信息安全丛书

INFOSEC

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
方关宝　戴宗坤　编著

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课教材之一。《信息系统安全》和《信息系统安全工程学》这两本专业课教材，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

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

系统工程。于 1994 年 6 月美国国防部把其作为军队标准公布。它的商用版本是 EIA/IS632。有关系统工程标准和模型的发展史如图 1.1.2－1 所示。

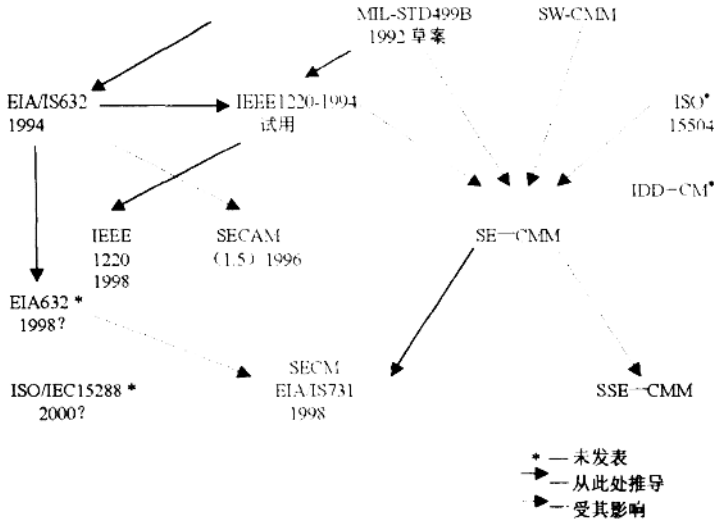

图 1.1.2－1 系统工程标准和模型的历史

在系统的整个生命周期内不断地应用系统工程过程将一些规定的问题转化为设计上的要求。提供满足顾客需求的能力，包括人的因素、产品因素以及过程因素在内的一整套系统解决方案（参见图 1.1.2－2 关键项）。

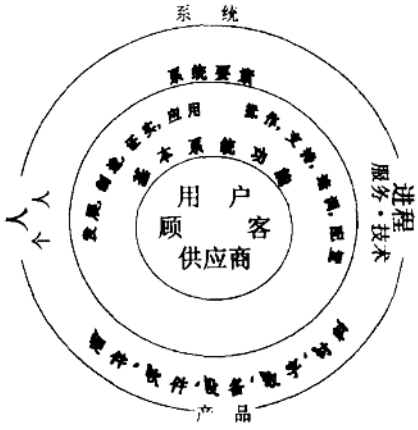

图 1.1.2－2 系统工程关键项

当项目进入现场运行后、在缺乏运行支持和培训支持的时候，这些问题通常用新的开发和更改的需求来表示。基于需求的性能和问题的代替解决方案有一个不断地定义和改善的过程。解决方案会使用现存的、有限的开发手段或者使用在以产品和过程的应用为基础的技术来实现多种技术的转换。在有需求的地方，就要建立、实施和控制技术转换的方法。转换的准则和实现方法（实现什么、何时实现、为谁实现、谁来实现）通过任务和执行活动共同制定。这些都包括在整个生命周期内产品和过程可接受的成熟度的定义中。首选解决方案由成

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)。

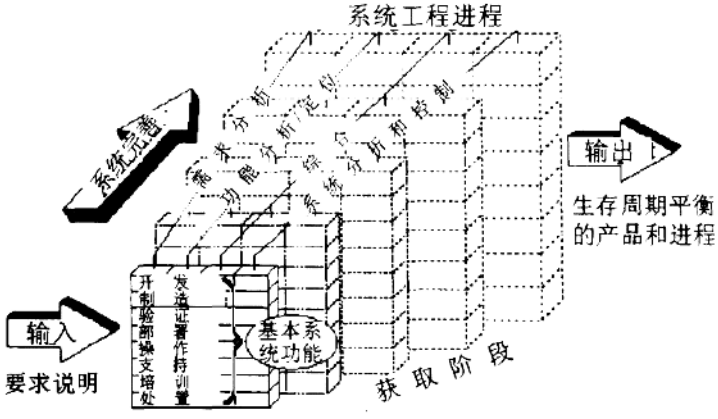

图 1.1.2－3　生命周期平衡解决方案

1.2　系统工程及过程

系统工程模型如下图所示。

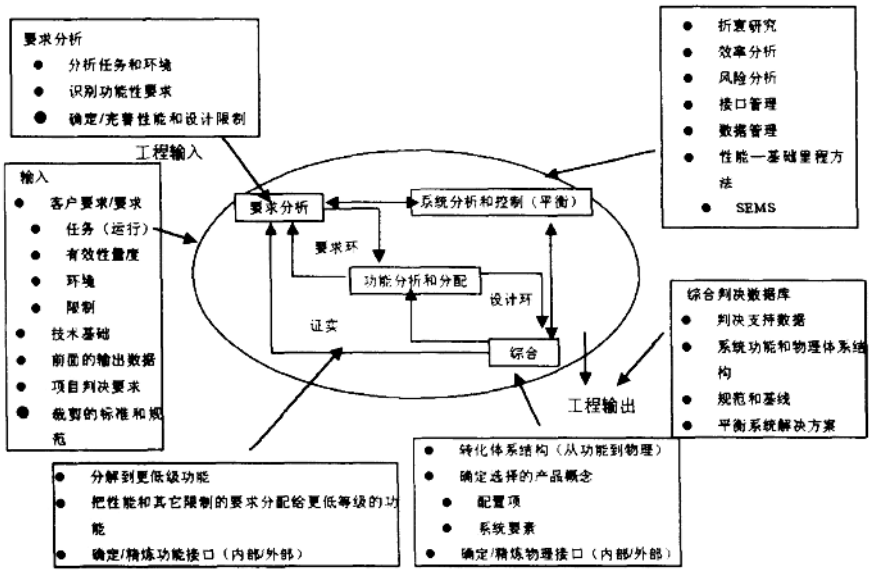

图 1.2－1　系统工程模型

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。