

信息安全丛书

信息系统 安全工程学

关义章 蒋继红 编著
方关宝 戴宗坤

金城出版社



信息安全丛书

信息系统安全工程学

关义章 蒋继红 编著
方关宝 戴宗坤

金城出版社

图书在版编目(CIP)数据

信息系统安全工程学/关义章等编著. —北京:金城出版社, 2000.9
ISBN 7-80084-303-3

I.信… II.关 III.信息系统-安全技术 IV.G202

中国版本图书馆 CIP 数据核字(2000)第 69818 号

金城出版社出版发行

(北京市朝阳区和平街 11 区 37 号楼 100013)

河北省高碑店市鑫昊印刷有限责任公司印刷

787×1092 毫米 1/16 16.5 印张 410 千字

2000 年 9 月第 1 版 2001 年 5 月第 4 次印刷

*

ISBN 7-80084-303-3/T·5

定价: 29.50 元

前 言

本书(《信息系统安全工程学》)是四川大学信息安全研究所为信息安全工程专业本科生和研究生教学而组织编写的两本专业教材之一。《信息系统安全》和《信息系统安全工程学》这两本专业教材,前者重点在于给出信息系统安全的基础理论背景知识、安全体系结构、支持安全体系的安全服务框架及其机制性技术,以及信息系统安全测试评估的体系及基本知识;后者着重从系统工程方法切入,对信息系统安全工程生命期各阶段的准备、实施、过程监控及反馈、调整进行系统描述。可以说,这两本书可互为姊妹篇。就两本书所涉猎的范围和知识广度而言,它们对于从事信息系统管理、工程设计、施工、质量控制的各类技术和管理人员均会有所帮助。

本书包括四篇十一章。第一篇系统工程有三章,介绍了系统开发总体的系统方法,系统工程过程要求,以及系统工程的详细要求,是全书的基础。第二篇信息系统安全工程由第四、五、六章构成,首先介绍了信息系统安全工程和系统工程的关系,然后详细地讨论了信息系统生命周期安全工程的各个阶段,以及信息系统安全工程的基本功能,是本书的重点之一。第三篇信息安全测评和认证包括第七、八、九、十章,在介绍我国信息安全测评认证体系后,详细地讨论了测评方法和准则,是本书的另一重点。第四篇信息系统安全工程示例,用两章篇幅,分别详细介绍了政务信息系统工程和金融信息系统工程,是信息系统安全工程方法的具体运用和实践,相信对于理解和掌握信息系统安全工程方法有所裨益。

全书取材新,涉及的内容十分广泛,对于本科生、研究生的学习,可在内容、重点和深度方面根据学时数进行选择。

本书由四川大学信息安全研究所组织。关义章、蒋继洪、戴宗坤、刘永澄、罗万伯、唐三平等参与结构设计。关义章主笔撰写第1、2、3、11和12章,蒋继洪主笔撰写第4、5和6章,方关宝主笔撰写第7、8、9和10章。关义章、戴宗坤参加了全过程的组织和协调。全书由戴宗坤统稿,罗万伯、唐三平、戴云燕等参与了部分文字校订工作,罗万伯、戴云燕编辑了全部附录。本书的三位主笔是四川大学的兼职教授,它的顺利出版是四川大学和信息产业部电子第30所在信息安全人才培养方面精诚合作的结果。

本书从策划到编写完成,一直得到中国工程院院士何德全教授的热情鼓励和指导以及中国信息安全测评认证中心吴世忠、罗建中研究员的大力支持。四川大能士信息技术有限公司的领导、信息产业部电子第30所的领导,以及四川大学信息安全研究所全体同志为本书的完成提供了优越的工作环境和多方面的帮助。同时从其他各位老师和同行的著作(包括网站)中也得到了帮助。作者在此一并表示衷心的感谢。

由于书稿涉及许多新内容和研究课题,尽管作者已尽了最大努力,仍自感问题难免。望读者不吝赐教斧正,以利再版修订,至臻完美,为推动我国信息系统安全工程高级技术人才的培养共同出力。

作 者

2000年8月10日

目 录

第一篇 系统工程	(1)
第 1 章 系统工程概述	(1)
1.1 范围和背景	(1)
1.1.1 范围	(1)
1.1.2 背景	(1)
1.2 系统工程及过程	(3)
第 2 章 系统工程过程要求	(4)
2.1 要求分析	(4)
2.1.1 要求	(4)
2.2 功能分析/分配	(4)
2.2.1 功能性分析	(5)
2.2.2 分配	(5)
2.3 综合	(5)
2.3.1 设计	(5)
2.3.2 设计认证	(6)
2.4 系统分析与控制	(6)
2.4.1 折中研究	(6)
2.4.2 系统/成本效益性能分析	(7)
2.4.3 风险管理	(7)
2.4.4 配置管理	(7)
2.4.5 接口管理	(8)
2.4.6 数据管理	(8)
2.4.7 系统工程主进度表(SEMS)	(8)
2.4.8 技术性能测量(TPM)	(8)
2.4.9 技术评审	(9)
2.4.10 对变化的响应	(9)
第 3 章 系统工程的详细要求	(10)
3.1 系统工程规划	(10)
3.1.1 系统工程管理计划(SEMP)	(10)
3.1.2 系统工程主进度表(SEMS)	(11)
3.1.3 系统工程详细进度(SEDs)	(12)

3.2 功能性任务	(12)
3.2.1 可靠性和可维护性	(12)
3.2.2 生存能力	(12)
3.2.3 电磁兼容性和无线电频率管理	(13)
3.2.4 人的因素	(13)
3.2.5 系统保险及健康的危害	(13)
3.2.6 系统安全	(13)
3.2.7 可生产性	(13)
3.2.8 综合的后勤支持(ILS)	(14)
3.2.9 测试和评估	(14)
3.2.10 综合故障诊断	(14)
3.2.11 可运输性	(14)
3.2.12 基础设施支持	(15)
3.2.13 其它功能领域	(15)
3.3 杠杆选择	(15)
3.3.1 非开发项目(NDI)	(15)
3.3.2 开放系统体系结构(OSA)	(15)
3.3.3 重用	(15)
3.3.4 双重使用的技术	(16)
3.4 普遍深入的开发考虑	(16)
3.4.1 计算机资源	(16)
3.4.2 材料、过程和部件控制	(16)
3.4.3 原型	(16)
3.4.4 仿真	(16)
3.4.5 数字数据	(16)
3.5 系统/成本有效性	(17)
3.5.1 制造分析及评估	(17)
3.5.2 认证分析和评估	(17)
3.5.3 部署分析和评估	(17)
3.5.4 运行分析和评估	(18)
3.5.5 支持性分析和评估	(18)
3.5.6 培训分析和评估	(18)
3.5.7 处理分析和评估	(19)
3.5.8 环境分析和效果评审	(19)
3.5.9 生命期成本分析和评估	(19)
3.5.10 模型	(19)
3.6 实现任务	(19)
3.7 技术评审	(20)
3.7.1 评审的责任	(20)
3.7.2 结构评审	(20)

3.7.3 代替方案的系统评审(ASR)	(21)
3.7.4 系统要求评审(SRR)	(21)
3.7.5 系统功能评审(SFR)	(21)
3.7.6 预先设计评审(PDR)	(22)
3.7.7 关键的设计评审(CDR)	(23)
3.7.8 系统认证评审(SVR)	(23)
3.7.9 物理配置的审计(PCA)	(23)
3.7.10 子系统评审	(24)
3.7.11 功能评审	(26)
3.7.12 临时系统评审	(26)
3.8 系统工程能力评估	(26)
 第二篇 信息系统安全工程(ISSE)	(27)
第4章 基本概念及其与系统工程的关系	(27)
4.1 概述	(27)
4.2 系统工程	(28)
4.3 信息系统安全工程	(31)
4.3.1 系统安全工程流程	(31)
4.3.2 信息系统安全工程的各“阶段”概述	(31)
4.4 与系统获取的关系	(37)
4.4.1 任务需求的确定(先期概念阶段)	(38)
4.4.2 阶段0——概念研究和定义	(38)
4.4.3 阶段1——演示与确认	(38)
4.4.4 阶段2——设计和制造开发	(39)
4.4.5 阶段3——生产和部署	(39)
4.4.6 阶段4——运行与支持	(39)
 第5章 信息系统生命期安全工程	(40)
5.1 先期概念阶段	(40)
5.2 概念阶段	(41)
5.3 要求阶段	(41)
5.4 系统设计阶段	(42)
5.5 初步设计阶段	(43)
5.6 详细设计阶段	(43)
5.7 实现和测试阶段	(44)
5.8 配置审计阶段	(45)
5.9 运行和支持阶段	(45)

第 6 章 ISSE 基本功能	(47)
6.1 安全规划与控制	(49)
6.1.1 商业决策和工程规划	(49)
6.1.2 ISSE 梯队	(50)
6.1.3 规划 ISSE 对认证和认可(C&A)的输入	(51)
6.1.4 ISSE“报告”	(52)
6.1.5 技术数据库和工具	(54)
6.1.6 与获取/签合同有关的规划	(55)
6.1.7 INFOSEC 保证规划	(57)
6.2 安全要求的确定	(60)
6.2.1 系统要求定义综述	(60)
6.2.2 安全要求分析的一般课题	(62)
6.2.3 安全要求定义综述	(65)
6.2.4 先期概念阶段和概念阶段——ISSE 的要求活动	(68)
6.2.5 要求阶段——ISSE 的要求活动	(69)
6.2.6 系统设计阶段——ISSE 的要求活动	(69)
6.2.7 从初步设计到配置审计阶段——ISSE 的要求活动	(70)
6.3 安全设计支持	(70)
6.3.1 系统设计	(70)
6.3.2 ISSE 系统设计支持活动	(71)
6.3.3 先期概念和概念阶段安全设计支持	(73)
6.3.4 要求和系统设计阶段的安全设计支持	(74)
6.3.5 初步设计阶段到配置审计阶段的安全设计支持	(75)
6.3.6 运行和支持阶段安全设计支持	(75)
6.4 安全操作分析	(75)
6.5 生命周期安全支持	(77)
6.5.1 安全的生命期支持的开发方法	(77)
6.5.2 部署的系统的安全监控	(79)
6.5.3 系统安全评价	(80)
6.5.4 配置管理	(80)
6.5.5 培训	(81)
6.5.6 后勤和维护	(81)
6.5.7 系统的修改	(82)
6.5.8 处理	(82)
6.6 安全风险的管理	(83)
6.6.1 安全的验证和确认	(83)
6.6.2 安全风险的管理(SRM)	(85)
6.6.3 安全风险分析和 C&A	(88)

第三篇 信息安全测评认证体系	(90)
第7章 组织体系	(90)
7.1 我国信息安全测评认证体系的发展概况	(90)
7.2 国家信息安全测评认证管理委员会	(91)
7.2.1 性质	(91)
7.2.2 宗旨	(92)
7.2.3 管委会的组成和机构设置	(92)
7.2.4 管委会职责	(92)
7.2.5 管委会议事规则	(94)
7.2.6 经费	(94)
7.2.7 罚则	(95)
7.3 中国国家信息安全测评认证中心	(95)
7.3.1 中国国家信息安全测评认证中心的性质	(95)
7.3.2 中国国家信息安全测评认证中心的主要职责	(95)
7.3.3 中国国家信息安全测评认证中心的组织领导	(95)
7.3.4 中国国家信息安全测评认证中心的经费来源	(96)
7.4 中国国家信息安全测评认证中心测试实验室	(96)
第8章 标准体系	(97)
8.1 评估所依据的标准	(97)
8.2 我国现有的 FP(保护轮廓)	(97)
8.3 ISO 9000 簇	(97)
8.3.1 ISO 9000 簇标准的构成	(97)
8.3.2 质量管理和质量保证标准的应用	(99)
第9章 技术体系	(102)
9.1 标识和鉴别	(102)
9.1.1 登录控制	(102)
9.1.2 口令字选择	(102)
9.1.3 鉴别数据保护	(102)
9.1.4 会话挂起	(102)
9.1.5 用户帐号和轮廓	(102)
9.2 访问控制	(103)
9.2.1 自主访问控制(DAC)	(103)
9.2.2 DAC 属性控制	(103)
9.2.3 强制访问控制(MAC)	(103)
9.2.4 MAC 属性控制	(103)
9.2.5 输入/输出	(103)
9.2.6 信息标号	(103)

9.2.7 对象重用	(104)
9.2.8 基于角色的访问控制(RBAC)	(104)
9.2.9 RBAC 属性控制	(104)
9.2.10 防火墙访问控制	(104)
9.3 审计	(104)
9.3.1 审计事件	(104)
9.3.2 入侵检测和响应	(104)
9.3.3 审计迹保护	(105)
9.4 审计迹分析/浏览	(105)
9.4.1 完整性	(105)
9.4.2 TOE 完整性	(105)
9.4.3 数据鉴别	(105)
9.5 可用性	(105)
9.5.1 资源消费量	(105)
9.5.2 错误处理	(105)
9.5.3 工作安排	(105)
9.6 私密性	(106)
9.6.1 基于用户身份的私密性	(106)
9.6.2 基于资源/服务的私密性	(106)
9.7 数据交换要求	(106)
9.7.1 数据交换机密性	(106)
9.7.2 数据交换完整性	(106)
9.7.3 抗抵赖	(106)
第 10 章 测评认证	(107)
10.1 测评认证的定义	(107)
10.2 申请资格	(107)
10.3 测评认证类型	(107)
10.4 认证程序	(107)
10.5 型号认证和产品认证	(107)
10.5.1 意义	(107)
10.5.2 认证申请方式	(108)
10.5.3 认证活动的主要阶段及时间	(108)
10.5.4 认证活动各阶段主要内容	(108)
10.5.5 投诉/申诉	(111)
10.6 国家信息安全测评认证产品认证申请书(格式示意)	(111)
10.7 信息安全测评认证	(118)
10.7.1 信息安全测评认证业务内容	(118)
10.7.2 认证申请方式	(118)
10.7.3 认证活动的主要阶段及时间	(118)

10.7.4 认证活动各阶段主要内容	(118)
10.7.5 投诉/申诉	(120)
10.8 国家信息安全测评认证信息系统(网络)评估申请书(格式示意)	(121)
第四篇 信息系统安全工程示例	(128)
第 11 章 政务网系统安全	(128)
11.1 政务网资源和服务及网络拓扑	(128)
11.1.1 政务网的资源	(128)
11.1.2 政务网的服务和应用	(131)
11.2 政务网拓扑	(131)
11.3 政务网的安全需求分析	(131)
11.4 政务网的安全风险分析	(134)
11.5 政务网的安全保密规划与设计	(137)
11.5.1 政务网安全保密方针	(137)
11.5.2 政务网安全设计原则	(138)
11.5.3 政务网安全目标	(139)
11.5.4 安全保密技术	(140)
11.6 主要安全机制及其实现方法	(142)
11.6.1 物理安全防护	(142)
11.6.2 访问控制	(142)
11.6.3 安全鉴别	(143)
11.6.4 权限控制	(143)
11.6.5 通信保密	(143)
11.6.6 数据完整性	(143)
11.6.7 数字签名	(144)
11.6.8 安全审计	(144)
11.6.9 病毒防范	(144)
11.6.10 系统安全备份	(145)
11.7 政务网安全措施	(145)
11.7.1 概述	(145)
11.7.2 制定政务网的安全策略应当考虑的因	(145)
11.7.3 具体安全措施	(149)
11.8 安全管理	(153)
11.8.1 安全组织管理	(153)
11.8.2 结束语	(163)
第 12 章 金融信息系统总体安全考虑	(164)
12.1 概述	(164)
12.2 系统设计的目标	(164)

12.3 系统安全风险和威胁分析	(165)
12.3.1 安全环境	(165)
12.3.2 被动攻击	(168)
12.3.3 主动攻击	(168)
12.3.4 攻击造成的后果	(168)
12.4 交易所综合网络的资源	(169)
12.5 系统安全需求	(171)
12.6 设计原则	(171)
12.7 安全策略及安全体系设计	(172)
12.7.1 安全策略	(172)
12.7.2 安全体系	(172)
12.8 系统安全设计	(173)
12.8.1 各经纪公司业务处理安全	(173)
12.8.2 配置说明	(173)
12.8.3 金融数据加密机的密钥管理	(174)
12.9 远程交易安全	(176)
12.9.1 设计一:经纪公司独立管理方式	(177)
12.9.2 Internet 网上交易安全	(178)
12.10 大楼局域网安全	(178)
12.10.1 网络安全	(178)
12.10.2 基于 VPN 设备(IP 密码机)的安全设计	(181)
12.10.3 基于数据密码机的安全设计	(182)
12.10.4 系统安全审计和监控	(182)
12.10.5 物理安全	(182)
12.10.6 病毒防范	(183)
12.10.7 安全方案特点	(183)
12.11 安全方案实施	(183)
12.12 安全管理	(184)
12.13 结束语	(184)
12.14 设备简介	(184)
12.14.1 安全交易受理机	(184)
12.14.2 安全服务器	(184)
12.14.3 个人桌面安全机	(184)
12.14.4 审计监控服务器	(185)
12.14.5 网络加密机	(185)
12.14.6 金融数据密码机系列	(186)
12.14.7 数据密码机	(187)
12.14.8 防火墙	(187)
12.14.9 安全文电系统	(188)
12.14.10 密钥管理中心(发卡中心)	(188)

12.14.11 防电磁辐射设备·····	(189)
12.14.12 防病毒系统·····	(189)
附录 A 参考文献·····	(191)
附录 B 缩略语·····	(193)
附录 C 本书中使用的一些术语·····	(201)
附录 D 国外信息安全测评认证体系介绍·····	(227)
D.1 前言·····	(227)
D.2 美国的信息安全测评认证体系·····	(227)
D.3 英国的信息安全测评认证体系·····	(228)
D.4 澳大利亚的信息安全测评认证体系·····	(231)
D.5 加拿大的信息安全测评认证体系·····	(233)
D.6 德国的信息安全测评认证体系·····	(235)
D.7 法国的信息安全测评认证体系·····	(240)
D.8 荷兰的信息安全测评认证体系·····	(241)
D.9 西班牙信息安全测评认证体系·····	(242)
D.10 以色列的信息安全测评认证体系·····	(243)
D.11 韩国的信息安全测评认证体系·····	(244)
D.12 日本的信息安全测评认证体系·····	(245)

第一篇 系统工程

第1章 系统工程概述

1.1 范围和背景

1.1.1 范围

本章定义系统开发总体的系统方法。它要求：建立和实现结构化、学科化、文档化且与系统工程过程一体化的成果；多学科联合作业；满足用户需求的产品和过程的同步开发。为了容易实现主要应用通常要确定系统工程过程。系统工程定义了技术评审的要求。系统工程的任务是提供为评价达到系统目标的进程所用的方法论。

为了新的系统产品和过程的开发、升级、修改以及为了在所有获取和支持阶段解决系统现场的问题，本章将提供全面的、结构化的和多学科的新的系统产品和过程开发方法。本章及下一章适用于对新技术及其应用的改进和开发所提供的技术努力；可用于大、小规模系统、一次或多次的采购以及对目前产品和过程的替代。它适用于任何系统而与系统组成无关，甚至包括那些由各种不同的单元、硬件和软件集成的系统。

系统工程涉及到整个系统的设计和管理，包括硬件、软件和其它系统单元。在分析、折中和实现工程方法论时都必须综合考虑上述因素。多学科配合，满足用户需求的产品和过程同步开发、密切结合的系统工程成果。系统工程过程通常被详细说明成促进主要应用的过程。本章的任务是提供为评价达到系统目标的进程所用的方法论。

为了新的系统产品和过程的开发、升级、修改以及为了在所有获取和支持阶段解决系统现场的问题，本章将提供全面的、结构化的和受过训练的方法。本章及下一章适用于对新技术及其应用的改进和开发所提供的技术努力；可用于大、小规模系统、一次或多次的采购以及对目前产品和过程的替代。它适用于任何系统而与系统组成无关，甚至包括那些由各种不同的单元、硬件和软件集成的系统依然如此。为了项目的有效实施，这些内容可以进行裁剪。

系统工程涉及到整个系统的设计和管理，包括硬件、软件和其它系统单元，在分析、折中过程中和工程方法论上考虑时都必须综合上述因素。

1.1.2 背景

系统工程标准化工作很久以前就受到极大的重视，特别在软件工程中。1992年5月以MIL-STD-499B-工程管理的提案提交评审以求升级和进行重大的改写，名字也改变成为

本、进度、性能和风险共同决定。技术风险管理与过程是不可分割的,并且还包括风险的鉴定、量化和影响的评估以及整个获取周期内对风险缓解措施的实现。为保证设计能充分满足要求,将引入一个综合的、能响应的确认。累进的确认从解决方案的个体(各系统元素)到整个系统都要进行。这种结构化和多学科化的过程,是通过在八个基本系统功能上的应用,去定义和选择从整个生命周期的眼光来看最优的解决方案,即生命周期平衡解决方案(见图 1.1.2-3)。

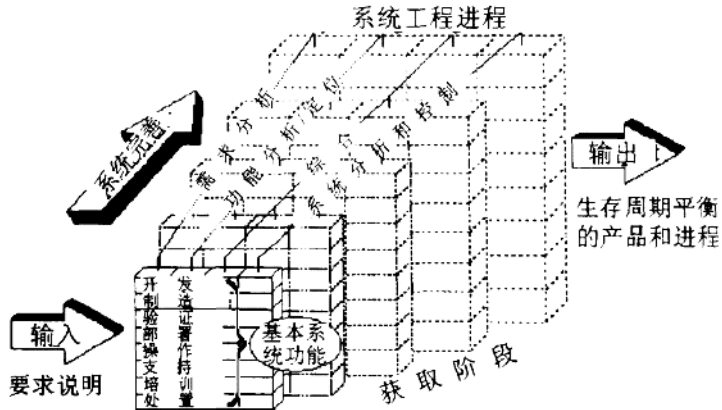


图 1.1.2-3 生命周期平衡解决方案

1.2 系统工程及过程

系统工程模型如下图所示。

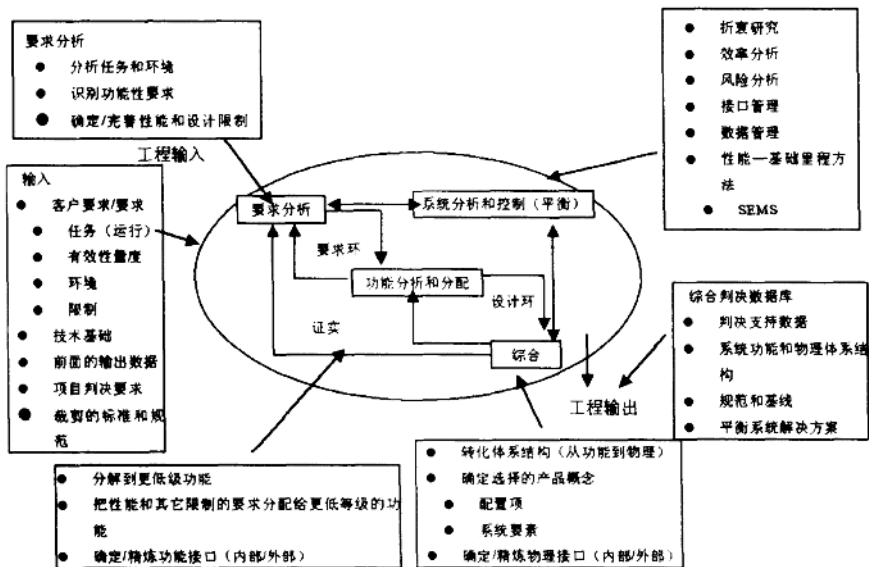


图 1.2-1 系统工程模型

第2章 系统工程过程要求

执行活动将采用要求分析的系统工程过程、功能性分析/分配、综合、系统分析和控制，通过持续不断的努力来达到合同目标和在系统生命期内确定需求、设计和解决方案。

2.1 要求分析

执行活动将分析客户的要求、目标和在客户任务方面的各种要求、实现环境以及识别出的系统特征，从而确定每个基本系统在功能上和性能上的要求。在分析前要进行评审和修正，改进任务和环境的定义，以便支持系统的定义。要求分析与功能分析迭代进行以便开发取决于附加系统定义的要求（即，对已识别出的功能，其他系统的项目、性能需求）并核实那些人员、产品、过程的解决方案（通过综合）是否可以满足客户的需求。

在实施要求分析时，执行活动将要：

- 帮助提炼出客户目标和要求；
- 确定最初的性能目标并改善成为要求；
- 识别和确定限制各种解决方案的约束（即，任务和实现环境不利因素对自然和人类的影响）；
- 确定基于客户提供的有效方法的功能和性能要求。当有效手段不能提供详细要求时，执行活动将开发和使用一组与客户任务、实现环境、需求、要求、目标以及设计限制有关的有效手段。

2.1.1 要求

在要求分析中要识别出功能要求并且作为过程输入将用作功能分析的最高级功能。

性能要求将：

- 在基于系统生命期内的各种因素的所有已被识别的功能基础上被开发出来。
- 依据评估中必然事件的等级、系统成功的危险程度以及与其它要求的关系被特征化。

2.2 功能分析/分配

执行活动将确定和综合出特别需要的功能性的体系结构，以支持有关人员、产品、过程和风险管理方面解决方案的综合。功能分析/分配要不断地进行以便：

- 成功地确定能满足更高层次功能要求所必须的低层次功能，以及确定多套可选择的功能要求；
- 在要求分析基础上确定任务和环境要求，并确保高层次的要求能够被满足；
- 降低性能要求和设计限制；
- 通过综合来确定和改善满足要求的合理的代替解决方案并且把得到的要求放到功能体系结构中。