ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20261—2020
代替 GB/T 20261—2006

信息安全技术　系统安全工程 能力成熟度模型

Information security technology—System security engineering—Capability maturity model

(ISO/IEC 21827:2008,Information technology—Security techniques—Systems security engineering—Capability maturity model,MOD)

2020-11-19 发布　　2021-06-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20261—2006《信息技术　系统安全工程　能力成熟度模型》，与 GB/T 20261—2006 相比，主要技术变化如下（主要变化对比表见附录 G）：

——修改了部分规范性引用文件（见第 2 章，2006 年版的第 2 章）；

——增加了术语和定义，即“基本实践”“能力”“信息安全事态”“信息安全事件”“过程域”“风险管理”；

——修改了术语和定义中“保障”“工程组”“工作产品”的定义；并把“残留风险”修改为“残余风险”（见第 3 章，2006 年版的第 3 章）；

——删除了术语“惯例”（见 2006 年版的 3.24）；

——修改了部分章条标题，合并、调整和删除了部分内容关联和不适合作为国家标准的内容（见 4.1、4.2、4.3、4.4、4.5、4.6、5.1）；

——删除了原第 5 章，原第 6 章、第 7 章调整为第 5 章、第 6 章（2006 年版的第 5 章，第 6 章、第 7 章）；

——增加了第 6 章中 BP.06.03 定义安全测量，以及 ISO/IEC 21827：2008 相对于 ISO/IEC 21827：2002 增加及修订的内容（见第 6 章）；

——增加了附录 A 和附录 B（见附录 A、附录 B）；

——修改了附录 C 中对能力等级的 5 个级别的定义，与现行标准 GB/T 30271 等标准描述一致；

——修改了附录 D 中的系列过程域编号与过程域描述不匹配的错误信息（见 D.6.1.1、D.7.7.3、D.9.3.3、D.11.1.1、D.11.4、D.11.4.1、D.12.3.1）；

——增加了附录中为便于标准模型与现行安全服务映射关系的附录 F（见附录 F）；

——增加了与 GB/T 20261—2006 的主要变化对比表（见附录 G）。

本标准使用重新起草法修改采用 ISO/IEC 21827：2008《信息技术　安全技术　系统安全工程　能力成熟度模型》。

本标准与 ISO/IEC 21827：2008 相比在结构上有一定调整，附录 A 中列出了本标准与 ISO/IEC 21827：2008 的章条标号对照一览表。

本标准与 ISO/IEC 21827：2008 相比存在技术性差异，附录 B 中给出了相应的技术差异及原因的一览表。

本标准做了下列编辑性修改：

——将标准名称修改为《信息安全技术　系统安全工程　能力成熟度模型》。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：北京永信至诚科技股份有限公司、中国信息安全测评中心、中新网络信息安全股份有限公司、中国电子技术标准化研究院、北京天融信网络安全技术有限公司、北京奇安信科技有限公司、北京江南天安科技有限公司、公安部第三研究所、国家信息中心、北京邮电大学、北京启明星辰信息安全技术有限公司。

本标准主要起草人：孙明亮、朱胜涛、王军、温哲、李斌、位华、王琰、张晓菲、蔡晶晶、陈冠直、王龑、郭颖、郑新华、杨建军、刘贤刚、上官晓丽、许玉娜、任卫红、袁静、高亚楠、余慧英、李小勇、吕俐丹、侯晓雄、米凯、吴璇、乔鹏、刘蕾杰、梁峰。

本标准所代替标准的历次版本发布情况为：

——GB/T 20261—2006。

引　言

本标准依据国际标准最新版本(ISO/IEC 21827:2008),结合国内最优实践,从系统安全工程的科学性和可指导性出发进行修订,对标准术语、安全工程过程域及能力维进行更新和优化。

0.1　概要

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——各种各样的组织都在实践安全工程。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实践。部分组织关注高层次问题(例如涉及运行使用或系统体系结构),另一部分组织则涉及低层次问题(例如,机构选择或者设计),还有些组织两者都涉及。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]是针对所有此类组织而设计的。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® 使用方法是必需的。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)已定义的安全工程实践。除此之外,组织可能需要考虑模型范围内不同实践之间的关系,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。

本标准与过程评估系列标准(ISO/IEC 330XX 系列),特别是 ISO/IEC 33020 有关,因为它们都涉及过程改进和能力成熟度评估。但是,过程评估系列标准适用于所有过程,而 SSE-CMM® 则专注于安全性。

1)　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,要使用几组不同的实践。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。在系统运行期间下,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。

2)　对策开发者

在一个组专注对策开发的情况下,可能要通过 SSE-CMM® 的实践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的其他组(例如软件组)提供输入和指南的实践。提供制定对策服务的组需要理解这些实践之间的关系。

3)　产品开发者

SSE-CMM® 包含部分专门针对理解客户安全需要的实践。要求与客户反复商讨,以便确定这些需要。如果某个产品的开发不受特定客户的约束,该产品的客户就是通用客户。在这种情况下,如果要求考虑客户,可以把产品营销组或其他组作为假想的客户。

安全工程专业人员都理解,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:

- 客户基本类型(产品、系统和服务);

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。

- 保障要求(高与低);
- 对开发和运行组织的支持。

下面讨论两个不同客户群之间的差异,保证要求的不同程度以及 SSE-CMM® 中每个差异的影响。这些是作为组织或行业部门如何确定在其环境中正确使用 SSE-CMM® 的示例。

4) 特定的行业部门

各个行业反映了其特定的文化、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,可预见 SSE-CMM® 的概念可以容易地在所有行业部门中转化成其自身的语言和文化。

0.2 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收入)信任度;
- 标准机制——客户用于评价提供者的安全工程能力。

评估范围应由评估机构确定,如果有必要应与评估人员讨论。

如果使用模型和评估方法的用户透彻地理解模型的正确使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 TR 33014:2013 中找到。

0.3 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,获取者和用户一定要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:

1) 对工程组织

工程组织包括系统集成商、应用开发商、商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、可预计的过程和实践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。

2） 对于获取组织

获取者包括从外部/内部来源获得的系统、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。

3） 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。

信息安全技术　系统安全工程 能力成熟度模型

1　范围

本标准给出了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,它关注信息技术安全(ITS)领域内的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,更不会涉及具体的方法,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。

本标准界定了SSE-CMM®是专门用于改进和评估安全工程能力的模型,不能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"协调安全实践"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。

本标准适用于:

- 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;
- 对产品开发人员、安全系统开发人员和集成商,以及提供计算机安全服务和计算机安全工程组织的要求;
- 政府部门、商业界、学术界的各种类型和规模的安全工程组织;
- 系统安全工程的需求方、提供方和评估方。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.1—2015　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(ISO/IEC 15408-1:2009,IDT)

GB/T 25069—2010　信息安全技术　术语

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2016,IDT)

GB/T 30271—2013　信息安全技术　信息安全服务能力评估准则

ISO/IEC 15288　系统和软件工程　系统生存周期过程(Systems and software engineering—System life cycle processes)

ISO/IEC 33020　信息技术　过程评估　过程评估的过程测量框架(Information technology—Process assessment—Process measurement framework for assessment of process capability)