中华人民共和国国家军用标准

FL　　GJB 900－90

系统安全性通用大纲

General program for system safety

1990－10－31 发布　　1991－04－01 实施

国防科学技术工业委员会　批准

目　　次

1　主题内容与适用范围 …… (1)
2　引用标准 …… (1)
3　术语 …… (1)
4　一般要求 …… (2)
5　工作项目说明 …… (5)
5.1　管理与控制 …… (5)
5.2　设计与分析 …… (8)
5.3　验证与评价 …… (12)
5.4　安全性培训 …… (14)
5.5　软件系统安全性 …… (15)
附录A　《系统安全性通用大纲应用指南》(参考件) …… (21)
A1　主题内容 …… (21)
A2　确定安全性要求 …… (21)
A3　风险评价 …… (21)
A4　工作项目的选择 …… (23)
A5　剪裁工作项目指南 …… (23)
A5.1　管理与控制 …… (23)
A5.2　设计与分析 …… (27)
A5.3　验证与评价 …… (29)
A5.4　安全性培训 …… (31)
A5.5　软件系统安全性 …… (31)

中华人民共和国国家军用标准

系统安全性通用大纲

GJB 900—90

General program for system safety

1 主题内容与适用范围

1.1 主题内容

本标准规定了军用系统安全性的一般要求和管理与控制、设计与分析、验证与评价、培训、软件系统安全性等方面的工作项目，作为订购方提出具体系统的安全性要求和承制方制定具体系统的安全性大纲(以下简称安全性大纲)的基本依据。

1.2 适用范围

本标准主要适用于军用系统寿命周期内的研制和生产阶段，也适用于其它阶段的有关安全性的工作。

2 引用标准

GJB451	可靠性维修性术语
GJB368	装备维修性通用规范
GJB450	装备研制与生产的可靠性通用大纲
GJB437	军用软件质量保证
GJB439	军用软件开发规范
GB2894	安全标志

3 术语

3.1 事故

mishap

造成人员伤亡、职业病、设备损坏或财产损失的一个或一系列意外事件。

3.2 安全性

Safety

不发生事故的能力

3.3 危险

hazard

可能导致事故的状态。

国防科学技术工业委员会 1990—10—31 发布　　1991—04—01 实施

3.4 危险可能性

hazardous probabitity

产生某一种危险的事件发生的总的可能性。

3.5 危险严重性

hazard Sevearity

对某种危险可能引起的事故可信的最严重程度的估计。

3.6 风险

risk

用危险可能性和危险严重性表示的发生事故的可能程度。

4 一般要求

安全性大纲是包括系统安全性管理和系统安全性工程工作的文件，其目的是在系统寿命周期内用及时、经济有效的方法满足系统安全性要求，提高其使用效能。

订购方应根据本标准的规定向承制方提出安全性大纲要求，包括安全性定性、定量要求，试验项目要求和基本的工作项目要求。这些要求经双方商定后，应纳入合同的有关文件中。

承制方应根据签订合同或任务书要求，按本标准的规定制订和实施安全性大纲。

在制定安全性大纲时，必须一开始就与质量管理、可靠性、维修性、人素工程、健康保障等工作综合权衡与协调，以达到最佳的费用效益。

4.1 剪裁要求

安全性大纲应满足本章中的一般要求，包括所指定的5章中的工作项目。

a. 本标准规定的工作项目及其要点应按国家有关文件的规定，根据产品的类型、重要程度、经费与进度要求剪裁确定，并在军用系统的招标书、合同或任务书中明确规定。

b. 本标准规定的"由订购方规定的细节"是订购方应提出的有关要求，也是剪裁工作项目要点的根据之一，其中注有"*"标记的是必须确定的事项。

c. 附录A是剪裁本标准工作项目及有关条款的指南。

4.2 安全性大纲目标与要求

安全性大纲应保证：

a. 及时地、经济地进行符合任务要求的安全性设计；

b. 在系统寿命周期内识别、评价和消除系统中的危险或将其风险减少到订购方可接受的水平；

c. 考虑并应用以往的安全性资料，包括其它系统的经验、教训；

d. 在采用新的设计方法、材料、生产工艺和试验技术时，寻求最小风险；

e. 将消除危险或将风险减少到订购方可接受水平所采取的措施记录成文；

f. 在系统的论证、研制和订购中及时并充分地考虑安全性特性，以尽量减少在使用中为改善安全性进行的改装；

g. 在设计、技术状态或任务要求更改时，使风险保持在订购方可接受的水平；

h. 考虑与系统有关的所有危险器材的安全性并便于退役处理。

4.3 安全性信息要求

安全性信息包括系统论证、研制、生产、使用和退役等各阶段中有关的安全性数据、资料以及文件等。其要求如下：

a. 应建立安全性信息闭环系统，并制定信息必要的管理要求和程序。

b. 记录重要的安全性信息，作为历史资料或修改有关设计手册和规范的参考资料。

c. 订购方应按安全性大纲要求向承制方提供有关的安全性信息。

d. 承制方应按信息管理要求或后勤保障信息要求，对研制生产、试验和使用过程中所得到的安全性信息进行收集、传递、分析、处理、反馈和归档。

e. 承制方向订购方提供的安全性大纲各项工作项目的资料的内容、格式及交付日程，应由订购方规定。

4.4 系统安全性设计要求

应在考查系统设计所用的有关标准、规范、条例、设计手册和其它设计指南资料后，确定系统安全性设计要求。一般的系统安全性设计要求如下：

a. 通过设计(包括器材选择和代用)消除已判定的危险或减少有关的风险。当必须使用有潜在危险的器材时，应选择在系统寿命周期内风险最小者；

b. 危险的物质、零部件和操作应与其它活动、区域、人员及不相容的器材隔离；

c. 设备的位置安排应使工作人员在操作、保养、维护、修理或调整过程中，尽量避免危险例如：危险的化学药品、高压电、电磁辐射、切削锋口或尖锐部分等；

d. 尽量减少恶劣环境条件(例如：温度、压力、噪声、毒性、加速度、振动、冲击和有害射线等)所导致的危险；

e. 系统设计时应尽量减少在系统的使用和保障中人为差错所导致的风险；

f. 为把不能消除的危险所形成的风险减少到最低程度，应考虑采取补偿措施，这类措施包括：联锁、冗余、故障安全保护设计、系统防护、灭火和防护服、防护设备、防护规程等；

g. 用隔离或屏蔽的方法保护有冗余的分系统的电源、控制装置和关键零部件；

h. 当各种补偿设计方法都不能消除危险时，在装配、使用、维护和修理说明书中应给出报警和注意事项，并在危险零部件、器材、设备和设施上标出醒目的标记，以使人员、设备得到保护。这些标记应符合 GB2894 的有关规定；

i. 尽量减轻事故中人员的伤害和设备的损坏；

j. 设计由软件控制或监测的功能，以尽可能减少危险事件或事故的发生；

k. 评审设计准则中对安全性不足或限制过多的要求，根据分析或试验数据，推荐新的设计准则；

l. 必须消除 I 级的和 II 级的危险(见 4.6.1)或将其相关的风险减少到订购方可接受水平。若无有效的措施，则应向订购方推荐替换的设计方案。

4.5 安全性措施优先次序要求

系统采取安全性措施的优先次序如下：

a. 最小风险设计。首先在设计上消除危险，若不能消除已判定的危险，应通过设计方案的选择将其风险减少到订购方规定的可接受水平。

b. 采用安全装置。若不能通过设计消除已判定的危险或不能通过设计方案的选择满足订购方的要求，则应采用永久性的、自动的或其它安全防护装置，使风险减少到订购方可接受水平。可能时，应规定对安全装置作定期功能检查。

c. 采用报警装置。若设计和安全装置都不能有效地消除已判定的危险或满足订购方的要求，则应采用报警装置来检测出危险状况，并向有关人员发出适当的报警信号。报警信号应明显，以尽量减少人员对信号作出错误反应的可能性，并应在同类系统内标准化。

d. 制定专用规程和进行培训。若通过设计方案的选择不能消除危险，或采用安全装置和报警装置也不能满足订购方的要求，则应制定专用的规程和进行培训。除非订购方放弃要求，对于 I 级和 II 级危险(见 4.6.1)决不能仅仅使用报警、注意事项或其它形式的提醒作为唯一的减少风险的方法。专用的规程包括个人防护装置的使用方法。对于关键的工作，必要时应要求考核人员的熟练程序。

4.6 风险评价

应按危险严重性和危险可能性划分危险的等级，进行风险评价，并根据有关风险的评价决定对已判定的危险的处理方法。

4.6.1 危险严重性

危险严重性等级给出了危险严重程度定性的度量。其规定见表 1。

表 1 危险严重性等级

等 级	事 故 说 明
I (灾难的)	人员死亡或系统报废
II (严重的)	人员严重受伤、严重职业病或系统严重损坏
III (轻度的)	人员轻度受伤，轻度职业病或系统轻度损坏
IV (轻微的)	轻于 III 级的损伤

对于具体的系统应给出系统报废、系统严重或轻度损坏、严重或轻度职业病明确的规定。其规定应得到订购方和承制方双方的认可。

4.6.2 危险可能性

危险可能性等级给出了发生危险的可能程度的定性度量，其规定见表 2。

表 2 危险可能性等级

等 级	个 体	总 体
A (频繁)	频繁发生	连续发生
B (很可能)	在寿命期内会出现若干次	经常发生
C (有时)	在寿命期内可能有时发生	发生若干次

续表 2

等　级	个　体	总　体
D （极少）	在寿命期内不易发生，但有可能	不易发生但有理由预期可能发生
E （不可能）	很不容易发生以至于可以认为不会发生	不易发生，但有可能发生

对于具体的系统，应明确规定频繁、很可能、有时、极少、不可能及总体的大小，其定义应得到订购方和承制方双方的认可。

5 详细要求

5.1 管理与控制

5.1.1 制定系统安全性工作计划（工作项目 101）

本工作项目要求承制方制定安全性工作计划，以实现安全性大纲所规定的全部任务。系统安全性工作计划至少应包括以下四个组成部分：执行工作计划的方法、合格的人选、各级管理部门的职责以及确保工作完成所需的资源。

5.1.1.1 工作项目要点

系统安全性工作计划应符合合同要求并作为执行合同的依据。系统安全性工作计划一般包括以下内容：

a. 实施安全性大纲的指导思想；

b. 系统安全性工作项目的实施细则，如工作项目要求、工作内容、完成状况、检查方法等；

c. 安全性工作组织、人员及其资格和职责；

d. 安全性工作进度表；

e. 安全性大纲评审点；

f. 系统安全性工作计划与系统总的研制计划协调的说明，包括与可靠性计划和维修性计划的协调；

g. 安全性信息收集、传递、分析、处理、反馈和归档等程序的说明；

h. 处理已判定危险的方法或过程；

i. 对设计人员、使用和维修人员的安全性培训；

j. 事故和危险的故障的分析的报告；

k. 系统安全性与其它安全性领域之间的接口：如核安全、靶场安全、爆炸物和军械安全、化学和生物安全、激光安全等；

l. 系统安全性与其它保障领域之间的接口：如质量管理、可靠性、维修性、人素工程、健康保障等。

5.1.1.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 101；

*b. 确定系统安全性工作计划在合同中地位；

c. 确定补充的工作项目或需要提供的补充信息；

d. 对事故和危险故障的报告要求。

5.1.2 对转承制方、供应方和建筑工程单位的安全性综合管理(工作项目 102)

本工作项目要求承制方对转承制方和供应方(以下简称转承制方)、建筑工程单位的安全性工作执行情况进行适当的监督与控制，以便必要时采取相应的措施，确保与承制方安全性大纲要求的一致性。

5.1.2.1 工作项目要点

承制方对转承制方和建筑工程单位的安全性工作进行审查、评价和采取相应监控措施的条款应在合同中规定。合同一般应包括以下内容：

a. 转承制方的安全性工作，包括工作的进度和有关的资料；

b. 转承制方制定与承制方的安全性大纲相协调的安全性大纲；

c. 承制方进行风险评价，考察整个系统的设计和使用，特别是各转承制方产品(包括软件)之间的接口，指导和协调各转承制方的安全性工作；

d. 承制方和各转承制方相互之间安全性信息的交换方法和内容；

e. 承制方评审转承制方的安全性工作；

f. 建筑工程单位按设施的安全性工作计划进行安全性工作；

g. 建筑工程单位和各有关单位相互之间安全性信息的交换方法和内容。

5.1.2.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 根据剪裁执行工作项目 101 和 102。

5.1.3 安全性大纲评审(工作项目 103)

本工作项目要求承制方按计划安排安全性大纲的评审，以确保安全性工作按预定程序进行并保证系统达到安全性定性、定量要求。

5.1.3.1 工作项目要点

a. 安全性大纲评审计划由承制方根据安全性工作计划制定，其内容应包括评审类型、评审点、评审要求等；

b. 承制方作出的安全性大纲评审的时间和评审内容的安排，应及时通知订购方，也应根据需要通知转承制方，以便有关各方参加评审；

c. 安全性大纲的评审应尽可能与系统设计的其它质量特性(例如性能、可靠性、维修性)的评审结合进行；

d. 在每一个评审点上所进行的安全性大纲评审都必须认真检查安全性大纲的执行情况、安全性工作进度，特别是对安全性大纲是否达到合同所规定的安全性要求进行评审和评价。

5.1.3.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 103；

b. 确定评审类型和内容；

c. 订购方参加评审的项目；

d. 记录评审结果；

e. 评审前、后需提交资料的交付日程。

5.1.4 对系统安全性工作组的保障(工作项目 104)

本工作项目要求承制方对订购方按有关规定建立的系统安全性工作组提供工作的保障。

5.1.4.1 工作项目要点

承制方应作为系统安全性工作组成员参加其工作，包括下列内容：

a. 汇报承制方安全性大纲实施情况，包括设计和使用风险评价的结果；

b. 提供危险分析摘要，包括问题的确定和解决的情况；

c. 汇报研制中事故和危险故障的分析结果，包括预防建议和措施；

d. 接受系统安全性工作组分配的工作。

5.1.4.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 104；

*b. 确定承制方人员要求和担任的工作，包括技术顾问等；

*c. 系统安全性工作组会议安排；

d. 对系统安全性工作组特殊的保障工作；

5.1.5 建立危险报告，分析和纠正措施跟踪系统(工作项目 105)

本工作项目要求建立危险跟踪闭环系统，跟踪并记录危险的确定、消除或将其风险降低到订购方可接受水平的过程。

5.1.5.1 工作项目要点

a. 建立危险跟踪的闭环系统；

b. 坚持填写"危险日志"，其中至少包含以下内容：

每个危险的说明；

每个危险的状况；

每个危险的可跟踪性(从危险的确定到解决的整个过程)。

5.1.5.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 105；

*b. 确定应记入危险日志中的最低危险限度；

c. 危险日志所需的完整资料；

d. 危险日志的记录程序。

5.1.6 试验的安全性(工作项目 106)

本工作项目要求承制方考虑试验中的安全性，提供已有的分析报告和其它安全性资料，采取措施满足各类试验的安全性要求，确保降低或消除试验中 I 级和 II 级的危险。

5.1.6.1 工作项目要点

5.1.6.1.1 试验计划

签订合同时就应制定试验的安全性计划，考虑以下内容：

a. 确定试验大纲中与安全性有关的进度关键点，在该点前应完成危险分析、风险评价或其它的安全性研究；

b. 对试验计划、规程和其它文件的分析、评估和批准进度，以确保在整个试验过程中考虑了安全性；

c. 在试验前的危险分析中考虑试验设备和测试仪器及其安装；

d. 满足订购方的特殊要求，并把所有已确定的试验环境所特有的危险通知订购方。

5.1.6.1.2 纠正措施

确保及时采取纠正措施，以降低或消除试验中的危险。

5.1.6.1.3 报告

建立关于试验中危险和相应措施状态的报告档案。

5.1.6.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 106；

*b. 制定试验适用的系统安全性的特殊要求；

*c. 满足 5.1.6.1 中所规定要求的进度安排。

5.1.7 系统安全性进展报告(工作项目 107)

本工作项目要求承制方定期地提供系统安全性进展报告。

5.1.7.1 工作项目要点

系统安全性进展报告应概述在规定的报告期内安全性大纲的进展情况，以及在下一个报告期内计划的工作，其中应包括以下内容：

a. 研制和生产各阶段安全性工作、进展及状况的概述，着重说明主要成效和问题；

b. 新发现的显著级危险和对已知危险的风险控制程度的重大变化；

c. 所有已提出的但仍未完成的纠正措施的现状；

d. 影响安全性大纲的费用和进度的重大变动；

e. 讨论报告期内已作安全性评审的承制方文件，指出该文件中的安全性内容是否可接受，有无改善安全性的措施；

f. 若有系统安全性工作组，可建议它下次会议的议程。

5.1.7.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 107；

*b. 规定报告周期。

5.2 设计与分析

5.2.1 初步危险表(工作项目 201)

初步危险表是一份危险清单，初步列出安全性设计中可能需特别重视的危险或需作深入

分析的危险部位，旨在使订购方能尽早地选择重点管理的危险部位。

5.2.1.1 工作项目要点

在设计初期承制方就应考察系统方案，编制初步危险表，确定设计中可能存在的危险。承制方应按订购方的意见做进一步的研究，分析初步危险表中选定的危险，以确定其重要程度。

5.2.1.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 201；

b. 确定特别注意点。

5.2.2 初步危险分析（工作项目 202）

本工作项目要求承制方进行初步危险分析并记录成文，以确定安全性关键的部位，评价各种危险及确定要采用的安全性设计准则。承制方应在系统研制的初期进行初步危险分析，获得设计方案的初始风险评价，以便在权衡研究和设计方案的选择中考虑安全性问题。对于与建议的设计或功能有关的危险，应利用有效的信息（包括类似系统的事故数据和其它经验教训），评估其危险严重性、危险可能性及使用约束，应考虑消除危险或将其风险减少到订购方可接受水平所需的安全性措施和替换方案。

5.2.2.1 工作项目要点

初步危险分析至少应考虑下列内容以确定和评价危险：

a. 危险品，例如：燃料、激光、炸药、有毒物、有危险的建筑材料、压力系统、放射性物质等；

b. 系统部件间接口的安全性（例如：材料相容性、电磁干扰、意外触发、火灾或爆炸的发生和蔓延、硬件和软件控制等），包括软件对系统或分系统安全性的可能影响；

c. 确定控制安全性关键的软件命令和响应（例如错误命令、不适时的命令或响应、或由订购方指定的不希望事件等）的安全性设计准则，采取适当的措施并将其纳入软件和相关的硬件要求中；

d. 与安全性有关的设备、保险装置和可能的备选方法，例如：联锁装置、冗余技术、硬件或软件的故障安全设计、分系统保护、灭火系统、人员防护设备、通风装置、噪声或辐射屏蔽等；

e. 包括使用环境在内的环境约束条件，例如：坠落、冲击、振动、极限温度、噪声、接触有毒物质、有害健康的环境、火灾、静电放电、雷击、电磁环境影响，包括激光辐射在内的电离和非电离辐射等；

f. 操作、试验、维修和应急规程，例如：人素工程、操作人员的作用、任务要求等的人为差错分析；设备布置、照明要求、可能外露的有毒物质等因素的影响，噪声或辐射对人的能力的影响，载人系统中的生命保障要求及其安全性问题，例如坠落安全性、应急出口、营救、救生等；

g. 设施、保障设备，例如：用于含有危险物质的系统或组件的储存、组装、检查、检验等方面的设备，射线或噪声发射器，电源等。

5.2.2.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 202；

*b. 确定要报告的危险可能性和危险严重性的最低限度；

c. 确定需特别检查或消除的所有危险和危险区域。

5.2.3 分系统危险分析(工作项目 203)

本工作项目要求进行分系统危险分析并记录成文,确定与分系统有关的危险以及由分系统的部件和设备之间功能关系所导致的危险,确定分系统部件的使用和故障对系统安全性的影响方式。若未规定分析的方法,承制方在进行分系统危险分析前,拟用的方法应得到订购方的认可。

5.2.3.1 工作项目要点

承制方应进行分系统危险分析,以确定其中因性能、性能下降、功能故障或意外动作等可能导致危险的或其设计不满足合同安全性要求的所有部件和设备(包括软件),分析应确定:

a. 故障模式,包括可能的人为差错和单点故障以及分系统部件故障对安全性的影响;

b. 软件事件、故障和偶然事件(例如定时不当)对分系统安全性的可能影响;

c. 软件规格说明中的安全性设计准则已得到满足;

d. 软件设计需求及纠正措施的实现方法不影响或降低分系统的安全性或引入新的危险。

5.2.3.2 由订购方规定的细节

根据需要,包括下列事项的细节:

*a. 执行工作项目 203;

*b. 确定要报告的危险可能性和危险严重性的最低限度;

c. 要分析的分系统;

d. 拟用的分析技术和(或)格式。

5.2.4 系统危险分析(工作项目 204)

本工作项目要求进行系统危险分析并记录成文,确定系统设计中有安全性问题的部位,特别是分系统之间的接口的危险(包括可能的安全性关键的人为差错)并评价其风险,确定系统的使用和故障模式对系统及其分系统的影响。若未规定分析的方法,承制方在进行系统危险分析前,拟用的分析方法应得到订购方的认可。

5.2.4.1 工作项目要点

本分析应包括评审各分系统间关系的下列内容:

a. 是否符合规定的安全性准则;

b. 独立的、相关的和同时发生的危险事件,包括安全装置的故障或产生危险的共同原因;

c. 由于分系统的正常使用导致另一分系统或整个系统安全性的降低;

d. 设计更改对分系统的影响;

e. 人为差错的影响;

f. 软件事件、故障和偶然事件(如定时不当)对系统安全性的可能影响;

g. 软件规格说明中的安全性设计准则已得到满足;

h. 软件设计需求及纠正措施的实现方法不影响或降低系统的安全性或引入新的危险。

5.2.4.2 由订购方规定的细节

根据需要,包括下列事项的细节:

*a. 执行工作项目 204;

*b. 确定要报告的危险可能性和危险严重性的最低限度；

c. 拟用的分析技术和(或)格式。

5.2.5 使用和保障危险分析(工作项目 205)

本工作项目要求进行使用和保障危险分析并记录成文，以确定和评价系统使用中与环境、人员、规程和设备有关的危险。若未规定分析的方法，承制方在进行使用和保障危险分析前，拟用的分析方法应得到订购方的认可。

5.2.5.1 工作项目要点

本分析应确定和评价系统使用中的危险，应考虑：计划的系统配置和(或)状态；设施的接口；计划的环境；保障工具或其它设备，包括软件控制的自动测试设备或规定使用的设备；操作或工作的次序，同时进行工作的影响和限制；生物因素；有关规定或合同规定的人员安全和健康要求；可能的非计划事件，包括由于人为差错产生的危险。

为消除已判定的危险或将其风险减少到有关规定或合同规定的可接受水平，确定所需的安全性要求或备选方案。

分析应确定：

a. 在危险条件下进行的各项工作及其工作时间以及在这些工作或工作时间内尽量减少风险需要采取的各种措施；

b. 为消除危险或减少有关风险所需的系统硬件或软件、设施、工具或保障和检测设备在功能或设计要求上的更改；

c. 对安全装置和设备的要求，包括人员安全和生命保障设备；

d. 报警、注意事项以及特别应急措施，例如：应急出口、营救、脱离、安全动作、放弃等；

e. 危险器材的装卸、使用、贮存、运输、维修及处理要求。

5.2.5.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 205；

*b. 确定要报告的危险可能性和危险严重性的最低限度；

c. 拟用的分析技术和(或)格式。

5.2.6 职业健康危险分析(工作项目 206)

本工作项目要求进行职业健康危险评价并记录成文，确定有害健康的危险并提出保护措施，以便将有关风险减少到订购方可接受水平。

5.2.6.1 工作项目要点

职业健康危险评价应考虑：

a. 有毒物质，例如：致癌物或有致癌嫌疑的物品、一般毒品、窒息物、对呼吸器官有刺激的物品等；

b. 物理因素，例如：噪声、热应力或冷应力、电离辐射或非电离辐射等；

c. 系统、设施和人员防护装置的设计要求(例如：通风、噪声衰减、辐射屏蔽等)以保证使用和维修的安全。当没有可行的工程设计可把风险减少到可接受水平时，必须规定其他防护措施，例如：防护服，可把风险减少到可接受水平的具体使用或维修操作规程，并应得到订购方的

认可。

5.2.6.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 206。

5.2.7 工程更改建议的安全性评审（工作项目 207）

本工作项目要求对工程更改建议进行安全性评审并记录成文，以确定工程更改对系统安全性的影响。工程更改包括安全性要求的偏离和（或）放弃。

5.2.7.1 工作项目要点

承制方应分析每个工程更改方案，以确定与其有关的危险，评价相关的风险，并预计工程更改对安全性的影响。

承制方应提供工程更改不会增加新的危险的依据，当工程更改将降低系统安全性水平时，必须通知订购方并获得订购方的认可。

5.2.7.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 207。

5.2.8 订购方提供的设备和设施的安全性分析（工作项目 208）

本工作项目要求对订购方提供的设备和设施进行安全性分析，以确定在系统中应用的安全性。

5.2.8.1 工作项目要点

5.2.8.1.1 承制方应确定订购方应提供的设备和设施的安全性关键的性能和设计资料。

5.2.8.1.2 若订购方能提供有效的资料，承制方应：

a. 确定所需的安全性分析及进行分析的时间；

b. 确定订购方提供的设备和设施与系统的其它部分的接口的安全性分析；

c. 以上两项应经订购方认可后执行。

5.2.8.1.3 若订购方无有效的资料，承制方应通过分析、试验和检查确定所需安全性关键的资料；拟用的方法应提交订购方，经订购方认可后执行。

5.2.8.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 208；

*b. “安全性关键的”的定义；

*c. 确定要报告的危险可能性和危险严重性的最低限度。

5.3 验证与评价

5.3.1 安全性验证（工作项目 301）

本工作项目要求验证安全性关键的硬件、软件和规程是否符合安全性要求并记录成文，其验证方法应得到订购方的认可。

5.3.1.1 工作项目要点

5.3.1.1.1 承制方应通过试验、演示或其它方法验证安全性关键的硬件、软件及规程是否符

合安全性要求。

5.3.1.1.2 评审所有试验(包括设计验证、使用评价、技术资料的验证、生产验收、贮存寿命验证)的试验计划、试验规程和结果,以确保充分验证了设计的安全性(包括使用和维修规程),包括验证因设计无法消除的Ⅰ级危险而设置的安全装置、报警装置等。

5.3.1.2 由订购方规定的细节

根据需要,包括下列事项的细节:

*a. 执行工作项目 301;

*b. "安全性关键的"的定义或确定安全性关键的设备和规程;

c. 制订验证安全性要求的试验计划、规程和报告或对它们的输入信息。

5.3.2 安全性评价(工作项目 302)

本工作项目要求在系统试验或使用前或合同完成时对所假定事故的风险进行全面评价并记录成文。

5.3.2.1 工作项目要点

承制方应确定硬件、软件和系统设计的所有安全性特性并确定系统各种规程可能导致的危险。

安全性评价应包括:

a. 危险分类与分级的安全性准则和方法;

b. 为确定系统中存在的危险而进行的分析与试验,包括:仍有残余风险的危险,以及为把有关风险减少到合同规定的可接受水平而已采取的措施;为验证安全性准则要求和分析而进行的试验的结果;

c. 安全性大纲执行的结果,包括列出全部显著危险以及用来确保人员和财产安全所需的具体安全性建议或预防措施的清单。按危险在正常或不正常使用条件下会不会发生,对清单上的危险进行分类;

d. 由系统中产生或在系统中使用的所有危险器材,包括:确定器材类型、数量及可能的危险;在装卸、使用、贮存、运输、维修和处理期间所需的安全性防护措施和规程;器材安全性数据;

e. 作出书面结论:所有已判定的危险均已消除或有关的风险已控制在合同规定的可接受水平;系统已可以进行试验或投入使用或者进入研制的下一阶段。

承制方应按合同要求对所承制的系统与其它系统的接口的危险提出可行的处理建议。

5.3.2.2 由订购方规定的细节

根据需要,包括下列事项的细节:

*a. 执行工作项目 302。

5.3.3 安全性符合有关规定的评价(工作项目 303)

本工作项目要求进行安全性符合有关规定的评价并记录成文,以确保系统的安全设计及在系统试验或使用前或合同完成时全面地评价所假定的风险。

5.3.3.1 工作项目要点

5.3.3.1.1 承制方应验证系统的设计和规程是否符合合同或国家、军用和行业的安全性标

准、规范及有关法规等。

5.3.3.1.2 安全性符合有关规定的评价包括必要的危险分析、设计图纸和规程评审及设备的检查。

5.3.3.1.3 安全性符合有关规定的评价应包括初步危险分析、分系统危险分析、系统危险分析、使用和保障危险分析必要的内容和技术，以确保系统设计、使用、维修和保障的安全性。

5.3.2.1.4 安全性符合有关规定的评价应：

a. 确定和评价系统中存在的或本系统特有的接口、安装、试验、使用、维修或保障引起的残余危险；

b. 确定必要的特殊的安全性设计特性、装置、规程、技能、培训、设施、保障要求及人员防护设备；

c. 确定危险器材及其安全装卸、使用、贮存、运输、维修及处理所需的预防措施和规程。

5.3.3.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 303。

5.4 安全性培训

5.4.1 系统安全性主管负责人的资格(工作项目 401)

本工作项目用于确定承制方系统安全性主管负责人的资格。系统安全性主管负责人有权协调或批准承制方有关系统安全性的文件。

5.4.1.1 工作项目要点

系统安全性主管负责人应符合下列条件：

a. 至少具有或相当理工科或管理专业大学本科毕业以上水平；

b. 经系统安全性方面的专业培训并经考试合格；

c. 具有下列方面之一的工作经历(经历的长短由有关部门自定)：

系统安全性管理；

系统安全性分析；

系统安全性设计；

系统安全性研究；

系统的使用安全性；

事故调查；

人素工程；

产品质量保证工程；

可靠性工程；

维修工程。

5.4.1.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 401；

b. 确定其它最低资格要求。

5.4.2 培训(工作项目 402)

本工作项目要求对承制方和订购方的有关人员进行培训，这些人员在承制方的工作中将参与下列方面的工作：确定危险及其分类，分析产生的原因、影响，采取防护和控制措施，制订和执行规程、检查表；消除人为差错；研制保险装置、保护设备、监控和报警装置；及制订应急规程。

5.4.2.1 工作项目要点

5.4.2.1.1 试验、使用和保障人员的培训

承制方应对试验、使用和保障人员进行安全性培训，培训计划和考核中应包括已批准的安全性规程。试验、使用和保障人员的资格要由相应的具有审定职能的部门确认。

5.4.2.1.2 设计、研制和生产人员的培训

承制方应根据系统危险分析和使用危险分析的结果，制定相应的安全性培训计划，分别对承制方设计、研制和生产的各级各类人员进行培训。

5.4.2.1.3 订购方管理人员的培训

承制方也应对参与承制方工作的订购方管理人员进行安全性培训。

5.4.2.2 由订购方规定的细节：

根据需要，包括下列事项的细节：

*a. 执行工作项目 402。

5.5 软件系统安全性

本节只适用于按下列文件开发的大型或复杂软件：

GJB437 军用软件质量保证

GJB439 军用软件开发规范

对于其它软件的系统安全性工作，则应在 5.2 和 5.3 中的工作中考虑。

5.5.1 软件需求危险分析(工作项目 501)

本工作项目要求承制方应用初步危险表(工作项目 201)和系统级的初步危险分析(工作项目 202)的结果，进行软件需求危险分析并记录成文，检查软件的需求和设计，确定软件的不安全模式，对软件系统进行初始的安全性评价。承制方应在方案设计评审时提出安全性关键的计算机软件成分(包括过程、程序、例程、模块、功能、表、变量、值或计算机程序状态及其接口等)的清单，分析的最终结果应在软件需求评审时提交。

5.5.1.1 工作项目要点

5.5.1.1.1 承制方应建立软件安全性跟踪系统，以记录软件的安全性需求及其实现过程。

5.5.1.1.2 承制方应分析系统或部分系统说明书和软件需求规格说明：

a. 保证已经正确和完整地规定了系统安全性要求，并已恰当地转化为软件需求，并确保软件安全性需求能恰当地影响软件的设计，以及操作员手册、用户手册和诊断手册的制订。承制方至少应考察以下文件：

系统或部分系统说明书和分系统说明书；

软件需求规格说明；

接口要求说明书和其它接口文件；

功能流程图和有关资料；

存贮分配和程序结构文件；

与涉及计划的测试、生产、贮存、修理、使用和最终处置的安全性要求有关的基本信息；

与系统能源、有毒物质和其它危险事件源(特别是由软件直接或间接控制的)有关的信息；

软件开发计划、软件质量评估计划和软件配置管理计划；

有关的历史资料。

b. 确定与上述说明书和文件有关的危险。

5.5.1.1.3 承制方应提出与安全性有关的对上述文件的更改建议、设计要求和测试要求，并将其纳入软件概要设计文档和详细设计文档及软件测试计划中。

5.5.1.1.4 承制方应从软件安全性的角度保障方案设计评审和软件需求评审。

5.5.1.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 201、202 和 501；

*b. 在所分析的系统、分系统或部件范围内“安全性关键的”的定义；

*c. 设计评审所需的承制方保障程度；

5.5.2 概要设计危险分析(工作项目 502)

本工作项目要求承制方应用软件需求危险分析的结果进行概要设计危险分析并记录成文，以确保概要设计中的安全性水平。概要设计危险分析应在软件详细设计开始前基本完成，分析结果应在概要设计评审时提交。

5.5.2.1 工作项目要点

5.5.2.1.1 进行危险的风险评价

承制方应进行危险的风险评价，以确定在概要设计后需作进一步分析的安全性关键的计算机软件成分。

a. 承制方应确定由初步危险分析、分系统危险分析和软件需求危险分析所判定的危险与可能影响或控制这些危险的计算机软件成分和低层次软件单元的关系，这些软件成分和所有指定的其它成分均为安全性关键的计算机软件成分。

b. 承制方应评价现有的设计文档，以确定安全性关键的计算机软件成分与其它安全性关键的和非安全性关键的计算机软件成分是否相关和相关的程度，那些影响安全性关键的计算机软件成分的输出的计算机软件成分也为安全性关键的计算机软件成分。

5.5.2.1.2 分析概要设计

承制方分析 5.5.2.1.1 中确定的安全性关键的计算机软件成分的概要设计以确保概要设计中正确地和完整地规定了所有的安全性要求。承制方应确定在概要设计的何处，以及在什么条件下可能出现不可接受的危险。分析中应包括输入输出时序、多重事件、失序、事件、事件失败、错误事件、不恰当的数值、不利环境、死锁、硬件故障敏感性等。

5.5.2.1.3 提出设计更改建议

根据初步危险分析、分系统危险分析、软件需求危险分析和概要设计危险分析的结果，承制方应更改软件概要设计文档以消除危险或将其风险降低到可接受水平。

5.5.2.1.4 将安全性需求纳入软件测试计划

承制方应将安全性需求以及对安全性关键的计算机软件成分和安全性关键的条件的测试纳入软件测试计划。承制方应将安全性专用的测试纳入软件测试计划、系统测试计划和整个系统测试大纲，这些测试计划应包括在模拟和使用状态下的测试规定。

5.5.2.1.5 保障概要设计评审

承制方应从软件安全性的角度保障概要设计评审。

5.5.2.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 203、501 和 502；

*b. 在所分析的系统、分系统或部件范围内"安全性关键的"的定义；

*c. 设计评审所需的承制方保障的程序。

5.5.3 详细设计危险分析(工作项目 503)

本工作项目要求承制方应用软件需求危险分析和概要设计危险分析的结果，进行详细设计危险分析并记录成文，以验证软件设计是否已正确地体现了安全性需求并对安全性关键的计算机软件成分进行分析。本分析应在软件开始编程前基本完成，其分析结果应在详细设计评审时提交。

5.5.3.1 工作项目要点

5.5.3.1.1 危险的风险评价

承制方应进行危险的风险评价以确定需作进一步分析的软件成分。

a. 承制方应确定由初步危险分析、软件需求危险分析、分系统危险分析和概要设计危险分析判定的危险与软件详细设计中规定的低层次软件成分的关系，这些成分为安全性关键的计算机软件成分。安全性关键的计算机软件成分的确定应随详细设计危险分析一直进行到实际可行的最低层次。

b. 承制方应评价软件详细设计文档和其它详细设计文件，在计算机软件配置项目及计算机软件成分各层次上确定安全性关键的软件与指定的其它软件是否相关和相关的程度。

5.5.3.1.2 分析详细设计

承制方应对由危险的风险评价确定为安全性关键的软件成分的软件详细设计进行安全性分析，以确保在设计中正确地和完整地规定和体现所有的安全性需求。承制方应确定在详细设计的何处以及在什么条件下，将出现或可能出现不可接受的危险。

5.5.3.1.3 提出设计更改建议

根据详细设计安全性分析的结果，承制方应对详细设计提出更改建议，以消除危险或将危险的严重性降低到订购方可接受水平。

5.5.3.1.4 制定测试要求

承制方应参与制定测试计划、说明和规程的要求及其更改的历次过程。承制方应制订安全性关键的计算机软件成分的测试说明和规程。

5.5.3.1.5 确定用户手册、操作员手册和诊断手册要求

承制方应确定安全性有关的信息(如注意和警告事项)，以体现在计算机系统诊断手册、计

算机系统操作员手册、固件保障手册和软件用户等手册及其它手册中。

5.5.3.1.6 使编程人员明确安全性关键的计算机软件成分

承制方应对编程人员明确安全性关键的计算机软件成分，并向编程人员提出来自概要设计规格说明和设计文档中的明确的与安全性有关的编程建议和安全性需求。

5.5.3.1.7 保障详细设计评审

承制方应从软件安全性的角度保障详细设计评审，应在详细设计评审时报告软件安全性分析的结果，报告中应包括概要设计安全性需求和实现、保障分析及所应用的方法和任何未解决的风险问题。

5.5.3.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 204、501、502 和 503；

*b. 在所分析的系统、分系统或部件范围内"安全性关键的"的定义；

*c. 设计评审所需的承制方保障的程度。

5.5.4 软件编程危险分析(工作项目 504)

本工作项目要求承制方进行软件编程危险分析并记录成文，分析程序的编制和系统的接口，应利用详细设计危险分析的结果，确定其中可能导致或促成影响安全性的事件、故障和条件。本分析工作应与编程同时进行，并贯穿系统的寿命周期。

5.5.4.1 工作项目要点

5.5.4.1.1 软件分析

承制方应对所有安全性关键的计算机软件成分进行危险分析，包括以下工作：

a. 分析：

安全性关键的计算机软件成分的正确性和完整性，及其输入或输出时序、多重事件、关序事件、事件失败、错误事件、不恰当的数值、不利环境、死锁、硬件故障敏感性等方面的问题；

系统说明书和要求文件中提出的安全性准则在软件中的实现情况；

可能使系统处在危险状况下工作的硬件故障、软件故障、瞬时错误和其它事件的可能组合；

对输入数据流中特殊字符或不正确数据的不执行处理的正确性；

故障安全保护和故障可用的模式；

输入过载或过界状态。

b. 进行安全性关键的计算机软件成分的内部路径和控制处理流程分析；

c. 向订购方提出对规格说明、设计和测试文档中的设计、编程和测试的更改建议；

d. 保障所有安全性关键的计算机软件成分的非正式评审。

5.5.4.1.2 评审编程文档

承制方应确保所有安全性关键的计算机软件成分和所有源程序完整地、准确地记录和注释，所用的记录和注释方式应使得将来不熟悉原有的程序的程序员在更改程序时，减少引入新的危险的可能性。

5.5.4.1.3 保障测试准备状态评审

承制方应从软件安全性的角度保障测试准备状态评审。测试准备状态评审是评审软件测试规程是否符合软件测试方案，能否完成测试的要求，其目的是保证承制方作好了正式软件测试的准备。

5.5.4.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 201、501、503 和 504；

*b. 在所分析的系统、分系统或部件范围内"安全性关键的"的定义；

*c. 设计评审所需的承制方保障的程度。

5.5.5 软件安全性测试(工作项目 505)

本工作项目要求承制方进行软件安全性测试并记录成文，验证安全性需求的实现情况，以确保已消除所有的危险或将其风险控制到可接受水平。

5.5.5.1 工作项目要点

5.5.5.1.1 单元测试、综合测试、验收测试和系统测试

承制方应参与安全性关键的计算机软件成分的所有层次的测试，包括单元测试、综合测试、验收测试和系统测试。

a. 承制方软件安全性工作人员应确保严格地按照批准的测试计划、说明、规程和用例进行安全性关键的计算机软件成分的测试，并准确地记录成文、分析和报告结果。承制方应确保纠正软件中的缺陷并重新测试。

b. 除在正常条件下测试外，应测试软件，以表明软件不会因可能的单个或多个输入错误而导致不安全状态。

c. 承制方应确保在系统综合应力测试和系统验收测试时软件正确地和安全地运行。系统验收测试应在实际的使用条件下进行。

5.5.5.1.2 外购软件

除非订购方明确提出可不必考虑外，应分析和测试系统中的外购软件。外购软件包括市场采购的、有专利的和不是为本系统专门开发的其它软件。无论外购软件是否修改，都应进行分析和测试。

5.5.5.1.3 订购方提供的软件

除非订购方明确提出可不必考虑外，无论承制方对其软件是否修改，都应对订购方提供的软件按在执行合同时开发的软件进行软件安全性分析和测试。

5.5.5.1.4 危险的处理

承制方应纠正软件的缺陷以消除在系统综合测试和系统验收测试中发现的所有危险或将其风险降低到可接受水平。纠正后的软件应在同样的条件下重新测试，以确保已消除危险和不会出现其它危险。

5.5.5.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 501 和 505；

*b. 在所分析的系统、分系统或部件范围内"安全性关键的"的定义；

*c. 设计评审所需的承制方保障的程度；

5.5.6 软件与用户接口分析(工作项目 506)

本工作项目要求承制方进行软件与用户接口分析并记录成文，制定软件用户规程。

5.5.6.1 工作项目要点

承制方应分析不能由系统设计或其它措施消除或控制的危险，提出以下设计更改建议并制订及相应的操作规程：

a. 对每个危险状态提供探测方法；

b. 对每个探测到的 II 级危险状态提供安全生存和恢复的方法；

c. 增设报警特性以警告操作员或驾驶员注意会导致设备故障的软件错误；

d. 对过程或事件提供安全的清除方法；

e. 对安全性关键的系统或成份的状态提供明确的和完整的显示方式，在显示完所有数据后，才可越过容许超越的潜在的安全性关键的故障，或清除状态数据，例如，一个系统中有一系列故障，这些故障若单独发生从安全性上是可以超越的，若同时发生多重故障可能导致系统的报废，所以操作人员在发出超越命令或状态显示复位命令前应了解所有的安全性关键的故障。

5.5.6.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 501 和 506。

5.5.7 软件更改危险分析(工作项目 507)

本工作项目要求承制方分析软件的所有更改(包括修改和修补)并记录成文，以确定是否会引入新的危险。

5.5.7.1 工作项目要点

5.5.7.1.1 除非更改的性质能说明不必要进行更改分析外，否则对规格说明、需求、设计、编程、系统、设备和测试计划、说明、规程、用例或准则的任何更改都应进行软件危险分析和测试。更改危险分析应从更改建议所影响的文档或系统的最高层次开始。

5.5.7.1.2 承制方应表明更改不会产生新的危险，不会影响已解决的危险，不会使现存的危险更严重以及不会对任何安全性关键的计算机软件成分或有关的和接口的程序产生不利影响。

5.5.7.1.3 承制方应评审受更改影响的文档，以保证文档中正确地反映了软件中所有已做的与安全性有关的更改。

5.5.7.1.4 承制方应将执行本工作项目的方法、过程和其它信息包含在软件配置管理计划中。

5.5.7.2 由订购方规定的细节

根据需要，包括下列事项的细节：

*a. 执行工作项目 501 和 507；

*b. 在所分析的系统、分系统或部件范围内“安全性关键的”的定义。

附 录 A
《系统安全性通用大纲》应用指南
（参考件）

本附录提供了制定安全性大纲，剪裁本标准有关条款的指南。

A1 剪裁要求

由于系统的类型和研制要求不同，以及各种条件的限制，因而要求订购方和承制方在签订合同或拟订研制任务书之前，剪裁本标准规定的安全性工作项目及其要点，并将费用效益作为剪裁的基本依据。

剪裁的目的是防止不加区别地照搬标准条款。

剪裁的基本要求是：

a. 删除对某具体系统不适合和不必要的要求；

b. 修改某些条款或补充本标准中没有包括的技术要求；

c. 协调本标准与其它标准之间重复或不一致的问题。

经过剪裁的要求、工作项目及其要点均应编入合同等有关文件中。

本标准规定的每一工作项目中均有"由订购方规定的细节"，这些细节是由订购方提出，经双方协商和权衡，最后反映在合同的有关文件中，这些细节包括条款的说明、补充要求和向对方提供的必要信息，目的是使承制方能正确地执行这些工作项目及其要点。

A2 确定安全性要求

订购方应根据系统战术技术指标要求，提出适合具体系统的安全性大纲要求，包括定性和定量的安全性要求。这些要求以招标或其它的形式向承制方提出。承制方应根据招标或任务要求，进行分析与研究，将相应的工作项目与要求列入投标文件中，经订购方、承制方双方协商和调整，最后将工作项目和要求在合同或任务书中规定，并反映在有关技术文件中。

A3 风险评价

为决定采取什么措施解决判定的危险，必须制订确定有关风险水平的评价系统。有效的风险评价模型能使决策者恰当地了解有关风险程度与将风险减少到可接受水平所需的费用（包括进度）的关系。

为尽可能地消除危险，应确定危险严重性和危险可能性等级，以便采取解决措施。按系统安全性措施的优先次序，首先是通过设计消除危险，因此在设计初期，只考虑危险严重性的风险评价一般就能满足使风险达到最小的要求。对设计初期未能消除的危险，则应根据危险严重性和危险可能性的风险评价确定纠正措施和解决已判定的危险。

确定危险的等级可用定性分析得到可比较的风险评价，或通过发生概率的定量分析得到危险状态的指数。表 A1 和表 A2 给出了危险的风险评价表的两个例样，可用于得出定性的风险指数，以安排解决措施。表 A1 中，其风险指数为 1A、1B、1C、2A、2B 和 3A 的危险应立即采取解决措施；指数为 1D、2C、2D、3B 和 3C 的危险需要跟踪。表 A2 中，风险指数 1 到 20 的确定是稍带有任意性的，这张表的设计对每一种危险可能性和严重性组合都给出了不同的指数，这样可以避免在把指数作为危险的可能性和严重性等级的数字乘积的情况下出现相同的结果，

例如 2×6＝3×4＝4×3。这两个表只是风险评价方法的例样，不一定适合所有的大纲。

表 A1　危险的风险评价表例 1

危险可能性等级	危险严重性等级			
	I(灾难的)	II(严重的)	III(轻度的)	IV(轻微的)
A(频繁)	1A	2A	3A	4A
B(很可能)	1B	2B	3B	4B
C(有时)	1C	2C	3C	4C
D(极少)	1D	2D	3D	4D
F(不可能)	1E	2E	3E	4E

危险的风险指数	建议的准则
1A，1B，1C，2A，2B，3A	不可接受
1D，2C，2D，3B，2C	不希望有的，需订购方决策
1E，2E，3D，3E，4A，4B	订购方评审后可接受
4C，4D，4E	不评审即可接受

表 A2　危险的风险评价表例 2

危险可能性等级	危险严重性等级			
	I(灾难的)	II(严重的)	III(轻度的)	IV(轻微的)
A(频繁)	1	3	7	13
B(很可能)	2	5	9	16
C(有的)	4	6	11	18
D(极少)	8	10	14	19
E(不可能)	12	15	17	20

危险的风险指数	建议的准则
1—5	不可接受
6—9	不希望有的，需订购方决策
10—17	订购方评审即可接受
18—20	不评审即可接受

A4 工作项目的选择

工作项目的选择取决于系统的复杂性、系统的寿命周期阶段、投资、进度等因素，表 A3 和表 A4 给出了工作项目选择的通用指南。

A5 剪裁工作项目指南

A5.1 管理与控制

A5.1.1 制定系统安全性工作计划(工作项目 101)

系统安全性工作计划是实施安全性大纲最基本的文件，通常是承制方必须做的一项工作。为实现安全性大纲目标，承制方要通过计划来组织、指挥、协调、检查、监督和控制安全性的全部活动。

承制方制定系统安全性工作计划的作用是：

a. 有利于管理和实施安全性大纲；

b. 反映承制方在研制工作中对安全性工作的重视程度；

c. 便于订购方评价承制方为实施和控制安全性工作所规定的各项程序；

表 A3 系统安全性工作项目实施表

本标准条款编号	工作项目	类型	战术技术指标论证阶段	方案论证及确认阶段	研制阶段	生产阶段
5.1.1	制定系统安全性工作计划(101)	管理	G	G	G	G
5.1.2	对转承制方、供应方和建筑工程单位的安全性综合管理(102)	管理	S	S	S	S
5.1.3	安全性大纲评审(103)	管理	S	S	S	S
5.1.4	对系统安全性工作组的保障(104)	管理	G	G	G	G
5.1.5	建立危险报告，分析、纠正措施跟踪系统(105)	管理	S	G	G	G
5.1.6	试验的安全性(106)	管理	G	G	G	G
5.1.7	系统安全性进展报告(107)	管理	G	G	G	G
5.2.1	初步危险表(201)	工程	G	S	S	NA
5.2.2	初步危险分析(202)	工程	G	G	G	GC
5.2.3	分系统危险分析(203)	工程	NA	G	G	GC
5.2.4	系统危险分析(204)	工程	NA	G	G	GC

续表 A3

本标准条款编号	工 作 项 目	类型	战术技术指标论证阶段	方案论证及确认阶段	研制阶段	生产阶段
5.2.5	使用和保障危险分析(205)	工程	S	G	G	GC
5.2.6	职业健康危险分析(206)	工程	G	G	G	GC
5.2.7	工程更改建议的安全性评审(207)	管理	NA	G	G	G
5.2.8	订购方提供的设备和设施的安全性分析(208)	工程	S	G	G	G
5.3.1	安全性验证(301)	工程	S	G	G	S
5.3.2	安全性评价(302)	管理	S	S	S	S
5.3.3	安全性符合有关规定的评价(303)	管理	S	S	S	S
5.4.1	系统安全性主管负责人的资格(401)	管理	S	S	S	S
5.4.2	培训(402)	管理	NA	S	S	S
5.5.1	软件需求危险分析(501)	工程	S	G	G	GC
5.5.2	概要设计危险分析(502)	工程	S	G	G	GC
5.5.3	详细设计危险分析(503)	工程	S	G	G	GC
5.5.4	软件编程危险设计(504)	工程	S	G	G	GC
5.5.5	软件安全性测试(505)	工程	S	G	G	GC
5.5.6	软件与用户接口分析(505)	工程	S	G	G	GC
5.5.7	软件更改危险分析(507)	工程	S	G	G	GC

注：符号说明

G——适用　　管理——安全性管理

S——根据需要选用　　工程——安全性工程

GC——仅设计更改时适用

NA——不适用

表 A4　设施的安全性工作项目实施表

本标准条款编号	工　作　项　目	类型	规划和要求制定	方案设计	最终设计	建筑
5.1.1	制定系统安全性工作计划(101)	管理	S	G	G	S
5.1.2	对转承制方、供应方和建筑工程单位的安全性综合管理(102)	管理	S	S	S	S
5.1.3	安全性大纲评审(103)	管理	G	G	G	G
5.1.4	对系统安全性工作组的保障(104)	管理	G	G	G	G
5.1.5	建立危险报告、分析、纠正措施跟踪系统(105)	管理	G	G	G	G
5.1.6	试验的安全性(106)	管理	G	G	G	G
5.1.7	系统安全性进展报告(107)	管理	S	S	S	S
5.2.1	初步危险表(201)	工程	G	NA	NA	NA
5.2.2	初步危险分析(202)	工程	G	S	NA	NA
5.2.3	分系统危险分析(203)	工程	NA	S	G	GC
5.2.4	系统危险分析(204)	工程	NA	G	G	GC
5.2.5	使用和保障危险分析(205)	工程	S	G	G	GC
5.2.6	职业健康危险分析(201)	工程	G	S	NA	NA
5.2.7	工程更改建议的安全性评审(207)	管理	S	S	S	S
5.2.8	订购方提供的设备和设施的安全性分析(208)	工程	S	S	S	S
5.3.1	安全性验证(301)	工程	NA	S	S	S
5.3.2	安全性评价(302)	管理	NA	S	G	S
5.3.3	安全性符合有关规定的评价(303)	管理	NA	S	S	S
5.4.1	系统安全主管负责人的资格(401)	管理	S	S	S	GC
5.4.2	培训(402)	管理	S	S	S	GC
5.5.1	软件需求危险分析(501)	工程	S	S	S	GC
5.5.2	概要设计危险分析(502)	工程	S	S	S	GC

续表 A4

本标准条款编号	工 作 项 目	类型	规划和要求制定	方案设计	最终设计	建筑
5.5.3	详细设计危险分析(503)	工程	S	S	S	GC
5.5.4	软件编程危险分析(504)	工程	S	S	S	GC
5.5.5	软件安全性测试(505)	工程	S	S	S	GC
5.5.6	软件与用户接口分析(506)	工程	S	S	S	GC
5.5.7	软件更改危险分析(507)	工程	S	S	S	GC

注：符号说明同表 A3

d. 反映承制方对系统安全性要求的保证能力。

系统安全性工作计划的内容包括要实现的目标，组织及其职能，工作进度以及实施的方法。

对于大型系统在订购方对整个系统安全性工作有成熟意见时，或对于小型系统，可由订购方制定系统安全性工作计划。

A5.1.2 对转承制方、供应方和建筑工程单位的安全性综合管理(工作项目 102)。

承制方负责研制的系统中有一些项目要通过合同转给转承制方、供应方(以下简称转承制方)和建筑工程单位，承制方应将安全性要求及相应的工作通过转包合同分配给转承制方和建筑工程单位。承制方要确保转承制方和建筑工程单位所提供的设备和设施符合系统安全性要求。承制方的安全性大纲中应具有相应的管理措施，例如：考察转承制方和建筑工程单位对设备和设施的安全性保证能力；在转包合同中提出转包项目的安全性要求；参加一定的专题会议或评审活动；对转包项目的安全性大纲进行监督和控制；对转承制方和建筑工程单位的安全性工作给予必须的协助和指导；要求转承制方和建筑工程单位提供安全性信息等。

A5.1.3 安全性大纲评审(工作项目 103)

评审是对系统研制工作从一个阶段转入另一个阶段的重要决策手段。大纲评审中实际上包括了两种性质的安全性评审：

a. 安全性设计评审。主要评审安全性设计的可行性，以及系统的安全性是否达到合同规定的要求。这种评审是系统设计评审的一个重要组成部分。

b. 安全性工作评审。主要评审安全性工作项目的进展情况和关键问题。

在重大系统的研制初期，应至少每季度进行一次大纲评审，随着研制的深入，评审间隔时间可以延长。若有关的安全性鉴定部门有要求，需进行特殊的系统安全性评审。

A5.1.4 对系统安全性工作组的保障(工作项目 104)

订购昂贵、复杂或关键的系统、设备或重大设施时，若订购方有系统安全性工作组，为增强对安全性工作的管理，承制方向系统安全性工作组提供保障是有益的并可能是必须的。所需承制方保障程度应在合同中详细规定。

A5.1.5 建立危险报告、分析和纠正措施跟踪系统(工作项目 105)

承制方或订购方应坚持填写危险日志,在确定某个危险达到或超过订购方规定的最低限度后就应立即记入危险日志,并完整地记录消除危险或降低其有关风险采取的所有措施。订购方应确定必须消除的危险和可接受危险的风险水平。

A5.1.6 试验的安全性(工作项目 106)

必须尽早拟定试验计划,考虑需要进行危险分析的试验进度关键点和试验场所要求,并评审试验文件。

A5.1.7 系统安全性进展报告(工作项目 107)

承制方可按月或季度提交系统安全性进展报告,以便订购方及时了解系统安全性工作的进展情况。

A5.2 设计与分析

A5.2.1 初步危险表(工作项目 201)

承制方应尽早地提出初步危险表,订购方可根据其结果决定后续危险分析(初步危险分析、分系统危险分析等)的范围。

A5.2.2 初步危险分析(工作项目 102)

初步危险分析是系统研制阶段或设施订购的规划和要求确定阶段进行的危险分析的初步工作。

初步危险分析的目的是全面地识别危险状态及所有由此带来的系统的问题。初步危险分析也适用于初步考察现役系统的安全性状态。初步危险分析是其它危险分析的基础。

A5.2.2.1 初步危险分析至少应包括以下内容:

a. 评审相应的安全性历史资料;

b. 列出主要能源的分类表;

c. 调查各种能源,确定其控制措施;

d. 确定系统必须符合的有关人员安全、环境安全和有毒物质的安全性要求以及其它有关规定;

e. 提出纠正措施的建议。

A5.2.2.2 因为初步危险分析需在研制的初期进行,其分析资料可能不完整和不准确,所以应选择便于修改的分析模型,以便随设计的进行不断地修改和完善。若分系统的设计已达到可进行详细的分系统危险分析,则应终止初步危险分析。进行初步危险分析需以下信息:

a. 各种设计方案的系统和分系统部件的设计图纸和资料;

b. 在系统预期的寿命期内,系统各组成部分的活动、功能和工作顺序的功能流程图及有关资料;

c. 在预期的试验、制造、贮存、修理、使用场所和以前类似系统或活动中与安全性要求有关的背景资料。

A5.2.3 分系统危险分析(工作项目 203)

A5.2.3.1 应考察每个分系统或部件,以确定与使用或故障模式有关的危险,尤其是要确定部件的使用或故障对整个系统安全性的影响,还应确定消除已判定的危险或降低其风险所必

需的措施。

A5.2.3.2 当分系统的设计已足够详细或设施的订购进入方案设计阶段时，就可以进行分系统危险分析。分析应随设计的进行不断修改，也应评价部件的设计更改是否影响系统的安全性，应仔细选择分系统危险分析技术，以尽量减少给系统危险分析带来的问题。

A5.2.3.3 若分系统中的软件是按GJB137、GJB139要求开发的，在评价软件对分系统危险分析的影响时，承制方应监控和应用软件开发过程各阶段的输出结果，并向订购方报告需纠正的软件问题，以便于及时处理。

A5.2.4 系统危险分析(工作项目201)

A5.2.4.1 在初步设计评审点或设施方案设计评审点，就应开始系统危险分析，并应在设计完成前不断地修改。应评价设计更改以确定对系统及其分系统的安全性影响。在系统危险分析中应提出消除已判定的危险或降低其风险的纠正措施。

A5.2.4.2 系统危险分析应考察所有的分系统接口的下列方面：

a. 符合在系统或分系统要求文件中规定的安全性准则；

b. 对系统或人员会产生危险的独立或从属故障的各种可能组合，应考虑控制装置和安全装置的故障；

c. 系统及分系统的正常使用会怎样降低系统的安全性；

d. 对设备或人员会产生新危险的系统、分系统中的接口、逻辑与软件的设计更改；

应仔细选择系统危险分析技术，以尽量减少给系统危险分析与其它危险分析的综合分析带来的问题。

A5.2.4.3 若系统中的软件是按GJB137、GJB139要求开发的，在评价软件对系统危险分析的影响时，承制方应监控和应用软件开发过程各阶段的输出结果，并向订购方报告需纠正的软件问题，以便于及时处理。

A5.2.5 使用和保障危险分析(工作项目205)

A6.2.5.1 承制方应对以下活动进行使用和保障危险分析：系统制造、部署、安装、装配、试验、使用、维修、运输、贮存、改装、退役和处理。当系统的设计或使用条件变动时，承制方应修改使用和保障危险分析。使用和保障危险分析也可有选择地应用在设施订购中，以保证使用和维修手册中含有合理的安全性及健康要求。

A5.2.5.2 应尽早地进行使用和保障危险分析，为系统设计提供输入信息。在系统试验和使用前也应进行本分析。使用和保障危险分析工作作为闭环重复过程是非常有效的，所以在系统的设计更改前，应采用使用和保障危险分析，评价工程更改建议。使用和保障危险分析需以下信息：

a. 系统、保障设备和设施的说明；

b. 规程和操作手册草案；

c. 初步危险分析、分系统危险分析和系统危险分析报告；

d. 有关的要求、约束条件和人员能力；

e. 人素工程资料和报告；

f. 经验教训，包括以往入为差错造成的事故。

A5.2.5.3 为有效地实现使用和保障危险分析的目标，应将其分析结果分发到各有关部门。应仔细选择使用和保障危险分析技术，以尽量减少给使用和保障危险分析与其它危险分析的综合分析带来的问题。

A5.2.6 职业健康危险分析(工作项目 206)

A5.2.6.1 职业健康危险分析的第一步是确定涉及系统及其保障的潜在有毒物质数量或物理因素的量级；下一步是分析这些物质或物理因素与系统及其保障的关系，根据这些物质或物理因素的量级、类型以及与系统及其保障的关系评价人员可能接触的场合、方式及接触频度(如可能)；最后一步是在系统及其保障设备或设施的设计中采用经济效益好的控制措施，将人员与有毒物质或物理因素的接触降低到可接受水平。若控制措施的寿命周期费用很高，则需考虑更改系统设计方案。

A5.2.6.2 职业健康危险分析不是要求按健康防护来支配系统的设计，而是保证决策人员了解系统中的健康危险及其影响，以便权衡作出合理的决策。

A5.2.6.3 应考虑以下与系统及其保障有关的因素：

a. 物质的毒性、数量及物理状态；

b. 有毒物质或物理因素的使用及释放；

c. 意外接触的可能性；

d. 产生的危险废物；

e. 有毒物质的装卸、输送与运输要求；

f. 防护服或保护设备的需求；

g. 定量接触水平所需的检测设备；

h. 可能处于危险下的人数；

i. 可能使用的工作控制手段，例如：隔离、封闭、通风、噪声或辐射屏蔽等。

A5.2.6.4 订购方应根据对化学物理因素接触极限的有关规定，或与生物环境工程部门(或医务部门)协商，确定健康危险的可接受风险水平。

A5.2.7 工程更改建议的安全性评审(工作项目 207)

必须评价工程更改对系统安全性的影响。往往纠正一个缺陷时，由于疏忽可能引入另外的缺陷，所以需进行工程更改的安全性评审，以防止引入新的危险。若工程更改降低了系统的安全性水平，则必须得到订购方的认可。

A5.2.8 订购方提供的设备和设施的安全性分析(工作项目 208)

仅当订购方提供的设备和设施与承制方开发的硬件或软件直接连接时，才需要进行本分析工作。

承制方应通过收集已有的分析文件，充分地了解订购方提供的设备和设施的有关危险及其风险的控制措施，然后将其用于系统设计中。若无有效的分析文件，承制方应进行必要的分析，以确保其接口的安全性。

A5.3 验证与评价

A5.3.1 安全性验证(工作项目 301)

A5.3.1.1 在系统说明书、系统要求等文件中规定的安全性要求，许多需要通过分析、检查

演示或试验来验证。此外，在设计和研制期间，为消除危险所采用的重新设计、控制装置、安全装置等措施也需验证。

A5.3.1.2 大多数安全性验证将在系统和分系统试验计划和规程中概述，但对研制过程中判定的危险所采取的风险控制措施的验证，可能需要制定特殊的试验计划和规程。

A5.3.1.3 应考虑用诱发故障或模拟故障来验证安全性关键的设备和软件的可接受性及其故障模式，对研制期间所发现的危险，如果用分析或检查无法确定所采取的措施能否有效时，则应进行安全性试验以评价所采取的措施的有效性，应将该试验包含在系统安全性工作计划及试验计划中。若安全性试验工作因费用高而不可行时，安全性特性或规程可由工程分析、类推、试验室试验、功能模拟或小尺寸模拟来验证，这些方法都要经过订购方的认可。应尽可能地将安全性试验纳入系统试验和演示计划中。

A5.3.2 安全性评价（工作项目 302）

安全性评价的重要性在于使用户或试验人员了解系统所有残余的不安全设计或操作特性。安全性评价应尽可能地对未能消除危险的风险进行定量的评价，以确定控制措施、禁止事项或安全规程。

A5.3.3 安全性符合有关规定的评价（工作项目 303）

A5.3.3.1 安全性符合有关规定的评价是要验证系统的安全性设计，并对在系统的使用或试验之前所假定的风险进行综合评价。这是一种针对使用的分析，涉及系统、设备或设施的安全使用，几乎涉及到系统的各个方面。但该评价是一般性的，只需深入到验证系统的安全性或确定各种风险及系统安全使用必要的防护措施所需的程度。该评价可能是低风险的系统中唯一的分析工作，也可作为试验或使用前的安全性评审，以综合在更详细的危险分析中所发现的使用安全性问题。

系统的低风险可能是：

a. 系统主要是由现成设备装配而成，很少或根本没有新的设计；

b. 是一个在其技术上或复杂程序上本来就是低风险的系统；

c. 符合国家标准、国家军用标准或行业标准及其有关规定，足以保证系统的安全性。

安全性符合有关规定的评价也可用于必须接受的有较高风险的系统（例如先进的研制项目），但仍需保证安全使用，必须识别危险并将其风险减少到可接受的水平。

A5.3.3.2 本评价可以系统研制的任何阶段进行，当有足够的信息时，就应立即开始评价工作。例如，对设备的评价应该从设备部件的设计时或从转承制方或供应方接收设备说明书时开始。

A5.3.3.3 安全性符合有关规定的评价至少应包括以下内容：

a. 有关安全性标准的确定及系统符合标准情况的验证。订购方可能在说明书或其它合同文件中规定了有关标准，但并不妨碍承制方应用其它适用的标准。承制方也应考察现有类似系统的安全性历史资料。验证工作可通过几种方法完成，包括分析、检查、试验等。

b. 系统危险的分析与处理。即使系统全部由完全符合有关标准的设备组成，也可能由于独特的使用、接口、安装等产生危险，本评价的另一目的是要确定、评价和消除这类危险，或将其有关风险减少到可接受水平。为达到这一目的，本评价应采用其它危险分析的技术，以保证

获得安全的系统。

c. 确定特殊的安全性要求。承制方应根据上述分析得出安全性设计特性和其它必须的预防措施，确定系统安全使用及保障所需的所有安全性防护措施，包括系统以外的或承制方职责外的可行的防护措施。例如，由于合同未考虑现成设备的重新设计或改装，或承制方可能不负责提供必需的应急信号灯、防火设备或人员安全设备，因此，其风险必须用特殊的安全设备和通过培训来控制。

d. 确定危险器材及其安全使用所需的防护措施和规程。

A5.4 安全性培训

A5.4.1 系统安全性主管负责人的资格(工作项目 401)

某些系统要求系统安全性主管负责人要具有特定的资格，其资格要求可采用本标准中工作项目 401 中的部分或全部规定，或者由订购方规定的最低资格要求。必须时，应对有关人员进行培训，以提供获取资格的机会。

A5.4.2 培训(工作项目 402)

A5.4.2.1 许多安全性大纲要求对系统研制、试验和使用人员进行资格培训。完善的安全性大纲只有在所有参予者都清楚各自的工作时才能有效地实施。为设计无危险的系统，承制方的设计工程师需懂得基本的系统安全性原理。完善的培训计划首先应培训设计工程师；也需对负责人进行培训，使其认识到及早地进行安全性设计的重要性，以避免重新设计或更改设计；需对承制方和订购方试验人员进行设备的安全装卸、操作及试验方面的培训；需对使用和维修人员进行其相应的安全性培训。

A5.4.2.2 可用不同的方法进行培训，并应进行考核，其中进行正式的课堂培训是最有效的方法。

A5.4.2.3 承制方的安全性培训计划应在系统安全性工作计划(工作项目 101)中详细叙述。

A5.5 软件系统安全性

软件系统安全性工作的目的是：

a. 确定系统和系统中软件的安全性要求；

b. 确保安全性说明书中的要求准确地转化为系统或部分系统说明书和软件需求规格说明的要求，并将系统或部分系统说明书和软件需求规格说明中的安全性要求准确地转化为软件的设计和编程；

c. 确保在系统或部分系统说明书和软件需求规格说明中明确地规定需用的安全性准则，包括故障安全保护、故障可起动、故障可用、故障仍可工作和故障可自动恢复等；

d. 确定控制或影响安全性关键的硬件功能的计算机软件成分，这些成分应指定为安全性关键的计算机软件成分；

e. 对为会导致或促成影响安全性的事件、故障和环境而设计或执行的安全性关键的计算机软件成分及其系统接口进行分析；

f. 分析安全性设计要求的实现，以确保达到要求的目标，分析应验证不存在损害安全性特性的单个或可能的多重故障. 安全性要求的实现应不会引起新的危险或对其它安全性要求有不利的影响；

g. 确保实际编制的软件不会引起危险的功能或妨碍正常的功能，而产生危险状态；

h. 有效地减轻系统硬件危险的异常现象；

i. 确保充分测试安全性设计要求，包括故障测试。

进行软件系统安全性分析的技术和方法有：

a. 软件故障树分析；

b. 软件潜在分析；

c. 设计预排；

d. 编程预排；

e. 皮特里网络分析；

f. 软件与硬件综合的关键路径分析；

g. 核安全性交叉校验分析；

h. 交叉参考列表分析。

由于各种技术和方法有不同的侧重点，故对具体软件成分详尽的软件危险分析可能需应用多种方法。此外，应用良好的软件工程经验是设计安全的和便于分析的软件所必不可少的。

软件系统安全性分析必须在论证阶段的早期开始，并应设计得易于修改。为确保有效的分析，需以下信息：

a. 系统或部分系统说明书、软件需求规格说明、接口要求说明书和其它说明系统各种软件—软件、软件—硬件、软件—操作员的接口和系统可能遇到的正常和异常环境的配置文件；

b. 在系统预期的寿命周期内，系统各组成部分的活动、功能和工作顺序和时序的功能流程图、时序图和相关资料；

c. 计算机程序功能流程图(或其相当的功能资料)，程序的设计语言、贮存和时序配置图以及其它的程序结构文档；

d. 涉及计划的测试、生产、运输、装卸、贮存、修理、预期的工作和保障环境及类似程序或活动的经验教训的与安全性要求有关的基本信息；

e. 已知的危险事件源，包括能源和有毒物质源，特别是可由软件控制的事件源；

f. 软件开发计划、软件质量评估计划、软件配置管理计划和其它的系统和分系统开发计划文档；

g. 系统测试计划、软件测试计划和其它测试文档。

应将软件危险分析整理成文，作为系统安全性危险分析报告的组成部分。

A5.5.1 软件需求危险分析(工作项目 501)

A5.5.1.1 软件需求危险分析应利用初步危险表(工作项目 201)和系统级的初步危险分析(工作项目 202)的结果，应从总体上检查安全性关键的计算机软件成分，以获得软件系统的初步安全性评价。软件需求危险分析的结果可作为其它安全性分析的输入。安全性关键的计算机软件成分要用概要设计危险分析和详细设计危险分析作进一步的分析。

A5.5.1.2 软件需求危险分析工作在作系统要求分配时开始。首先，软件需求危险分析应建立软件安全性需求的跟踪系统，记录每个需求的实现情况。本分析也应完整地评审和分析软件的需求，旨在确定现行的需求(以及由初步危险表和系统级的初步危险分析得出的需求)，并保

证把那些需求准确地纳入软件需求规格说明中。

此外，分析应得出需要的和建议的工作，以消除判定的危险，或将有关的风险减少到可接受水平，并提出初步测试需求。本工作一般包括以下内容：

a. 评审系统或部分系统说明书、分系统说明书、软件需求规格说明、接口要求说明书和其它系统方案及要求文件，确保：

已将安全性要求分配到软件；

已确定出初步危险表和系统级的初步危险分析得出的危险；

由系统说明书到详细软件规格说明中的安全性要求的可跟踪性。

b. 分析功能流程图(或其相应的功能资料)、程序设计语言、数据流图、贮存和时序分配图表及其它程序文档，以确保满足规格说明和安全性需求。

A5.5.2 概要设计危险分析(工作项目 502)

概要设计危险分析在软件要求评审后开始，并根据软件需求危险分析细化概要设计危险分析，它应包括：

a. 确定出初步危险分析、分系统危险分析和软件需求危险分析判定的危险与具体的计算机软件成分的关系，并将控制或影响危险的计算机软件成分确定为安全性关键的计算机软件成分；

b. 检验软件以确定计算机软件成分之间是否相关和相关的程度，直接或间接影响安全性关键的计算机软件成分的软件单元也要确定为安全性关键的计算机软件成分，并分析其不希望的影响；

c. 分析安全性关键的计算机软件成分的概要设计是否符合安全性需求，并将分析结果送交软件设计人员和系统负责人；

概要设计危险分析的结果应在概要设计评审时提交，并作为评审内容的一部分。

A5.5.3 详细设计危险分析(工作项目 503)

A5.5.3.1 承制方可应用软件需求危险分析和概要设计危险分析的结果分析软件的详细设计。分析工作应在概要设计评审后开始，根据概要设计危险分析而细化，是概要设计危险分析的继续。分析应在软件编制前基本上完成，其结果在详细设计评审时提交。

A5.5.3.2 本分析应包括分析由输入或输出时序、多重事件、失序事件、事件失败、错误事件、不恰当的数值、不利环境、死锁和硬件故障敏感性等可能引起的错误。

A5.5.3.3 本分析应包括以下内容：

a. 确定出初步危险分析、软件需求危险分析和概要设计危险分析判定的危险与具体的低层次计算机软件成分的关系，并将控制或影响危险的成分确定为安全性关键的计算机软件成分。必须分析其正确性及其不希望的影响；

b. 考察软件以确定低层次软件成分之间是否相关和相关的程度，直接或间接影响安全性关键的计算机软件成分的软件单元也确定为安全性关键的计算机软件成分。必须分析其正确性及其不希望的影响；

c. 分析安全性关键的计算机软件成分的详细设计是否符合安全性设计要求，并将分析的结果送交软件设计人员和系统负责人；

d. 确定要包括在测试计划、说明和规程中的需求；

e. 确定要包括在计算机系统操作员手册、软件用户手册、计算机系统诊断手册、固件保障手册以及其它手册中的需求；

f. 确保程序编制人员了解哪些是安全性关键的计算机软件成分，向程序编制人员提供与安全性有关的编制建议和需求。

本分析的结果和在本分析前进行的所有安全性分析的结果应在详细设计评审时提交，并作为评审内容的一部分。

A5.5.4 软件编程危险分析(工作项目 504)

本分析考察安全性关键的计算机软件成分和其它计算机软件成分的源程序和目标程序，以验证设计实现情况。该工作必须与编程同时开始，并不断修改直至完成软件的测试。本分析应确定消除已判定的危险或将有关的风险减少到可接受水平所需的工作。分析人员应参与程序的评审、预排及程序的匹配评审。本分析应考察：

a. 安全性关键的计算机软件成分的正确性以及输入或输出时序、多重事件、错误事件、失序、不利环境、死锁、不恰当的数值和其它敏感类型；

b. 软件成分中可能导致或促成影响安全性的不希望事件的设计或编程错误；

c. 安全性关键的计算机软件成分是否符合适用的系统或部分系统说明书或软件需求规格说明中提出的安全性准则。必须在源程序和目标程序级以及在概要和详细设计层次考察软件的安全性关键的部分。

d. 安全性关键的计算机软件成分的安全性设计需求的实现情况，以确保满足需求的目标。分析人员应确保外围硬件或其它模块的单个或可能的多重故障不会影响软件的安全性特性。进行的软件测试应能测试出安全性特性，包括故障模式和中止路径测试；

e. 使系统在危险方式下运行的独立、从属或交叉相关的硬件或软件故障，非设计的程序转移、单个或多重事件、或失序事件的可能组合；

f. 过界、过载输入状态或它们的多重组合。

此外，本分析要求评审正在制订的软件文档以确保其中包括了软件的安全性特性和需求。软件编程危险分析的结果应在测试准备状态评审时提交，作为评审内容的一部分。编制程序时，必须及时向程序员提供低层次单元的软件编程危险分析结果。

A5.5.5 软件安全性测试(工作项目 505)

完成一个软件单元的编程后应立即开始测试较低层次的单元，软件的系统级测试在通过测试准备状态评审后开始，承制方的安全性工作人员进行的测试和测试保障包括以下内容：

a. 对安全性关键的计算机软件成分进行适当的安全性测试以确保所发现的危险已消除或已将风险减少到可接受水平；

b. 为了测试安全性关键的计算机软件成分的安全和正确地运行，应向测试工作人员提供测试过程，用例和输入；

c. 确保按批准的测试过程测试所有的安全性关键的计算机软件成分，并准确地记录测试结果；

d. 不仅在正常的状态下还要在异常的环境和输入状态下测试软件，确保在这些状态下软

件正确地和安全地运行；

e. 进行软件应力测试和验收测试以确保软件在应力状态下正确地和安全地运行；

f. 无论是否修改了外购软件，均需确保该软件在系统内正确地和安全地运行；

g. 无论是否修改了订购方提供的软件，均需确保该软件在系统内正确地和安全地运行；

h. 确保在系统综合和系统验收测试中发现的危险和缺陷已得到纠正和重新测试，以保证无遗留问题。

A5.5.6 软件与用户接口分析(工作项目 506)

应确定用户与程序的接口以确保系统安全地工作。甚至在做完所有的安全性分析和设计更改后，系统中仍可能存在不能通过设计消除或严格控制的危险，因此，必须制定下列工作规程：

a. 提供检测危险征兆或潜在危险状态的方法以预防危险的发生；

b. 控制危险使得只有在特殊的情况下和操作员特定的命令下才发生；

c. 向操作员、用户和其它人员提供报警的功能，指示可能即将出现或正在出现的潜在危险状态；

d. 确保发生危险后系统能够生存；

e. 若预防和控制规程失败，或危险已发生，提供损坏控制和恢复规程；

f. 提供在 II 级危险状态下生存和恢复的规程；

g. 根据需要，提供安全地中止或取消一个事件、过程或程序的能力；

h. 向操作员提供系统或软件故障报警的功能，并确保操作员了解所有同时存在的故障，这可能会改变消除或超越故障的方式；

i. 确保危险数据显示明确，并向操作员提供作出安全性关键决策所需的所有数据。

A5.5.7 软件更改危险分析(工作项目 507)

更改危险分析是考察和分析说明书、要求、设备、软件设计、源程序和目标程序的更改(包括修改和修补)对安全性的影响。若不进行更改分析，则更改后系统就不能认为是安全的，分析应包括以下内容：

a. 分析系统、分系统、接口、逻辑、规程和软件的设计更改以及程序更改对安全性的影响，确保更改不会产生新的危险，不会影响已解决的危险，不会使现存的危险变得更严重，和不会对任何有关的(或接口的)设计或程序有不利的影响；

b. 对更改进行测试，以确保新的软件中不包含危险；

c. 确保将更改适当和正确地纳入编程中；

d. 评审和修改有关文档以反映这些更改；

e. 将执行本工作项目的方法和过程纳入软件配置管理计划。

附加说明：

本标准由航空航天工业部提出。

本标准由航空航天工业部三0一所负责起草。

本标准主要起草人：张红春、杨兆生、王立群、赵世宗。