ICS

T

中华人民共和国国家标准

GB/T XXXXX—XXXX

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以安全为导向的分析

Road vehicles — Functional safety — Part 9:Automotive Safety Integrity Level(ASIL)-oriented and safety-oriented analyses

(ISO26262-9:2011,MOD)

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

GB/T XXXXX《道路车辆 功能安全》包括十个部分：

——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：生产和运行；

——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。

本部分为GB/T XXXXX的第9部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分修改采用国际标准ISO 26262-9：2011 《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以安全为导向的分析》（英文版）。

本部分的附录A为资料性附录。

本部分由国家标准化管理委员会提出。

本部分由全国汽车标准化技术委员会（SAC/TC114）归口。

本部分起草单位：

本部分主要起草人：

引　言

ISO 26262 是以 IEC61508 为基础，为满足道路车辆上特定电子电气系统的需求而编写。

ISO 26262 适用于道路车辆上特定的由电子、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。

安全是未来汽车发展的关键问题之一，不仅在驾驶辅助和动力驱动领域，而且在车辆动态控制和主被动安全系统领域，新的功能越来越多地触及到系统安全工程领域。这些功能的开发和集成将强化对安全相关系统开发流程的需求，并且要求提供满足所有合理的系统安全目标的证明。

随着技术日益复杂、软件内容和机电一体化应用不断增加，来自系统性失效和硬件随机失效的风险逐渐增加。ISO 26262 通过提供适当的要求和流程来避免风险。

系统安全是通过一系列安全措施实现的。安全措施通过各种技术（例如，机械、液压、气压、电子、电气、可编程电子等）实现且应用于开发过程中的不同层面。尽管 ISO 26262 针对的是电子电气系统的功能安全，但是它也提供了一个基于其它技术的与安全相关系统的框架。ISO 26262：

a) 提供了一个汽车安全生命周期(管理、开发、生产、运行、维护、报废)，并支持在这些生命周期阶段内对必要活动的剪裁；

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；

c) 应用汽车安全完整性等级规定 ISO 26262 中适用的要求，以避免不合理的残余风险；

d) 提供了对于确认和认可措施的要求，以确保达到一个充分、可接受的安全等级；

e) 提供了与供应商相关的要求。

功能安全受开发过程(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、维护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开发活动和工作成果相互关联。ISO 26262 涉及与安全相关的开发活动和工作成果。

图1为ISO 26262的整体架构。ISO 26262基于V模型为产品开发不同阶段提供过程参考：

— 阴影"V"表示标准中第 3、4、5、6 和 7 部分之间的关系；

— 以“m-n”方式表示的具体条款中，“m”代表特定部分的编号，“n”代表该部分章条的编号。

示例：“2-6”代表 ISO 26262-2 的第六章

图1 ISO 26262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以安全为导向的分析

1 范围

GB/T XXXXX适用于安装在最大总质量不超过3.5吨的量产乘用车上的包含一个或多个电子电气系统的与安全相关的系统。

GB/T XXXXX不适用于安装在特殊用途车辆上的特定的电子电气系统，例如为残疾驾驶者设计的车辆。

已经完成生产发布的系统及其组件或在本标准发布日期前开发的系统及其组件不适用于本标准。对于在本标准发布前完成生产发布的系统及其组件进行进一步的开发或变更时，仅修改的部分需要按照本标准开发。

本标准针对由电子电气安全相关系统的故障行为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。本标准不针对与触电、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，除非危害是直接由电子电气安全相关系统的故障行为而引起的。

本标准不针对电子电气系统的标称性能，即使这些系统（例如主动和被动安全、制动系统、自适应巡航系统）有专用的功能性能标准。

本部分规定了对支持过程的要求，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，

—安全分析。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 XXXXX-1:201X，道路车辆 功能安全 第1部分：术语；

GB/T XXXXX-2:201X，道路车辆 功能安全 第2部分：功能安全管理；

GB/T XXXXX-3:201X，道路车辆 功能安全 第3部分：概念阶段；

GB/T XXXXX-4:201X，道路车辆 功能安全 第4部分：产品开发：系统层面；

GB/T XXXXX-5:201X，道路车辆 功能安全 第5部分：产品开发：硬件层面；

GB/T XXXXX-6:201X，道路车辆 功能安全 第6部分：产品开发：软件层面；

GB/T XXXXX-8:201X，道路车辆 功能安全 第8部分：支持过程；

3 术语和定义

GB/T XXXXX-1给出的术语和定义适用于本部分。

4 要求

4.1 一般要求

如声明满足GB/T XXXXX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 XXXXX-2 的要求，已经计划安全活动的剪裁并表明这些要求不适用，或，

b) 使不符合项可被接受的依据是存在的， 并且按照 GB/T XXXXX-2 的要求对该依据进行了评估。

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。

安全活动的结果以工作成果的形式给出。“前提条件”是那些作为前一阶段的工作成果而应在本阶段提供的信息。如果条款的某些要求是依照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，但在某些案例中，GB/T XXXXX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。

4.2 对表格的诠释

表属于规范性表还是资料性表取决于上下文。在实现满足相关要求时，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（在最左侧栏以顺序号标明，如 1,2,3），或

b) 一个选择的条目（在最左侧栏以数字后加字母标明，如 2a，2b，2c）。

对于连续的条目，全部方法应按照ASIL等级推荐予以使用。除了所列出的方法外，如果应用所列出方法以外的其它方法，应给出满足相关要求的理由。

对于选择性的条目，按照ASIL等级指示的要求，应采用适当的方法组合，不依赖于组合的方法是否在表中列出。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，则应采用具有更高推荐等级的方法。应给出组合方法满足相关要求的理由。

注：在表中所列出的方法的理由是充分的。但是，这并不意味着有偏袒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，未推荐或反对该方法。

4.3 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，应满足每一子章条的要求或建议。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章的内容，应遵循c分解后的ASIL等级。

如果GB/T XXXXX中ASIL等级在括号中给出，则对于该ASIL等级，相应的子章节应被认为是推荐而非要求。这里的括号与ASIL等级分解无关。

5 关于 ASIL 剪裁的要求分解

5.1 目的

本章提供了将安全要求分解为冗余安全要求的规则和指导，以允许更细节层面的ASIL剪裁。

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过程。从安全目标开始，在开发阶段得出并细化安全要求。ASIL等级作为安全目标的一个属性，由后续每个安全要求继承。功能和技术安全要求向每个架构要素的分配，开始于初步的架构设想，结束于硬件和软件要素。

设计过程中的ASIL 剪裁方法称为“ASIL 分解”。在分配过程中，可从包括存在充分独立的架构要素等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地执行安全要求，及

— 分配一个可能更低的ASIL等级给这些分解后的安全要求。

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。

注1：ASIL 分解是一种ASIL 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、硬件或者软件安全要求。

注2：作为一项基本原则，ASIL分解需要安全要求具有冗余性，且分配给充分独立的架构要素。

注3：使用同质冗余（例如：通过复制设备或复制软件）的情况下，考虑到硬件和软件的系统性失效，不能降低ASIL等级，除非相关失效的分析提供了存在充分独立性或潜在共因指向安全状态的证据。因此，同质冗余因缺少要素间的独立性，通常不足以降低ASIL等级。

注4：通常，ASIL 分解不适用于在多通道架构设计中用来确保通道选择或开关的要素。

通常，ASIL分解允许将安全要求的ASIL等级在几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 XXXXX-5）在ASIL分解后仍保持不变。

5.3 本章的输入

5.3.1 前提条件

应具备下列信息：

— ASIL分解所在层面（系统、硬件或软件）的安全要求，按照GB/T XXXXX-3:8.5.1、GB/T XXXXX-4:6.5.1、GB/T XXXXX-5:6.5.1或GB/T XXXXX-6:6.5.1；及

— ASIL分解所在层面（系统、硬件或软件）的架构信息，按照GB/T XXXXX-4:7.5.2、GB/T XXXXX-5:7.5.1或GB/T XXXXX-6:7.5.1。

5.3.2 支持信息

可考虑下列信息：

— 相关项定义（参见GB/T XXXXX-3: 5.5）；及

— 安全目标（参见GB/T XXXXX-3: 7.5.2）。

5.4 要求和建议

5.4.1 如果应用 ASIL 分解，应满足本章的所有要求。

5.4.2 进行 ASIL 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 分解，可将几个安全要求分配给同一独立要素。

5.4.3 应将初始安全要求分解为由充分独立要素执行的冗余安全要求。

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：此要求通过定义提供了冗余。

5.4.5 按照 GB/T XXXXX-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 分解后保持不变。

5.4.6 如果在软件层面应用 ASIL 分解，应在系统层面检查执行分解后要求的要素间的充分独立性，且应在软件层面、硬件层面或系统层面采取适当的措施来获得充分的独立性。

5.4.7 如果对初始安全要求的 ASIL 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) 相关安全机制宜被赋予分解后的最高 ASIL 等级；

注：通常，与预期功能相比，安全机制具备更低的复杂度和更小的规模。

b) 安全要求应被分配给预期功能，并按照相应分解后的 ASIL 等级执行。

注：如果选择了分解方案 ASILx(x) +QM(x)，则 QM(x)意味着对于执行分配给预期功能的安全要求的要素开发，质量管理体系可能是充分的。QM(x)也意味着质量管理系统可支撑预期功能和安全机制间独立性的理由。

5.4.8 如果不能通过关闭要素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。

5.4.9 对安全要求应用 ASIL 分解时，则：

a) 应按照 5.4.10 应用 ASIL 分解；

b) ASIL 分解的应用可能多于一次；

c) 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)”。

5.4.10 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），或使用可得出更高 ASIL 等级的方案。

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

a) 对于一个等级为 ASIL D 的要求，可按照以下方案之一进行分解：

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。

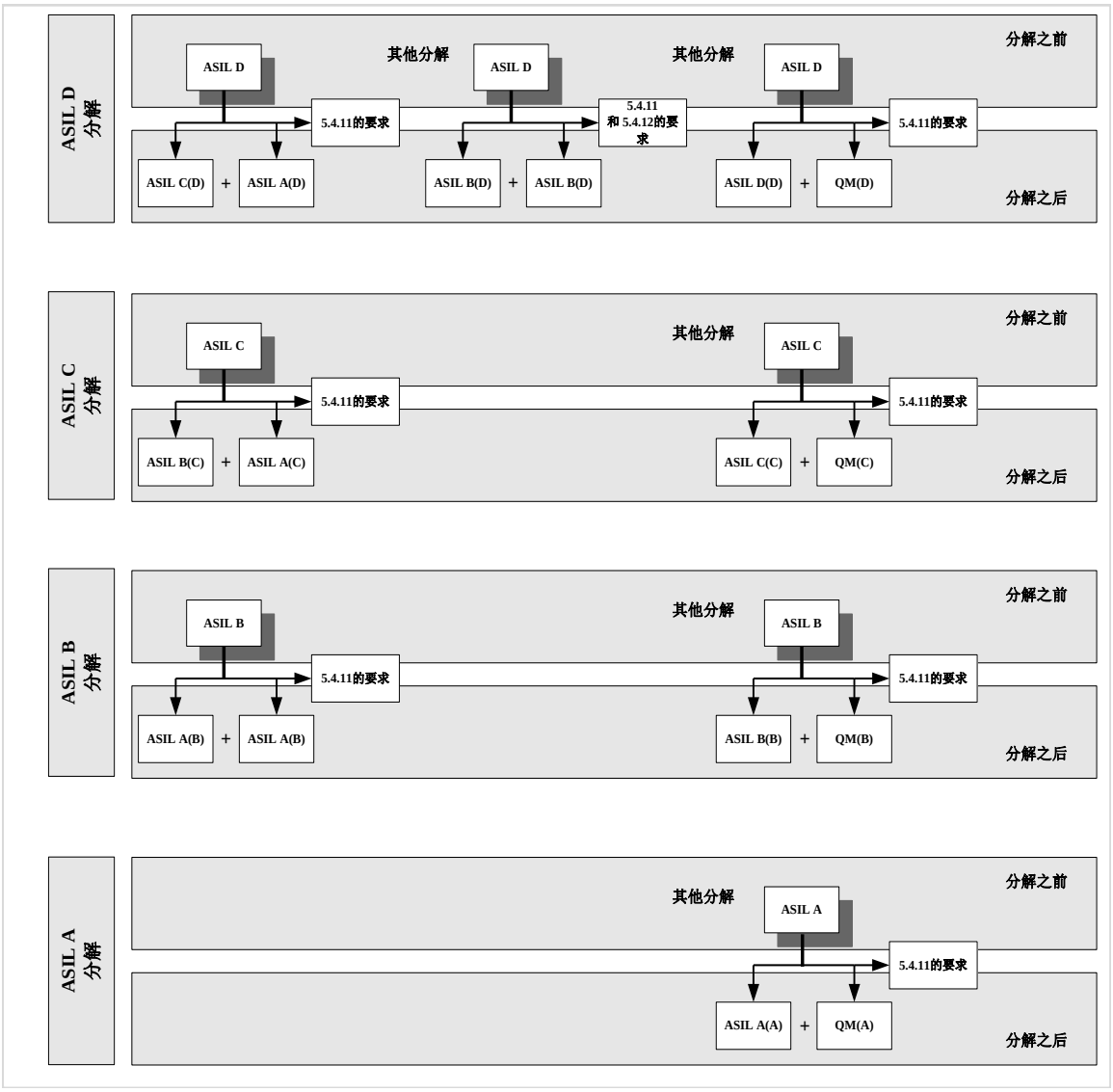
b) 对于一个等级为 ASIL C 的要求，可按照以下方案之一进行分解：

1) 一个ASIL B(C) 的要求和一个ASIL A(C)的要求；或
2) 一个ASIL C(C) 的要求和一个QM(C)的要求。

c) 对于一个等级为 ASIL C 的要求，可按照以下方案之一进行分解：

1) 一个ASIL A(B) 的要求和一个ASIL A(B)的要求；或
2) 一个ASIL B(B) 的要求和一个QM(B)的要求。

d) 一个 ASIL A 的要求不应被进一步分解，除非需要分解成一个 ASIL A(A) 的要求和一个 QM(A) 的要求。



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，如最右列所示。

注：每个分解步骤的最上面阴影框内代表分解前的 ASIL 等级。

图 2 ASIL 分解方案

5.4.11 当使用 5.4.10 中给出的任何分解方案时，则 ：

a) 应按照安全目标的ASIL等级实施符合GB/T XXXXX-2：6.4.7的认可措施；
b) 应具备分解后要素充分独立性的证据。

注：如果相关失效分析（参见 GB/T XXXXX 本部分第 7 章）未发现可导致违背分解前安全要求的相关失效起因，或每个识别出的相关失效的起因都按照安全目标的 ASIL 等级被安全措施充分控制，则要素是充分独立的。

5.4.12 当使用 5.4.10 a）2）中给出的 ASIL D 分解方案时，则：

a) 应按照GB/T XXXXX-8中第6章ASIL C的要求来定义分解后的安全要求；

注：与 ASIL B 相比，ASIL C 要求更正式的标记法，从而更有效的避免系统性失效，并降低两个 ASIL B(D) 实施间的相关性。

b) 如果用相同的软件工具开发分解后的要素，那么这些软件工具应考虑为开发ASIL D相关项或要素的软件工具，并符合GB/T XXXXX-8中软件工具使用的置信度。

5.4.13 应至少按照 GB/T XXXXX-4 和 GB/T XXXXX-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 XXXXX-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）。

5.4.14 在应用了分解的设计过程的每个层面，应按照分解前的 ASIL 等级要求开展对分解后的要素的相关集成活动及后续活动。

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

本章为以下提供了在同一要素内共存的准则：

— 安全相关的子要素与没有分配 ASIL 等级的子要素；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，依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（参见 GB/T XXXXX-4：7.4.2.3）。

在分配了不同 ASIL 等级的子要素共存情况下，或未分配 ASIL 等级的子要素与安全相关的子要素共存情况下，避免将某些子要素的 ASIL 等级提高到要素的 ASIL 等级可能是有益的。为达到该目的，本章为确定要素中子要素的 ASIL 等级提供了指导。本章以要素中某个子要素与其余子要素间的干扰分析为基础。

干扰是由未分配 ASIL 等级或分配了较低 ASIL 等级的子要素到分配了较高 ASIL 等级子要素的导致违背安全要求的级联失效的表现（参见 GB/T XXXXX-1：1.13 和 1.49 的定义）。

当确定要素中子要素的 ASIL 等级时，关注级联失效的相关失效分析（参见 GB/T XXXXX 本部分第 7 章）支持了免于干扰的理由。

6.3 本章的输入

6.3.1 前提条件

应具备下列信息：

— 分析所开展层面（系统、硬件或软件）的安全要求，按照 GB/T XXXXX-3:8.5.1、GB/T XXXXX-4:6.5.1、GB/T XXXXX-5:6.5.1 或 GB/T XXXXX-6:6.5.1；及

— 分析所开展层面（系统、硬件或软件）的要素架构信息，按照 GB/T XXXXX-4:7.5.2、GB/T XXXXX-5:7.5.1 或 GB/T XXXXX-6:7.5.1。

6.3.2 支持信息

无。

6.4 要求和建议

6.4.1 本章可用于设计过程的任意细化步骤，平行于架构要素和子要素的安全要求分配，典型地在系统设计、硬件设计或软件架构设计的子阶段，按照 GB/T XXXXX-4、GB/T XXXXX-5 或 GB/T XXXXX-6。

6.4.2 应用本章之前应将安全要求分配给要素的子要素。

注：安全要求向子要素的分配生成了安全相关子要素和未分配 ASIL 等级的子要素。

6.4.3 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
b) 要素的每个子要素。

6.4.4 如果未分配 ASIL 等级的子要素和安全相关子要素共同存在于同一要素中，如果能证明未分配 ASIL 等级的子元素不直接或间接地违背分配给该要素的任何安全要求，即：它不干扰要素中安全相关的任何子要素，则应仅视其为 QM 的子要素。

注 1：这意味着从该子要素到安全相关要素的级联失效是不存在的。

注 2：这能通过设计预防措施获得，诸如考虑软件的数据流和控制流，或硬件的 I/O 端口及控制线。

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。

6.4.5 如果同一要素中存在不同 ASIL 等级(包括 QM(x))的安全相关子要素(参见 5.4.10)，若能证明对分配给要素的每个安全要求，某个子要素不干扰任何分配了较高 ASIL 等级的其它子要素，则应仅视该子要素为较低 ASIL 等级的子要素否则，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。

6.5 工作成果

6.5.1 作为要素中子要素属性的 ASIL 等级的更新，由 6.4 得出。

7 相关失效分析

7.1 目的

相关失效分析旨在识别出可绕开给定要素间所要求的独立性、绕开免于干扰、使独立性无效或使免于干扰无效，并违背安全要求或安全目标的单一事件或原因。

7.2 总则

相关失效分析考虑如下架构特征：

— 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；

— 硬件要素间的物理距离，有隔离或无隔离；

— 共同的外部资源。

根据 GB/T XXXXX-1 的定义，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：引发不同电子设备以一种基于设计方式失效或使用的方式失效的高强度电磁场 ，是共因失效的一个例子；影响车辆功能表现的有偏差的车速信息（车速失效），是级联失效的例子。

相关失效可同时显现，或在足够短的时间间隔内产生同时失效的效果。

示例 2：如果设计用于探测功能异常表现的监控和被监控的功能受相同的事件或原因影响，则在被监控功能失效前的某个时刻，可视监控无效。

7.3 本章的输入

7.3.1 前提条件

应具备下列信息：

— 所应用层面（系统、硬件或软件）的独立性要求，按照 GB/T XXXXX-3:8.5.1、GB/T XXXXX-4:6.5.1、GB/T XXXXX-5:6.5.1 或 GB/T XXXXX-6:6.5.1；

— 所应用层面（系统、硬件或软件）的免于干扰要求，按照 GB/T XXXXX-3:8.5.1、GB/T XXXXX-4:6.5.1、GB/T XXXXX-5:6.5.1 或 GB/T XXXXX-6:6.5.1；及

— 独立性或免于干扰的要求所应用层面（系统、硬件或软件）的架构信息，按照 GB/T XXXXX-4:7.5.2、GB/T XXXXX-5:7.5.1 或 GB/T XXXXX-6:7.5.1。

注：架构信息用于确定相关失效分析的范围。

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：割集检查或者 FTA 中重复的相同事件可表明相关失效的潜在可能性。

注 3：归纳分析法也可支持该识别：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可提供相关失效潜在可能性的额外信息。

7.4.2 应评估每个识别出的相关时效的潜在可能，以判定其合理性，即：存在导致相关时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：为评估随机硬件失效导致违背安全目标，需要对随机硬件失效进行量化时（参见 GB/T XXXXX-5），因不存在通用且充分可靠的方法来量化此类失效，共因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 此评估应适当考虑以下：

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、近似度）的代表性示例。IEC 61508 中提供的信息可作为建立此类检查清单的基础。

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

a) 随机硬件失效；

示例：共用模块（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。

b) 开发错误；

示例：要求错误、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。

c) 生产错误；

示例：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。

d) 安装错误；

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

e) 维修错误；

示例：过程、流程和培训相关的错误；排除故障相关的错误；元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。

f) 环境因素；

示例：温度、振动、压力、湿度/冷凝、污染、腐蚀、毒害、电磁兼容性。

g) 共同外部资源失效；及

示例：供电、输入数据、系统间数据总线和通信。

h) 特定工况下的压力。

示例：磨损和老化。

7.4.5 应具备相关失效及其影响的合理性的理由。

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

7.4.6 应按照 GB/T XXXXX-8 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。

7.5 工作成果

7.5.1 相关失效的分析，由 7.4 得出。

8 安全分析

8.1 目的

安全分析的目的在于检查相关项及要素的功能、表现及设计的故障和失效后果。安全分析也提供了关于导致违背安全目标及安全要求的条件和原因的信息。

此外，安全分析也有助于识别出在先前危害分析和风险评估过程中未被发现的新功能性危害或非功能性危害。

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包括故障和失效的原因的识别；

— 对关于故障探测或失效探测的额外要求的识别；

— 对探测故障或失效所需的响应行为/响应措施的制定；及

— 对关于验证安全目标和安全要求得到满足的额外要求的识别，包括安全相关的车辆测试。

概念和产品开发阶段中，在恰当的抽象层面执行安全分析。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)；

— 定性 ETA。

注 1：当没有更合适的软件特定分析方法存在时，可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 XXXXX-5）。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；

— 可靠性框图。

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

安全分析的另一种分类原则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，由已知的原因预见未知的影响；

— 演绎分析方法是由上而下的方法，由已知的影响探寻未知的原因。

示例：系统、设计和过程 FEMA、ETA 和马尔科夫模型是归纳分析方法。FTA 和可靠性框图是演绎分析方法。

8.3 本章的输入

8.3.1 前提条件

应具备下列信息：

— 安全分析所需开展层面（系统、硬件或软件）的安全要求，按照 GB/T XXXXX-3:8.5.1、GB/T XXXXX-4:6.5.1、GB/T XXXXX-5:6.5.1 或 GB/T XXXXX-6:6.5.1；

— 安全分析所需开展层面（系统、硬件或软件）的要素架构信息，按照 GB/T XXXXX-4:7.5.2、GB/T XXXXX-5:7.5.1 或 GB/T XXXXX-6:7.5.1；及

注 1：架构信息用于确定安全分析的范围。

— 安全计划，按照 GB/T XXXXX-2：6.5.1。

注 2：安全计划包含安全分析的目标。

8.3.2 支持信息

可考虑下列信息：

— 故障模式（来自外部）

8.4 要求和建议

8.4.1 应按照合适的标准或指南开展安全分析。

8.4.2 安全分析的结果应表明相关安全目标或安全要求是否得到了满足。

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目标或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，在系统层面、硬件层面或软件层面进行实施，分别按照 GB/T XXXX-4 、GB/T XXXX-5 或 GB/TXXXX-6。

8.4.5 对于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，应按照 GB/T XXXXX-8 中的变更管理要求，引入到危害分析和风险评估中，并进行评估。

8.4.6 安全分析中用到的故障模式应与适当的开发子阶段保持一致，例如 GB/T XXXXX-5 中硬件设计、硬件架构度量的评估和因硬件随机失效导致违背安全目标的评估 。

8.4.7 应利用安全分析中的故障模式和分析结果来确定是否需要额外的安全相关测试案例。

8.4.8 应按照 GB/T XXXXX-8 验证安全分析的结果。

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

— 相关项或要素与其它相关项或要素之间的交互；或

— 相关项或要素的使用；

b) 对每个已识别的故障的后果评估，以确认违背安全目标或安全要求的潜在可能性。

c) 对每个已识别故障的原因的识别；及

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

注：完成对相关项内部和外部与其它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 如果定量安全分析适用，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 XXXXX-5）的定量数据；

b) 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；

c) 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

d) 诊断测试间隔，紧急运行间隔和从故障探测到修复的时间间隔。

8.4.11 如果用定性安全分析来支持对定量要求的符合性，应恰当选择这些安全分析的详细程度。

8.5 工作成果

8.5.1 安全分析，由 8.4 得出。

附录A

（资料性附录）

ASIL导向和安全导向分析概览

表A.1提供了ASIL导向和安全导向分析的目的、前提条件和工作成果的概览。

表 A.1 ASIL 导向和安全导向分析概览

条目	目的	前提条件	工作成果
5 关于ASIL剪裁的要求分解	本章提供了将安全要求分解为冗余安全要求的规则和指导，以允许更细节层面的ASIL剪裁。	ASIL分解所在层面（系统、硬件或软件）的安全要求； ASIL分解所在层面（系统、硬件或软件）的架构信息。	5.5.1 架构信息的更新； 5.5.2 作为安全要求和要素的属性的ASIL等级更新。
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： ——安全相关的子要素与没有分配ASIL等级的子要素；及 ——分配了不同ASIL等级的安全相关子要素	分析所开展层面（系统、硬件或软件）的安全要求； 分析所开展层面（系统、硬件或软件）的要素架构信息。	6.5.1 作为要素中子要素属性的ASIL等级的更新。
7 相关失效分析	相关失效分析旨在识别出可绕开给定要素间所要求的独立性、绕开免于干扰、使独立性无效或使免于干扰无效，并违背安全要求或安全目标的单一事件或原因	所应用层面（系统、硬件或软件）的独立性要求； 所应用层面（系统、硬件或软件）的免于干扰要求； 独立性或免于干扰的要求所应用层面（系统、硬件或软件）的架构信息。	7.5.1 相关失效的分析
8.安全分析	安全分析的目的在于检查相关项及要素的功能、表现及设计的故障和失效后果。安全分析也提供了关于导致违背安全目标及安全要求的条件和原因的信息。 此外，安全分析也有助于识别出在先前危害分析和风险评估过程中未被发现的新功能性危害或非功能性危害。	安全分析所需开展层面（系统、硬件或软件）的安全要求； 安全分析所需开展层面（系统、硬件或软件）的要素架构信息。	8.5.1 安全分析