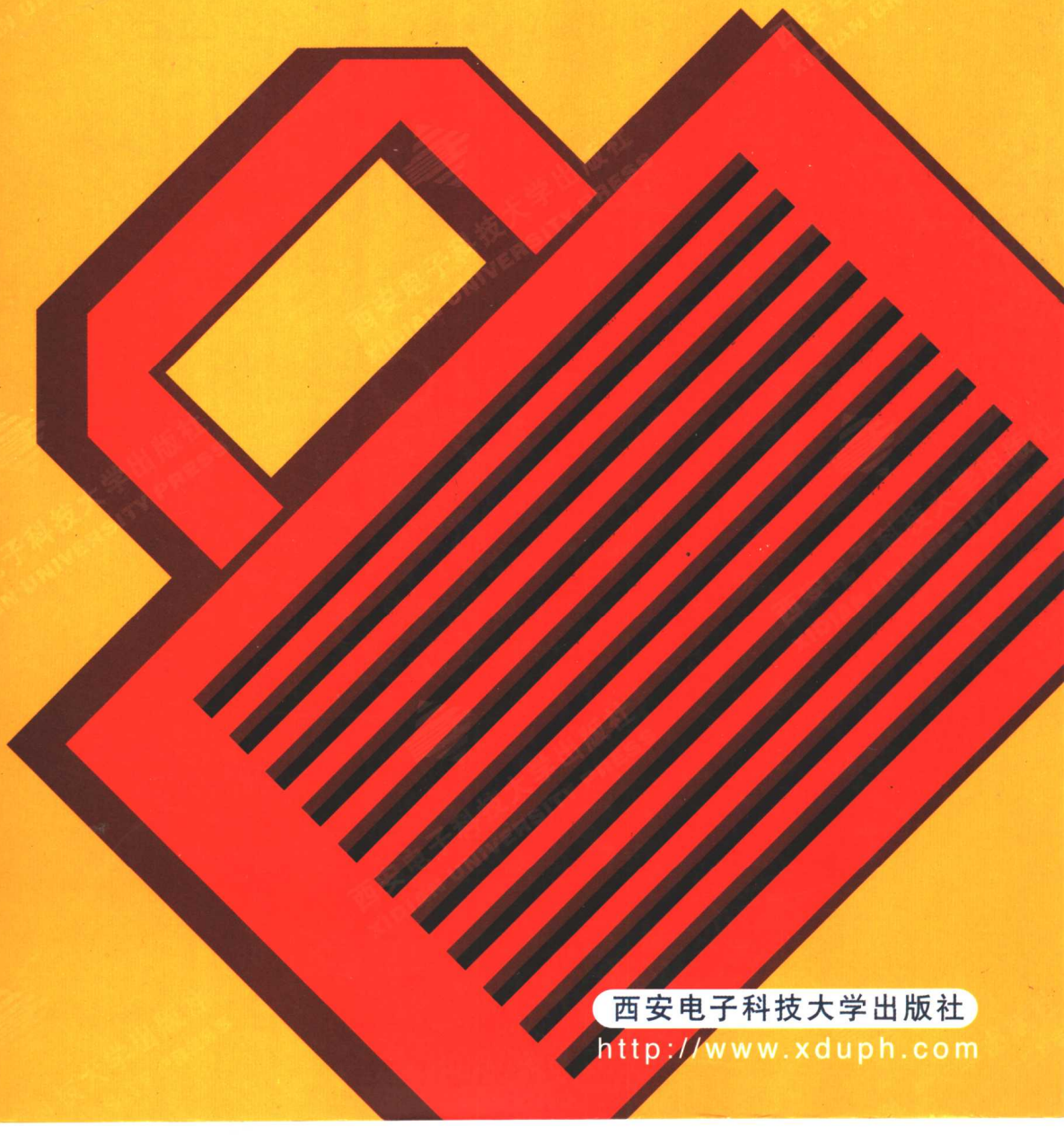
系统安全工程能力成熟度模型 (SSE-CMM) 及其应用

- SSE-CMM项目组 编写
- 蔡皖东 等编译



西安电子科技大学出版社
http://www.xduph.com

系统安全工程能力成熟度模型(SSE-CMM)及其应用

SSE-CMM 项目组　编写

蔡皖东等　编译

西安电子科技大学出版社

2004

内 容 简 介

一个组织或企业从事工程的能力将直接关系到工程的质量。国际上通常采用能力成熟度模型(CMM)来评估一个组织的工程能力。根据统计过程控制理论，所有成功企业都有一个共同特点，即具有一组定义严格、管理完善、可测量的工作过程。CMM 模型认为，能力成熟度高的企业持续生产高质量产品的可能性很大，而工程风险则很小。为了将 CMM 模型引入到系统安全工程领域，有关国际组织共同制定了面向系统安全工程能力的成熟度模型(SSE-CMM)。该模型是在 CMM 模型的基础上，通过对安全工程进行管理的途径将系统安全工程转变为一个具有良好定义的、成熟的、可测量的先进工程学科。该模型已作为国际标准被推荐使用。

本书着重介绍了 SSE-CMM 模型的 2 0 版本及其评估方法。共分十章，分别为：SSE-CMM 简介，CMM 概念，模型体系结构，SSE-CMM 使用，通用实践，基本实践，SSAM 简介，评估方法阶段，发起组织指南和评估组织指南。附录中给出了评估规划及其评估过程中所使用的标准化表格。

本书是目前国内首家对该模型进行详细介绍的出版物，适用于从事信息技术安全的公司、企业及其相关管理和技术人员，也适合从事系统安全评估的组织和个人使用。

图书在版编目（CIP）数据

系统安全工程能力成熟度模型(SSE-CMM)及其应用 / SSE-CMM 项目组编写；蔡皖东等编译

—西安：西安电子科技大学出版社，2004 5

书名原文：Systems Security Engineering Capability Maturity Model

ISBN 7-5606 -1383 - 7

Ⅰ 系… Ⅱ ① 美… ② 蔡… Ⅲ 计算机系统—安全技术—软件工程 Ⅳ TP309

中国版本图书馆 CIP 数据核字（2004）第 031400 号

策　　划　霍小齐

责任编辑　潘恩祥　霍小齐

出版发行　西安电子科技大学出版社（西安市太白南路 2 号）

电　　话　(029)88242885　88201467　　邮　编　710071

http: //www.xduph.com　　E-mail xdupfxb@pub.xaonline.com

经　　销　新华书店

印　　刷　陕西画报社印刷厂

版　　次　2004 年 5 月第 1 版　2004 年 5 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印张 11 375

字　　数　265 千字

印　　数　1～4000 册

定　　价　18 00 元

ISBN 7 - 5606 - 1383 - 7 / TP • 0734

XDUP 1654001 - 1

编 译 者 序

一个组织或企业从事工程的能力将直接关系到工程的质量。国际上通常采用能力成熟度模型(CMM，Capability Maturity Model)来评估一个组织的工程能力。CMM模型是建立在统计过程控制理论基础上的。统计过程控制理论指出，所有成功企业都有共同特点，即具有一组定义严格、管理完善、可测量的工作过程。CMM模型认为，能力成熟度高的企业持续生产高质量产品的可能性很大，而工程风险则很小。

为了将CMM模型引入到系统安全工程领域，1994年4月，美国国家安全局、美国国防部、加拿大通信安全局以及60多家著名公司共同启动了面向系统安全工程的能力成熟度模型(SSE-CMM，Systems Security Engineering Capability Maturity Model)项目。该项目的目的是在CMM模型的基础上，通过对安全工程进行管理的途径将系统安全工程转化为一个具有良好定义的、成熟的、可测量的先进工程学科。1996年10月，SSE-CMM 1.0问世，SSE-CMM项目主管单位选择了5家公司对该模型进行长达一年的试用，根据试用中积累的经验对模型进行了多次修改，于1998年10月公布了SSE-CMM 2.0版本，并提交给国际标准化组织申报国际标准。

SSE-CMM模型将各种系统安全工程任务抽象为11个有明显特征的子任务，而完成一个子任务所需要实施的一组工程实践称为一个过程域(Process Area)。SSE-CMM模型为每个过程域定义了一组确定的基本实践(Basic Practice)，并规定每一个基本实践对于完成该任务都是不可缺少的。

一个组织每次执行同一个过程时，其执行结果的质量可能是不同的。SSE-CMM模型将这个变化范围定义为一个组织的过程能力。对于“成熟”的组织，每次执行同一任务的结果质量变化范围比“不成熟”的组织要小。为了衡量一个组织的能力成熟度，其过程完成的质量必须是可度量的。为此，SSE-CMM模型定义了5个过程能力级别，每个级别用一组共同特性(Common Feature)来标识，每个共同特性则用一组通用实践(Generic Practice)来描述。这里的组织是指执行过程或接受过程能力评估的一个组织机构，它们可以是一个企业、企业的一个部门或者是一个项目组。

系统安全工程的目的是通过分析企业存在的安全风险，建立与之相平衡的安全需求，并将安全需求贯穿于系统安全工程活动的整个生命周期。系统安全工程包括概念定义，需求分析，系统设计、开发、集成、安装、操作、维护以及退役。另外还涉及到众多的安全问题，如计算机安全、网络安全、通信安全、信息安全、操作安全、管理安全、物理安全、辐射安全和人员安全等。系统安全工程还需要证实安全机制的正确性和有效性，证明系统安全的信任度能够达到用户的要求，或者系统遗留的安全脆弱性和风险在用户所容许的范围内。

过程能力成熟度模型所定义的工作过程具有连续性、可重复性和有效性。一个组织在工作实践中的表现在很大程度上是可预测的，一个具有高过程能力的企业生产出高信任度产品的可能性是很大的。虽然对一个组织的过程能力评估不能完全取代对该组织产品的认证，也不能直接担保产品质量的好坏，但是可以为产品信任度的评估提供有力的佐证，并且可以大大简化繁琐的安全产品认证实践，加快安全产品的测评过程，从而节省大量的认证费用。

随着我国电子政务、电子商务及企业信息化的发展，对网络信息安全提出了很高的要求，大大推动了信息安全产品市场。很多公司都加入到信息安全产品开发的行列中，难免会出现产品质量良莠不齐的局面，导致用户对信息安全产品缺乏信任。因此，研究 SSE-CMM 模型及其评估技术对于加强信息安全产品认证、改善企业工程能力、规范信息安全产品市场等都具有十分重要的意义。

为了促进 SSE-CMM 模型的推广使用，SSE-CMM 项目组规定，SSE-CMM 模型的内容是免费的，包括当前版本和以后修订版本。为了将 SSE-CMM 模型介绍给我国广大读者，我们组织编译和整理了 SSE-CMM 2.0 版本及其评估方法，全书由蔡皖东校对和统编，参加翻译工作的有王珂、田广利、朱锐、张赟、李莉、李立松、赵振国和熊明辉等。

由于编译者水平有限，书中难免存在一些错误和不足之处，欢迎广大读者批评指正。

编 译 者

2004 年 1 月

目　录

第 1 章　SSE-CMM 简介

1.1　引　　言

系统安全工程能力成熟度模型(SSE-CMM，Systems Security Engineering Capability Maturity Model)描述了一个组织的安全工程过程的重要特性，为了确保安全工程的良好性，这些特性是必须的。SSE-CMM 是从工程实现中所观察到的经验抽象而成的，并没有规定一个特定的过程或顺序，该模型是一个安全工程的通用标准，包含了如下内容：

- 整个生命周期，包括系统开发、运行、维护及淘汰等。
- 整个组织，包括管理、组织和工程活动。
- 与其他学科的紧密联系，包括系统、软件、硬件、人类活动和测试工程，系统管理、运行和维护等活动。
- 与其他组织的相互联系，包括信息获取、系统管理、产品认证、可信度评估等。

本书包含两部分内容：SSE-CMM 模型和 SSE-CMM 评估方法。SSE-CMM 模型详细描述了 SSE-CMM 的规则和体系结构，包括模型的使用方法；如何更好地利用模型的建议；模型实施的经验；模型属性的描述以及模型再次开发的要求等。SSE-CMM 评估方法描述了评估一个组织安全工程能力的过程和工具。

用户和安全产品提供商都非常关注和重视安全产品、安全系统及安全服务的改进。在安全工程领域中，已经有一些被广泛接受、约定俗成的准则，但是这些准则还缺少一个能够全面评估安全工程实践的框架。SSE-CMM 提供了这种框架，可以作为衡量系统安全性的标准，以提高安全工程准则应用的性能。SSE-CMM 的目标是把安全工程发展成一种有完整定义的、成熟的和可测量的工程学科。

必须指出的是，安全工程是一个独立的工程学科，需要建立统一的理论、技术、技能及实施过程。只有这样，才能保证建立一个真正的安全工程能力成熟度模型。这里的独立性并不和“安全工程必须随系统的改变而作相应改变”的前提相冲突。实际上，良好定义和可接受的系统活动能够使安全工程更加有效。

现代统计过程控制理论表明，重视生产过程的质量能够有效地提高所生产产品的质量，而成熟组织的工程实践正是从这些受重视的生产过程中提炼出来的。如果给予开发安全系统和可信产品所需要的费用和时间，则生产过程可能会更加有效。因此，安全系统的运行和维护依赖于人类和技术相关联的过程。为了有效地控制这种相互依赖性，必须重视一个组织正在使用的生产过程的质量和利用这种生产过程的成熟度。

随着社会对信息可信度的日益重视，对信息的保护变得十分重要。许多产品、系统和

服务都需要保护信息资源，安全工程已经从原来的仅仅保护政府级数据扩展到很多方面，如财务转账、契约合同、私人信息、网络信息等。这种趋势提升了安全工程的重要性。

SSE-CMM 适用范围有如下几个方面：

- SSE-CMM 规定了安全工程的行为，即整个可信产品或安全系统的生命周期，包括概念定义、需求分析，以及系统设计、开发、集成、安装、运行、维护及淘汰。
- SSE-CMM 适用于安全产品开发商、安全系统开发商和集成商以及提供安全服务和安全工程的组织。
- SSE-CMM 适用于各类安全工程组织，如金融、政府、学术等。

尽管 SSE-CMM 能够明显提升安全工程的能力，但并不意味安全工程独立于其他工程准则之外。相反，SSE-CMM 提供了一种集成的观点：在工程准则中，安全问题无所不在，如系统、软件、硬件及人为因素等，通过定义相应的模型组件来适应这种情况。“协调安全实践”共同特性(Common Feature)将安全和其他工程准则与一个工程组织内的工作组整合起来。同样，“协调安全”基本实践(Basic Practice)定义了安全工程活动中的协调对象和机制。

实践安全工程的组织包括产品开发商、服务提供商、系统集成商、系统管理员以及安全专家等。在这些组织中，一些工作小组负责处理“高级事务”，如处理操作事务或系统结构；另一些工作小组负责处理“低级事务”，如产品选型和设计，还有一些工作小组兼做这两部分。这些组织能够根据特定的形式或特殊的联系来区分不同的工作小组。

SSE-CMM 是为所有这样的组织设计的。应当指出，一个组织或企业的经营状况不能用是否使用 SSE-CMM 来说明，重视 SSE-CMM 的组织并不一定就比那些不重视的组织好，即使使用了 SSE-CMM，也不一定使用模型所涉及的所有方法。

根据不同组织的实际情况，模型所定义的某些安全工程实践将会起作用，但不是全部。并且，该组织需要从模型不同实践间的联系来决定它们的应用。下面通过例子说明 SSE-CMM 是如何应用于组织或团体的。

1) 安全服务提供商

为了测量一个组织执行风险评估的过程能力，需要多个实践小组开展评估活动。在系统开发和集成过程中，一个实践小组需要对该组织的确定和分析安全脆弱性的能力进行评估，并对操作影响进行评估。在操作过程下，一个实践小组需要对该组织的监控系统安全态势的能力进行评估，标识和分析系统脆弱性，评估操作影响。

2) 决策制定者

对于关注决策制定者的小组来说，一个组织的过程能力应当通过 SSE-CMM 实践的组合来确定。模型包含了如何决定和分析安全脆弱性，评估操作影响，为其他小组(如一个软件开发小组)提供输入等实践，为决策制定者提供服务的小组需要理解这些实践之间的关系。

3) 产品开发者

SSE-CMM 包含了如何理解用户安全需求的实践，这需要通过与用户的交流来弄清他们的需求。在开发一个产品时，应当独立于特定的用户。在这种情况下，产品市场小组或其他小组可以作为假想的消费者，从而获得用户需求。

安全工程的实践者要意识到为了达到产品开发要求，产品环境和所使用的方法可能比产品本身更加复杂多变。然而，在产品和工程环境相关问题上还存在一些争论，包括产品

计划、开发、发布和维护等方面，例如：

- 用户库类型(产品，系统或服务)；
- 保证要求级别(高与低)；
- 对开发和运行组织的支持。

这个例子说明了一个组织或企业可以根据他们的环境来确定如何适当地使用 SSE-CMM。关于不同用户库的差异，不同保证要求级别的差异，以及在 SSE-CMM 中这些差异的影响等将在下面讨论。

4) 特定的工业部门

每一个工业部门都有他们各自的特点、术语及风格。通过减少角色的依赖性和组织结构的关联性，所有工业部门都能够容易地将 SSE-CMM 概念转换成他们自己的语言和文化。

SSE-CMM 及其评估方法可以用于下列场合：

- 工程组织作为评估他们的安全工程实践和提出改进意见的工具；
- 安全工程评估组织(如系统认证和产品评估)作为建立基于组织能力信心(如一种系统或产品安全保证要素)的基础；
- 用户作为评估提供商安全工程能力的标准机制。

SSE-CMM 中的一切都是免费的，包括当前和后续版本，并且以后重新修改和发布 SSE-CMM 中的内容也是免费的。

1.2　使用 SSE-CMM 的好处

近年来，人们对信息安全问题越来越重视，并采用必要的安全产品来保护信息系统安全和信息隐秘性。在市场上，这样的安全产品以两种方式出现：经过评估的产品(或称已评估产品)和没有经过评估的产品(或称未评估产品)。由于产品的评估需要很长的时间和高昂的费用，因此已评估产品投放市场的时间通常都比较晚，不能解决当前面临的安全威胁。对于未评估产品，用户应当在充分考虑其他用户对该产品评价的基础上独自地作出判断和选择。现在，很多安全工程服务都是在后一种情况下进入市场的。

在这种情况下，要求一个组织以十分成熟的心态来使用安全产品，尤其需要考虑下面一些因素：

- 持久性：将来的应用需要以前的知识。
- 可重复性：保证工程能够安全地重复操作的方法。
- 效率：保证开发者和评估人员的工作效率。
- 可信性：对安全需要充分信任的可信性。

为了达到上述目标，需要一种机制能够引导组织理解和改进他们的安全工程实践。为了满足这种机制的要求，SSE-CMM 被设计成安全工程实践的形式，并且以提高安全系统、可信任产品以及安全工程服务的质量和可用性，降低发布成本为目标。SSE-CMM 特别针对以下组织：

1) 工程组织

工程组织包括系统集成人员、应用程序开发人员、产品销售商以及服务提供者，

SSE-CMM 给这些组织带来的好处是：

- 减少可重复、可预测过程和实践所带来的重复性劳动。
- 确定真实能力来独自地执行资源选择。
- 被评估组织的资质和改进受到重视。

2) 控股组织

控股组织是指可以获得来自外部/内部资源与最终用户的系统、产品和服务的组织，SSE-CMM 给这些组织带来的好处是：

- 可重复使用的建议语言和评估方法的标准文本。
- 降低选择不合格产品的风险。
- 减少对基于工业标准的统一评估的异议。
- 对产品或服务信任度的可重复性和可预测性。

3) 评估组织

评估组织包括系统认证人员、系统估价人员、产品评估人员和产品估价人员，SSE-CMM 给这些组织带来的好处是：

- 过程评估结果的可重复性，系统或产品改进的独立性。
- 对安全工程以及与其他学科集成的信任度。
- 基于对能力的信任，可以减少安全评估的工作量。

1.3 SSE-CMM 项目简介

1. 项目历史

1993 年 5 月，美国安全局(NSA)针对安全方面的特殊需求首次提出了 SSE-CMM 模型。1995 年 1 月，信息安全协会被邀请参加首次的公共系统安全工程(FPSSE)CMM 工作组，该组织中的 60 多个代表重新确认了这一模型的重要性。为此，成立了专门的工作组进行前期的开发工作，并于 1995 年 3 月召开了第一次工作会议。经过工作组的不懈努力，于 1996 年 8 月公布了 SSE-CMM 模型的第一个版本，1997 年 4 月公布了 SSE-CMM 评估方法。

为使 SSE-CMM 模型及其评估方法更加有效，工作组从 1996 年 6 月到 1997 年 6 月做了大量的试验，根据试验结果对模型进行了修改和补充，形成了 SSE-CMM 模型和评估方法的 1.1 版本。SSE-CMM 模型第一个版本的试验包括两个系统集成商、两个服务提供商和一个产品开发商。试验是在有助于模型验证的各种组织中实施的，包括：各种规模的组织；合同驱动的系统开发和市场驱动的产品开发；高级和低级可信度的开发；开发、运营及服务提供者组织。

1997 年 7 月，第二次公共系统安全工程(SPSSE)CMM 工作组成立，它是公众安全工程能力成熟度模型开发团队，主要致力于模型的应用研究，尤其在获取、过程改进、产品与系统保证等领域，其目标是使模型实用化。

2. 项目组织

SSE-CMM 项目在安全工程协会和有关国家政府组织的积极参与和大力资助下取得了

很大的进展。

SSE-CMM 项目结构如图 1.1 中所示，它包含了指导小组，评估方法小组，模型维护小组，生命周期支持小组，特征、保证及测量(PAM)小组；投资、计划和采纳(SPA)小组，关键评论家和协会评论家。

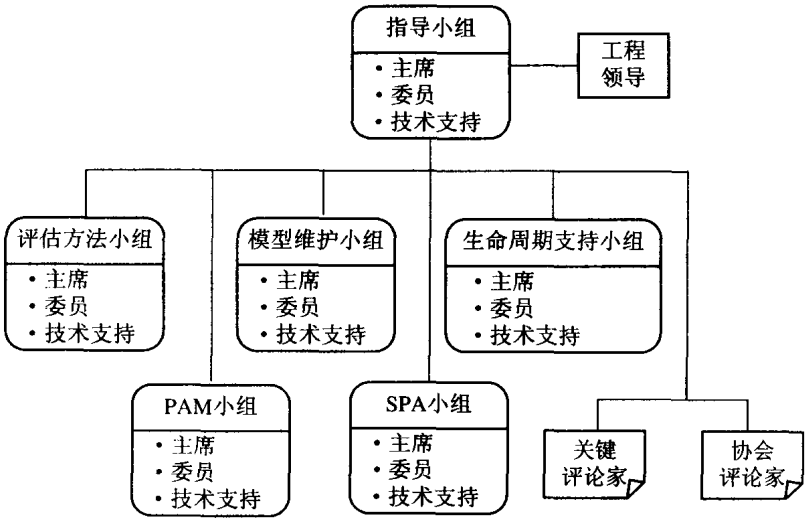


图 1.1　SSE-CMM 项目结构

3. SSE-CMM 项目组成

指导小组提供 SSE-CMM 工作过程、产品和进度的指导，鼓励广泛地接纳和采用 SSE-CMM。

评估方法小组负责维护 SSE-CMM 评估方法（SSAM），包括第三方评估方法的开发。必要的话，评估方法小组还将规划、支持和分析一种试验程序来测试第三方评估方法。

模型维护小组负责模型的维护，包括确保过程域涵盖所有团体的安全活动，最大程度地减少 SSE-CMM 与其他模型冲突的可能性，并在文档中正确地区分与其他工作的关系。

生命周期支持小组负责为评估者资格和评估小组可比性开发和建立一种机制，设计和实现一种数据库，以维护评价数据，并发行有关解释和维护指南。

PAM 小组的任务是研究和验证 SSE-CMM 有关的概念，确定和证实 SSE-CMM 的作用，标识和验证与 SSE-CMM 使用相关的安全和过程测量。

SPA 小组负责研究和发起倡议选项(如果需要的话，可以定义和规划一个组织去维护 SSE-CMM)，开发和维护集成化的项目进度，促进和鼓励不同团体使用 SSE-CMM。

关键评论家对 SSE-CMM 项目工作产品做出正式的评论，并给出适合的评语。

协会评论家也会对产品提出意见，但不是正式的。

这些工作小组各司其职，SSE-CMM 项目的发起者、赞助商以及有关国家政府组织提供了技术交易、项目简化和技术支持所需的资金。

1.4 与其他工程学科的联系

表 1.1 显示了 SSE-CMM 与其他工程学科的联系和工作目标，这些工作有助于更好地理解 SSE-CMM，这也是安全工程模型一个独特的地方。

表 1.1 SSE-CMM 与其他工程学科的联系

学 科	目 标	方 法	范 围	状 态
SSE-CMM	定义、改进和评定安全工程能力	持续的安全工程成熟度模型和评估方法	安全工程组织	版本 2.0
SE-CMM	改进系统或产品工程过程	持续的系统工程实践成熟模型实践和评估方法	系统工程组织	参见 EIA731
SEI CMM for Software	改进软件开发管理	发展的软件工程模型成熟度和管理实践	软件工程组织	并入 CMMI
Trusted CMM	改进高集成度软件开发过程及其环境	发展的软件工程模型成熟度和包含安全在内的管理实践	高集成度软件组织	未知
CMMI	将现有过程改进模型整合到一个单一的体系结构框架中	分类、合并和安排过程改进构造块来简化模型	工程组织	发布了部分草稿
Sys. Eng. CM (EIA731)	定义、改进和评定系统工程能力	持续的系统工程成熟度模型和评估方法	系统工程组织	释放版本
Common Criteria	通过技术级可重用的保护文件来改进安全	伴随着一个评估过程，一系列有关安全的功能和要求	信息技术	版本 2.0
CISSP	使安全专业成为一种公认学科	安全知识以及为安全专业而设立认证考试	安全从业者	正在使用
Assurance Frameworks	通过界定证据范围来改进安全保证	建立保证论据和有效产生证据的结构化方法	安全工程组织	研究论文
ISO 9001	改进组织质量管理	质量管理实践的特定要求	服务组织	广泛应用
ISO 15504	软件过程改进和测评	软件过程改进模型和评估方法学	软件工程组织	发布了 9 部分
ISO 13335	改进信息技术安全管理	指导信息和服务过程达到或保持一定的安全等级	安全工程组织	发布了 3/5

第2章 CMM 概 念

本章描述了 SSE-CMM 中所使用的概念和结构，给出了设计 SSE-CMM 的必备信息，关键概念和结构描述，有助于进一步理解 SSE-CMM 模型及其基础知识。

SSE-CMM 给出了一个广泛的标准架构，将安全工程改造和提升为一个成熟的、可测量的学科。模型及其评估方法将保证安全是工程中不可分割的一部分，工程涉及到硬件、软件和系统，并关系到企业安全问题。这个模型定义了一个安全工程过程的特征，该过程是被明确定义、管理、评估和控制的，并且在所有工程类型中都是有效的。

2.1 过 程 改 进

过程是执行一个给定目标的步骤序列，它可以是系统任务，支持工具，产品设计以及某些最终结果(如产品、系统及服务等)的改进。过程是产品成本、进度及质量的决定因素之一，越来越多的工程团体开始关注如何改进生产产品和提供服务的过程。

过程能力是指一个组织的潜在能力，这是一个组织内部所希望执行的范围。过程性能是测量一个特定项目的实际结果是否超过了范围。W.Edwards Deming 在《Out of the Crisis》一书中提到一个例子："在一个工厂车间中，经理发现在特定产品线上出现了问题，在这个产品线上的工人制造出了很多的次品。表面上，他可能要求工人更加努力地工作。实际上，他通过采集数据，计算次品的百分比，其计算结果表明，次品数量和每天的波动范围是可预测的。"

这个例子说明了一个统计过程控制的系统，一个特定的范围定义了能力，其变化极限是可预测的。这也是一个生产次品的稳定系统，它说明一个基于统计过程控制的系统并不能避免产生次品。

但是，这并不是说每一个重复过程都会得到相同的结果。重要的是采用数据控制过程使我们知道能够改进哪些地方。很多组织都利用了 CMM 作为统计控制过程的参考。

另一个概念是过程成熟度，它说明了一个被明确定义、管理、评估和控制的特定过程是有效的，过程成熟度说明了一种潜在增长的能力，并指示一个组织的过程丰富性和应用于整个组织的一致性。

Deming 和日本人合作将统计控制过程概念应用于工业中，在《Characterizing the Software Process：A Maturing Framework》一书中，W.Humphrey 描述了一种软件过程成熟度框架来说明 Deming 所提出的软件开发过程。W. Humphrey 认为，"就像可应用于软件行业那样，统计过程控制概念可以应用于自动化、影视、钟表和钢铁业中，尽管各行各业存在一定的差异。在统计过程控制下，软件开发过程能够在成本、进度和质量等方面获得可

预期的结果”。W. Humphrey 描述了将统计过程控制概念应用于软件过程，引导一个组织通过增加适当的步骤来改进其过程能力，进而提高过程成熟度级别，他所描述的这些级别构成了软件 SEI(Security Engineering Institute)-CMM 的基础。

CMM 是一个框架，它能够将一个工程组织从组织凌乱和效率低下的状态发展成为高度结构化和高效的状态。对一个组织来讲，使用该模型将意味着在统计过程控制下进行过程实践，以提高其过程能力。将 CMM 应用于软件的结果是：很多软件组织在成本、生产率、进度和质量等方面都显示出了良好的效果。

SSE-CMM 将统计过程控制概念应用于安全工程，其目的是在开发安全系统和产品过程中，对成本、进度和质量等进行有效的控制。

2.2 预 期 结 果

基于对软件行业和其它团体的分析，过程和产品改进的某些结果是可预测的。

(1) 改进预测性。组织成熟度的首要改进是可预测性。随着能力的提高，理想结果和实际结果之间的差异将会减小。例如：能力级别低的组织所制定的开发计划经常因为一些不可知的因素而变得不确定，而能力级别越高的组织就越能准确地预测出一个项目的成本和进度等因素。

(2) 改进可控性。组织成熟度的第二个改进是可控性。随着过程能力的提高，更多的结果将有利于更精确地建立和修订目标。可选行为的正确性应能根据过程经验和其它项目过程结果来评价，以便选择最好的控制方法来应用。改进的结果是具有高能力级别的组织将会在可接受范围内更加有效地控制性能。

(3) 改进过程效率。组织成熟度的第三个改进是过程效率，其改进结果提高了组织成熟度。随着组织的成熟，将带来成本降低、开发周期缩短、产量增加和质量提高等益处。对于成熟度低的组织，开发周期很长，因为要纠正错误而增加了重复劳动量。与此相比，成熟度高的组织，能够通过提高过程效率和减少重复劳动成本来缩短开发周期。

2.3 消 除 误 解

下面是使用 CMM 时所产生的一些误解。

误解 1 CMM 定义了工程项目

普遍的错误观念认为 CMM 定义了一个特殊的过程。CMM 为组织定义它们自己的过程提供了指导，以便改进过程。这种指导提出了一些可能没有被考虑到的过程。对于帮助定义、管理、监控和改进该组织的过程来说，CMM 描述的“WHAT”行为必须执行，它要优于“HOW”正确地执行特定行为。

作为特定工程学科的 CMM，如 SSE-CMM，要求必须执行某些基本工程行为，这些基本工程行为是该工程学科工程过程的一部分，但并没有规定如何正确地执行这些工程行为。

在应用 CMM 后，一个重要的任务是加强工程组织开发和改进其工程过程，它依赖于定义、证明和管理工程过程，对贯穿于整个组织的过程进行标准化。这种方法并不针对特定的开发周期、组织结构和工程技术。

误解 2　CMM 是工具书和训练手册

CMM 倾向于指导组织改进他们执行一个特定过程（如安全过程）的能力。CMM 并不是为帮助个体改进他们的特定工程技巧而编写的工具书和训练手册。CMM 的目的是指导一个组织通过采纳CMM中所描述的原理和使用CMM中所定义的技术来定义和改进他们的工程过程。

误解 3　CMM 是产品评估的替代品

CMM 评估不能代替产品评估和系统认证，但是，通过 CMM 评估的确有助于发现潜在的弱点。统计过程控制下的过程并不意味着没有缺点，由于它使得缺点更加可预测，因此某种形式的分析样本仍然是必需的。

如果期望从使用 SSE-CMM 中得到好处，则应当在使用 SEI-CMM 上获得经验。要想在 SSE-CMM 评估和认证中得到想要的东西，安全工程团体一定要在“安全工程成熟度将意味着什么”上达成一致看法，这需要研究如何在团体内部持续地使用 SSE-CMM，就像 SEI-CMM 那样。

误解 4　需要太多的文档

在理解 CMM 时，读者很容易被太多的建议过程和计划所吓倒。CMM 中包含了必需的证明过程和程序，并保证它们被正确地执行。如果从 CMM 中看到大量的过程、计划和其他形式的文档，那么读者可以不必另行制定各种文档。一个简单的安全计划能够满足许多过程域的要求。CMM 仅仅说明了正确的信息类型而已。

2.4　关 键 概 念

本节着重解释在理解或使用 SSE-CMM 时容易混淆的一些关键概念。该模型中的一些特定名词，如“通用实践”和“基本实践”等将在定义和描述该模型时详细地讨论。

1) 组织和项目(Organization and Projects)

在 SSE-CMM 中使用这两个词来说明组织结构的两个方面。在商业实体内部已有的其它词汇并不是被整个商业行业公认的。在 SSE-CMM 中选用这两个词是因为它们容易被大多数用户普遍采用和理解。

2) 组织(Organization)

为了达到 SSE-CMM 的目标，一个组织可以定义为一个公司的一个部门、整个公司或其它实体（如政府代理或服务分支），其负责多个项目的监督。典型的，一个组织内部的所有项目在发布结构的顶端共享公共策略，一个组织可能由分散在不同地理位置上的项目组成，并支持基础结构。组织术语暗示了一个基础结构，以支持共同的战略、商业和有关过程的功能。这种基础结构必须存在，它有利于一个企业提高其产品的生产、发布、支持和销售的效率。