第 1 章　安全关键系统概论

当你看到本书的时候，立即会产生许多问题：什么是安全关键系统？它的作用如何？又是怎样分类的？它经历了怎样的发展历程，现状如何？它研究哪些内容？所有这些问题，你可以从本章的论述中得到明确的回答。

1.1　什么是安全关键系统？

John Rushby 给关键系统(Critical System)作了如下定义：关键系统是指一旦发生故障可以导致不可接受后果的系统。不可接受的后果包括生命的死亡、财产的损失、环境的破坏或机密信息的泄露。依次称作生命关键（life critical）、财产关键(money critical)、环境关键(enviroment critical)和信息关键(information critical)等系统。

安全关键系统(Safety Critical System)采用了 ENV 50129—1999 的定义：凭借它自身可以达到为了实现所要求的安全功能必须的安全完整性等级的系统，或者说对安全承担直接责任的系统。

安全关键计算机系统（Safety Critical Computer System）——若以计算机为核心子系统构成安全关键系统的监控系统时，则把这种监控系统称为安全关键计算机系统，这是本书讨论的对象，为简单起见称为安全关键系统。

安全关键系统具体地是指空间技术、航空、铁路、公路、水路运输、核电站、石油和化工、国防和武器装备、机器人以及医疗仪器等高风险系统。为了更深入地理解安全关键系统，对它们做进一步的讨论。

空间技术或称太空技术。这里主要指的是宇宙飞船和气象、海洋、通信等卫星。它为人类探索和利用宇宙空间，为人类生产力发展和生活质量提高作出了巨大贡献，但是人类为此也付出了高昂的代价。1986 年 1 月 28 日美国“挑战者”号航天飞机升空不久发生爆炸，7 名宇航员丧生，经济损失惨重。飞机失事原因是由于固体火箭推进器的橡胶密封圈因温度太低而失效，导致火箭裂缝，火焰直向外燃箱喷射，点燃箱中 200 多万 m^3 的氢和氧而发生爆炸。另外，发射中心违规，按规定气温低于 10.5℃不能发射，但该中心却在气温 −3.3℃ 时发射，这是导致悲剧发生的根本原因。10 年后，1996 年 6 月 4 日早晨，欧洲第一枚阿丽亚娜 5 型火箭升空后 40 s 到达 3 700 m 上空发射装置开始偏离飞行轨道、随后爆炸。火箭价值 5 亿英镑。事故的主要原因，一是在设计上，没有根据阿丽亚娜 5 型火箭的特点进行‘定位软件’的重用，而是照搬阿丽亚娜 4 型火箭的“定位软件”，并用相同版本的软件装入双倍冗余的计算机中；二是在测试和合格认证中，先入为主地断定惯性制导系统没问题，而未进行惯性制导系统的闭合仿真认证。结果，恰恰就是由于照搬“定位软件”引起惯性制导系统出现问题，而酿成大祸。

化学工业。这个领域使用安全关键计算机系统的目的就是在实现化学反应过程的自动控

制中，防止火灾、爆炸、有毒物质的泄漏等对人的伤害和对环境的污染。不幸的是，灾难仍时有发生。1984 年 12 月 3 日凌晨，美国碳化物联合公司设在印度博帕尔市的一家农药厂，因管理紊乱，缺少保证安全的冷却装置，加上违规操作，误将水注入储罐，与异氰酸甲脂形成放热的反应，使温度急剧升高，压力超过正常压力的 20 倍,致使防爆膜破裂,罐内的 45t 液态的异氰酸甲脂氧化后外溢，致使熟睡中的人们受到侵害，中毒或窒息；导致 4 000 人死亡,20 万人中毒，5 万人的眼睛受到严重伤害， 19 000 人形成终身残废；无数的牲畜和农作物被毁；事故后的 5 年中，中毒者每天相继死亡 1 人；幸存者免疫力下降，不断受到各种疾病感染；受害的妇女，自然流产率比普通妇女高 4 倍。

核电站。这个领域的根本安全问题是防止放射性泄露。但是，灾难还是降临了人间。1986 年 4 月 27 日切尔诺贝利核电站发生爆炸。至少 92 000 人从周围地区撤离,25 万儿童很快转送到夏令营。在苏联、意大利、法国、德国、斯堪的那维亚等国家中,在人、动物、食品、产品、乳制品上等等检测到高等级的辐射。由此可见，灾难影响地域之广泛。切尔诺贝利城实际上已被摧毁，成了一片废墟。当时记下了 31 人死亡，然而死亡人数在不断地增加。据估算，清除污染的工作人员中近 1 万人死亡。至少 50 万人受到放射性污染，仅在 22.9 万名清除污染的工作人员中，大约有 8 500 人在 1991 年前死亡。

机器人。机器人在现代自动化生产系统中的广泛使用，极其显著地提高了生产效率和产品质量，有力地改善了有毒、有害工种工人的安全卫生条件。机器人的安全问题实际上就是要实现科幻小说家 I. Asimov 提出的“机器人三定律”：

第一定律：机器人不得伤害人类。

第二定律：机器人必须服从人类的命令，除非这命令违反了上述第一定律。

第三定律：机器人必须保护自己的生存，除非这种保护违反了上述第一、第二定律。

实际上，国外曾多次发生工业机器人打死工人的悲剧。 1981 年 7 月 4 日,日本的川崎重工业明石工厂，一工人被机器人挟住胸部而压死。由于工厂是无人化的，被挟住的工人没人发现，当偶然过路的其他工人发现时已经倒地死亡。 1984 年 11 月，在日本发生了机器人从上方袭击作业者的事故，击破安全帽的塑料薄膜，继而穿透被害人的头骸骨而致死，灾害现场惨不忍睹。据统计,1987 年至 1990 年末日本已有 11 人被机器人打死。由此可见，机器人的安全性是至关重要的。

民用航空。这个领域广泛实现了航空器驾驶舱自动化和空中交通管理的自动化。高新技术的应用在给民航带来经济效益的同时也带来了安全效益，有效地避免了飞机失控、相撞等传统飞机经常发生的事故。至今，已成了最安全的交通工具。但是，即使驾驶自动化水平很高的第三代喷气客机有时也难逃机毁人亡的噩运。由于自动驾驶仪成功地取代了许多原先由人来完成的工作，在某些方面甚至比人做的更好，因此某些驾驶员产生了过分依赖自动驾驶的思想，驾驶员忽略了对飞机的监控。例如， 1992 年某航空公司的一架 B737-300 飞机，在临近机场下降改平飞时，自动油门发生故障，右发一直保持慢车位，造成飞机长时间推力不对称，结果，自动驾驶仪横侧操纵能力饱和，致使飞机坡度不断增加。当飞行员发现情况异常时，为时已晚。实际上，这起事故可以由驾驶员及时断开自动油门改为手动操纵油门就能避免。另外，空中交通管理的失误是造成机毁人亡的另一个重要原因。 2002 年 7 月 1 日德国时间晚 11 时 43 分,一架俄罗斯图-154 客机与敦豪国际快运公司的一架波音-757 货机，在德国南部靠近瑞士的博登湖附近 12km 的高空相撞坠毁，机上 71 人全部罹难。当时负责对两架飞机进行飞行

监控的是瑞士空中导航公司，事发时，所属瑞士苏黎世空管中心的飞机防撞自动报警系统正因保养检修而关闭，而值班的两名空管人员又有一人离岗休息。事后，对图-154客机黑匣子数据的解读表明，这架飞机的驾驶员收到改变飞行高度的时间，距撞机前只有短短 44 s ,实际上至少应在 1.5 min 前就开始降低飞行高度。 7月 13 日瑞士空中导航公司值班导航员表示，他愿意承担对 7月 1 日两架飞机高空相撞事故的责任。很显然，这完全是由地面导航员指挥失灵造成的重大事故。

20世纪 70年代令航空界震惊的是，事故原因因素分类统计表明，“人为因素”已经上升为现代航空事故的主要原因因素，占到 80%～90%，这中间又以人犯错误最为常见（包括过分依赖驾驶自动化）。

铁路运输。铁路运输是一个庞大而复杂的交通系统，它的高风险表现在列车碰撞和脱轨事故直接造成人员伤亡和财产损失的严重性上。此外，与其它交通系统相比，超越或交错的自由度极低，在短时间设定迂回通路又不容易，这就会使局部事故造成大范围的运输障碍，进一步加剧了经济损失。为此，铁路运输部门围绕防止列车碰撞和脱轨，在整个铁路运输系统的各个环节上采取了一系列安全措施，取得了很好的效益。

尽管如此，列车碰撞和脱轨事故仍难以避免。美国联邦铁路管理局的事故报告表明，从 1985年到 1987 年共发生了 171 起事故，其中碰撞和脱轨事故只占了 14 起，但死亡人数却在总死亡人数 23人中占了 20 人，受伤人数在总受伤人数 831 人中占了 446人。其中，1987 年 12月发生在马里兰州 Chase 的重大恶性事故,是由 3 台货物机车组成的列车未能观察信号而通过道岔从支线进入正线，与一列时速为 169km 的客运列车撞击，造成 16 人死亡，176 人受伤。因此，高度重视避免列车的碰撞是非常必要的。

随着生产的发展和人们生活水平的提高，客运量在不断增长，高速铁路运输的重要性已经日益为人们所认识，它是解决大通道旅客快速输送问题的最有效途径，已经成为世界各国和我国铁路必然的发展趋势。但是，它在带来效益的同时也带来更大的风险，这就必然去探索一套全新的安全理论和措施，降低碰撞和脱轨的风险。

公路交通。随着汽车工业的发达并且进入千家万户，更由于高速公路的大量修建，在给人们的出行带来便利的同时也加大了风险。为此，每年将 1/5 左右的汽车生产费用投放到车载电子和计算机系统上，在地面上还配置了高速公路交通管理电子信息系统。

公路交通的主要危险是汽车的碰撞和汽车的失事。为了避免碰撞，在发现前方有障碍物时，通常采取停车或绕行的措施。然而，停车或绕行如发生在铁路平交道口、隧道或视野不好的拐弯处，往往却成了引发碰撞事故的原因。因此，对汽车的安全状态，被时时刻刻变化的环境条件所左右。根据德国 1995 年发表的统计结果,25%的公路交通事故是尾追碰撞。尤其在恶劣的气候条件下，甚至会发生多米诺骨牌式的尾部碰撞。为了解决这个问题，发达国家都在研究制造汽车的避撞自动控制系统，这是进一步降低高速公路风险的重要方向。

军事防御系统。在科罗拉多州夏延山下人工开凿的一个巨大山洞群里，由庞大复杂的指挥、控制、通信系统构成的北美防空联合司令部早期警报指挥中心，时时刻刻等待着原苏联人即将进攻的信号。由于一个价值仅 45美分的极小的计算机集成电路芯片失效，曾在 1979 年 11月 9 日和 1980 年 6月 3 日两次发生虚假的原苏联人进攻的警报。第一次， 1 000枚具有击中原苏联本土目标能力的民兵式洲际弹道导弹处于初级戒备状态； 10架战术战斗机起飞。第二次，战略空军司令部值班军官命令全部待命的 B-52机组人员登机并启动引擎。战争处于一

触即发状态。由此看来，军事防御系统的虚假信息造成多么大的危险。但是各子系统的彼此独立，其间配合又是松散的，很快就证明警报是假的，很快解除了警报，恢复了安宁。

武器装备。武器装备的最大特点就是从它诞生之日起就存在着巨大的危险（称固有危险),稍有疏漏,其后果不堪设想。俄罗斯‘库尔斯克’号潜艇,2000 年 8 月 12 日在巴伦支海上参加军事演习出事沉没，艇上 118 名海军官兵全部遇难。它震惊了全世界！ 2002 年 7 月 26 日，俄罗斯总检察院总检查长乌斯季诺夫宣布，调查结果显示，2000 年 8 月 12 日,在巴伦支海参加军事演习的“库尔斯克”号核潜艇上人员在准备发射鱼雷时，由于易燃物质过氧化氢从鱼雷上一个微小的裂缝泄露，鱼雷装置发生爆炸。爆炸引起潜艇隔舱内温度急剧上升至 2 000℃到 3 000 ℃的高温，在第一次爆炸发生 2 s 后，潜艇内存放的其它鱼雷又发生了第二次大爆炸，它摧毁了 80％的船体。幸存的艇员全部逃到了第 9 舱，他们在那里为生存奋斗了 8 h。这个震惊世界的大悲剧，罪魁祸首却是鱼雷上的一个微小裂缝。因此，武器装备比其它安全关键系统，在安全性上有着更高的要求。

医疗系统。由于“人命关天”，医疗系统本来就是一个高风险部门。由于以计算机为核心的各种医疗仪器和设备研制成功并投入临床使用，使许多人力所不能及的医疗行为变得很容易实现。减轻了病人的痛苦，提高了医疗水平；对推动医疗系统的现代化发挥了巨大作用。但也必须清醒地认识到，这些医疗仪器的风险也在加大，哪怕一个很小的失误也会带来不可挽回的严重后果。

Therac-25 是基于计算机的电子加速器放射治疗系统，已经安装了 11 台,美国 5 台,加拿大 6 台。根据调查，由于操作人员的差错，对仪器的安全校验粗心大意以及取消了硬件安全联锁等原因,从 1985 年到 1987 年共发生了 6 次过剂量放射线照射，最大的达到正常值的 100 多倍,最后造成 4 人死亡的严重后果。

通过对各类安全关键系统的讨论，使我们认识到：

1. 安全关键系统就是指各种高风险系统，它具有很高的酿灾潜势。这种潜势一旦失控而释放，就会造成巨大灾难。

2. 安全关键系统是一个规模庞大、各子系统间配合紧密、相互作用极其复杂的系统，并总是与时俱进、采用当代高新技术，有的本身就是属于高新技术范畴。

3. 安全关键系统的绝大多数是在非常恶劣、危险的环境下运行，有些环境因素人类也难以驾驭。

4. 由于 1、2、3 原因，即使一个很小的设计失误、一个小零件的故障、或使用人员的一个小差错，都会导致安全关键系统发生意想不到的多重故障，最终酿成事故。

5. 安全关键系统一旦酿成事故，就会造成大量的人员伤亡、巨额财产损失以及大范围环境破坏的惨重灾难。人类必须严肃、认真、科学地对待安全关键系统。

6. 科学技术的进步在为人类造福的同时，也带给人类新的更大的威胁。正是人类与高风险的不断斗争中,不仅推动了‘软’安全科学理论和技术的发展,诸如安全管理学、安全系统学、安全法学、安全经济学；而且也有力地促进了“硬”安全科学理论和技术的形成和发展，其中以计算机为核心的安全关键系统理论就是一例，也是本书关注的重点。

7.“硬”安全科学理论和技术的形成和发展，改变了人类对安全关键系统认识的被动局面，可以这个科学体系为指针，指导我们更好地分析每一种安全关键系统的特殊性，主动地全面地采用更为合适的安全技术，研制出更加安全可靠的安全关键系统；指导我们更主动更深入地探

索安全关键系统的规律，不断地充实它、发展它。

应该看到，用安全科学理论指导安全关键系统的实践，并将安全技术合理地用于安全关键系统中，已获得重大经济效益和社会效益。使许多安全关键系统能够正常运行，并在系统发生故障时发挥了保证安全的重大作用。1992 年我国用长征 2 号捆绑式运载火箭发射“澳星”就是令人信服的实例。3 月 22 日第一次发射，4 个助推器点火过程中，突然出现故障，当即采取控制措施，终止了发射，保全了“澳星”和火箭。一场重大的损失和灾祸避免了，但给人们留下了深思。在火箭发射出现故障的刹那间，发射系统实现了自动关机，这一成功的安全系统控制事例，说明中国科技工作者用安全系统理论与火箭发射安全工程相结合，结出了成功的硕果。终止发射后，科技人员能够在短时间内查明故障原因，又一次显示出他们已把握住系统中各安全因素及其相互作用的内在规律。

1.2 安全关键系统的结构

1.2.1 系统与环境

安全关键系统的结构如图 1.1 所示，它由控制器、输入接口、输出接口、人机接口、传感器和转换器（也称为执行机构）等部分组成。其中，控制器、输入接口、输出接口等组成了广义控制器，人机接口、传感器和转换器组成了环境接口，而各类系统使用人员、受控对象或物理过程等组成了环境。广义控制器按一定的方式通过环境接口与环境进行相互作用。

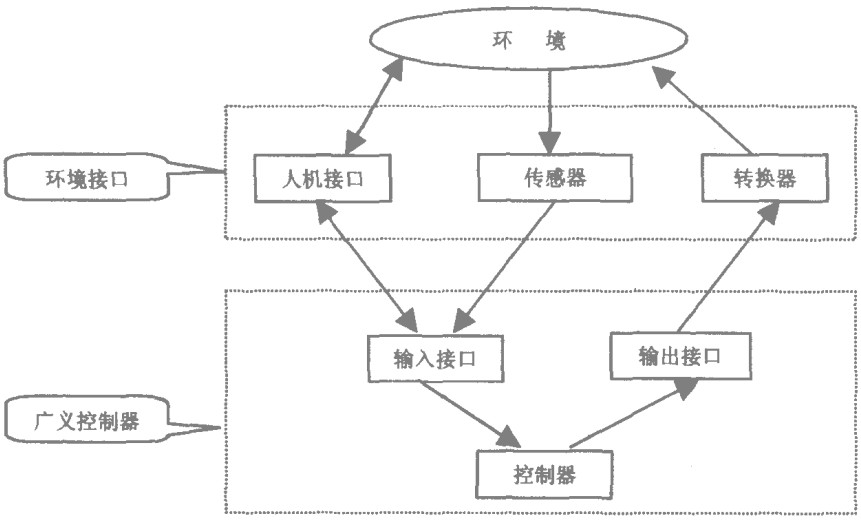

图 1.1 一个典型的实时系统结构

在图 1.1 中，操作员、维护员、管理员等各类系统使用人员通过人机接口与广义控制器进行交互，该接口至少提供显示和记录功能；受控对象或物理过程通过传感器将自身的状态信息以某种电信号方式输入给控制器；输入接口把人所发出的指令、输入电信号等转换为控制器能够接受的形式；控制器完成规划、计算和控制等任务；转换器接受控制器所发出的命令，改变受控设备的状态；输出接口把控制器的命令转换为转换器能够识别的信号。

安全关键系统的物理结构可以是集中式的，也可以是分布式的。控制器可以是一个由继电装置所构成的电气控制器、或者是一个由电子元器件所构成的电子控制器，或者是一个由计

算机所构成的可编程控制器，而计算机则既可以是一个简单的微处理机系统，或者是一个复杂的多处理机系统，或者是一个地理上分布的分布式计算机系统。

1.2.2 层次模型

图 1.1 中所示的控制器多为可编程控制器。为便于研究这类实时计算机系统的体系结构，我们先来介绍计算机体系结构的层次结构模型。一个计算机系统可以从多个层次对其特征进行描述，这些层次包括：

（1）应用虚拟机器级；
（2）高级语言虚拟机器级；
（3）汇编语言虚拟机器级；
（4）操作系统虚拟机器级；
（5）传统机器级；
（6）微程序机器级。

在此，我们在上述计算机体系结构的层次结构的应用虚拟机层次之上增加了一个“环境接口”层次，因为实时系统的设计需要深刻地了解和掌握环境中所包含的物理过程、外部设备、操作人员等的工作特性。扩充后的实时系统体系结构的层次结构模型如图 1.2 所示。

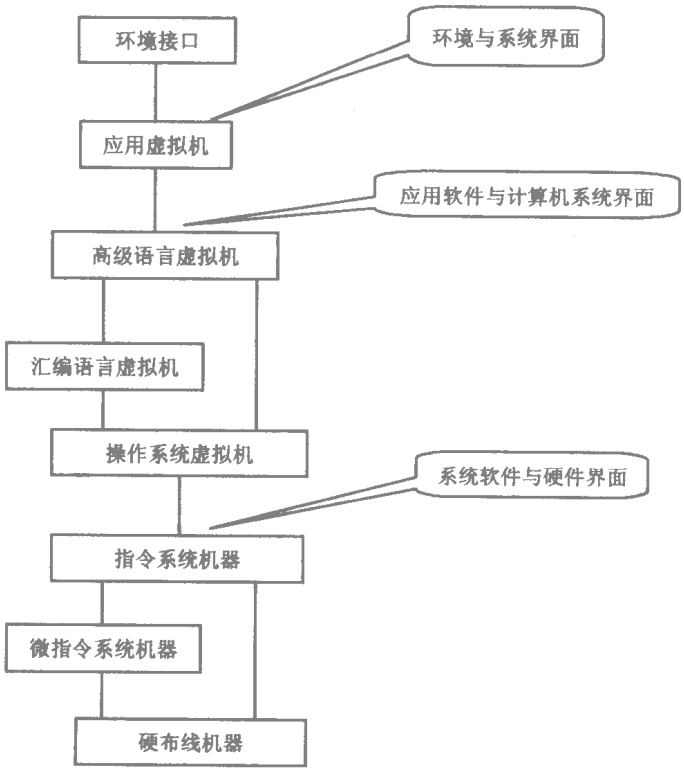

图 1.2 实时计算机体系结构的层次结构

环境接口是环境与系统交互作用的接口，它主要由传感器、转换器和人机接口等组成，是一个典型的数字与模拟的混合系统。从计算机应用人员视角看，应用虚拟机是面向某种、某一类或者某几类专门应用的机器，如飞行控制计算机、列车运行控制计算机等。它是以应用软件形式展现在应用人员面前的。这样，在环境接口与应用虚拟机之间就形成了一个“环境与系统

界面”，明确该界面的特性和内容是应用软件开发人员和负责环境接口设计与实现的电气工程师工作的基础。

该层次模型中的其它虚拟机与计算机体系结构层次模型中的相应虚拟机是相同的，但引入了一个新的界面，即“应用软件与计算机系统界面”。对这一界面的深刻理解，将有利于计算机系统开发人员构造出高性能的计算机系统（由系统软件与硬件构成）。

环境与系统的界面、应用软件与计算机系统的界面在计算机体系结构中不是作为重点来强调的，而在操作系统虚拟机与指令系统机器（也称为传统机器）之间所形成的系统软件与硬件的界面（也称为软件与硬件的界面）才是计算机体系结构设计所研究的重点。但是，对于实时系统体系结构设计而言，重点是上述三个界面的划分及其上下层内容的确定，这称为界面的定义。

1.3 安全关键计算机系统与其它学科的联系

安全关键计算机系统理论和技术涉及到许多其它学科的知识、理论和技术，其中主要包括实时系统、可信(dependable)系统、系统安全工程和信息安全工程等多种学科。

1.3.1 实时系统

从1.1节对安全关键系统的讨论中，可以看到时间因素的重要性。阿丽亚娜4型火箭定位软件的运行时间为45 s,而阿丽亚娜5型火箭定位软件的运行时间为60 s。但阿丽亚娜5型火箭的水平速度可比4型快5倍，这样就造成了升空后还在进行定位控制，以致产生出一个错误的，很高的水平偏离值，并最终导致爆炸。这是没有正确确定定位软件运行时间带来的严重后果。在1.1节讨论的公路交通事故，提到德国1995年的调查结果:25%的事故是尾追碰撞。同时也指出，如果司机的反应时间降到半秒，这类事故的一大半就可以避免。由此看来，安全关键系统应是一个实时系统。

那么什么是实时系统？

实时系统是计算机的一种应用模式，它的基本特征是实时运行方式。在德国工业标准DIN44300的9.2.11条款中有这样的定义：实时运行是计算机的一种运行方式，其程序是持久可用的。它接收来自外部的输入数据，并能在预定的时间内获得计算结果。根据不同的应用，由外部进入计算机的数据，可以是随机分散的，也可以是事先确定的。

从计算机外部来看，实时系统的正确性不仅取决于输出的结果，而且还取决于产生输出结果的时间。从计算机内部来看，实时程序的正确性不仅依赖指令执行的逻辑顺序而且还与执行的时间有关。正确的定时不完全取决于计算机的处理速度，而更主要的取决于环境。总之，实时系统是一个必须满足时间约束的系统，既使在超过规定的时限得到正确的结果，这个系统也是失败的。

根据违反时间约束的后果，实时系统可以分为两种基本类型：强实时系统（又称硬实时系统）(Hard real time systems)和弱实时系统(又称软实时系统)(Soft real time systems)。

强实时系统是必须满足时间约束以避免灾难性后果的实时系统，或者说，时间的正确性是关键的、重要的实时系统。例如，城市中运行的汽车，司机必须不停地观察周围环境，诸如街道、交通信号灯、其它交通工具、行人、动物等等,对可能出现的情况必须及时作出反应,在允许

的最后期限采取措施，否则就会发生碰撞事故。

弱实时系统是一个如不满足时间约束不会造成灾难性后果的实时系统，或者说时间的正确性是重要的，但不是关键的。例如，在飞机订票系统中，支持此系统的计算机首先不能妨碍客户的订票请求，必须在客户能接受的时间内作出答复。如果此时计算机出了故障，这就意味着丢失了一名乘客或带来不良影响，但不会造成灾难性后果。

总之，对弱实时系统来说，它对环境反应时间的滞后，其后果只是增加代价而不会带来灾难性后果；而强实时系统对环境反应时限的超出是不可容忍的，所付出的代价是极其巨大的，后果是极其惨重的。

安全关键计算机系统就是强实时系统，通常又称为安全关键实时系统。由此可以看出，讨论安全关键系统的实时性，对实现安全关键系统的安全性具有非常重要的意义。

那么，对安全关键系统有哪些实时要求？

1. 及时性

及时性用时限(deadline)表示，这是对实时系统的最基本的要求。系统对事件发生的响应、主要数据的获取、数据的处理以及最终给出结果必须在规定的时限内完成。

一个实时任务 Ji 可以用图 1.3 所示的参数表示它的时间特性。

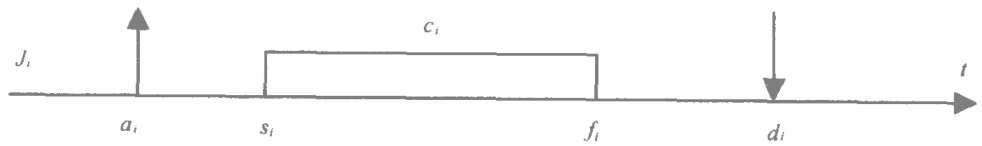

图 1.3 时间约束参数

到达时间(Arrival time)a_i：又称请求时间(request time)或释放时间(release time)，它是一个任务变成准备执行的时间。

起动时间(Start time)s_i：它是一个任务开始执行的时间。

计算时间(Computation time)c_i：它是处理器执行无中断的任务所必须的时间。

终止时间(Finishing time)f_i：它是一个任务终止它的执行的时间。

时限 d_i：它是一个任务必须在此之前完成的时间，以避免对系统的损害。

滞后(Lateness)L_i：$L_i=f_i-d_i$ 它表示一个任务的完成相对于时限 d_i 的延迟，如果一个任务在时限 d_i 之前完成，L_i 是负值。

超越时间(Exceeding time)E_i：$E_i=\max(0,L_i)$，它是一个任务在时限 d_i 以后停止活动的时间。

松弛时间(Slack time)X_i：$X_i=d_i-a_i - c_i$，它是为了一个任务在它的时限内完成，它的活动可以延迟的最大时间。

如果 c_i 在它的时限之后结束可能引起系统的灾难性后果，那么这个任务就是强实时任务。如果 c_i 错过它的时限只能减少系统的特性，但不危及正确的行为，那么这个任务就是弱实时任务。

同时性(Simultancity)：一般来说，一个实时系统常常有多个输入源，且在时间上是重叠的，这就要求系统具有并行处理能力，以便能在同一时限内对多个输入源作相应处理。此时的及时性称为同时性。

安全关键系统就是要在最坏的情况下能够保证在时限内完成每一个强实时任务。任何一

个任务时限是根据应用和根据实时系统的环境来确定的。

2. 可预测性(predictability)

可预测性是指在设计时就可以预见实时系统的行为和能够满足的所有时限，这些行为和时限是确定的而不是随机的。

这就是说，尽管系统的外部事件是随机的，但实时系统作出的反应必须是精确的、可规划的，因而是可预测的。仅当实时系统的行为在时间和关于外部事件的反应上成为可精确预估的情况下，才能达到实时系统的时限要求，只有在实时系统的行为和时限是完全可以预先确定的前提下，才有可能对安全关键系统的应用实行“安全许可证”制度。由此可以看出，可预测性对实时系统（尤其是强实时系统）是多么重要。

总之，由于安全关键（计算机）系统就是一个强实时系统，因此它就需要实时系统时间约束分析方法和实现时间约束的各种技术的支持。

1.3.2 可信性(Dependability)

从 1.1 节对安全关键系统的讨论中，可以看出产品质量对保障系统的安全性是多么重要。那么什么是产品质量呢？

根据 GB/T6583-ISO8402 的定义，“产品质量是反映实体满足规定和潜在需要能力的特性之总和。”在合同环境或法规环境下，“需要”是给定的。而在其它环境中，“潜在需要”应予标识和确定。这里的“需要”包括以下内容 性能,实用性,可信性,安全性,环境要求,经济性和美学。这是一个全新的质量观，其中最突出的是对可信性给予了极大重视。

可信性作为集合性术语，首先由法国学者 J. C. Laprie 于 1985 年引入的：可信性是计算机系统的这样一种性质，使得它所提供的服务有足够理由认为是可信赖的。他为构建可信的计算机系统提供了一个概念框架和明确的开发模式。 1994 年版的 ISO-9000 质量管理和质量保障标准系列把可信性作为质量的一个重要内容， ISO 和 IEC 联合发布了可信性管理及可信性要素的标准。那么什么是可信性呢？

可信性是一个非定量的集合性术语，它用来表示可用性及其影响因素：可靠性，维修性，维修保障性。它仅用于量化条款中的一般描述。它的定量指标是分别通过可用性、可靠性、维修性、保障性的定量指标来表示的。

可靠性(reliability) 是产品在规定的条件下和规定的时间内，完成规定功能的能力，它的概率度量也称可靠度 $R(t)$。

维修性(maintainability) 是产品在规定的条件下和规定的时间内，按规定的方法进行维修时，保持或恢复到规定状态的能力，维修性的概率度量也称维修度 $M(t)$。

可用性(availality) 是产品在任一随机时刻需要和开始执行任务时，处于可工作或可使用状态的程度。可用性的概率度量 $A(t)$又称“可用度”。产品的“能工作时间”(up time)是产品处于能完成规定功能状态的时间；产品的“不能工作时间”(down time) 是产品处于不能完成规定功能状态的时间。不能工作时间 T_N包括直接维修时间 T_M，由于保障资源补给或管理原因未能及时对产品进行维修所延迟的时间叫“延误时间”(delay time)T_D：

$$T_N = T_M + T_D \tag{1.1}$$

设产品在较长时间内，累计能工作时间为 T_U，累计不能工作时间为 T_N，则使用可用性 A_O为

$$A_O = T_U/(T_U + T_N) \tag{1.2}$$

在理想情况下，T_N 中的 $T_D=0$，此时为固有可用性 A_i

$$A_i = T_U/(T_U + T_M) \tag{1.3}$$

显然，可用性取决于可靠性、维修性及维修保障性。

可信性是构成产品效能并影响其寿命周期费用的重要因素，也是重要的技术指标。它更是实现安全性的基本的先决条件。

然而，产品或系统的可信性要受到自身的故障、差错、失效等负面因素的损伤。根据国际标准 IEC—61508—4 并参考了 J. C. Laprie 的文章，这些概念的意义可表示如下：

故障(fault)——是指可以引起功能单元完成所要求功能的能力降低或丧失的异常状态。简言之，故障就是功能单元的缺陷。这种异常状态或缺陷可以是硬件的物理缺陷，也可以是硬件或软件设计中的人为差错。

差错(error)——是指计算、观察、测量值或状态与真实值、规定值或理论的正确值或状态之间的不一致。或者说差错是在特定环境下故障的暴露，使组成系统的功能单元的输出偏离商定的需求规范。

失效(failure)——是指功能单元完成所要求功能的能力的终止。

总之，故障是功能单元内部的缺陷，它是产生差错的原因，而差错是故障在信息层上的体现，又是引发系统失效的原因。

为了达到所要求的可信性指标，必须针对上述负面因素实行可信性工程：

可靠性工程(reliability engineering)

产品或系统的可靠性主要是通过防止或降低故障发生的可能性，或一旦发生，消除或降低其不良影响的技术达到的，主要包括故障防止、故障排除、故障容许和故障预报等技术。

维修性工程(maintainability engineering)

为达到产品或系统的维修性要求而进行的一套设计、研制、生产或试验工作叫维修性工程。目的是使产品或系统易于维护和修复。

维修保障工程(maintenance engineering)

在产品或系统的安装、运行及维修阶段，需要维修保障，它需要资源和指南，以规定的维修方针、程序、工具、试验设备、文件、需要支持这方针的其它设施、维修人员的培训大纲等为基础。

可测试性工程(testability engineering)

产品或系统的可靠性及维修性特性都受到用于监视、检测、定位故障的机内、机外设施及产品特性蜕化的影响。在可信性规范中，阐述测试性需求的那部分内容，应当指导这些设计活动。

总之，由于安全关键系统必须是一个高可信系统，因此，它就需要可信性分析、评价方法和可信性工程的支持。

1.3.3 安全工程

从 1.1 节对安全关键系统的讨论中，可以看出造成系统事故的根本因素是由于组成系统的各种物质都存在着危险性，一旦条件具备它就会突变为事故。安全工程学的基本任务就是识别（预测）、评价和控制危险，从而达到优化安全性的目的，那么什么是危险、什么是安全呢？

人类在最原始的生存活动中，经常遇到雷电、洪水、猛兽的伤害和攀登、奔袭中的伤残。当代人对安全的认识最直观、印象最深刻的也是意外死亡和伤残。人类经过漫长的历史和无数

伤害和致残，才逐步形成了“事故”这个概念。由此可知，对安全的认识，首先从认识事故开始，没有事故，就无所谓安全。因此，安全科学研究的特殊矛盾就是安全与事故（灾祸）的矛盾。但是，人类在长期的实践中也认识到，事故之所以发生，是由于客观世界存在造成事故的一种现实的或潜在的条件，或者说存在引发事故的可能性，人们把这种‘条件’或‘可能性’抽象为‘危险”概念，并清楚地意识到，只要预知危险进而控制危险，就能避免事故的发生，达到保障安全的目的。事故发生以后的分析，也就是找出导致该事故的现实条件，以便更好地指导今后对危险的预测和控制，有效实现“安全第一，预防为主”的方针。正因为如此，把安全科学研究的主要矛盾也可表述为安全和危险的矛盾更切合实际。为了便于掌握安全科学的基础知识，以利于安全关键计算机系统的研究，必须首先搞清危险和安全这两个最基本的概念。

1. 危险(hazard)

该词中的‘危’应当理解为事故、灾害，而其中的‘险’应当理解为造成事故、灾害的可能性。

IEC 61508-4 国际标准把它定义为‘危害的潜在根源”。这里的‘危害’则被定义为“人身伤害或者由于财产或环境的破坏而直接或间接地造成人的健康的损害”。

危险状态(hazardous situation）是指人、财产或环境暴露在危险中的情况。例如人登高或下梯子。

危险事件(hazardous event）是指导致危害的危险状态。例如人在梯子上失足导致跌落，这实际上就是事故。

2. 风险(risk)

IEC 61508－4 国际标准把风险定义为：危害发生的概率和危害严重性的组成。

事实上，危险在一定条件下突变为事故，所造成的后果受两个因素的影响：一是发生事故的概率，另一个是发生事故造成后果的严重程度。如果事故发生的概率很小，即使后果十分严重，风险也不会很大；反之，若事故发生概率很大，虽然每次后果不严重，但风险也可能很大。为了比较危险性，采用风险作为衡量标准，其表达式为

$$R\text{（风险）} = S\text{（严重性）} \times P\text{（频度）} \tag{1.4}$$

严重性。表示发生一次事故造成的损失数值，包括直接损失和间接损失。直接损失包括人身伤亡所支出的费用(医疗、丧葬、抚恤费、补助和救济费、歇工工资)、善后处理费(处理事故的开销、现场抢救与清理费、事故罚款与赔偿费)、设备财产损失价值(固定资产、流动资产损失价值)。间接损失包括：停产、减产损失价值，处理环境污染的费用，补充新职工的培训费，工作损失的价值及其它损失。

频度。表示在一定的时间内或生产周期内事故发生的次数。

3. 安全(safe)

(1)安全

安全这个词，在希腊文中的意思就是‘完整”，而在梵语中的意思是‘没有受伤’或‘完整”，在拉丁文中又有“卫生”(salvus）之意。一般用通俗的话来说，就是人们在生活和生产过程中，生命得到保证，身体免于伤害。安全的定义有多种，有人定义为“不发生导致死伤、职业病、设备或财产损失的状态”。

(2)安全性(safety)

安全性是衡量维持安全能力的度量。

Leveson N. G 在 1986 年发表的题为‘software safety-why, What and How?’的论文中把

安全性定义为“在任何环境中免除风险程度的度量”。

IEC 61508 国际标准明确地把安全性定义为“免除不可接受的风险（freedom from unacceptable risk）。”从这个定义可以看出：

（1）风险不仅是度量危险的指标，也是用来度量安全的指标；

（2）安全不是绝对的，只要风险降低到可以接受的程度，就认为是安全的；

（3）安全的本质含义就是要免除不可接受的风险。

总之，安全工程学就是要分析安全关键系统的危险，进而进行风险评价，采取各种安全措施，将安全关键系统的风险降低到可以接受的程度。

.3.4 信息安全

根据 1.1 节的讨论，安全关键系统可以概括为两大类：第一类称生命安全关键系统，它的主要保护对象是人，在英语中用 Safety 表示这种系统的安全性；第二类是信息安全关键系统，它的主要保护对象是信息(或数据),在英语中用 Security 表示这种系统的安全性。两个英语词条都译成汉语的“安全”，但两个英语词条的含义却有着严格的区别。

Safety 所指的安全性主要是针对系统自身的故障、外部环境的影响以及人的失误等无意行为的威胁，保护人的生命不引起死亡或伤害，不导致财产的损失和环境的破坏。生命安全关键系统的失效造成的危害具有立即性和直接性。在整个系统的生存周期，运用安全工程的、管理的原理、准则和技术，在运行的有效性、时间以及费用的约束下，通过分析、设计及管理过程来识别、评价和控制危险，从而优化安全性。

Security 所指的安全性主要针对人的蓄意行为对信息（或数据）的威胁，保护信息不被泄露、篡改。信息的安全性首先是信息的保密性，其次是信息的完整性，最后是拒绝服务。信息关键系统的失效所产生的危害不具有立即性、直接性，它只是增大产生其它危害的能力和可能性。信息安全性的实现主要采用信息防护技术，诸如加密、访问控制和鉴别。

Security 所指的安全性有两个重要指标：

（1）信息的保密性，是指不发生未经授权的泄露信息的能力。

（2）信息的完整性，是指不发生错误地更改信息的能力。对 Safety 所指的安全性来说，信息的完整性比信息的保密性更为重要。

随着科学技术的发展，这两个领域正在相互交叉、融合。尤其是开放式信息网络在生命安全关键计算机系统的应用，加速了相互交叉、融合的进程。这主要反映在以下几个方面：

（1）威胁。在生命安全关键计算机系统也要考虑人的蓄意行为的破坏威胁；信息安全关键计算机系统也要考虑人的无意行为和系统自身故障、外部环境影响的威胁。

（2）需求。对一个安全关键系统既有 Safety 的安全需求,又有 Security 的安全需求。针对这种情况,D. P. Eames 和 J. Moffett 提出 Safety 和 Security 需求的集成方案。

（3）技术。信息安全系统采用 Safety 安全技术，全面提高信息的保密性和完整性， Marc Farley 等著的《网络安全与数据完整性指南》就是最好的例证。另一方面，也采用 Security 安全技术提高 Safety 的安全性。例如,D. F. C. Brewer 提出采用‘基准监督器概念’和‘数据策略模型”等数据安全技术;N. G. Leveson 根据信息安全核（Security Kernel）提出了 Safety 安全核概念;D. E. Denning 提出了用数据库数据的安全性支持 Safety 安全性的建议。

总之，由开放式信息网构成的安全关键计算机系统离不开信息安全技术的支持。

1.4 安全关键系统的分类

在 1.1 节中，实际上是根据不同的高风险部门，对安全关键系统已进行了分类。由于部门的不同，系统的危险性也各有其特点，采取的安全措施也各有所侧重。这些已在 1.1 节中讨论了，此处不再重复。

由于不同的高风险部门，其被控对象也不同，当然反映被控对象特征的物理量也不同，据此可将安全关键系统分成两大类：

(1) 数字系统。被控对象只有开关量需要监控。整个系统主要由开关器件和数字器件所组成。计算机对输入的开关量只进行逻辑运算处理，处理结果的输出仍然是开关量。这类系统的典型代表是铁路信号控制系统。该系统的直接控制对象是道岔、信号机，道岔只有定位和反位两种状态，信号机也主要只有禁止和容许两种显示。轨道电路也只有空闲和被列车占用两种状态，计算机进行的处理是实现道岔、信号机、轨道电路之间联锁关系的逻辑运算。

(2) 混合系统(Hybrid System)。被控对象既有开关量，也有随时间连续变化的物理量。整个系统有数字器件又有模拟器件。计算机对输入量的处理包括逻辑函数运算又有连续函数的运算。处理结果的输出有开关量又有模拟量。这类系统包括智能汽车、机器人、飞行器和空中交通的控制系统，化工厂过程控制系统等。混合系统已形成一个独立的研究领域。

1.5 安全关键系统的回顾

通过前几节的讨论，安全关键系统从应用上看涉及许多高风险部门，从理论上看又与许多学科密切相联。现在我们仅就几个主要问题作一简要的回顾，以利对安全关键系统的更深入的探索。

1.5.1 安全系统对故障安全概念的影响

对于“什么样的系统是安全的”这一问题的认识，人们有一个逐步发展的过程，它直接影响了安全系统的体系结构、组成和实现技术的发展。我们以安全系统的定义的进化历程来说明这一影响。

定义 1-5-1 一个系统，当其内部发生任何故障时，该系统能够给出一个预定的输出值，这样的系统就称为故障—安全系统。

在该定义中，所谓的预定输出值指的是能够控制设备于安全侧的输出值。如指挥交通的信号灯，禁上通行是安全侧（显示红灯），而准许通行是危险侧（显示绿灯）。某一设备安全侧与危险侧的划分决定于该设备的动作的可能后果，对信号灯，显示绿灯，则可能带来撞车的后果；显示红灯，就避免了这一严重后果。一般认为，危险后果指的是人员伤亡或巨大财产损失。对安全系统中的设备，一般均能找到安全侧和危险侧。

根据这一安全系统的定义，要求使用故障一安全元器件来构成系统，且某个元器件因故障而产生的安全侧输出能导致整个系统产生安全侧输出。基于电气元器件的安全系统的典型实例是铁路的电气集中设备，它是用安全型继电器来构成的，该继电器属于故障一安全器件。

当出现了采用电子元器件的安全系统后，人们又提出了如下有关安全系统的定义。

定义 1-5-2 若任意一个系统产生故障时，能够继续维持正常工作时的输出值，或者产生预定的输出值，则称该系统是故障安全的。

该定义与前一个定义的不同之处是认为系统在产生故障的情况下，若能继续保持正常工作的外部特性，那也算是安全的。导致这一修订的原因有：

（1）对数字器件，难以区分哪个值是危险的或者是安全的，因为其内部故障所导致的器件的输出值是随机的；

（2）电子电路的内部故障并不总能反映到其输出端的异常，这对模拟电路和数字电路都是适用的。这样，从输出端看，该内部故障被电路本身屏蔽了。

根据这一定义，安全系统可以用通用电子元器件来构造，但电路所实现的功能必须满足某些特性，例如，对于逻辑系统，要求它所实现的函数必须是单调的或者是混合单调的。当然，安全电子系统也可以用专用故障安全电子元器件来构造。因此，提出上述定义的意义是很大的：

（1）允许采用通用元器件来构造安全系统，这就可以充分利用通用技术的好处，如低成本、高性能等；

（2）为冗余技术在安全系统中的应用提供了理论依据，因为采用冗余技术可以大大提高产生故障的系统仍继续提供正确输出值的可能性。

在上述两种定义中，一般认为系统只需保证当发生一个故障时使系统的输出仍然正确或者为某个预定值，并不考虑系统内部连续产生或同时产生两个以上故障的情况。这种考虑在基于电气元器件的安全系统中是符合实际情况的。但对于基于电子元器件的安全系统，一般还要求尽量把单个故障及时地检测出来。这一要求可以用广义或扩展故障安全概念来描述。

Nicolaidis、Noraz 和 Courtois 等人建立了基于传统故障安全系统理论和并发差错检测系统理论的广义故障安全系统理论。该理论建立了完全故障安全、强故障安全等概念；提出了用自校验的基本功能电路与强故障安全的转换器互连，以构成强故障安全电路的结构；实现了基于内建自测试技术的 MOS VLSI 强故障安全接口电路（如表决器）。本章作者也曾提出过用于描述具有部分自测试能力的故障安全电路特性的扩展故障安全概念。上述概念、原理和方法主要是建立在将并发差错检测系统理论引入到故障安全系统理论的思想上的，采用的基本技术是差错检测码、多模冗余方法和特殊信号编码方法（如频率编码）等。

所谓系统是广义故障安全的，指的是系统在正常工作条件（只需正常输入矢量）下，其内部故障在最坏情况下将使系统的原始输出固定于某个预定的输出子集中，且该故障无需任何外加激励（专门用于检测故障的输入矢量）就能被自动检测。广义故障安全系统理论定义了两个重要的系统特性：完全故障安全和强故障安全。

定义 1-5-3 一个系统对于它所考虑的单故障集是完全故障安全的，若它对于该故障集是故障安全的和自测试的。

上述定义所描述的系统将实现完全故障安全目标。该目标指的是当第一个故障被检测到以前，系统所产生的所有错误输出均位于安全合法输出集中。如果系统无任何内部故障检测机制，那么，为了实现该目标，要求系统必须具有如下特性。

定义 1-5-4 一个系统相对于它所考虑的单故障集是强故障安全的，若（1）系统相对于该故障集是完全故障安全的，或者（2）系统相对于该故障集是故障安全的，而且如果系统产生该故障集中的另一个新故障，情形（1）或（2）仍成立。

也可以用扩展故障安全概念来描述对内部故障具有自测试能力的故障安全系统。

定义 1-5-5 一个系统对它所考虑的单故障集是扩展故障安全的，若它对任意一个故障，对任意合法输入，其输出要么是正确的，要么是安全的或者是非法的。

上述定义在形式上与传统故障安全系统的定义很相似，只是允许出现故障后的系统的输出既可以是安全合法输出，也可以是非法输出，这在广义故障安全系统的相关定义中并未明确指出。对系统的输出集作这样的划分后，若采用并发差错检测技术，扩展故障安全系统的差错就可能通过差错校验器来检测。

在广义故障安全系统理论和扩展故障安全概念的基础上，本章介绍如下一组以扩展故障安全为核心的概念，下述概念与广义故障安全系统理论中的相应概念是类似的。

定义 1-5-6 一个系统对于它所考虑的单故障集是完全扩展故障安全的，若它对于该故障集是扩展故障安全和自测试的。

该定义所描述的系统将实现完全扩展故障安全目标。该目标指的是在给定的故障假设下，系统所产生的所有错误输出将或者位于安全合法输出集中，或者位于非法输出集中。

上述故障安全系统概念的发展使得系统可以通过进一步引入自测试技术来提高系统的可维修性和可用性。

传统的故障安全电路在出现内部故障时可能产生错误的输出（但属于安全值），由于电路不具有故障自测试能力，因此，累积的故障最终将致使电路失去故障安全特性。广义故障安全电路虽然具有故障自测试能力，能有效地提高电路的 MTTF 值,但当检测出故障后,要定位故障，则是不行的。若还要将发生永久性故障的模块替换掉，则就有更大的困难。传统的办法是系统先中断正常的服务，然后采用在线或离线方式进行故障诊断，即施加所有的测试码，查故障字典，确定故障模块，再确定故障的性质，最后，将根据故障的性质进行相应的修理。但是，如果使故障安全电路具有并发差错定位能力，即在正常工作条件（只需正常输入矢量）下，无需任何外加激励（用于定位故障的输入矢量）就能自动定位其内部的故障，那么，故障诊断过程就可大大加快。这样反过来又会有利于进一步提高系统的可维护性。基于这一思路，把故障安全技术与并发差错定位技术结合起来，将使电路在内部产生故障时，其功能输出保持正确或安全，同时还给出相应的差错（故障）定位信息。

电路的并发差错定位基于对电路的划分，即把电路划分成多个模块。

定义 1-5-7 一个电路对它所考虑的单故障集是健壮故障安全的，若对某个模块所考虑的单故障集中的任意一个故障，对任意合法输入，电路的输出要么是正确的，要么是安全的或者属于对应于该模块发生故障时所产生的输出集中的一个值。

定义 1-5-8 一个电路对应于所考虑的单故障集是完全健壮故障安全的，当且仅当它对应于该故障集是健壮故障安全和故障定位的。

定义 1-5-9 一个电路对应于所考虑的单故障集是故障定位的，当且仅当它对于该故障集中的任意一个故障，至少存在一个合法输入，能够使电路给出对应于该模块发生故障时所产生的输出集中的一个值。

上述定义表明，在某个模块发生故障的情况下，合法输入必将导致电路或者生成正确合法输出，或者生成安全合法输出，或者给出对应于该模块的差错定位子集中的输出，且至少存在一个合法输入，它能够使电路给出差错定位输出。这意味着完全健壮故障安全电路中的所有故障是可定位的。完全健壮故障安全电路将实现完全健壮故障安全目标，该目标指的是在给定的故障假设下，当完全健壮故障安全电路由于故障而产生第一个安全合法输出或者非法输

出时，该输出矢量总是可以区分的，即不同模块中的故障将导致电路产生属于不同的故障定位输出集中的输出。

从传统的故障安全观点出发，容易导致提出绝对安全的要求，即要求系统在故障发生后，只能处于“正常工作状态”或“安全故障状态”,绝对不能处于“危险故障状态”,否则,系统将可能产生危险输出值。前面所提到的有关安全系统的定义均充分体现了这一要求。正如任何系统均无法提供完全的绝对可靠性一样，任何系统实际上也难以提供完全的绝对安全性。长期以来，大量的事实也证明了这一点。因此，应该允许一个符合实际情况的安全系统在故障发生后,可能处于“正常工作”“安全故障”或者“危险故障”三个状态之一,但是系统处于危险故障状态的可能性必须尽量降低至一个用户可以接受的程度。这也是安全性的概率评估所要求的。

1.5.2 安全元件和器件技术的影响

1. 电路技术的发展促使新型安全器件的产生

以传统铁路运输控制系统为例，所使用的基本电气元器件是安全型继电器，它一般是靠衔铁的重力和接点补簧片的反弹力来保证吸合接点断开的。选用不易熔化的材料作接点，以保证不熔焊和不粘连。它的励磁吸合接点具有如下特性：

(1) 继电器失磁时，即断开而不受残磁的影响；

(2) 继电器失磁时，即断开而不受机械的影响；

(3) 在接点断开瞬间，即使产生有电火花或电弧也不致粘连。

对于基于电子电路的安全系统，构造故障安全系统的根本条件是要有实现基本单调函数的故障安全基本逻辑电路。它是一种只出现 0 错误而不出现 1 错误，或者只出现 1 错误而不出现 0 错误的不对称失效元件，前者被称为 0 型不对称失效元件，后者被称为 1 型不对称失效元件。不对称失效电子元件的主要缺点是工作速度还不够高，大规模集成困难，而且有些器件和通用逻辑器件的兼容性差。

由于 NOR 和 NAND 运算是功能完备的，故可以用其中之一构成任何二值函数。如果一个基本单调减小函数的安全侧输出值应为 1，那末，实现任意函数的逻辑电路可以用 0 型故障安全 NOR 门(或 NAND 门)及 1 型故障安全 NOR 门(或 NAND 门)来实现。

可以证明，并发差错检测电路是扩展故障安全电路的一类，而并发差错定位电路是健壮故障安全电路的一类。从 20 世纪 60 年代末开始，并发差错检测系统的设计和实现得到了重视和发展，并取得了许多成果，它们可分为自校验系统和专用器件两类。

(1) 自校验系统

包括自校验微处理机（如 Intel8080、MC68000,以及 MIL-STD-1750A 的自校验版本)、自校验算术逻辑单元（ALU）和自校验微程序控制器等。

(2) 专用器件

包括各种具有自校验特性的校验器，如强分离码的双轨码校验器等。

上述器件在早期一般是在门级实现的，近年来，有的是用 MOS 工艺实现的。而且，在 VLSI 电路技术条件下，产生了许多新型的自校验器件，它们所依据的电路实现模型和故障模型也更为合理。

2. 容错电子器件使安全系统的结构和组成的实现得以保证

前已述及，构成安全系统的方法经历了一个不断完善的过程，期间也出现了多种系统结构，这些结构均要求不同的组成和实现技术，但基础是要有容错电子器件。例如，只有有了故障安全的接口电路，才能使基于多模冗余和安全接口互联的安全系统结构得以实现，这类系统结构在国内外铁路运输控制系统中得到了广泛应用。

3. 商业通用(COTS)设备的使用促进了安全系统传统设计方法的改变

在电气元器件广泛应用的时代，安全系统主要采用专用器件来构造，但进入电子元器件应用的时代后，这一情况有所改变。例如，在铁路信号设备的生产中，出于经济因素的考虑。不要求为其生产专用的安全型电子元器件，也不要求制订特殊的测试标准。然而，这一时期在如军事这样的其它关键领域，却仍然实施特殊的标准和技术要求。自从计算机进入关键领域后，情况开始出现了根本性质的变化。电子元器件、计算机硬件和软件的质量越来越高，性能越来越好，COTS 软硬件产品在各种关键系统的实验样机和产品中所占的比例逐步提高。其中的原由除了降低成本外，还有这样一来可以获得高性能价格比的产品。由于备件充分，系统的维修性也得到了提高，而可选用的 COTS 产品型号多，种类齐全，这既缩短了开发周期，也缩短了产品的上市时间，又可以降低开发费用，降低了集成与测试的费用，同时还可充分利用新技术所带来的种种好处，使得产品的技术含量增高，从而极大地提高了产品在市场上的竞争力。

然而，COTS 产品在容错方面一般存在许多弱点，而且还不容易改进，因为 COTS 产品供应商一般不会为了一个需求量有限的关键领域来修改设计、增加开销或降低性能。此外，对 COTS 产品的修改也会致使其与原来的测试设备不一致，而为了消除这种不一致就需要再对测试设备进行修改，这样一来就大大降低了原本因采用 COTS 产品而获得的商业利润。相对于 COTS 硬件产品而言，COTS 软件产品本身、基于 COTS 软构件的开发技术，以及软件体系结构还有一些问题未得到满意的解决。

因此，安全系统的设计人员在选择 COTS 产品时必须按一定的原则进行。最重要的是这些产品的安全性必须得到充分的验证，以保证它们符合系统的整体安全性的要求。设计人员可以在较高的系统层次上采用多种容错技术来构造一个高可靠、高安全的应用系统，而无须从最底层（如芯片级，或者是板级）开始设计。比如设计单位可以从生产安全产品的供应商处购买一套安全 COTS 硬件和系统软件，然后根据应用要求开发应用软件；也可以从一般产品供应商处购买主要的 COTS 硬件和系统软件，然后从安全产品供应商处购买或者自行开发特殊的安全配件（如故障安全接口、安全管理软件），再自行开发应用软件。

1.5.3 应用对安全系统的影响

应用是推动工程科学技术向前发展的重要因素。各种应用对安全系统会提出各种要求，其中有些要求是相同的，如高性能价格比、高可靠性、高安全性、高可维修性等，而有些要求是不同的，如具体功能、系统的规模等。应用领域所提出的高安全性要求推动了安全系统的发展，安全系统的发展经历了如下变化。

1. 系统功能从简单发展到复杂

以铁路信号控制系统为例，站间闭塞从一开始把两个车站之间的线路划分为一个闭塞区间，采用半自动闭塞设备控制，发展到把站间线路划分为多个闭塞区间，采用自动闭塞设备控制，功能复杂了，而且，设备元器件也从采用安全型继电器，过渡到采用分立式电子元器件，然后发展为采用集成电路和微处理机。区间闭塞设备的主要控制对象是闭塞区间的轨道电路和