中华人民共和国国家标准

UDC 621.3-192
:007.3
GB 7826—87
IEC 812—1985

系统可靠性分析技术 失效模式和效应分析(FMEA)程序

Analysis techniques for system reliabillty —Procedure for failure mode and effects analysis (F ME A)

1 范围

本标准阐述失效模式和效应分析（F ME A）与失效模式、效应及危害度分析（F ME C A），并就如何达到各种目的提供以下指南：

——提供完成分析所必需的程序；

——确定合适的术语、假设、危害度和失效模式；

——确定基本原则；

——提供必要的表格形式的实例。

鉴于F ME C A是F ME A分析的扩展，所有用于F ME A表示的一般定性分析，均可适用于F ME C A。

本标准等同采用国际标准IEC 812 (1985)。

2 总则

失效模式和效应分析（F ME A）以及失效模式、效应和危害度分析（F ME C A）是可靠性分析方法，这种分析致力于在实际使用中找出对系统性能有显著影响的各种失效。

一般而言，任何部件的失效或失效模式均对系统性能有不利影响。在进行系统可靠性、安全性和有效性的研究中要求作定性和定量分析，而且这两者是互为补充的。应用定量分析方法可计算或预测在特定条件下执行任务期间或长期运行中的系统性能指标。典型指标分可靠度、安全性、有效度、失效率、失效前平均时间（M T T F）等。

F ME A是以具有明确失效判据(或主要失效模式)的部件级或分装置级为基础的。从基本单元失效特征和系统功能结构出发，F ME A用来确定单元失效和系统失效之间的关系；或单元失效与系统工作不正常、操作受到抑制以及性能或完整性下降等之间的关系。为了评价次级或更高一级系统或子系统的失效，可能还需要考虑事件的时间顺序。

狭义地说，F ME A仅限于对硬件失效模式的定性分析，而不包括人为差错和软件错误，尽管实际系统中往往会遇到后两种情况。但广义地说，这些因素也被包括在内。

失效后果的严重性用危害度来描述。危害度用系统丧失能力和对人身的伤害程度来分类或划分等级，有时也按其发生的概率来表示。最好分别地确定这些概率。

F ME A一个逻辑上的扩展是考虑失效模式的危害度和失效模式发生的概率。这种确定失效模式的危害度分析，被广泛地称为F ME C A。

2.1 分析目的

F ME A和F ME C A对可靠性保证规划来说是十分重要的技术，它可以用于广泛的问题和遇到的技术系统中。为了适应一定的目的，完成F ME A和F ME C A的深度和方式可以变化。在计划论

国家标准局1987-06-03批准　　1988-01-01实施

证和技术设计阶段，进行有限的分析，而在设计和开发阶段得到进一步完善。然而，要记住，FMEA只是可靠性和维修性规划中所要求进行的各种工作和活动中的一部分。FMEA是一种归纳法，用以对系统可靠性和安全性方面完成从低分析级到高分析级的定性分析。

为了进行FMEA，需要根据系统结构作出的状态图和可靠性方框图。

对于下列各种情况需要分别作图：

——对于不同的系统失效判据；

——功能退化或降低保证的功能；

——安全性；

——替换的工作阶段。

FMEA和FMECA的目的可以包括：

a. 评价在系统的各功能级上，对每个被鉴别产品的失效模式所导致的事件顺序和效应作出评价（无论什么原因或发生在哪一个功能级）；

b. 按系统的正确功能或性能以及对于可靠性和（或）安全性方面的影响，确定每个失效模式的重要性和危害度；

c. 按失效模式的可检测性、可诊断性、可测量性、构件的可更换性、补偿和运行措施（修理、维护和后勤等）以及其他有关特性，将有关的失效模式分类；

d. 在具备数据的前提下，对失效的重要性和发生的概率进行估计。

2.2 应用

2.2.1 FMEA的适用范围

FMEA主要是用于研究部件和设备失效的一种方法，并能应用于以不同技术（电的、机械的、液压传动装置等）及其以多种技术为基础组合成的各种系统。FMEA还可用于软件和人类行为的研究。

2.2.2 FMEA在一个工程项目内的应用

使用者应该明确为了什么目的和怎样把FMEA用于自己的技术项目中。FMEA可以单独使用，也可以作为其他可靠性分析方法的一种补充和支援。对FMEA有要求，是为了了解硬件特性和推论系统或设备运行时的情况。不同工程项目对FMEA的需要情况可能会有很大的差别。

FMEA既是协助设计评审的一种技术；也是一种保证及评价方法，在系统和子系统设计的最初阶段就可加以应用。FMEA适合于各种级别的系统设计。要求对完成FMEA工作的人员进行特殊的培训，而且他们必须与系统的工程师和设计人员通力合作。随着工程的进展以及当设计有修改时，FMEA必须作及时的修正。在工程结束以前，可以用FMEA来检查工程设计，FMEA还可用作论证所设计的系统是否达到标准、规程和满足用户要求的基础。

由FMEA得到的信息，可鉴别生产和安装期间的工艺过程控制和检查试验，以及鉴定、批准、交收和启动试验的重点。同时，它还可以为诊断和维修程序提供重要的信息。

在确定产品或设计应用FMEA的范围与方式时，应当考虑需要FMEA结果的特定目的，以及FMEA与其他工程活动在时间上的相互配合。还应考虑，对不希望发生的失效模式和效应，预先设置一定程度的报警和控制措施的重要性。这就在特定级别上（系统、子系统、部件等）获得了定性的FMEA方法，从而把反复设计和研制过程联系起来。

为保证利用FMEA这种技术，在可靠性规划中应给予明确规定。

2.2.3 FMEA的用途

FMEA的具体用途和效益如下：

a. 找出各种失效，当这些失效单独发生时，就会导致不可接收或有严重的影响，并且可以确定对期望的或所要求的工作可能有严重影响的失效模式，这些影响可以包括从属失效；

b. 确定下列各项的要求：

——冗余；

——提高发生失效后的“失效—安全”概率的设计；

——进一步的减额和（或）简化设计；

c. 选择替换的材料、零件、部件或整件；

d. 鉴别严重失效的后果、设计评审和修改设计；

e. 提供所需要的逻辑模型，以估计系统在工作条件下出现异常的概率；

f. 揭示安全性受到危害及会引起产品责任问题或与各种规程要求的不一致性；

g. 确保试验大纲能够发现各种潜在的失效模式；

h. 确立预防和避免耗损失效的工作周期；

i. 提出需要进行重点质量控制、检验和制造过程控制的关键环节；

j. 通过较早发现设计中的各种缺陷而避免昂贵的设计改动；

k. 建立在试验、检测和使用期间对数据记录和监测的要求；

l. 为选择修理和维护点、机内测试设备以及适当的测试点和编写故障检修指南提供资料；

m. 促进或帮助确定试验判据、试验计划和诊断程序等。例如，性能试验、可靠性试验；

n. 找出要求作最坏情况分析的电路（参数漂移的失效模式往往要求作最坏情况分析）；

o. 协助设计故障隔离顺序、替换工作模式和重组结构；

p. 方便下列人员之间的通讯联系：

——一般工程师和专门化工程师之间；

——设备的承制方和他的供应方之间；

——系统的使用者和设计师或生产者之间；

q. 使分析者的知识和对所研究设备的特点理解更为深化；

r. 对系统设备的研究提供一种系统的和严格的方法。

2.2.4 FMEA 的局限性和缺点

FMEA 用于由部件导致整个系统失效的分析时是非常有效的。

然而，对于具有多种功能和由大量元器件组成的复杂系统，实施 FMEA 可能感到很困难和很繁琐。这是由于对来自系统而必须考虑的详细资料为数太多。这些困难还会随系统可能存在的工作模式以及修理和维护方针的考虑而增加。

另一个局限性是通常不包括人为差错的后果，人机关系的研究是一个专门问题。通常，人为差错按时间顺序在系统工作期间显现出来，对其影响的研究必须通过一定的方法，例如因果分析法进行。尽管如此，FMEA 还是能够用来识别对人为因素很敏感的部件。当环境的影响很重要时，FMEA 表现出更多的局限性。在考虑这些影响时，要求对系统的不同部件的特征和性能有非常全面的了解。

应该注意，人为误差和环境影响是构成共模或共因失效的主要原因，在 3.6.1 款中将涉及这个问题。

3 FMEA 的基本原则

3.1 术语

除了特别说明的以外，所有术语均符合 GB 3187—82《可靠性基本名词术语及定义》的规定。

3.2 基本概念

与 FMEA 有关的基本概念为：

——将系统分解为基本“单元”；

——为了完成 FMEA，需要的系统功能结构图和各种数据；

——失效模式的概念；

——危害度概念（如需要作危害度分析）。

在详述 FMEA 实施步骤之前和最终阶段，主要应说明一下 FMEA（和 FMECA）和其他定性（和定量）分析方法之间存在的联系。

3.3 定义系统功能结构

分析工作应该从有足够信息的，而且从感兴趣的最低级别(如部件、电路或组件）开始。在最低的分析级上，列出该级的每个单元可能出现的各种失效模式，以及每种失效模式对应的失效效应，无论是单独的还是顺序的，对下一个更高功能级上考虑失效效应时，上述失效效应又都被解释为一个失效模式。连续迭代就会在有关的方面产生全部需要分析的各功能级，直至系统或最高功能级上的失效效应。

重要的是确定用作分析而被分解的功能级，例如，系统可分解为子系统、可更换的最小产品或零部件（元器件）等。与之有关的还必须考虑非电气产品。当要求得到定量结果时，可选择的级别必须是对每个失效模式或差错模式能获得适当的（而且可靠的）失效率数据，或者能对这些失效率作出合理的假设。选择分解级别，要求对基本组成单元的失效模式有可靠而详尽的了解，除此之外对选择分解级建立严格的规则是不可能。

3.4 完成FMEA所需的信息

3.4.1 系统结构

要求以下信息：

——系统的不同组成单元的特征、性能、作用和功能；

——各单元之间的联系；

——冗余的级别和冗余系统的性质；

——系统在整个装备中的位置（如有可能的话）；

对所有需要分解级，直至最高级，都要求有关于功能、特征和性能的数据。

3.4.2 系统的启动、运行、控制和维修

应该说明系统在不同工作条件下的状态，以及在不同运行阶段、系统及其部件构成和位置的变化。应对系统的最低性能要求给出定义，而且就规定的性能和损害程度而论，应考虑有效性和安全性的特殊要求。

必须了解以下情况：

——每项任务的持续时间；

——周期性试验的时间间隔；

——系统在发生严重后果之前，能用于采取纠正活动的时间；

——整个装备、环境和人员情况；

——修理活动及其所需的时间，设备和（或）人员情况。

进一步要求的信息是：

——系统开机时间的操作程序；

——工作期各阶段的控制；

——维护和（或）维修；

——例行测试的程序（如果使用的话）。

3.4.3 系统的环境

应该规定系统的环境条件，包括周围环境条件和由装备中其他系统形成的局部环境。应该对系统与其辅助设备或其他系统和人机接口的相互关系等进行仔细描述。

所有这些因素在系统的设计阶段通常都不太清楚，因此需要作些假设。随着工程的进展，数据将必然会完善，FMEA应按新的信息或变化了的假设作修改。

FMEA和任何其他分析都要求一定的系统模型，即对系统的有关信息作简化。对某些失效模式的性质及其后果的严重性可作些假设。例如，有时在安全性研究中，涉及某些失效对系统的影响，可作些保守（或余量相当大的）假设。

在硬件上实施FMEA可以就效应、危害度及各种条件概率作出决策，这种决策包括鉴别软件的单元、顺序和时序。在这种情况下，必须清楚地鉴别实情，因为以后的任何变动或软件的改进，均可

以修改FMEA和由此产生的评价。FMEA的修正和有关的评价可以作为开发软件和批准更改的条件。

3.5 系统结构的表示方法

系统的结构和运行可以使用特别的图形符号来表示，方框图通常用来显示系统所有的基本功能。

在图中，方框是用表示每个功能的输出和输入的线条连接在一起的。通常，每种功能和每个输入的性质必须准确地给予描述。也可以用几种图去覆盖系统工作的不同阶段。

一般来说，用图示法，包括与解析方法紧密相关的故障树、因果图等，有助于更清楚地理解系统的结构和工作情况。然而，这就引出FMEA与这些方法之间的关系问题，这个问题见3.8条。

3.6 失效模式

失效模式是在一个系统的部件中能被观察到的一种失效现象。

作为FMEA的基本依据，对系统列出全部可能的或潜在的失效模式清单是至关重要的，元器件或设备的制造厂应参与所出售元器件或设备的失效模式的鉴别，其方式如下：

——如该元器件是新产品，则可参照具有类似功能、结构产品以及参照并已完成各种试验的其他元器件产品；

——如果是通常使用的元器件，则可参照实验室试验结果、失效报告和性能记录；

——如果是可以分解成多种基础件的复杂部件，则也可按系统对待，作定性的分析；

——从元器件工作的典型物理参数和功能可以推断潜在的失效模式。

应该对失效模式进行分类，两种常用的分类方法是：

a. 从可靠性的定义出发，导出的基本失效模式（见表1）；

b. 尽可能完整地列出各类失效模式（见表2）。

3.6.1 共模（或共因）失效（CMF）

在可靠性分析中，仅仅考虑随机独立失效是不够充分的，还可能发生共同模式（或共同原因）失效，（记为CMF）这种失效模式是由于同一原因，如设计或人为错误，在几个系统或部件上同时发生失效从而引起系统性能退化。CMF是事件相依不独立，在两个或多个部件上引起相同原因的失效（不包括由初次失效引起的二次失效）。

利用FMEA可以对CMF作定性分析。因为FMEA程序，逐一地调查每个失效模式及其原因，并识别所有定期测试和维护的程序。可以用FMEA方法去研究可能诱发的潜在CMF原因。

这些原因可分为五个主要类别：

a. 环境影响（正常的、不正常的和偶然性的）；

b. 设计缺陷；

c. 制造缺陷；

d. 组装差错；

e. 人为差错（操作期或维修期）。

依赖于这些分类对照表，来仔细地识别所有可能引入CMF的原因。

仅仅靠冗余技术不能完全解决CMF的问题，在处理共模失效时，采用几种方法的组合是有效的。如功能的多样性、不同形式的冗余、物理分隔、测试等。可以使用上述的对照表去检查每组方法的相关性和效率。严格地讨论预防CMF的预防措施已超出了FMEA的范围。

3.6.2 人为因素

在一些系统设计中允许某些人为错误，如铁路信号系统中提供的机械联锁、使用计算机时或修改数据的密码。当系统中具有预防措施时，其预防设施失效的效应将依赖于差错的类型。对于一个不会有其他故障的系统来说，还应考虑人为失误的模式以便检查预防措施的有效性，尽管列不完整，但是列出部分模式也是有益的。

3.6.3 软件差错

由于软件差错而导致的功能失常，将会引起各种效应，这些效应的危害度同时取决于硬件和软件的

设计。对这类差错或不适当的假设及其效应分析，只能在有限的范围内才可能，而且也超出了FMEA的范围。但是可以估计出软件可能的差错对有关联硬件的效应。

3.7 危害度的概念

关于任何失效状态的程度，显然要从失效发生的概率及其效应的严重性这两方面来加以叙述。危害度的概念使分析定量化并作为F ME A的补充，因为危害度基本上是一个与失效后果的严重性及其出现的概率相关的概念，所以还没有一个适用系统的危害度的通用判据。严重性本身取决于所考虑的对象在失效后所产生的后果，是否危及生命安全、造成重大破坏，或影响服务的效果等，可以按多种不同方式来定义。

由于危害度的概念需要考虑下列各种问题而对F ME A过程大有好处，这些考虑是：

——为排除一种特殊危险或增加“失效—安全”的概率，降低失效率或降低破坏性结果的风险和缩小其范围，应对产品进行更深入的分析研究；

——要求在制造期间给予特别注意的产品，要进行严格的质量控制，或对特殊操作的控制；

——在采购规范中涉及设计、性能、可靠性、安全或质量保证的特殊要求；

——转承包单位生产的验收标准，包括需要经严格试验的各种参数；

——各种特殊的程序、措施、保护装置、监控或告警系统等；

——预防偶然事件投资的最大成本效益问题。

为了定义危害度，需要一个数值尺度以便按照所考虑的判据来判断后果的严重性。附录B给出了按后果严重性分成四个等级的例子。这种等级数的实际选择是相当任意的。在本例中等级数是依据所考虑的相关判据的组合而定的，并且涉及以下因素：

——人身安全（伤、亡）；

——系统功能的丧失；

——环境影响和器材损坏；

“突变的”、“致命的”、“严重的”、“轻度的”等术语已广泛应用，但是在GB 3187—82标准中的定义可能符合，也可能不符合F ME A运用的特定情况。这些词在各种不同的研究领域中，可以专门给予定义。

3.8 F ME A和其它分析方法之间的关系

有必要讨论在一项工程中如何组合应用系统可靠性和有效性的各种不同的分析方法。

F ME A（或F ME C A）可以单独应用。归纳法经常作为其它分析方法的补充，尤其是用演绎法的推断研究。在设计阶段主要用归纳法呢还是用推断法？常常很难作出决定，因为，在思维和分析过程中，两者是结合在一起的。当在工业设备和系统中鉴别风险等级时，优先采用归纳法，因而FMEA是一种基本的分析工具。然而，在必须研究多重失效和顺序效应时，它应该由其他方法来补充。

按照工程项目的计划，一种方法可以在另一种方法之前得到发展。在设计的最初阶段，当仅仅确定了功能、系统的一般结构和子系统时，可以分别用可靠性方框图或故障树来描述系统的完好功能或失效路径。然而，在系统设计之前，适用于子系统的F ME A的归纳过程可以帮助描述系统的这些图。在这种情况下，F ME A方法不可能是确定的程序，而是一个思维过程，这种过程难于用很严格的表格形式来表达。一般说来，对于分析一个包含各种功能、大量部件，以及各部件之间有相互作用的复杂系统来说，F ME A提供基本的而不是充分的分析。

4 分析过程

系统设计和使用中的多变性和复杂性要求研制工作与可利用的信息相一致，以便高度适应具体的F ME A分析程序，下面是在F ME A研究中所用的基本步骤：

a. 定义系统及其功能和最低的工作要求；

b. 拟定功能和可靠性框图以及其他图表或数学模型，并作文字说明；

c. 确定分析的基本原则和用于完成分析的相应文件；

d. 找出失效模式、原因和效应，以及他们之间相对的重要性和顺序；

e. 找出失效的检测、隔离措施和方法；

f. 找出设计和工作中的预防措施，以防止特别不希望发生的事件；

g. 确定事件的危害度（仅适用于FMECA）；

h. 估计失效概率（仅适用于FMECA）；

i. 对考虑的多重失效的特定组合进行调查（选作）；

j. 建议。

完成FMEA程序可以不作危害度分析，若不作时，则略去步骤g和h。

4.1 定义系统及其要求

4.1.1 定义系统

一个系统的完整定义包括它的主要和次要功能、用途、预期的性能、系统的约束条件和构成失效的条件等。由于任何给定的系统都有一个或多个工作模式，并且可能处在系统工作的不同阶段，因此，系统的定义还应包括系统工作的每个模式及其持续工作期内的功能说明。

4.1.2 定义功能要求

必须定义系统及其组成单元可接收的功能和性能，以及不可接收的性能特征。功能要求应包括：工作和不工作状态下所规定的特征，所有相关的时间周期和全部环境条件。

4.1.3 定义环境要求

应该清楚地定义系统预期的工作环境、暴露环境和贮存环境，并规定在特定环境下所期望的性能要求。环境可以包括多种因素，如温度、湿度、辐射、振动、压力等。作为控制使用的系统还应进一步考虑心理、生理等环境因素对人员执行任务、系统运行等影响。

4.1.4 管理的要求

在规定系统要求时应考虑到所有适用于生产管理、使用、工作时的副产品以及有关其他影响系统设计的因素。

4.2 拟定框图

表示系统功能因素的图表，对于了解技术功能和以后的分析都是需要的。

这些图表应该展示各个单元之间的任何串联和冗余关系，以及他们之间功能上的相关性，这样就可以通过系统来追踪功能失效。对系统可能替换的不同工作方式，可能需要若干个图表，对于每一种工作模式，可以分别作出逻辑图。方框图至少应包括以下内容：

a. 将系统分解为包含功能关系的若干主要的子系统；

b. 对每个单元都适当的标明其所有的输入端、输出端和识别代码，并且每个子系统要始终用这些代码；

c. 能提供“故障—安全”措施的所有冗余，替换信号通路和其他工程特性。

4.3 建立基本准则

4.3.1 分析的级别

选择系统的分析级别，其基本准则取决于所需要的结果和设计资料的可利用性，使用的指导准则如下：

a. 根据设计构思和规定的输出要求选定最高系统级；

b. 作有效分析的最低系统级，应该是具备为建立功能定义和功能说明所必需的信息的那一级。最低系统级的选择受过去经验的影响。对于设计成熟、具有良好的可靠性、可维护性和安全记录的系统不必作详细分析。相反地对任何新设计的和可靠性历史未知的系统则需要作详细的分析，并应以较低的系统级为最低系统级别；

c. 在确定较低系统级时，被规定的或预期的维修和修理级，可能是一个有价值的依据。首先应找出完成系统维修的最低系统级（找出最小可替换单元），分析工作将在完成维修的最低系统的上一级进行，对于系统的关键性单元，分析工作可做到最低的可替换单元。

4.3.2 FMEA 文件

为完成FMEA，对于所研究的系统及其与之有关的项目设计一种具体的表格是有益的。表格的安排参照附录A的形式，通常需要填写以下内容：

a. 待分析的系统单元名称；

b. 由系统单元完成的功能；

c. 确认系统单元的识别代码；

d. 失效模式；

e. 失效原因；

f. 失效效应；

g. 失效检测方法；

h. 失效重要性的定性说明和替换的措施；

i. 备注；

在FMECA工作表格中可以增加以下内容：

j. 危害度；

k. 失效概率。

4.4 失效模式、原因和效应

一个系统的成功运行是以系统的某些关键单元的性能为条件的。系统性能评价的要点是识别关键单元。为了有效地加速识别失效模式、原因和效应的过程，可以借助于按以下几个方面预先准备的失效模式清单：

——系统的用途；

——系统包含的特殊单元；

——工作模式；

——有关的操作规范；

——时间制约；

——环境。

在FMEA中，失效模式、失效原因和失效效应的定义依赖于分析的级别。在分析的过程中，从较低级别上找出的失效效应，在较高级别上可以变成失效原因等等。

4.4.1 失效模式

表1给出了一个一般性失效模式分类。

实际上每种失效模式均可归入表1的一种或几种分类之中，但对具体的分析工作而言，表1的分类方法显得太粗，因此把表1扩展为表2。用表2所列的失效模式足以概括系统任何单元的失效。当结合使用可靠性方框图的输入、输出特性时，就可鉴别和描述所有潜在的失效模式。

4.4.2 失效原因

应鉴别并记述与各种假定的失效模式相联系的可能原因，找出每种失效模式的原因以便估计出现的概率，揭示二次效应并提出建议的修正措施。由于一种失效模式可能有一种以上的原因，必须找出并记述每种失效模式的所有相互独立的潜在原因，还需要考虑在相邻级别的失效原因。

表2还有另一种效用，即有效地确定某种失效模式和失效原因，例如，一个电源可具有被称为“运行中失效”的一般性失效模式，具体的失效模式为“无输出”(29)而失效原因为“开路（电的)”(31)。

表 1　一般性失效模式分类举例

1	提前运行
2	在规定时刻开机不能运行
3	在规定时刻关机不能停止运行
4	运行中失效

表 2　各类失效模式清单

序号	失效模式	序号	失效模式
1	结构失效（破损）	18	错误动作
2	捆结或卡死	19	不能关机
3	振动	20	不能开机
4	不能保持正常位置	21	不能切换
5	打不开	22	提前运行
6	关不上	23	滞后运行
7	误开	24	错误输入（过大）
8	误关	25	错误输入（过小）
9	内部漏泄	26	错误输出（过大）
10	外部漏泄	27	错误输出（过小）
11	超出允差（上限）	28	无输入
12	超出允差（下限）	29	无输出
13	意外运行	30	短路（电的）
14	间歇性工作	31	开路（电的）
15	漂移性工作	32	漏泄（电的）
16	错误指示	33	对于系统特性、要求和运行限
17	流动不畅		制的其它独特失效条件

4.4.3　失效效应

每种假设的失效模式对系统单元的工作、功能、状态的后果都要加以识别、评价和记录。同时还要考虑维修、人员情况和系统的目的。失效效应应集中于正在分析的方框图上，并受到考虑中的失效影响的特定单元。

一种失效效应还可能影响上一级直到最高的分析级。因此，对每个较高级别的失效效应都要进行评价。

4.4.3.1　局部效应

局部效应是指在所考虑单元上失效模式的效应，在输出端上每个假定失效的后果都与二次效应一起加以说明。确定局部效应的目的是在评价现有的替换措施或提出推荐的修正措施时提供一个判定依据。在某些场合下，除了失效模式本身之外可能没有什么局部效应。

4.4.3.2　最终效应

确定最终效应时，通过所有中间功能级的分析来评价和定义假定的失效对于最高功能级的影响。

所描述的最终效应可以是多重失效的后果（例如，由于安全装置失效导致的灾难性失效，该事件是由两方面原因引起，即安全装置失效并且安全装置所保护的主要性能又超过了允许限度时才会发生）。这些由多重失效引起的最终效应应在工作表格中指出。

4.5 失效检测方法

应说明失效模式的检测方法。应列出并分析与正在考虑的失效模式具有相同表现的其他失效模式。还应考虑工作期间，冗余单元是否需要单独的失效检测。

4.6 失效重要性的定性说明和替换措施

失效的相对重要性应记在工作表格中。在给定的系统级上，对预防或减轻失效模式效应的其他预防措施，其设计特征的识别和评价也应记录在工作表格内。这样，工作表格才能清楚地反映出设备内部功能不良的真实状态。其他的改进措施包括：

——如果一个或多个单元失效，仍能继续工作的冗余单元；

——替换的工作方式；

——监测或报警装置；

——允许有效工作或限制危害程度的任何其他手段。

在设计过程中，设备的功能单元（硬件和软件）可以进行重新组合或重新安排以改变其能力，这种情况下，在重作 **F ME A** 之前，应对有关的失效模式重新考察。

4.7 工作表格的备注栏

如果不作危害度分析，则工作表格的备注应记入与各栏记述有关的内容，有关改进设计的建议也记在这一栏并在总结中作进一步阐述。也可以记述以下内容：

——任何异常条件；

——冗余单元失效的效应；

——特别重要的设计特征；

——对扩大该行记录项目的任何说明；

——关于对顺序失效分析的其它项目。

5 危害度分析

希望能估计相关失效模式的发生概率和定量描述一种失效效应的危害度。失效模式发生概率和失效效应的危害度两者定量化，有助于采取正确的修正措施，确定修正工作的重点，以及建立起可接受和不可接受风险之间的清楚界限。按照系统的各种要求、目标和约束条件，对所考虑的每种失效效应，根据它对整个系统性能的危害度加以分类。对设备的每个项目都应确定致命失效的清单。虽然，通常有可接受的和适合于大多数设备的分类，基于以下结果，按照其严重性把它们定性地分为：

a. 造成工作人员或公众的伤亡；

b. 造成其它设备或设备本身的损坏；

c. 由于无输出或丧失功能造成的经济损失；

d. 由于设备不能完成其主要功能造成的任务失效。

附录 **B** 是基于伤亡、设备受损失和功能下降为例编制的危害度等级的例子。

危害度分类的选择要求细心和审慎地作出决定。因为象性能、费用、进度、安全和风险等这些因素关系到对系统的评价，所以必须清楚地考虑所有的相关因素。

5.1 失效模式的概率

每一种假定的失效模式发生的概率是通过使用分析的方法导出的。估计在特定工作环境下，一种特定的失效模式的发生概率，要求一个有统计意义的可靠性数据库。

直接使用上述来源的数据，可在进行 **F ME A** 的同时完成预测工作。

5.2 危害度的估计

可以利用危害度网格来进行危害度的估计。使用危害度网格时，通常用失效模式的危害度等级作

纵坐标，而以失效模式发生概率（或频率）为横坐标，见图1，适当地把频率或概率分为四类：很低、低、中等和高。在很多例子中，概率或频率并不是等间格划分的。

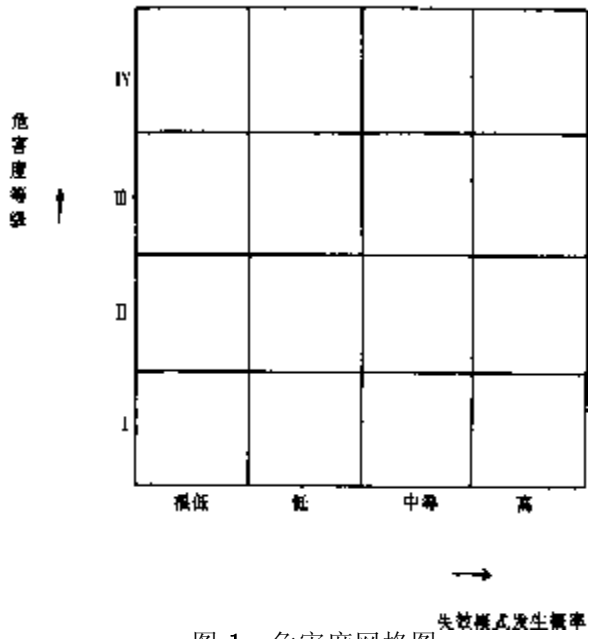


图1　危害度网格图

当已经划分失效模式的分类并给定一个概率或频率时，就可以用适当的网格图找出他们的数值，从网格图的原点向对角线方向作直线，线越长危害度越大，更需要采取修正措施。对每个危害度的分析，应按其分类确定一个概率或频率的范围。

6　分析报告

F ME A（或**F ME C A**）报告可以包括在一个更为广泛的研究文件中也可单独存在。无论哪种情况，报告应包括一个详细的分析记录和一个摘要。

摘要应包括对分析方法和分析级别、假设和基本规定的简短说明。此外应包括下列内容：

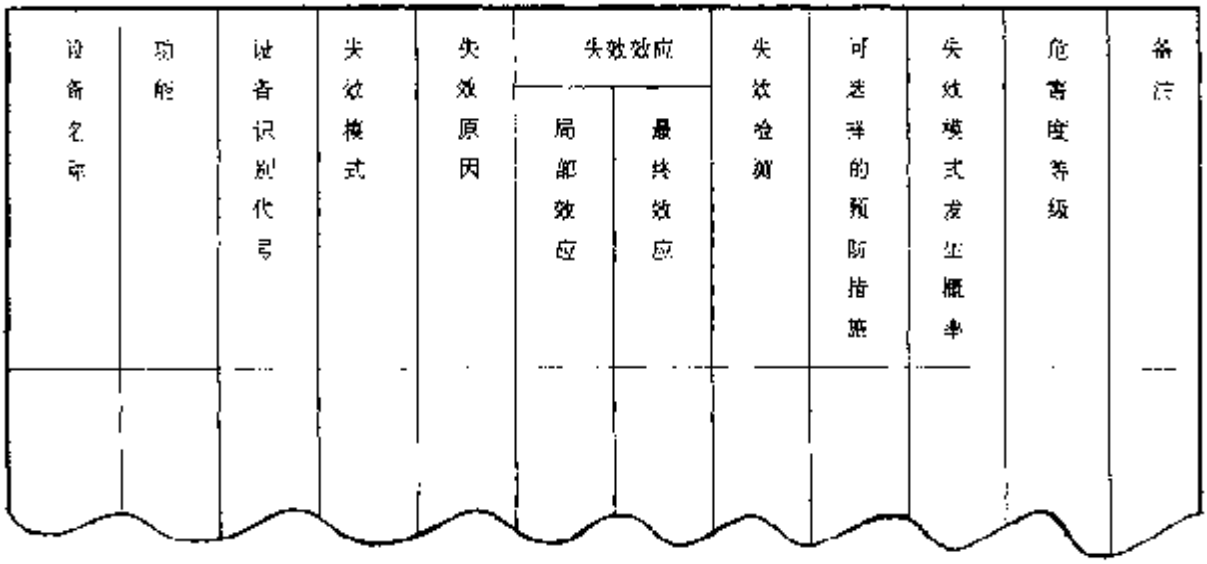
——为设计师、维修工作人员、计划员和使用者提出的建议；

——最初单独发生而又引起严重效应的失效；

——已经作为**F ME A**（或**F ME C A**）的结果被采纳的设计变更。

附 录 A
失效模式、效应及危害度分析工作表格
（参考件）

编号____分析者姓名____设计工程师姓名____日期____



附 录 B
失效效应危害程度的尺度举例
（参考件）

危害度等级	危害状态
Ⅳ	可能成为主要系统丧失功能，从而导致系统或其环境的重大损坏的潜在原因或造成人身伤亡潜在原因的任何事件
Ⅲ	可能成为主要系统丧失功能，从而导致该系统或其环境的重大损坏的潜在原因，而又几乎不危及人身安全的任何事件
Ⅱ	能造成系统功能、性能的退化而对系统或人员的生命或肢体没有可感觉的损伤的任何事件
Ⅰ	可能成为系统功能、性能退化的原因而对系统或其环境几乎无损坏，对人身安全无损害的任何事件

附加说明：
本标准由中华人民共和国电子工业部提出。
本标准由全国电工电子产品可靠性与维修性标准化技术委员会归口。
本标准主要起草人苏德清。