求，包括 QM(x)（参见 5.4.9）的安全相关子要素，仅当能证明对分配给要素的每个安全要求，所考虑的子要素不会直接或间接的违反分配给执行更高 ASIL 等级要求的子要素的任何安全要求时，才能视所考虑的子要素为较低 ASIL 等级的子要素。否则，由于不具备免于干扰的证据，应将共存安全相关子要素的最高 ASIL 等级分配给该子要素。

注：对免于干扰的评估应与分配给共存的子要素的最高ASIL等级要求相匹配（参见7.4.8）。

6.5 工作成果

6.5.1 要素中各子要素的 ASIL 等级属性的更新，由 6.4 得出。

7 相关失效分析

7.1 目的

本章的目的是：

a) 通过分析其潜在原因或引发因素，确认设计中充分实现了要求的独立性或免于干扰；及

如有必要，定义安全措施，以减轻可能的相关失效。

7.2 总则

相关失效分析的范围可能受给定要素的技术(例如软件要素、硬件要素或硬件和软件要素的组合)，以及所涉及的安全要求影响。

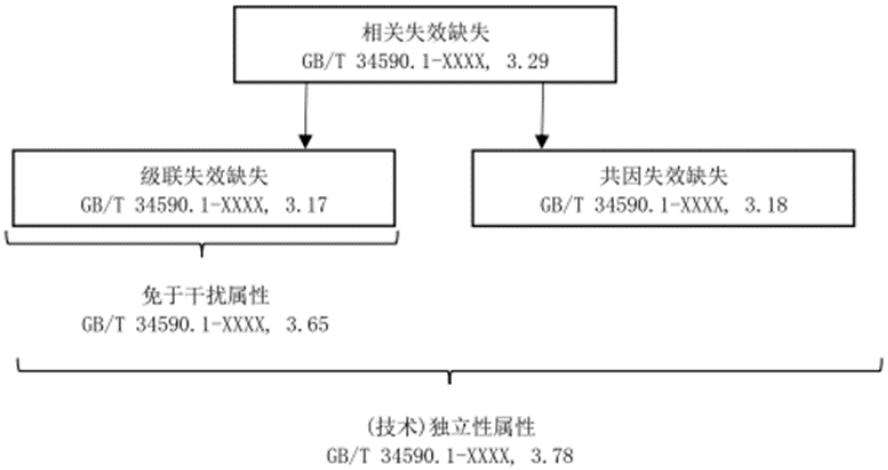


图3　不同类型相关失效之间的关系

图3描述了相关失效、免于干扰和技术独立性之间的关系。

免于干扰是用于证明分配了不同ASIL等级的，或者无ASIL等级和有ASIL等级的要素可以共存（参见第6章）。

免于干扰和不存在共因失效，是用于证明在进行ASIL等级分解时的独立性（参见第5章）。

注1：其他系统属性也可能要求独立性，从而不存在相关失效。例如：相关失效分析可被用于论证避免单点故障和潜伏故障的安全机制的有效性（参见GB/T 34590.5- XXXX,第8章）。

注2：相关失效分析可应用于系统或相关项的各种设计层面。

相关失效分析考虑架构特征，例如：

——相似的和不相似的冗余要素；

——由相同的软件或硬件要素实现的不同功能；

——功能及其相关安全机制；

——功能的分割或软件要素的分隔；

——硬件要素间的物理间距，有隔离或无隔离；

——共同的外部资源。

独立性受到共因失效和级联失效的威胁，而免于干扰仅受级联失效的威胁。

示例1：高强度电磁场会导致不同电子设备失效，失效方式取决于电子设备的设计或使用，该失效是一个共因失效。

示例2：错误的车速信息传递给其它车辆功能并影响其行为，是一个级联失效。

示例3：如果被设计用来探测功能异常表现的监控和被监控的功能两者受相同事件或原因的影响，则该监控可能在被监控功能失效前的某个时刻失效，是一个共因失效。

附录C提供了一个识别相关失效的框架示例。

7.3　本章的输入

7.3.1　前提条件

应具备下列信息：

——应用相关失效分析的系统、硬件或软件层面的独立性要求，按照GB/T 34590.3-XXXX的7.5.1、GB/T 34590.4-XXXX的6.5.1、GB/T 34590.5-XXXX的6.5.1或GB/T 34590.6-XXXX的6.5.1；

——应用相关失效分析的系统、硬件或软件层面的免于干扰要求，按照 GB/T 34590.3-XXXX 的 7.5.1、GB/T 34590.4-XXXX 的 6.5.1、GB/T 34590.5-XXXX 的 6.5.1 或 GB/T 34590.6-XXXX 的 6.5.1；

——应用相关失效分析的系统、硬件或软件层面的架构信息，按照 GB/T 34590.3-XXXX 的 7.5.1、GB/T 34590.4-XXXXX 的 6.5.3、GB/T 34590.5-XXXX 的 7.5.1 或 GB/T 34590.6-XXXX 的 7.5.1；及

注1：架构信息用于确定相关失效分析的边界。

——安全计划，按照 GB/T 34590.2-XXXX 的 6.5.3。

注2：相关失效分析的目的和范围取决于执行分析的子阶段和抽象层。在进行分析前，对这些信息进行定义，例如在安全计划中。

7.3.2 支持信息

无。

7.4 要求和建议

7.4.1 应按照第 8 章安全分析的结果识别出相关失效的潜在可能性。

注1：系统性失效和随机硬件失效都有可能成为相关失效。

注2：对相关失效的潜在可能性的识别可基于演绎分析法，例如，割集检查或者FTA中重复的相同事件。

注3：归纳分析法也可支持相关失效的潜在可能性的识别，例如，在FMEA中多次出现的具有相似失效模式的相似元器件或组件。

注4：应用于半导体的相关失效分析的示例可参考GB/T 34590.11-XXXX，4.7章。

7.4.2 应评估每个识别出的相关失效的潜在可能性，以判定其合理性，即是否存在导致相关失效并违背给定要素间所要求的独立性或免于干扰的合理可预见原因。

注：为进行随机硬件失效导致违背安全目标的评估，而需要对随机硬件失效进行量化时（参见 GB/T 34590.5），因不存在通用且充分可靠的量化方法，共因失效和级联失效的影响是在定性基础上预估的。

7.4.3 此评估应考虑所分析相关项或要素的运行工况，也应考虑其各种运行模式。

7.4.4 此评估应考虑以下适用的内容：

注1：合适的检查清单（例如：基于现场经验的检查清单）可支持对潜在相关失效合理性的评估。检查清单为分析员提供了根本原因和耦合因素（例如：相同的设计、相同的过程、相同的组件、相同的接口、相近的距离）的代表性示例。附录C可作为建立此类检查清单的基础。

注2：也可由是否遵守了旨在防止引入可导致相关失效的根本原因和耦合因素的过程指南来支持此评估。

a) 随机硬件失效；

示例1：共用模块的失效，例如大规模集成电路（微控制器、ASIC 等）的时钟、测试逻辑和内部电压调节器的失效。

开发错误；

示例2：需求错误、设计错误、实施错误、因使用新技术导致的错误和做更改时引入的错误。

生产错误；

示例3：过程、流程和培训相关的错误；控制计划和特殊特性监控中的错误；软件刷新和下线刷新相关的错误。

安装错误；

示例4：线束布置相关的错误；器件间互换性相关的错误；相邻的相关项或要素的失效。

服务错误；

示例5：过程、流程和培训相关的错误；问题处理相关的错误；器件间互换性相关的错误和由于反向的不兼容性导致的错误。

环境因素；

示例6：温度、振动、压力、湿度/冷凝、污染、腐蚀、毒害、电磁兼容性。

共同外部资源或信息失效；

示例7：供电、输入数据、系统间数据总线和通信。

特定工况下的压力；及

示例8：高工作负载、极端的用户输入或来自其它系统的请求、热冲击和机械冲击。

老化和磨损；

7.4.5 应具备相关失效及其影响的合理性的依据。

注：合理的相关失效是指那些按照7.4.2给出的评估发现了合理可预见原因的失效。

7.4.6 应按照 GB/T 34590.8-XXXX，第 8 章变更管理在开发阶段为合理的相关失效定义解决措施。

7.4.7 用于解决合理的相关失效的措施应包括用于预防其根本原因的措施、控制其影响的措施或减少耦合因素的措施。

示例：多样性是可用于预防、降低或探测共因失效的一种措施。

7.4.8 相关失效的分析应具有适当的细节程度和严格程度，以论证达到所要求的独立性或免于干扰的程度。

注：可用于证明对相关失效所进行分析的深度和严格程度是否合适的准则包括：

——ASIL 等级；

——安全概念所要求的要素之间的独立程度；

——产品复杂性；

——技术；及

——不利环境和其它压力因素的数量和程度

7.4.9 应按照 GB/T 34590.8-XXXX，第 9 章，对相关失效分析进行验证。

7.5 工作成果

7.5.1 相关失效分析，由 7.4 得出。

7.5.2 相关失效分析的验证报告，由 7.4.9 得出。

8 安全分析

8.1 目的

安全分析的目的是确保由于系统性故障或随机硬件故障而导致违背安全目标的风险足够低。根据应用，通过以下方法来实现:

——识别先前在危害分析和风险评估期间未识别的新危害;

——逐一识别可能导致违背安全目标或安全要求的故障或失效;

——识别其潜在原因;

——逐一支持故障预防或故障控制安全措施的定义;

——为安全概念的适用性提供证据;及

——支持安全概念、安全要求的验证，以及设计要求和测试要求的识别。

注：在GB/T 34590中，系统性故障没有按发生概率进行分析。然而，针对系统性故障的措施有助于降低违背安全目标或安全要求的总体风险。

8.2 总则

安全分析的范围包括：

——对安全目标和安全概念的确认；

——对安全概念和安全要求的验证；

——对可导致违背安全目标或安全要求的条件及原因的识别，包括故障和失效；
——对探测故障或失效的额外安全要求的识别；
——对探测到的故障或失效所需的响应（行为/措施）的制定； 及
——对为验证安全目标和安全要求是否得到满足所需的额外措施的识别,包括安全相关的车辆测试。

概念和产品开发阶段中,在恰当的开发层面执行安全分析。定量分析方法预测了失效的频率,而定性分析方法识别了失效但不预测失效频率。两种分析方法都依赖于对相关的故障类型和故障模型的了解。

定性分析方法包括:
——系统、设计或过程层面的定性 FMEA;
——定性 FTA;
——危害与可操作性分析(HAZOP);及
——定性 ETA。

注1：当没有更合适的软件特定分析方法存在时,可对软件应用上述定性分析方法。

定量安全分析是对定性安全分析的补充。它们用于验证硬件设计是否符合已定义的硬件架构度量评估目标值和因随机硬件失效导致违背安全目标的评估目标值(参见GB/T 34590.5-XXXX,第8章和第9章)。定量安全分析还要求掌握硬件要素定量失效率的知识。

定量分析方法包括:
——定量 FMEA;
——定量 FTA;
——定量 ETA;
——马尔科夫(Markov)模型;及
——可靠性框图。

注2：定量分析方法仅针对随机硬件失效，这些分析方法不适用于GB/T 34590中的系统性失效。

安全分析的另一种分类方法是基于分析的执行方法给出的:
——归纳分析方法是由下而上的方法,由已知的原因识别可能的影响;
——演绎分析方法是由上而下的方法,由已知的影响探寻可能的原因。

归纳分析和演绎分析相辅相成，因而增加了结果的覆盖面。

注：FEMA和ETA是典型的归纳分析方法，FTA和可靠性框图是典型的演绎方法。

安全分析的另一个分类是根据所选择的方法是否能够识别单点或多点故障，以便根据GB/T 34590.4-XXXX的6.4.2和GB/T 34590.5-XXXX的7.4.3来处理潜伏故障。

8.3 本章的输入

8.3.1 前提条件

应具备以下信息：
——安全分析开展所在系统、硬件或软件层面的安全要求，按照 GB/T 34590.3-XXXX 的 7.5.1、GB/T 34590.4- XXXX 的 6.5.1、GB/T 34590.5-XXXX 的 6.5.1，或 GB/T 34590.6-XXXX 的 6.5.1；及
——安全分析开展所在系统、硬件或软件层面的要素架构信息，按照 GB/T 34590.4-XXXX 的 7.5.2，GB/T 34590.5-XXXX 的 7.5.1，或 GB/T 34590.6-XXXX 的 7.5.1。

注：架构信息用于确定安全分析的边界。

8.3.2 支持信息

可以考虑下列信息：

——故障模型（来自外部）

8.4 要求和建议

8.4.1 应按照适当的标准或指南，以及定义的目标（如在安全计划中定义的目标）来开展安全分析。

注1：分析的详细程度与设计的详细程度相适应。故障模型取决于分析所基于的设计描述层面（系统、硬件、软件）及所实施的安全要求。对于半导体失效模式，可参考GB/T 34590.11-XXXX的4.3.2。

注2：此类标准和指南可包括定义安全分析深度和严谨度的准则。这些准则可取决于特定相关项的ASIL等级、复杂性或经验，以及它所应用的领域。

注3：安全分析的目的和范围取决于其所应用的子阶段及颗粒度。

8.4.2 安全分析的结果应表明是否与相关安全目标或安全要求相符合。

8.4.3 若不满足某个安全目标或安全要求，应利用安全分析的结果得出对导致违背安全目标或安全要求的故障或失效的预防措施、探测措施或影响减轻措施。

8.4.4 由安全分析得出的措施应作为产品开发的一部分，分别按照 GB/T 34590.4、GB/T 34590.5 或 GB/T 34590.6，在系统层面、硬件层面或软件层面进行实施。

8.4.5 按照 GB/T 34590.3-XXXX 第 6 章，在产品开发过程中由安全分析新识别出的、未被安全目标覆盖的危害，应包括在更新后的危害分析和风险评估中。相应的变更，应按照 GB/T 34590.8-XXXX，第 8 章来进行变更管理。

8.4.6 安全分析中用到的故障模型，应与分析所处开发子阶段的详细程度相适应，并与在该开发子阶段中保持一致。

注1：子阶段包括GB/T 34590.5中的硬件设计、对硬件架构指标的评估以及由于随机硬件失效而导致的违背安全目标的评估，或依据GB/T 34590.6进行的软件架构设计。

注2：关于软件架构层面的安全性分析，请参见GB/T 34590.6-XXXX，附录E。

8.4.7 如有必要，应使用安全分析中用到的故障模型和分析结果来确定是否需要额外的安全相关测试用例。

8.4.8 应按照 GB/T 34590.8-XXXX，第 9 章验证安全分析及其结果。

8.4.9 定性安全分析应包括：

a) 对可能导致违背安全目标或安全要求的故障或失效的系统性识别，来源于：

——相关项或要素本身；或

——相关项或要素与其他相关项或要素之间的交互；或

——相关项或要素的使用。

对每个已识别的故障的后果进行评估，以确认违背安全目标或安全要求的潜在可能性；

对每个已识别故障的原因的识别；及

对安全概念潜在薄弱环节的识别或对识别的支持，包括对处理诸如潜在故障、多点故障、共因失效及级联失效的安全机制的无效性的识别。

注：完成对相关项内部和外部与其他相关项或要素的交互的检查，是为了评估独立性程度或干扰程度。

8.4.10 如果定量安全分析被用于补充定性安全分析，则应包括：

a) 用于支持硬件架构度量评估和因硬件随机失效导致违背安全目标的评估（参见 GB/T 34590.5-XXXX，第 8 章和第 9 章）的定量数据。

对能够导致违背安全目标或安全要求的故障或失效的系统性识别。

对安全概念潜在薄弱环节（包括安全机制的无效性）的评估和评级；及。

诊断测试时间间隔，紧急运行时间间隔和从故障探测到修复的时间间隔。

8.5 工作成果

8.5.1 安全分析，由 8.4 得出。

8.5.2 安全分析验证报告，由 8.4.8 得出。

附 录 A
（资料性）
以汽车安全完整性等级为导向和以安全为导向的分析的概览

表A.1提供了以汽车安全完整性等级为导向和以安全为导向的分析的目的、前提条件和工作成果的概览。

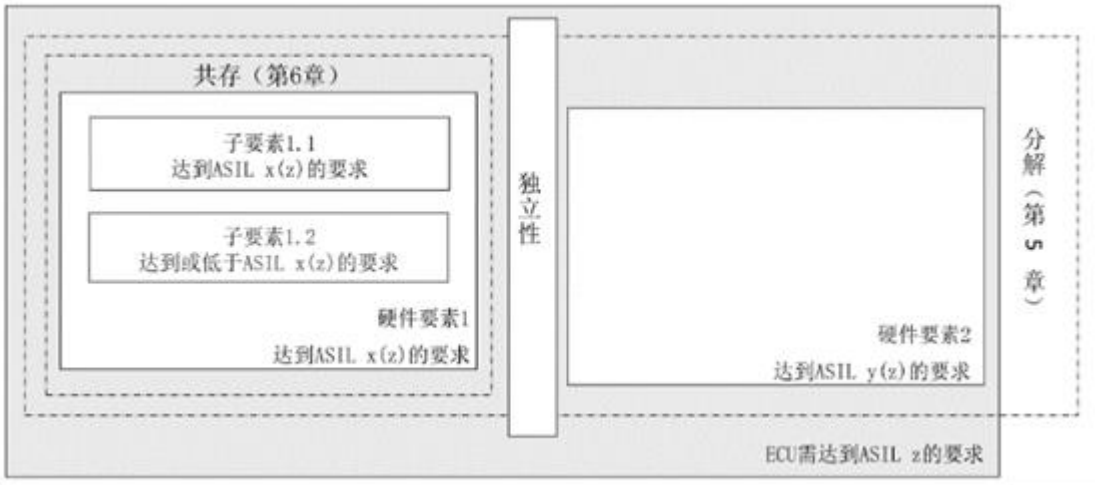
表A.1 以汽车安全完整性等级为导向和以安全为导向的分析的概览

章	目的	前提条件	工作成果
5 关于ASIL等级剪裁的要求分解	如果采用ASIL等级剪裁，本章的目的是： a)确保安全要求被分解为下一级详细的冗余安全要求，并将其分配给充分独立的设计要素；及 b)根据允许的ASIL等级分解方案应用ASIL等级分解。	——ASIL等级分解所在整车、系统、硬件或软件层面的安全要求，按照： GB/T 34590.3-XXXX,7.5.1或 GB/T 34590.4-XXXX,6.5.1或 GB/T 34590.5-XXXX,6.5.1或 GB/T 34590.6-XXXX,6.5.1 ———ASIL分解所在整车、系统、硬件或软件层面的架构信息，按照： GB/T 34590.3-XXXX,7.5.1或 GB/T 34590.4-XXXX,6.5.3或 GB/T 34590.5-XXXX,7.5.1或 GB/T 34590.6-XXXX,7.5.1	5.5.1 架构信息的更新，由5.4得出； 5.5.2 作为安全要求和要素的属性的ASIL等级更新，由5.4得出。
6 要素共存的准则	本章为以下提供了在同一要素内共存的准则： a) 安全相关的子要素与非安全相关的子要素；及 b) 分配了不同ASIL等级的安全相关子要素	——开展分析所在系统、硬件或软件层面的安全要求，按照： GB/T 34590.3-XXXX,7.5.1, 或 GB/T 34590.4-XXXX,6.5.1, 或 GB/T 34590.5-XXXX,6.5.1, 或 GB/T 34590.6-XXXX , 6.5.1; ——开展分析所在系统、硬件或软件层面的要素架构信息，按照： GB/T 34590.3-XXXX,7.5.1, GB/T 34590.4-XXXX,6.5.3, 或 GB/T 34590.5-XXXX,7.5.1, 或 GB/T 34590.6-XXXX,7.5.1; 及 ——将安全要求分配给所考虑的要素和子要素。	6.5.1 作为要素中子要素的ASIL等级的更新，由6.4得出
7 相关失效分析	本章的目的: a) 通过分析其潜在的原因或引发因素，确认在设计过程中充分达到了独立性或免于干扰的要求；及	——应用相关失效分析的系统、硬件或软件层面的独立性要求，按照： GB/T 34590.3-XXXX,7.5.1, GB/T 34590.4-XXXX,6.5.1,	相关失效分析, 由7.4得出 7.5.2相关失效分析验证报告, 由7.4.9得出

章	目的	前提条件	工作成果
	b)如有必要，制定安全措施，缓解可能的相关失效。	GB/T 34590.5-XXXX,6.5.1，或 GB/T 34590.6-XXXX,6.5.1 ——应用相关失效分析的系统、硬件或软件层面的免于干扰要求，按照： GB/T 34590.3-XXXX,7.5.1， GB/T 34590.4-XXXX,6.5.1， GB/T 34590.5-XXXX,6.5.1，或 GB/T 34590.6-XXXX,6.5.1 ——应用相关失效分析的系统、硬件或软件层面的架构信息，按照： GB/T 34590.3-XXXX,7.5.1， GB/T 34590.4-XXXX,6.5.3， GB/T 34590.5-XXXX,6.5.1，或 GB/T 34590.6-XXXX,6.5.1，及 ——安全计划按照： GB/T 34590.2-XXXX,6.5.3.	
8 安全分析	安全分析的目的是确保由于系统性故障或随机硬件故障而导致违背安全目标的风险足够低。根据应用，由以下实现： ——识别先前在危害分析和风险评估期间未识别的新危害； ——逐一识别可能导致违背安全目标或安全要求的故障或失效； ——识别其潜在原因； ——逐一支持故障预防或故障控制安全措施的定义； ——为安全概念的适用性提供证据;及 ——支持安全概念、安全要求的验证，以及设计要求和测试要求的识别。	——开展安全分析的系统、硬件或软件层面的安全要求，按照： GB/T 34590.3-XXXX,7.5.1， GB/T 34590.4-XXXX,6.5.1， GB/T 34590.5-XXXX,6.5.1，或 GB/T 34590.6-XXXX,6.5.1，及 ——开展安全分析的系统、硬件或软件层面的要素架构信息，按照： GB/T 34590.4-XXXX,7.5.2， GB/T 34590.5-XXXX,7.5.1，或 GB/T 34590.6-XXXX,7.5.1	8.5.1安全分析由8.4得出。 8.5.2安全分析验证报告由8.4.8得出。

附 录 B
（资料性）
要素共存和要求分解的架构示例

B.1 架构示例



图B.1 一个示例架构中的共存和分解

注：共存和分解，是GB/T 34590.4-XXXX第6章系统架构设计约束，和GB/T 34590.5-XXXX第7章硬件设计，以及GB/T 34590.6-XXXX第7章软件设计的一部分

B.2 共存（第 6 章）

——如果一个 ASIL x 要求被分配给要素 1，那么子要素 1.1 和子要素 1.2 继承 ASIL x。

——子要素 1.2 仅在满足以下条件时在较低的 ASIL 等级下开发:

——要素 1 的至少一个子要素能够满足要素 1 在 ASIL x 下的要求（例如：子要素 1.1）

——子要素 1.2 不能违反要素 1 的安全要求；及

——满足共存的准则（参见第 6 章）：从子要素 1.2 到子要素 1.1 没有级联失效（免于干扰）。

B.3 分解（第五章）

如果将ASIL z的要求分配给图B.1中的ECU，则可以在独立且冗余的硬件要素之间进行分解。

这相当于满足下列所有条件：

——使用第 5 章中描述的分解模式，即 ASIL z → ASIL x(z) + ASIL y(z)；

——硬件要素 1 本身满足 ASIL x(z)的 ECU 安全要求；

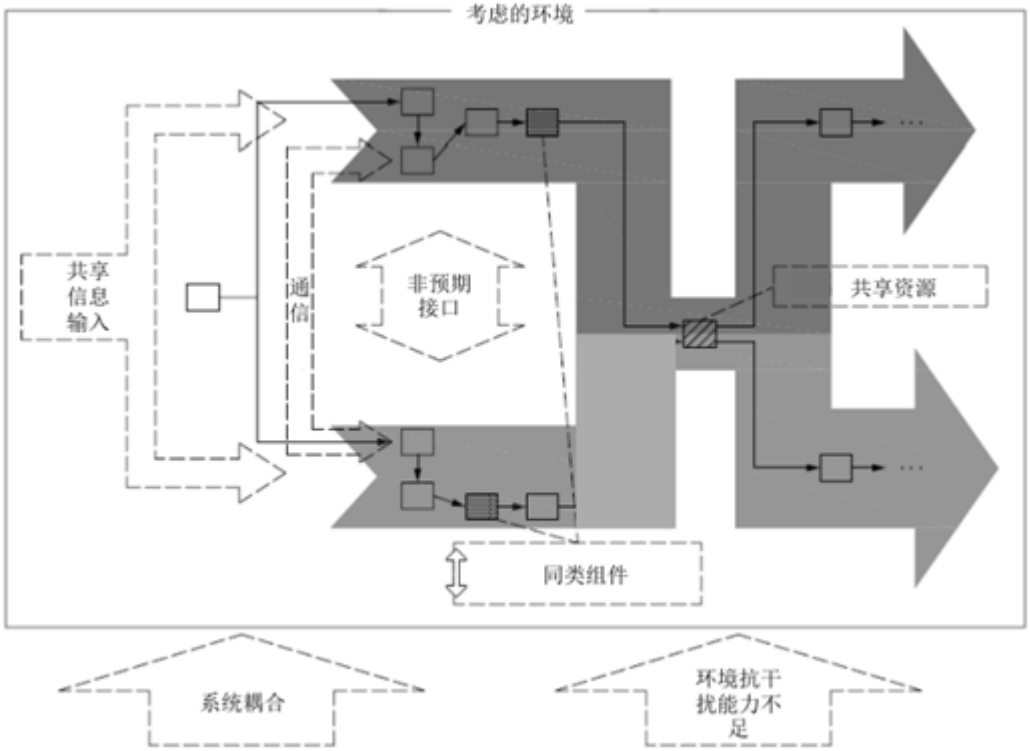
——硬件要素 2 本身满足 ASIL y(z)的 ECU 安全要求；

——硬件要素 1 和硬件要素 2 是相互独立的，从 ASIL Z 出发论证无从硬件要素 1 到硬件要素 2 的级联失效、无从硬件要素 2 到硬件要素 1 的级联失效、且无共因失效。

附 录 C
（资料性）
识别相关失效的框架

两个或多个要素之间的独立性通过证明不存在相关失效来确定，即不存在级联失效和共因失效。根据安全概念，例如为了支持ASIL分解，可能要求要素之间有独立性。

为了识别级联和共因失效，可以使用以下耦合因素类别来提高分析的完整性。



图C.1 要素间的耦合因素类别

注：灰色箭头表示连接各要素间的事件功能链，从而实现受耦合因素影响的功能。虚线箭头表示潜在影响系统及其要素的耦合因素的类别。

如表C.1所示，这些耦合因素类别可以作为检查清单应用于任何开发层面，包括系统、软件、硬件和半导体层面。此表提供了耦合因素的示例，这些示例可逐一映射到7.4.4中的标题。一些例子可以属于多个耦合因素类别，例如，软件标定参数可以被视为共享资源或共享信息输入。

表 C.1 系统、软件、硬件和半导体层面的示例

耦合系数类	GB/T 34590.9-XXXX,7.4.4中的主题	系统层面的示例	硬件层面的示例	软件层面的示例	半导体层面的示例
共享资源： 举例使用相同的软件、硬件或系统要素的两个要	a）随机硬件失效 g）共同外部资源或信息失效	—电源（参见环境抗干扰力不足） —线束 —数据和通信总线	—时钟 —两个关闭通道使用的相同H桥	—被其他2个软件组件使用的软件组件，例如 —数学或其他库	GB/T 34590.11中的“共享资源失效”和“单一物理根本原因”

耦合系数类	GB/T 34590.9-XXXX,7.4.4中的主题	系统层面的示例	硬件层面的示例	软件层面的示例	半导体层面的示例
素，它们会受到共享资源失效或者不可用的影响。		—功率级	—插座，插头连接器	— I/O程序，驱动 —多个软件要素使用的硬件资源	
共享信息输入： 从功能的角度看，即使在没有共享资源的情况下，连接到相同信息源的两个功能也会使用相同的信息。	a）随机硬件失效	—外部消息（例如CAN，Flexray或AUTOSAR RTE消息） —外部物理信号（例如磁场，远程/无线电信号） —电容/雷达/光学传感器检测到的读数值	—连接到原始物理的数字或模拟信号源	—对于两个软件函数的全局常量或变量 —由一个软件函数传递给多个其他函数的数据/函数参数/消息	GB/T 34590.11中的“共享资源失效”
环境抗干扰力不足： 相同或相似的物理特性的要素，可能会受到相同的外部环境干扰的影响	f）环境因素 h）特定工况下的压力	—机械耦合 —易燃材料	—对电效应的敏感度等级（可能产生电磁干扰、静电放电等） —硬件要素的接近程度（可能遭受灰尘，颗粒的潜在危害） —相同的外壳（可能遭受进水，潮湿的潜在危害）	不直接适用于软件本身。可以在系统和硬件级别上考虑影响软件行为的环境因素。	GB/T 34590.11中的“环境故障”
系统耦合： 由于共同的系统性的人为错误或工具错误而导致的要素失效。	b) 开发错误 c) 生产错误 d) 安装错误 e) 服务错误 h) 特定工况下的压力	—用于多个要素的相同生产过程 —用于多个要素的相同维修过程。		—相同的软件工具，如IDE、编译器、链接器、软件配置器 —相同的编程和/或建模语言 —相同的编译器/链接器	GB/T 34590.11中的 “开发错误”、“生产错误”、“安装错误” 和 “维修错误”
相同类型的组件： 由于共因失效，相同或非常相似组件的多个实例可能会共同失效。	a) 随机硬件失效 b) 开发错误	—相同类型的执行器/功率级，例如电机 — 相同类型的传感器	—相同类型的硬件部件和组件 —不同微控制器的相同电源 —相同的微控制器 —相同的专用集成电路	—相同的源代码扩展了两次，例如通过使用C语言宏 注：从不同位置调用的相同的库实例或相同的标准软件模块实例，被认为是共享资源。	GB/T 34590.11中的“开发错误”

耦合系数类	GB/T 34590.9-XXXX,7.4.4中的主题	系统层面的示例	硬件层面的示例	软件层面的示例	半导体层面的示例
通讯： 一个要素通过通信通道从另一个要素接收信息	a) 随机硬件失效 b) 开发错误 d) 安装错误 e) 服务错误 i) 老化和磨损	—同一系统的两个 ECU之间的CAN连接 —同一ECU内两个微控制器之间的通信	—两个硬件要素之间的电气连接	— 通过全局变量的数据流 — 消息传递 — 传递参数的函数调用	GB/T 34590.11中半导体的“共享资源失效”和“单一物理根本原因”
非预期接口： 两个要素通过一个非预期接口直接相互影响	a) 随机硬件失效 b) 开发错误 d) 安装错误 h) 特殊工况下的压力	—由于同步缺失，导致一个功能覆盖另一个功能	—由于硬件要素靠的很近，导致信号线之间产生潜在的串扰、热冲击、干扰等。	—由于使用相同的内存空间，导致可能出现错误的内存分配或内存泄漏	源于半导体的单一物理根本原因(参见 GB/T 34590.11)。

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] Lovric T. (ZF TRW), Metz P. (Brose), Schnellbach A. (Magna), Dependent Failure Analysis in Practice, VDA Sys Conference, July 6th–8th 2016, Berlin.

[3] Schnellbach, Magna Powertrain, Dependent Failure Analysis, The MPT approach, Safetronic. 2014 — Functional Safety in Automotive conference, 11th–12th Nov, 2014, Stuttgart.

[4] Abbreviated injury scale; Association of the advancement of Automotive medicine; Barrington, IL, USA Information is also available at www.aaam.org.

[5] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006; https://www.acea.be/publications/article/code-of-practice-for-the-design-and-evaluation-of-adas.

[6] BAKER, S.P., O'NEILL, B., HADDON, W., LONG, W.B., The injury severity score: a method for describing patients with multiple injuries and evaluating emergency care, The Journal of Trauma, Vol. 14, No. 3, 1974.

[7] BALOGH, Z., OFFNER, P.J., MOORE, E.E., BIFFL, W.L., NISS predicts post injury multiple organ failure better than ISS, The Journal of Trauma, Vol. 48, No. 4, 2000.