国防科技工业质量与可靠性专业技术丛书

危险分析与风险评价

遇 今 主编

航空工业出版社

第1章 绪 论

1.1 概述

安全性问题是随着社会生产劳动而产生，也随着生产的发展而发展，并日益受到人们的重视。在社会生产活动中，安全是指人不受到伤害（死亡或职业病）、物（设备或财产）不受到损失，环境不遭破坏。

武器装备通常用来杀伤、破坏敌方兵员和人员以及各种设施、资源财产等，但是由于其本身具有高能、毒性等物质，所以在研制、生产、使用及处置过程中也存在着威胁自身以及操作人员的安全、损坏己方设施和资源、破坏生态环境的因素。一旦发生事故，危害极大。例如，前苏联“联盟”11号飞船因返回舱中一个与外界连接的阀提前打开，造成3名宇航员死亡。俄罗斯海军北方舰队的“库尔斯克”号核潜艇于2000年8月12日在正常工作的状态下因易燃气体泄漏突然爆炸，沉入巴伦支海海底，舰艇上118名官兵全部遇难。美国“挑战者”号和“哥伦比亚”号航天飞机的两次爆炸，造成14名宇航员丧生。这些事故，不仅在经济上，而且在政治上都产生了不可挽回的损失。因此，安全问题始终是人们极为关注的大事。

在第二次世界大战后期，一些国家开始系统地研究安全性概念和安全性技术，并将安全性技术应用到武器装备的研制、生产和使用中。将安全性成为一门独立的学科则是在20世纪的50年代末。其推动力是美国在20世纪50年代及60年代早期的导弹发展计划的需要。当时液体推进剂导弹如宇宙神、雷神等导弹经常发生爆炸事故。对一些事故的调查发现，这些事故主要是由于设计缺陷、操作失误以及糟糕的管理决策所引起的。例如，1958年美国NIKE－AJAX防空导弹在阵地上爆炸，造成大量的人员伤亡、设施毁坏；60年代初弹道导弹地下井发射系统进行试验的1年半内，连续发生4次重大事故，每次损失数百万美元，还有人员伤亡。后来事故调查表明，主要的原因是装备设施本身存在重大的安全性问题，因此不得不报废已生产的装备、修改设计重新生产。在这一时期，美空军事故也频繁发生，损失了众多飞机及飞行员。此后，美国国防部、陆军和其它军种的各司令部制定并发布实施了一系列有关系统安全的指令、规范和标准。如美国空军导弹系统局于1962年7月出版了BSD62－41《空军弹道式导弹研制的系统安全性工程》。1978年美国国防部颁布了DODD5000.36《系统安全性工程和管理》，从采办政策上规定了武器装备安全性需求与政策。陆军部文件AR385－10提出了陆军的安全性大纲。美军分别颁布了美军标MIL－STD－882B《系

统安全大纲要求》（1987），美军标 MIL－STD－882C《系统安全大纲要求》（1993），美军标 MIL－STD－882D《系统安全实施标准》（2000）等。在 1990 年美国出版了 MIL－HDBK－764（MI）《陆军装备系统安全性工程设计指南》。同时美国军方委托一些大学开展研究，并形成了整套系统安全工程技术。美军方按照上述国防部指令和美军标的规定，建立了安全性保证的组织，以贯彻落实有关安全性的要求。

美国航空航天局（NASA）认识到了系统安全性的迫切需要，并将系统安全性大纲作为空间工作项目的一部分。NASA 在执行“阿波罗”空间计划时，由于全面地贯彻安全性大纲，从而保证了 1969 年“阿波罗”11 号飞船登月的成功。1971 年，虽然“阿波罗”13 号飞船在月球轨道飞行时发生了推进舱爆炸事故，但两名宇航员还是安全返回地面。由此可见，NASA 在执行安全性大纲方面是卓有成效的。

美国同时也在核、化工、冶炼、交通工业领域提出了安全性保证问题。

我国对安全问题极为重视。主要体现在劳动生产过程中劳动安全卫生制度上。我国的有关职业健康安全的法律、法规明确提出了“安全第一，预防为主”的方针。国家制定的劳动法规和职业健康安全法规中都把这一方针用法律形式固定下来，使这一方针成为职业健康安全工作的基本指导原则。在每一项生产活动中都应首先考虑安全因素，经常地查隐患、找问题、堵漏洞，自觉形成一套预防事故、保证安全的制度。对影响职业健康安全的产品，国家规定了严格的安全管理制度。1993 年我国国标《学科分类与代码》将“安全科学技术”确立为一级学科。

对于武器装备，为保证系统安全，我国在 1990 年颁发了 GJB 900—90《系统安全性通用大纲》。为指导安全性大纲的贯彻，1997 年颁发了 GJB/Z 99—97《系统安全工程手册》。

我国一些型号，目前已开始按 GJB 900 要求制定安全性大纲，开展安全性工作，例如神舟飞船工程。然而型号开展安全性工作尚缺乏经验。在武器装备研制、生产、使用过程中，无论在航天、航空、舰船、兵器等各工业领域，均发生过一些严重事故，因此必须要重视武器装备的安全性问题，开展系统安全工作。

1.2 基本概念

本节介绍与危险分析相关的几个基本概念。

1.2.1 危险

GJB 900 对危险（hazard）的定义为：可能导致事故的状态。

GB/T 28001—2001《职业健康安全管理体系　规范》对危险的定义为：可能导致伤害或疾病、财产损失、工作环境破坏或这些情况组合的根源或状态。

安全的对立面是危险，有危险的存在就有可能出现事故，对安全就有潜在的威

胁。因此研究安全性实质是研究危险。

危险源是引发不安全的因素。通常来源于：

(1) 物质或产品固有的危险特性（如能量或毒性）；

(2) 有害的环境；

(3) 产品（硬件或软件）的故障或失效；

(4) 人员行为失误（包括由心理、生理等因素所引起的行为失误）。

物质或产品本身存在的固有特性，如能量、有毒、易燃、易爆的特性，它们既有做功的本领，但也能伤害人体、物体。因此，一个系统在其预期工作条件下工作，意外释放能量、危险物质（如毒物），就可能造成事故。这种意外释放的能量、危险物质就构成了危险源，通常称它们为一般危险源。为了防止一般危险源产生事故，必须采取措施来约束、限制能量或危险物质的意外释放。

在正常情况下，系统中的能量或危险物质是受到约束或限制的，不会发生意外释放。但是，一旦这些约束或限制能量、危险物质的措施受到破坏（如故障或失效），则将发生事故。

导致能量或危险物质约束或限制措施破坏或失效的各种因素亦是危险源，通常称它们为故障危险源。故障危险源主要包括系统的故障（失效）、人的失误和环境因素。

一起事故的发生往往是两类危险源共同作用的结果。通常，一般危险源是事故发生的能量主体，决定事故后果的严重程度，故障危险源是一般危险源造成事故的必要条件，决定事故发生的可能性的大小。两类危险源相互关联、相互依存。一般危险源的存在是故障危险源发生作用的前提，故障危险源的出现是一般危险源导致事故的必要条件。

按能量释放理论，不同受害体对同一形式的能量具有不同的忍受能力。因此，可以划分出某一受害体对某一般危险源能量释放的忍受范围，而这种忍受范围是可以测量的。因此提出了忍受极限和安全忍受极限的概念。

所谓忍受极限是指大多数人能够忍受某一危险源释放的能量而不产生有害影响的极限值。

安全忍受极限是指对最敏感的人能够忍受而不产生有害影响的极限值。

例如，空气中含16%的氧时，对大多数人在这样的环境中可以生活。此即是忍受极限，而其安全忍受极限为18% ~ 19%的含氧量。不同国家的规定是不一样的。如美国OSHA则规定工作场所空气中氧含氧量至少为19.5%（忍受极限）。

对某一危险源而言，安全忍受极限，是可以接受的，它是该危险源的安全性设计的临界值。

1.2.2 风险

风险（risk）涉及的内容很多，其中包括：技术风险、进度风险、投资风险等。而本书的风险是特指技术风险中的危险风险。GJB900《系统安全性通用大纲》定义风

险为：用危险可能性和危险严重性表示发生事故的可能程度。风险又分为可接受风险和不可接受风险。

有危险的存在，就有风险，但是有些风险人们是可以接受的。例如，人类要利用核能，就有受核辐射的危险，这种危险是客观存在的。但人类可以采取各种措施使其在应用中受辐射危害风险小一些，甚至可使人绝对与之相隔离。虽然有受辐射的危险，但这种风险很小，人们可以接受。这说明人们更关心的是“风险”，而不仅仅是“危险”。因为直接与人发生关联的是“风险”。虽然客观危险性很大，但实际承担的风险很小。

随着现代管理对复杂系统分析能力的日益提高，使得对风险的预测成为可能，并且采取合适的措施可以把风险降低到某一水平。因此，可以把风险作为衡量系统安全程度的标准。这就是国际上为什么用风险来定义安全性的原因所在。

由于危险分析的重点是识别设计中存在的危险并指出其可能产生的后果，提出相应的改进措施，从而在系统中将其消除或降低其风险，并使其达到可接受水平。在工程实践中，完全从系统中将危险消除几乎是不可能的，即绝对为零的风险是没有的。例如，各种运载工具中推进剂，高压贮箱、气瓶，含有易燃、易爆，有的甚至有毒物质。这些危险源的存在是固有的，无法从设计中清除掉。因此要采取必要措施将风险降低到可接受水平。

人类的任何行为都包含着一定水平的风险，然而，人们总是希望尽可能减少风险至可忽略的程度。因此，存在一个选择可接受风险水平的问题。因为不能简单地说某一事物或行动是好还是不好。必须分析它所带来的风险是否超过了它所带来的利益，才能作出选择。

综合评价危险的状态，特别是对系统中残留危险的分析是很重要的。这些工作都需要通过风险评价来完成。进行风险评价的方法一般分为定性方法和定量方法两种（详见第 3 章）。

1.2.3 安全

GJB/Z 99—97《系统安全工程手册》对安全（safety）[①] 定义为：不发生可能造成人员伤亡、职业病、设备损坏、财产损失或环境损害的状态。

GB/T 28001—2001《职业健康安全管理体系　规范》对安全定义为：免除不可接受的损害风险的状态。

上述列举的两个对安全定义虽然描述不同，但内涵基本相同。其一是安全研究的对象是指人、物、环境不受损害；其二是安全是一种状态，而且是不发生不可接受的风险或不发生可能造成损害的一种状态。所谓不可接受的风险是指超出国家法律、法规的要求；超出社会公众普遍接受的程度；超出对产品目标需求。安全与否要对照风

① GJB900《系统安全性通用大纲》把 safety 翻译为安全性，其定义为不发生事故的能力。

险的接受程度来制定。随着时间、空间的变化，可接受的程度也会发生变化，从而使安全状态也产生变化。因此，安全是一个相对性的概念。例如，城市汽车交通事故每天都会发生，也会造成一定的人员伤亡和财产损失，这就是所谓“风险”。但相对于每天的交通总流量来说，人员伤亡和财产损失是很小的，是人们可以接受的，即从整体上说没有出现“不可接受的损害风险”，因而社会公众还认为现代的汽车运输是“安全”的。如美国每年的汽车事故为 15×10^6 次，平均每 250 次中有一人死亡，则汽车事故造成的社会死亡风险为 6×10^4 死亡/年，设美国总人口 2 亿，则汽车事故造成的个人死亡风险为 3×10^{-4} 死亡/（人·年）。因此，这一数字即为美国汽车事故的可接受风险水平，可作为评价美国汽车风险的基础。然而，这种“不可接受的损害风险”随着社会发展、技术进步会有新的变化，这就要努力采取措施以满足新的安全性要求。例如，国际上对核电站的安全性要求越来越严格。

1.2.4 事件链

从危险源的存在到最后发生事故是一个事件演变过程，是系统状态变化的过程，即从安全状态转移到不安全状态的过程。这一过程构成了一个事件链(scenario)(图 1-1)。

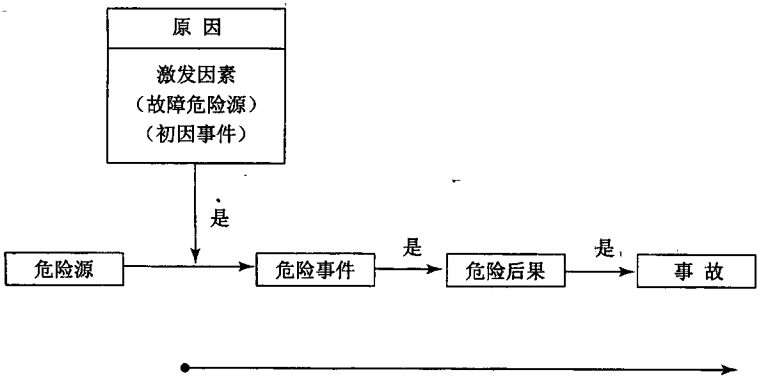

图 1-1 危险演变过程（事件链）

下面，对图 1-1 事件链作简单说明：

(1) 危险源

危险源是潜在的威胁系统安全或可能形成危害之源，是事件的主体。

(2) 激发因素（初因事件）

系统中存在危险源，只有存在某种激发因素才可能导致发生危险事件。因此激发因素是产生危险的原因（初因事件）。在一定条件下，激发因素本身也可能是危险源，即故障危险源。

(3) 危险事件（不希望事件）

危险事件反映系统功能或物理破坏的特征，这是危险演变过程中导致危险后果的

中间事件。在一定条件下，它也可能是后果。系统功能丧失或物理破坏即是危险征兆。通常这种征兆是可以观察或检测到的。根据观察或检测的结果，可以采取安全措施。应确定系统危险征兆的现象或参数，并通过系统设计（如检测装置）来实现观察或检测这种征兆。

(4) 后果及其严重性

后果是危险演变过程的结果，即危险事件对人、系统或生态环境的最后影响。

(5) 传播时间

从激发因素的发生传播到产生危险后果是一个时间过程。在这一时间内，根据观察或检测到的危险征兆信息，可以采取措施来防止严重后果的发生，保证系统安全。在危险分析中，定性的传播时间划分为：

——没有可用的时间；

——很有限的时间；

——有限的时间但很充分；

——长的可用时间。

如果在一定的传播时间内，没有时间或方法可以用来采取措施避免危险，那么这种危险就是灾难性的，即造成事故。如果可以通过采取措施及时阻止或避免危险，这时危险是可控制的。

例如，美国“阿波罗”飞船舱内采用了纯氧的设计方案，则：

危 险 源：飞船舱内的纯氧环境。

激发因素：静电火花或电气设备产生的火花。

危险事件：引燃火花附近的易燃物。

危险后果：火迅速蔓延到其它易燃物。

事　　故：宇航员伤亡。

采用纯氧设计导致宇航员伤亡的事件链如图 1－2 所示。

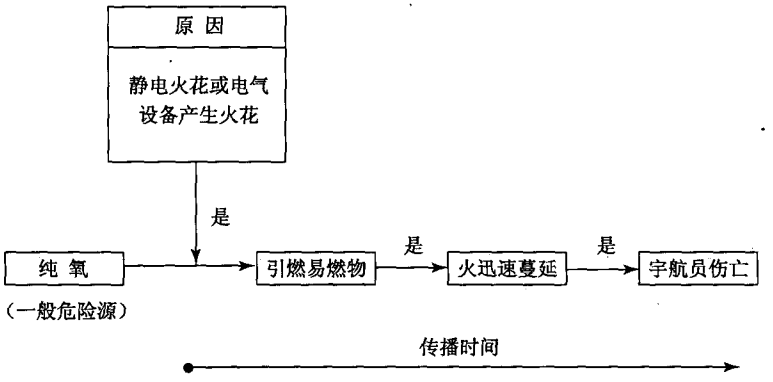

图 1－2　采用纯氧设计导致宇航员伤亡的事件链

1.2.5 危险分析

危险分析（hazard analysis）是对系统设计、使用以及环境有关的所有危险进行系统化分析，其主要内容包括：

（1）识别危险源，拟定危险源清单；

（2）对危险风险进行评价；

（3）确定安全性关键项目；

（4）对不可接受危险项目提出改进措施建议；

（5）确定残留危险项目。

因此，危险分析的实质是对危险演变过程的分析，设法阻止或减缓危险。通过危险分析来识别和评价危险，并按危害性和发生可能性来对其分类，以便在研制、生产、使用中可以消除或控制这些危险。危险分析可用来研究系统设计的不安全状态以及怎样纠正不安全状态的方法。如果危险不能消除，则通过分析可以提出最佳的控制方法和减轻或控制危险所能够产生有害影响的方法。

1.3 安全性与可靠性的关系

安全性与可靠性往往被误认为是等同的，实际上两者既有联系，又有区别。

可靠性是指在规定条件下，规定时间内系统完成其规定功能的能力。安全性则是指不可能出现导致事故的状态，而不管其规定的功能是否被完成。也就是说可靠性要求系统不失效，有能力去做什么，而安全性要求系统不会发生意外事故，不应做什么。可靠性考虑所有可能会发生的功能故障，而安全性则考虑那些能威胁安全的危险源，包括能造成事故的故障（而并非所有故障），还要考虑事前如何消除、控制系统的危险以及在意外事故发生时如何来减少损失。

就系统而言，通常可靠的系统也是安全的。系统不可靠意味着系统不能执行规定的功能，而当该功能对于保证系统安全是关键时，系统就不安全。但是在某些情况下，不可靠并不等于不安全。例如汽车在行驶中出现发动机熄火故障，就此而言对汽车内的人员不会引起伤亡事故，还是安全的。又如，我国某型运载器发射时曾经出现两台发动机自动熄火故障（可靠性问题），由于指挥员及时发出指令，停止其余发动机继续工作，火箭、卫星保住了，避免了严重后果（安全性问题），也就是说任务虽未完成但却安全。

在某些情况下，可靠性与安全性是互为矛盾的。一个典型例子就是对敏感火工品与钝感火工品的选用，前者使用可靠但不安全，后者安全但却不好用。有时为了提高可靠性，却降低了安全性，例如，在火箭的推进分系统中，为了提高可靠性采用冗余的设计方案。由于采用冗余设计，系统的密封接头增加，造成推进剂泄漏的可能性增加，因而导致着火事故的可能性也加大，安全性下降了。相反，有时为了提高安全

性，基本可靠性却降低了。例如，带有短路保护装置的电路，在电路出现短路时能保护电路（安全），但从可靠性角度，由于电路增加了短路保护装置，增加故障发生的可能性，可靠性下降了。在讨论火药点火装置设计方案时，经常会遇到装不装点火保险装置之争。其争论的实质是可靠性与安全性之间的权衡问题。

1.4 危险分析与系统安全关系

系统安全是通过安全性工作来保证的，即利用科学技术、管理的手段来识别、分析系统的危险，采取措施，把安全性设计进产品中，并得到有效的验证，将风险控制到可接受水平。系统所达到的安全程度将直接取决于管理及工程人员对其重视的程度。

系统安全工程基本实施要素，系统安全工作流程如图 1－3 所示，其概念如下。

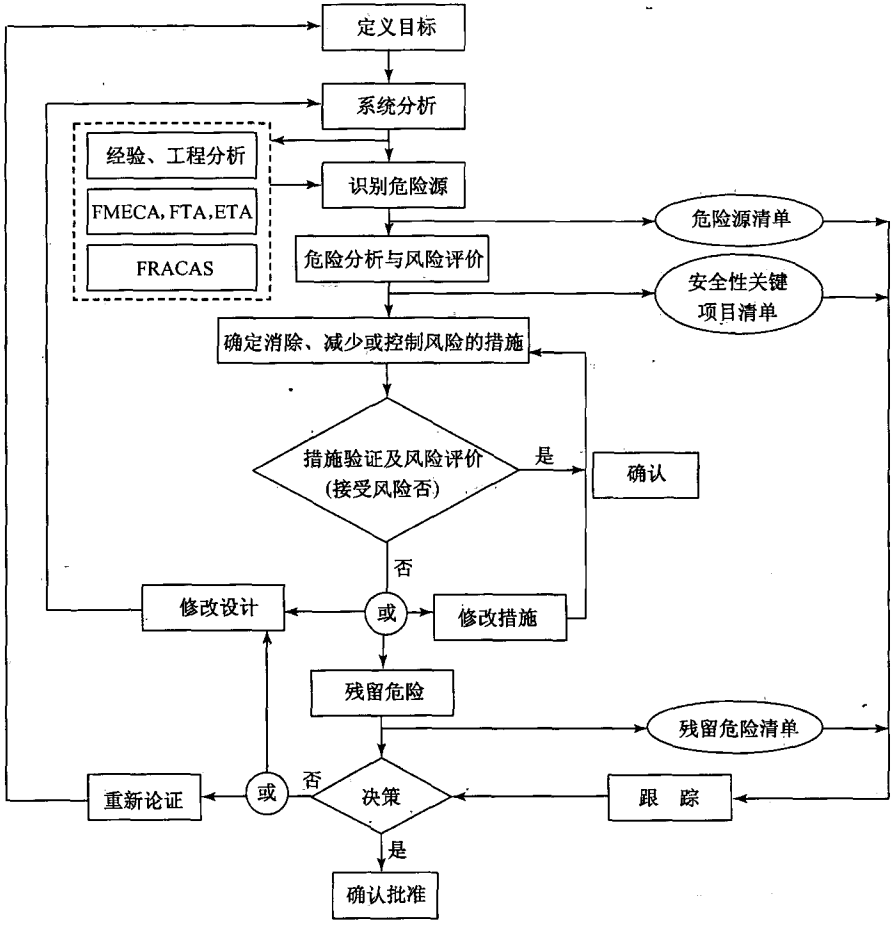

图 1－3 系统安全工作流程

(1) 定义目标

首先要确定系统安全目标或确定一个可以度量安全性的标准，以控制、评价系统设计、生产、试验、使用过程中的安全性。

(2) 系统分析

系统分析的目的在于了解系统的功能及其组成、工作过程以及使用条件。通常在完成系统分析后可确定任务剖面，任务剖面将有助于全面识别整个任务过程中对系统安全构成威胁的危险事件。

(3) 识别危险源

识别危险源是系统安全工作流程中的关键环节。如果不能识别出所有的危险源，就不能充分地控制危险，则不可能保证系统的安全。因此应全面地识别已存在的和潜在的危险源，做到一个不漏。完成该项工作可以形成危险源清单，它是安全性分析的基础。

(4) 危险分析与风险评价

危险分析与风险评价是在危险源清单基础上，分析每一危险的原因以及对系统的影响，以便使工程人员了解危险原因和危险后果之间的关系。将分析结果对照危险严重性、可能性分类准则，进行分类和风险评价，确定危险风险接受与否，并确定对哪些危险要采取安全措施，以消除或减少对系统的影响。通过这项工作可以产生一份安全性关键项目清单。

(5) 确定消除、减少或控制危险的措施

对不可接受风险的危险项目，均要采取消除、减少或控制危险的措施。首先要从设计上采取措施，要对照安全性设计准则修改设计，以求消除危险或将危险风险减少到可接受水平。

(6) 措施验证及风险评价

对确定的消除、减少或控制危险的措施的实施效果还要进一步进行验证和风险评价，以确定在采取措施后，能否将危险风险降低到可接受水平；是否会产生新的危险源。

(7) 确定残留危险

对同意保留的那些未采取控制措施，或虽然采取控制措施但又无法验证的不可接受的危险项，按残留危险处理。确定并汇总系统所有残留危险项。应将所有的残留危险形成清单，并说明保留理由。

(8) 系统安全评价与决策

系统安全取决于系统中的残留危险。通过系统安全评价，来评价系统的安全性是否满足要求。管理部门据此决策：如果满足要求，予以确认并批准；否则应修改系统方案或对指标要求重新进行论证或作出其它管理决策。

(9) 跟踪

对危险源、安全性关键项目，残留危险项目以及安全性“归零”项目进行跟踪，以支持管理决策。

上述过程结合管理上的监控，就构成了系统安全大纲的框架。由此可以看出，危险分析是系统安全工作的核心。

第 2 章　危险分析方法

要想保证系统安全，就必须首先识别系统中可能存在的危险源。有的时候，发生事故是由于设计人员未能识别和消除或控制某个危险。这是由于设计人员没有系统地分析危险的经验，只能看出直接显露的危险源，而不能识别隐蔽的危险源。

识别危险源至少应从以下几方面考虑：

（1）危险品（如推进剂、火药、火工品、有毒物品、电源和高压气源等）；

（2）系统工作时所处的环境，包括自然的、诱发的（如振动、冲击、极限温度、真空、雷电、电磁、离子辐射等）；

（3）系统功能故障或非正常工作状态；

（4）系统设计缺陷，包括机械结构件安全余量不足的项目、不相容（如材料间不相容、电磁干扰等）的项目、由潜通路而引发的不希望工作状态、接口不协调（如硬件之间、软硬件之间、软件之间、信息传递之间接口等）；

（5）关键指令和控制软件的缺陷；

（6）使用、测试、维修、保障过程中可能引发或引入的危险；

（7）误操作或违规操作；

（8）危险品贮存、搬运、运输，推进剂，易燃、易爆气体或液体泄出处理等；

（9）与安全有关的设备、安全防护装置以及其它安全保险措施；

（10）其它。

危险分析方法是系统识别危险源、分析危险原因及其影响的方法，其中包括：危险源检查单法，工程经验法和其它分析方法等。

2.1　危险源检查单法

应结合系统特点，编制危险源检查单，以识别系统设计、使用中可能存在的危险源。通常可使用以下 5 类危险源检查单。

2.1.1　典型危险源检查单

下面是航天系统典型危险源检查单的示例，这里的危险源检查单是不完全的，分析人员在识别危险源时，还要根据实际情况进行补充。

（1）系统导致的（内部的）技术危险

热动力学和流体力学：

——压力（压差、高、低、真空）；
——温度（高、低、温差）；
——材料的热性能；
——热传递（热辐射、对流）；
——液体喷射。
电学和电磁学：
——电压（高、中、低）；
——静电；
——电流（高电流、低电流）；
——磁场（诱导磁场、外部磁场）；
——电离；
——电火花。
辐射：
——光（红外线、可见光、紫外线）；
——放射性（核物质、X射线、激光）；
——明火。
化学：
——刺激物；
——酸性物质；
——窒息剂；
——有毒物质；
——腐蚀剂；
——可燃物；
——易爆物；
——易燃物；
——自燃物。
机械：
——压力（高、低、压差、真空）；
——振动；
——机械能（热能、动能、旋转能）；
——冲击能；
——机械特性（尖锐程度、粗糙程度、润滑程度、切割）；
——应力（拉伸、压缩、摩擦）；
——力（力矩、加速度）；
——脆性（脆性物质、撕裂敏感性）。

噪声。

(2) 系统导致的（内部的）生物危险

人的废物：

——呕吐物；

——汗及排泄物。

微生物：

——毒菌；

——细菌；

——病毒；

——真菌。

(3) 人员操作危险

心理危险：

——错误敏感性（决策、判断、信息处理）；

——注意力分散。

生理危险：

——生理弱点；

——生理限制；

——人员的不适（黑暗、光亮、噪声、不适的姿势）。

(4) 环境（外部）危险/空间

重力：

——零重力；

——多重力。

真空。

大气成分。

放射性污染物及污染物。

陨石及空间残骸。

温度。

辐射：

——太阳射线和强光；

——X 射线和核辐射。

(5) 环境（外部的）危险/地球

环境极限和气候：

——天气变化；

——尘，沙；

——风；

——雾，霜，潮湿，干燥；
——自然灾害；
——闪电。

2.1.2 危险能源检查单

能源从系统中释放时将威胁系统安全或造成危害的检查单。下面是航天系统危险能源检查单示例，对于要具体分析的系统，还要根据其系统的特点制定相应的危险能源检查单。

——推进剂；
——火工品；
——火炸药；
——充电电容；
——蓄电池；
——静电荷；
——簧装置；
——压力容器；
——悬挂装置；
——气体发生器；
——发电机；
——放射性能源；
——落体；
——弹射座椅；
——加热装置；
——泵，鼓风机，电扇；
——旋转机械；
——驱动装置；
——核能。

2.1.3 任务关键功能检查单

系统执行任务时，当这些关键功能发生故障或出现不正常的工作状态时，将威胁系统的安全或造成危害。下面是航天系统任务关键功能检查单示例，对于要具体分析的系统，还要根据其系统的特点制定相应的任务关键功能检查单。

——加注推进剂；
——安装火工品；
——发射前测试检查；

——宇航员进出座舱；
——由地面转为箭上或飞船上供电、供气；
——火箭点火；
——助推器分离；
——级间分离、再启动；
——逃逸；
——整流罩分离；
——第二级火箭点火；
——入轨；
——太阳能帆板展开；
——轨道定位；
——轨道修正；
——关键指令注入；
——地面测控；
——在轨宇航员操作；
——宇航员在轨活动；
——飞行中应急处理；
——离轨；
——开伞；
——着陆。

2.1.4 使用、维修和保障活动检查单

在使用、维修和保障时出现误操作、不按规程操作等将威胁系统安全或造成危害。下面是航天系统使用、保障活动检查单示例，对于要具体分析的系统，还要根据其系统的特点制定相应的使用、维修和保障活动检查单。

——焊接；
——清洁处理；
——极限温度操作；
——极限载荷操作；
——吊装，装卸，装配；
——主要部件、分系统、系统的验证试验；
——推进剂加注、运输、装卸；
——高能加压、气压或液压试验；
——核部件装卸、测试；
——武器安装、测试、试验；

——进入容器或狭窄空间；
——燃料加注。

2.1.5 危险检查单

通常在设计完成后或样机试验之前希望检查某个系统、分系统或操作、操作方法是否存在危险。正面的检查表可作为产品设计后评审危险的指导原则，也可作为设计准则使用。本书附录给出了危险检查单的示例。

2.2 工程经验法

可利用类似系统研制、使用的工程经验、安全性设计准则和有关的安全性数据，识别系统可能存在的危险源。通过总结类似系统的研制、使用经验，借鉴成功的经验和失败的教训。充分利用有关安全性数据，如有关故障的信息系统识别系统可能存在的危险源，包括硬件、软件、环境和人为失误的危险源。

2.3 其它分析方法

对于利用检查单或工程经验还不能识别出的故障危险源，可利用其它分析方法。包括：故障模式、影响及危害性分析（FMECA），故障树分析（FTA），事件树分析（ETA），危险与可运行性（HAZOP），潜在电路分析（SCA），报警时间分析、警示与报警分析和区域安全性分析等。

2.3.1 故障模式、影响及危害性分析

故障模式、影响及危险性分析（FMECA）是以故障模式为基础，以故障影响或后果为中心，根据分析层次，并通过因果关系推理、归纳进行的分析活动。通过FMECA，分析系统及其组成部分的硬件、软件的故障对系统的影响，特别是对安全性具有灾难性、严重后果影响的故障模式应引起特别重视，将其作为危险分析的故障危险源。FMECA与危险分析的接口如图2－1所示。

2.3.2 故障树分析

故障树分析（FTA）是以不希望发生的、作为系统失效判据的一个事件（顶事件）作为分析的目标，第一步去寻找所有的引起顶事件的直接原因，第二步再去寻找引起上述每一个直接原因的所有直接原因，以下同理，逐层地找下去。如果原因甲或乙发生会引起上一级事件发生，就用逻辑或（OR）门把它们和上一级事件连起来；如果原因甲或乙合在一起发生才引起上一级事件发生，就用逻辑与