ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20261—2006

信息技术　系统安全工程 能力成熟度模型

Information technology—Systems security engineering—Capability maturity model

(ISO/IEC 21827:2002,MOD)

2006-03-14 发布　　2006-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准修改采用 ISO/IEC 21827:2002《信息技术　系统安全工程　能力成熟度模型》(英文版),主要修改内容如下:

——在 2 规范性引用文件中增加 GB/T 20000.1、GB/T 9387.2、GB/T 18336.1 和 GB/T 11457;

——在 2 规范性引用文件中将 ISO/IEC 15504、ISO/IEC 15288 的引用版本修改为最新版本;

——在 3 术语和定义中增加了“惯例”作为 3.24 条,原国际标准中 3.24 条以后的术语编号依次下移;

——排除原国际标准中存在的错误。例如图 5 中横纵坐标的含义标识顺序颠倒,本标准中不存在“分析候选解决方案”这个过程域。

本标准是系统安全工程的一个过程参考模型,关注的是信息技术安全领域内某个或若干个相关系统实现安全的需求,其主要内容描述了用来实现信息技术安全的过程,尤其是过程的成熟度。

本标准的附录 A 和附录 B 为规范性附录,附录 C 为资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位:中国电子技术标准化研究所、中国电子科技集团公司第三十研究所、北京思乐信息技术有限公司。

本标准主要起草人:周平、吴源俊、王新杰、魏忠。

引　言

在计算机程序开发中——无论是操作系统软件、安全管理和执行功能、软件、应用程序中间件——各种各样的组织实施安全工程。因此，产品开发者、服务提供者、系统集成者、系统管理者，甚至是安全专家都要求有合适的方法和惯例。在这些组织中，有些组织涉及高层次问题（例如涉及运行使用或系统体系结构），另一些组织则关注低层次问题（例如，机制选择或者设计），还有些组织两者都有。许多组织可能专门研究某种特定类型的技术，或者某个专业范畴（例如，航海）。

SSE-CMM®[1)] 是针对所有这些组织而设计的。使用SSE-CMM®并不意味着一个组织就比另一个组织更关注安全，也不意味着任何SSE-CMM®使用方法是必须的。组织的业务核心也不会因为使用SSE-CMM®而发生偏离。

根据组织的业务核心，使用某些（而不是全部）已定义的安全工程惯例。除此之外，组织可能需要考虑模型范围内不同惯例之间的关系，以确定它们的可用性。下面的例子说明了各种不同的组织可以把SSE-CMM®用于软件、系统、设备开发和运行。

安全服务提供者

为了测量一个组织执行风险评估的过程能力，要使用几组不同的惯例。在系统开发或集成期间，可能需要评估该组织在确定和分析安全脆弱性以及评估运行影响方面的能力。在运行情况下，可能需要评估该组织在监视系统安全态势、识别和分析安全脆弱性以及评估运行影响方面的能力。

对策开发者

在一个组集中于对策开发的情况下，可能要通过SSE-CMM®的惯例组合来描述组织的过程能力特性。该模型包含若干提出确定和分析安全脆弱性、评估运行影响以及向涉及到的其他组（例如软件组）提供输入和指南的惯例。提供制订对策服务的组需要理解这些惯例之间的关系。

产品开发者

SSE-CMM®包含一些专门针对理解顾客安全需要的惯例。要求与顾客反复商讨，以便确定这些需要。如果某个产品的开发不受特定顾客的约束，该产品的顾客就是一般顾客。在这种情况下，如果要求考虑顾客，可以把产品营销组或其他组作为假想的顾客。

安全工程专业人员都明白，产品背景和产品开发方法随产品本身的变化而变化。不过，已经知道有一些与产品和项目背景有关的问题对产品的构思、生产、交付和维护方法有影响。下列问题对SSE-CMM®特别有意义：

- 顾客基本类型（产品、系统或服务）；
- 保障要求（高与低）；
- 对开发和运行组织的支持。

下面讨论两类不同顾客基础之间的差别、安全保障要求程度差别和这些差别在SSE-CMM®中的影响。所做的讨论作为一个关于某个组织或某个行业部门可能如何确定在其环境中合适地使用SSE-CMM®的例子。

特定的行业部门

各个行业反映了其独特的文化、术语和交流风格。通过尽可能降低角色相关性和组织结构关联性，

1) CMM 和 Capability Maturity Model 均是美国卡内基·梅隆大学（CMU）的服务商标，受相关法律和法规的保护。

可预见SSE-CMM®的概念可以容易地由所有行业部门转化成其自身的语言和文化。

如何使用SSE-CMM®

SSE-CMM®和应用该模型的方法(例如,评估方法)的预期用途如下:

- 工具——工程组织用于评价其安全工程实践和定义改进;
- 方法——安全工程评价组织(例如认证机构和评价机构)用于确定组织能力(作为系统或产品安全保障的输入)信任度;
- 标准机制——顾客用于评价提供者的安全工程能力。

如果使用模型和评估方法的用户透彻地理解模型的正确用法及其内在的限制条件,则在应用模型进行自我改进和选择供方的过程中可使用该评价技术。

关于使用过程评估的其他信息,可以在ISO/IEC 15504-4《信息技术 过程评估 第4部分:用于过程改进和过程能力确定的使用指南》中找到。

使用SSE-CMM®的好处

安全的趋势是从保护涉密的政府数据向包括金融交易、合同协议、个人信息以及互联网在内的更加广泛的利害攸关领域转移。已经出现相应的维护和保护信息的产品、系统和服务的衍生物。这些安全产品和系统一般以两种方式之一进入市场:长期而昂贵的评价或者无需评价。在前一种情况下,可信的产品往往要在确定它们的特性是必要的之后很长时间并且那些已部署的安全系统不再应付当前威胁时,才到达市场。在后一种情况下,获取者和用户必须只依赖产品或者系统开发者或运营商的安全声明。而且,以往的安全工程服务往往都带着这种警告进入市场。

这种情况要求组织以更成熟的方式实施安全工程。特别是在生产和准备安全系统和可信产品时,需要下列品质:

- 连续性——在以前的工作中获取的知识应用于今后的工作中;
- 可重复性——确保项目可以成功重复的方法;
- 有效性——有助于开发者和评价者更有效工作的方法;
- 保障——指出安全要求的置信度。

为了准备这些要求,需要某种机制用于指导组织去了解和改进它们的安全工程实践。正在开发的SSE-CMM®,以改进所要交付的安全系统、可信产品和安全工程服务的质量和可用性以及降低其成本为目标,提高安全工程实践水平,以适应这些需求。特别是可预见到有下列好处:

对工程组织:

工程组织包括系统集成商、应用开发商、产品厂商和服务提供商。对于这些组织来说,SSE-CMM®的好处包括:

- 由于可重复、可预计的过程和惯例使返工减少而带来的节约;
- 真实执行能力,特别是来源选择方面的信誉;
- 专注于度量到的组织能力(成熟度)和改进。

对于获取组织:

获取者包括从外部/内部来源获得系统、产品和服务的组织和最终用户。对于这些组织,SSE-CMM®的好处包括:

- 可重用的标准置标语言和评价手段;
- 减少选择不合格投标者的风险(性能,费用,进度);
- 由于以业界标准为基础统一评估,引起的异议不多;
- 产品或服务达到可预计、可重复的信任程度。

对于评价组织：

评价组织包括系统认证机构、系统认可机构、产品评价机构和产品评估机构。对于这些组织，SSE-CMM®的好处包括：

- 过程评估结果可重用，与系统或产品变更无关；
- 安全工程以及与其他学科的集成可信；
- 用证据证明能力，减少安全评价工作量。

信息技术　系统安全工程
能力成熟度模型

1　范围

系统安全工程能力成熟度模型(以下简称SSE-CMM®)是一个过程参考模型。它关注的是信息技术安全(ITS)领域内某个系统或者若干相关系统实现安全的要求。在ITS领域内,SSE-CMM®关注的是用来实现ITS的过程,尤其是这些过程的成熟度。SSE-CMM®的目的不是规定组织使用的具体过程,更不必说具体的方法。而是希望准备使用SSE-CMM®的组织利用其现有的过程——那些以其他任何信息技术安全指导文件为基础的过程。本标准的范围包括:

- 涉及整个生存周期的安全产品或可信系统的系统安全工程活动:概念定义、需求分析、设计、开发、集成、安装、运行、维护以及最终退役;
- 对产品开发商、安全系统开发和集成商,以及提供计算机安全服务和计算机安全工程组织的要求;
- 适用于从商业界到政府部门和学术界的各种类型和规模的安全工程组织。

尽管SSE-CMM®是专门用于改进和评估安全工程能力的模型,但这并不意味着应该独立于其他工程学科开展安全工程活动。相反,SSE-CMM®认为安全已经渗透到所有的工程学科领域(例如系统、软件和硬件)并且通过定义模型部件来处理这类利害关系,从而促进这类学科间的整合。公共特征"协调安全惯例"承认有必要使安全与所有涉及某个项目的或者共同处于某个组织内的学科和组整合在一起。与之类似,过程域"协调安全"定义了用于协调安全工程活动的目标和机制。

由于均关注过程改进和能力成熟度评估,本标准与ISO/IEC 15504(特别是第2部分)相关。不过,ISO/IEC 15504关注的是软件过程,而SSE-CMM®则是安全。

本标准与ISO/IEC 15504新的修订版(特别是第2部分)的关系更密切,并且符合ISO/IEC 15504-2中的方法和要求。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准。然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 8566　信息技术　软件生存周期过程(GB/T 8566—2001,idt ISO/IEC 12207:1995)

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 11457　软件工程术语

GB/T 18336.1　信息技术　安全技术　信息技术安全性评估准则　第1部分:简介和一般模型(GB/T 18336.1—2001,idt ISO/IEC 15408-1:1999)

GB/T 20000.1　标准化工作指南　第1部分:标准化和相关活动的通用词汇(GB/T 20000.1—2002,ISO/IEC 指南 2:1996,MOD)

GB/T 19715.1—2005　信息技术　信息技术安全管理指南　第1部分:信息技术　安全概念和模型(ISO/IEC TR 13335-1:1996,IDT)

ISO/IEC 15288　系统工程　系统生存周期过程