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)

3 术语和定义

GB/T 25069—2010、GB/T 29246—2017、GB/T 18336.1—2015、GB/T 30271—2013 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 25069—2010 中的某些术语和定义。

3.1

可核查性 accountibility

确保可将一个实体的行动唯一地追踪到此实体的特性。

[GB/T 25069—2010，定义 2.1.18]

3.2

认可 accreditation

权力机构为了对以下三个方面给出正式的认同、批准并且接受他们残余风险所采取的规程：

a) 有关自动化系统的运行，其中该系统运行在特定的安全模式下，使用一套特定的防护措施；

b) 有关承担特定任务的安全机构或个人；

c) 有关针对目标环境的安全服务。

[GB/T 25069—2010，定义 2.3.82]

3.3

评估 assessment

系统化的检验一个实体满足所规约的需求的程度。当用于可交付件时，与评价是同义的。

[GB/T 25069—2010，定义 2.3.66]

3.4

资产 asset

对组织有价值的任何东西。

[GB/T 25069—2010，定义 2.3.113]

3.5

保障 assurance

为使他人获得可交付件满足其安全目标的信心，而履行的适当行为和过程。

[GB/T 25069—2010，定义 2.3.10]

3.6

保障论据 assurance argument

由证据和推理支持的、清楚地证明保障需要是如何得到满足的一组结构化保障声明。

3.7

保障声明 assurance claim

系统满足安全需要的断言或支持性断言。

注：保障声明既针对直接威胁(例如，防止系统数据遭受外部攻击)，也针对间接威胁(例如，使系统代码漏洞尽可能小)。

3.8

保障证据 assurance evidence

可以据以做出保障声明判断或者结论的数据。

注：保障证据可由观察项、测试结果、分析结果和评估结果构成。

3.9

真实性 authenticity

确保主体或者资源的身份正是所声称的特性。真实性适用于用户、进程、系统和信息之类的实体。

[GB/T 25069—2010,定义 2.1.69]

3.10

可用性 availability

根据授权实体的要求可访问和可使用的特性。

[GB/T 29246—2017,定义 2.9]

3.11

基线 baseline

经过一个正式评审并通过的规约或产品,作为后续开发的基础。对其变更只有通过正式的变更控制规程方可进行。

[GB/T 25069—2010,定义 2.2.4.3]

3.12

基本实践 base practices;BP

系统工程过程中应存在的性质,只有当所有这些性质完全实现后,才可说满足了这个过程域的要求。

注:一个过程域由基本实践(BP)组成。

[GB/T 30271—2013,定义 3.1.2]

3.13

能力 capability

组织、体系或过程实现产品并使其满足要求的本领。

3.14

认证 certification

对可交付件是否符合规定需求所给出的正式保证陈述的规程。可由第三方执行认证或自行认证。

[GB/T 25069—2010,定义 2.3.84]

3.15

保密性 confidentiality

使信息不泄露给未授权的个人、实体、过程,或不被其利用的特性。

[GB/T 25069—2010,定义 2.1.1]

3.16

一致性 consistency

在某一系统或构件中,各文档或各部分之间统一的、标准化的和无矛盾的程度。

[GB/T 25069—2010,定义 2.1.62]

3.17

正确性 correctness

针对规定的安全要求,产品或者系统显示其正确实现这些要求的表现。

3.18

客户 customer

供方提供的产品的接收者。

注 1:在合同条件下,客户叫做买方。

注 2:客户可以是最终客户、用户、受益人或买方。

注 3:客户可以是组织外部的,也可以是组织内部的,见 ISO 9000。

3.19

有效性 effectiveness

对某一系统或者产品，在建议的或实际的运行使用环境下，表示其提供安全程度的特性。

3.20

工程组 engineering group

对与特定工程学科相关的项目或组织活动负责的人群（包括管理人员和技术人员）。

注：工程学科包括硬件、软件、软件配置管理、软件质量保障、系统、系统测试和系统安全。

3.21

证据 evidence

过程和（或）产品的可直接测量的特征，它体现具体活动满足规定要求的客观的、可表明的证明。

3.22

信息安全事态 information security event

表明一次可能的信息安全违规或某些控制失效的发生。

[GB/T 20985.1—2017，定义 3.3]

3.23

信息安全事件 information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全事态。

[GB/T 20985.1—2017，定义 3.4]

3.24

完整性 integrity

准确和完备的特性。

[GB/T 29246—2017，定义 2.40]

3.25

维护 maintenance

交付后为了纠正缺陷、改进性能以及其他属性或适应环境变化而对系统或组件进行修改的过程。

[GB/T 25069—2010，定义 2.3.97]

3.26

方法学 methodology

定义系统或产品的完整开发途径的标准、规程和支持方法的集合。

3.27

渗透轮廓 penetration profile

对渗透所要求的活动的定义。

3.28

规程 procedure

对执行一个给定任务所采取动作历程的书面描述。

[GB/T 25069—2010，定义 2.1.7]

3.29

过程 process

将输入转换成输出的相互关联或相关作用的活动集。

[GB/T 29246—2017，定义 2.61]

3.30

过程域 process area；PA

一组相关系统工程过程的性质，当这些性质全部实施后则能够达到过程域定义的目的。

[GB/T 30271—2013,定义 3.1.10]

3.31

可靠性 reliability

与预期行为和结果一致的特性。

[GB/T 29246—2017,定义 2.62]

3.32

残余风险 residual risk

风险处置后余下的风险。

注 1：残余风险可能包含未识别的风险。

注 2：残余风险也可以被称为“保留风险”。

[GB/T 29246—2017,定义 2.64]

3.33

风险 risk

对目标的不确定性影响。

注 1：影响是指与期望的偏离(正向的或反向的)。

注 2：不确定性是对事态及其结果或可能性的相关信息、理解或知识缺乏的状态(即使是部分的)。

注 3：风险常被表征为潜在的事态和后果,或者它们的组合。

注 4：风险常被表示为事态的后果(包括情形的改变)和其发生可能性的组合。

注 5：在信息安全管理体系的语境下,信息安全风险可被表示为对信息安全目标的不确定性影响。

注 6：信息安全风险与威胁利用信息资产或信息资产组的脆弱性对组织造成危害的潜力相关。

[GB/T 29246—2017,定义 2.68]

3.34

风险分析 risk analysis

理解风险本质和确定风险等级的过程。

注 1：风险分析提供风险评价和风险处置决策的基础。

注 2：风险分析包括风险估算。

[GB/T 29246—2017,定义 2.70]

3.35

风险管理 risk management

指导和控制组织相关风险的协调活动。

[GB/T 29246—2017,定义 2.76]

3.36

安全策略 security policy

用于治理组织及其系统内如何管理、保护和分发资产(包括敏感信息)的规则、指导和实践,特别是那些影响系统及相关要素的。

3.37

安全相关要求 security related requirement

直接作用于系统安全运行或者强制执行规定安全策略的要求。

3.38

系统 system

具有物理存在和既定目的的、完全由集成的、交互的组件组成的离散的可区分实体,每个组件不单独符合所要求的总体目的。

注 1：在实践中,系统是“在旁观者眼中的”,通常用联合名词来澄清其含义(例如,产品系统、飞机系统)。另一种方

式是使用上下文依赖的同义词(例如,产品、飞机)进行简单取代,尽管这可能使系统原理观点变得模糊。

注2:系统在其生存周期中,为了满足自身的需求,可能需要其他系统。例如,一个运行系统可能需要一个系统用于概念化、开发、生产、运行、支持或处置。

3.39

威胁 threat

不论是内部还是外部引起的,可能对信息、程序或系统造成损害或者波及其他损害的,敌对者的能力、意图和攻击方式,或者任何环境或事件。

3.40

威胁方 threat agent

故意或意外的人为威胁的原发方和/或发起方。

[GB/T 25069—2010,定义 2.3.95]

3.41

确认 validation

通过提供客观证据,证实满足特定预期使用或应用要求的行为。

[GB/T 29246—2017,定义 2.87]

3.42

验证 verification

通过提供客观证据,证实满足规定要求的行为。

注:也可称为符合性测试。

[GB/T 29246—2017,定义 2.88]

3.43

脆弱性 vulnerability

可能被一个或多个威胁利用的资产或控制的弱点。

[GB/T 29246—2017,定义 2.89]

3.44

工作产品 work product

在执行任何过程中产生出的所有文档、报告、文件、数据等。

[GB/T 30271—2013,定义 3.1.13]

注:一个工作产品可能被一个过程使用、生产或者改变。

4 系统安全工程概述

4.1 安全工程的开发背景

需求方和提供方都期望改进安全产品、系统和服务。安全工程领域已经存在一些普遍接受的原则,但是目前还缺乏评价安全工程管理的综合性框架。SSE-CMM®通过确定这样一个框架,提供了一个测量和改进安全工程原则应用性能的方法。

安全工程是一门独特的学科,要求专门的知识、技能和过程为开发安全工程特有的能力成熟度模型提供保证。这种要求与基于系统工程实施安全工程的要求并不相悖。事实上,充分定义的和公认的系统工程活动可以使安全工程在各种背景下有效开展。

现代统计过程控制认为,通过强调产品生产过程的质量管理以及过程中组织实践行为的成熟度,能够生产出质量更高的产品,并有效节约成本。倘若增加安全系统和可信产品开发要求的费用和时间,将保证过程更有效。安全系统的运行和维护依赖于人和技术的结合。强调所有这些过程的质量以及过程内在组织实践行为的成熟度,能够更好地管理这些依赖关系。

SSE-CMM®项目的目标是使安全工程提升成为一门得到定义的、成熟的和可度量的学科。SSE-CMM®和评估方法的开发是为了促成：

- 各个工程组关注安全工程工具、培训、过程定义、管理实践以及改进领域内的投资；
- 基于能力的保障，即基于工程组的安全实践和过程的成熟度的置信度的可信性；
- 通过按能力等级和与之相关的风险来区分投标者，选择有合适资格的安全工程提供方。

SSE-CMM®描述一个组织中为确保优质安全工程而需具备的安全工程过程的基本特性。该模型汇集了在行业中普遍遵循的实践，且不规定具体的过程或顺序。对于覆盖下列领域的安全工程实践，这个模型提供了一个统一的衡量尺度：

- 整个生存周期，包括开发、运行、维护和退役等活动；
- 整个组织，包括管理类、组织类和工程类活动；
- 与其他学科（例如，系统、软件、硬件、人机工程和测试工程，以及系统管理、运行和维护）的并发交互作用；
- 与其他组织的交互作用，包括获取、系统管理、认证、认可和评价。

SSE-CMM®的模型描述包括：该模型所依据的原理和体系结构的综述，模型的执行概要，正确使用该模型的建议，模型中包括的实践，以及模型属性描述。它还包括模型的开发要求。SSE-CMM®的评估方法描述用于对照该模型评价一个组织的安全工程能力的过程和工具。

4.2 安全工程的重要性

安全工程正成为一门越来越重要的学科，是多学科并发工程队伍里的一个关键组成部分，适用于系统和应用项目的开发、集成、运行、管理、维护和演化，以及产品的开发、交付和改进。安全关注的内容应在企业和业务过程的定义、管理和重新设计中提出。

通常，安全工程的目标包括：

- 识别与企业有关的安全风险；
- 按照已识别的风险确立一组均衡的安全需求；
- 把安全需求转变成安全指南，并纳入某个项目的实施活动中和某个系统配置或运行的描述中；
- 确定安全机制正确性和有效性的置信度或保障；
- 确定由于系统或它的运行中残留的安全脆弱性对运行造成的影响是可以容忍的（如：确定可接受的风险）；
- 从对系统可信性的综合理解上统筹考虑所有工程学科和专业的工作。

4.3 安全工程组织

安全工程活动由各种类型的组织实施，例如：

- 开发者；
- 产品销售商；
- 集成商；
- 采购方（采购组织或者最终用户）；
- 安全评价组织（系统认证机构、产品评定机构，或者运行认可机构）；
- 系统管理员；
- 可信的第三方（认证机构）；
- 咨询/服务机构。

4.4 安全工程生存周期

在下列所有的生存周期阶段都要推进安全工程活动：

- 概念阶段；
- 开发阶段；
- 生产阶段；
- 使用阶段；
- 支持阶段；
- 退役阶段。

4.5 安全工程和其他学科

安全工程活动和许多其他学科相关联，包括：

- 系统工程；
- 软件工程；
- 人机工程；
- 通信工程；
- 硬件工程；
- 企业管理。

注 1：关于系统工程的更多信息，见 ISO/IEC 15288，该标准从系统的角度观察安全。

注 2：关于软件工程的更多信息，见 GB/T 8566—2007，该标准从软件的角度观察安全。

安全工程活动应协调许多外部实体进行，因为残留运行影响的保障和可接受性是与开发者、集成商、采购方、用户、独立评价师以及其他群体共同确立的。正是由于众多组织之间的这些接口和必不可少的相互作用，使得安全工程特别复杂并且有别于其他工程学科。

4.6 安全工程专业

尽管在当前的安全和业务环境中，安全工程和信息技术安全是发展强劲的学科，但是也不应忽视其他传统安全学科，例如物理安全和人员安全。如果这些传统安全学科和其他专业学科分支在它们的工作中可以取得很好的效果，安全工程就应利用它们。下面的清单列出了部分专业安全学科分支的例子，同时给出简短描述，包括：

- 运行安全——目标是运行环境的安全性以及安全运行态势的维护；
- 信息安全——关于信息以及信息被操纵和处理期间的安全维护；
- 网络安全——涉及网络硬件、软件和协议以及网络中传输的信息的保护；
- 物理安全——核心是保护建筑物和物理场所的安全；
- 人员安全——关系到人员、人员可信性以及他们的安全意识；
- 安全管理——关系到安全性的行政管理和行政管理系统的安全性；
- 发射安全——处理由所有那些能够向安全区域以外传输信息的机器产生的不希望的信号。

5 模型体系结构

5.1 安全工程过程概述

SSE-CMM® 是安全工程最佳实践的汇编。本章提供安全工程的高层次描述，然后说明模型的体系结构如何反映这种基本认识。

安全工程过程分为三个基本领域：风险、工程和保障，见图 1。这些领域之间存在关联关系，并不相互独立，为研究方便，也可以针对单个进行研究。在最简单的层次上，风险过程识别所开发的产品或系统的内在风险，并且给出优先顺序。针对这些危险所呈现的问题，安全工程过程与其他工程学科一起确

定和实现相应的解决方案。最后，保障过程确立安全解决方案的置信度并且把置信度传递给客户。

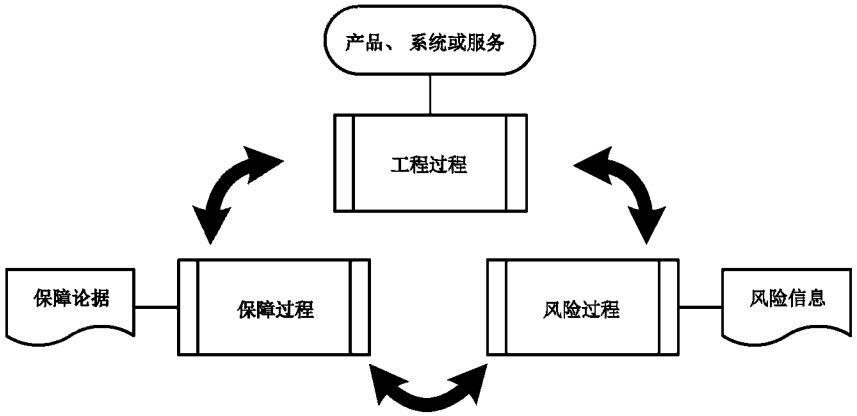

图 1　安全工程过程的三个主要领域

总而言之，这三个领域一起工作，其共同目标是确保安全工程过程的结果达到上述各个目标。

5.1.1　风险

安全工程的一个主要目标是减少风险。风险评估是识别尚未发生的问题的过程，其通过检查威胁和脆弱性的可能性以及研究安全事件的潜在影响来评估风险，见图 2。可能性是一个不确定因素，它将随具体情况的变化而变化，换句话说，可能性只能是在一定的限制范围内才能够进行预测。此外，由于安全事件可能不会发生，因此所评估的某特定风险的影响也存在相应的不确定性。因而，对于预计准确性而言，可能存在大量的不确定因素，所以对安全性作准确的预测和判断是非常困难的。一种简单经济同时又是局部的处理方式，是实现相关的事件检测技术。

一个安全事件由三个部分构成：威胁、脆弱性和影响。脆弱性是可能被某个威胁利用的资产属性，包括各种弱点。如果既没有威胁也没有脆弱性，就不会发生安全事件，因而也就没有风险。风险管理是协调、指挥和控制一个组织风险管理工作的活动，包括建立组织可接受的风险水平，并相应地识别、分析、评估和处置风险。管理风险是安全管理的一个重要组成部分。

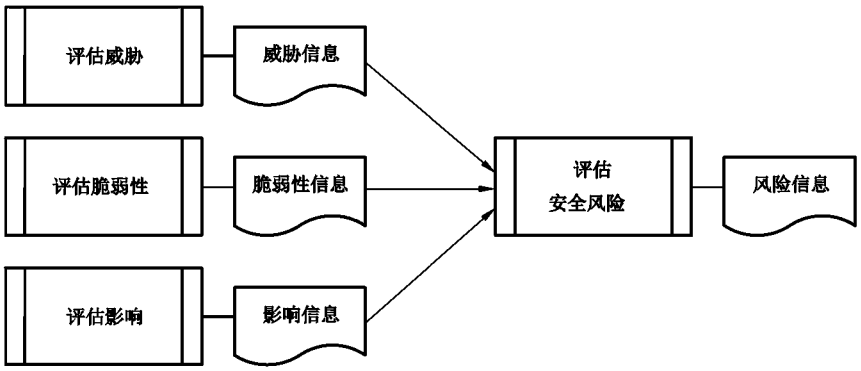

图 2　安全风险过程

通过采取防护措施处置风险，可能涉及威胁、脆弱性、影响或者风险本身。处置所有风险或者完全消除某特定风险是不可行的，这在很大程度上取决于风险处置成本以及相关的不确定性。因此，应接受某些残余风险。在不确定度比较高的情况下，风险接受。系统有关的不确定性是处于风险接受者控制的少数几个领域之一。SSE-CMM® 过程域包括的活动有助于确保供方组织分析威胁、脆弱性、影响以及相关的风险。

5.1.2 工程

安全工程包括概念、设计、实施、测试、部署、运行、维护和退役等阶段。在这整个过程中，安全工程师应与系统工程队伍的其他部分紧密配合开展工作。SSE-CMM® 强调安全工程师是一个更大团队的一部分，需要与其他学科的工程师合作并协调他们的活动。这有助于确保安全成为这个更大过程的一个组成部分，而不是一个独立而又独特的活动。

根据上述风险过程的信息，以及其他有关系统需求的信息、相关的法律和政策、安全工程师和客户一起确定安全需求，见图 3。一旦确定需求，安全工程师要确定和跟踪具体的安全要求。

建立安全问题解决方案的过程通常先确定可行的候选方案，然后评估候选方案，找到其中最可行的。整合这项活动与工程过程的其他活动的困难在于选择解决方案时不能只考虑安全，而是还应结合成本、性能、技术风险以及使用的简便性等因素一并考虑。

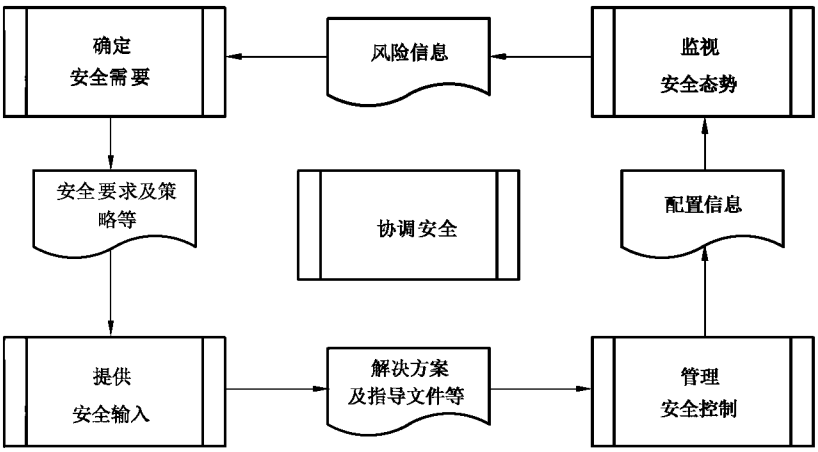

图 3 安全是整个工程过程的不可或缺的组成部分

在生存周期的后面阶段，需要安全工程师确保按照已经识别到的风险对产品和系统进行正确的配置，确保残余风险不会影响系统的安全运行。

5.1.3 保障

“保障”是非常重要的安全工程产品，目前存在多种形式的保障。SSE-CMM® 的一个贡献是对安全工程过程结果的可重复性赋予置信度。该置信度的理论基础是：一个成熟的组织比一个不成熟的组织更有可能重复这些结果，见图 4。

保障并不增加任何遏制安全风险的控制手段，而是提供已实施控制手段将减少风险的置信度。

保障是防护措施将发挥预期作用的置信度。该置信度来源于正确性和有效性两方面，其中正确性是指按照设计正确地实现防护措施；有效性是指防护措施可以有效地提供的满足客户需要的安全服务。

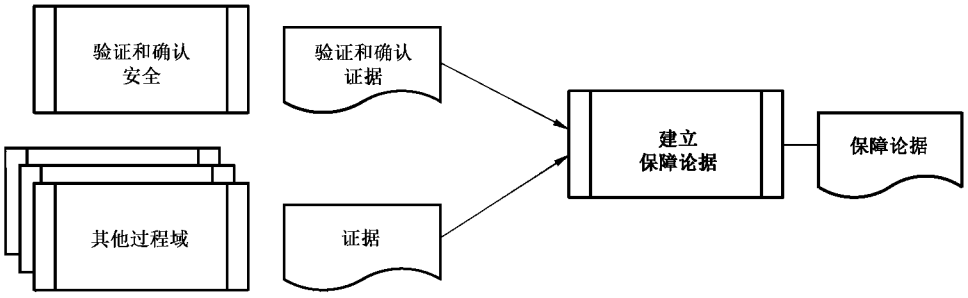

图 4 保障过程建立保障论据

保障可以论据的形式来传达。论据是指包括一组有关系统属性的声明，这些声明需要证据给予支持，而证据的形式通常是安全工程活动正常推进期间产生的文档。

SSE-CMM®活动本身涉及与保障相关证据的产生，例如过程文档化可以表明开发工作遵循了充分定义的、成熟的工程过程以便持续改进；而安全验证和确认则在建立产品或者系统的可信性的过程中扮演重要角色。

各个过程域中的许多工作产品示例将成为保障的一部分或者为证据做贡献。现代统计过程控制认为，通过关注生产产品的过程，可以更经济地、可重复地生产出更高质量和具有更高保障的产品。组织实践的成熟度将会影响和促进这个过程。

5.2 SSE-CMM®体系结构描述

5.2.1 基本模型

SSE-CMM®体系结构将安全工程过程的基本特征从其过程的管理和制度化特征中清晰地分离出来，从而用于确定安全工程组织的过程成熟度。为了确保分离，该体系结构涉及了“域”和“能力”两个维度，域维具体内容在第6章中描述，能力维的通用实践和能力成熟度概念分别在附录C和附录E中描述。需要说明的是，SSE-CMM®本身并不强调组织内的任何角色都一定要执行模型中所描述的任何过程，也没有要求一定要使用最新的和最好的安全工程技术或者方法。模型要求一个组织把包含有模型中描述的基本安全实践的过程放在适当的位置。在建立组织自己的、满足本组织业务目标的过程和组织结构方面，组织是自由的。

SSE-CMM®设计了两个维度，即“域”维和“能力”维。两维中，域维由共同定义安全工程的所有实践构成，其中这些实践被称为“基本实践”。

能力维描述过程管理和制度化能力的实践，这些实践被称为“通用实践”。通用实践描述的活动应作为基本实践实施时的一部分予以执行。

图5说明了基本实践和通用实践之间的关系。图5中，“识别系统安全脆弱性”是安全工程的一个基本实践（编号为“BP.05.02”），因而“分配资源”是安全工程的一个通用实践（编号为“GP 2.1.1”），该通用实践通过检查组织分配资源的过程来判断该组织完成工作的能力程度。按照图5，可以得到一种检查某个组织执行某个特定活动的能力程度的方法。比如，如果对问题“你的组织为识别系统安全脆弱性分配了资源吗？”的回答是“是”，那么调查者可以了解到该组织具备该能力。

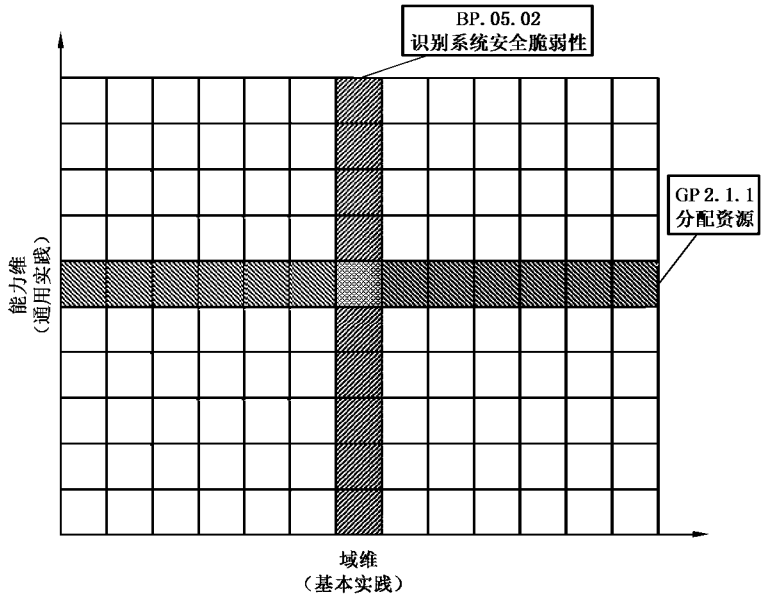

图5 模型对每个过程域的每项公共特征进行评价

通过把所有的基本实践和所有的通用实践结合在一起，并对类似的问题进行调查和答复，将得到一幅令人满意的、关于该组织安全工程能力的实况图。

5.2.2 基本实践

SSE-CMM®共包括130个基本实践，分布在22个过程域中，其中的62个基本实践分布在6.2所述安全工程领域的11个过程中；其余68个基本实践分布在11个描述项目和组织的过程域中，这些过程与来自系统工程和软件能力成熟度模型，为系统安全工程的过程提供背景和支持。安全工程领域的基本实践是根据广泛的现有资料、实践和专家意见综合得出的，所选择的基本实践代表了安全工程界的现行最佳实践，而不是没有使用过的实践。

识别安全工程基本实践是复杂的，因为很多活动具有不同名称，但其本质上却是相同的。其中部分活动发生在生命周期的后期，在不同的抽象层次上，通常由不同角色的个人执行。但是，如果一个组织只在设计阶段或在一个抽象的层次上执行，那么它就不能被认为已经实现了一个基本实践。因此，SSE-CMM®忽略了这些区别，并确定了对良好安全工程实践至关重要的基本实践的集合。

一个基本实践：

- 适用于企业的生存周期；
- 不和其他基本实践重叠；
- 代表安全界的一个“最佳实践”；
- 不是简单的反映最新技术水平；
- 可以在不同的业务背景中使用不同的方法；
- 不指定特定的方法或者工具。

已经使用满足广大安全工程组织需要的方法把基本实践安排到各个过程域中。把安全工程划分过程域的方法有许多，一类方法可能尝试模仿现实世界，创建与各个安全工程服务相匹配的多个过程域；另一类方法则试图反映构成安全工程基本构造块的各个概念领域。SSE-CMM®中涉及过程域，是在这些对立的目标之间折中后形成的结果。

每一个过程域都有一组目标，这些目标描述了组织对成功执行该过程域的期望。

一个过程域：

- 为了便于使用，把相关的活动组合到一个域中；
- 与有价值的安全工程服务相关；
- 适用于企业的生存周期；
- 能够在不同的组织和产品背景中实施；
- 能够作为一个独特的过程进行改进；
- 能够由具有相关利害关系的组织进行改进；
- 包含所有为满足该过程域的目标所需求的基本实践。

下面列出SSE-CMM®的11个安全工程过程域。在第6章中将详细描述这些过程域的内容，并定义它们的基本实践，附录F中阐述了常见信息安全服务与过程域的映射关系。这11个过程域如下：

- PA01 管理安全控制；
- PA02 评估影响；
- PA03 评估安全风险；
- PA04 评估威胁；
- PA05 评估脆弱性；
- PA06 建立保障论据；
- PA07 协调安全；
- PA08 监视安全态势；
- PA09 提供安全输入；

- PA10 确定安全需要；
- PA11 验证和确认安全。

SSE-CMM®还包括 11 个与项目和组织实践相关的过程域，这些过程域是根据系统工程能力成熟度模型改编的，在附录 D 中描述了这些过程域和其所包含的基本实践。这些过程域如下：

- PA12 确保质量；
- PA13 管理配置；
- PA14 管理项目风险；
- PA15 监督和控制技术工作；
- PA16 策划技术工作；
- PA17 定义组织系统工程过程；
- PA18 改进组织系统工程过程；
- PA19 管理产品线演化；
- PA20 管理系统工程支持环境；
- PA21 提供持续发展的技能和知识；
- PA22 与供方协调。

注：这些过程域的详细说明在附录 D 中，将来应与 ISO/IEC 15288 保持一致。

5.2.3 通用实践

通用实践应用于所有的过程，涉及过程的管理、测量和制度化，用于评估判定组织执行某个过程的能力。

通用实践按照“公共特征”进行逻辑归类，每个公共特征有一个或多个通用实践。“公共特征”描述一个组织特有的工作过程（在这种情况下是指安全工程域）的执行能力，按照能力成熟度递增划分了五个“能力等级”。最低的公共特征是“1.1 执行基本实践”。这个公共特征仅仅检查一个组织是否执行了某个过程域的所有基本实践。不同于域维的基本实践，能力维的通用实践是按成熟度进行等级划分的，高过程能力等级的通用实践位于能力维的顶端。

公共特征包含的通用实践有助于从整体上判断项目管理的优劣以及每个过程域的改进情况。通用实践（见附录 C）的分组是为了强调一个组织特有的安全工程实施手段的重大变化。表 1 中列出通用实践中的一些原则。

表 1 能力维原则

原则	SSE-CMM®中的表述形式
只有做它才能够管理它	基本执行级关注的是一个组织是否执行某个包含基本实践的过程
在定义组织范围的过程之前，理解有关项目（包括产品）正在发生的事情	计划跟踪级关注的是项目级定义、策划和执行问题
使用从项目中总结的最好经验来创建组织范围的过程	充分定义级关注的是对组织级的已定义过程的合理裁剪
只有知道了“它”是什么，才能测量它	尽管早期（例如，在计划跟踪级）就开始收集和使用项目基本测量数据很重要，但是在达到充分定义级，尤其是量化控制级之前，不指望在整个组织范围测量和使用数据
只有测量正确的对象时，对测量的管理才有意义	量化控制级关注的是与组织的业务目标紧密结合的测量
一种持续改进的文化要求一个由健全的管理实践、已定义的过程和可测量的目标形成的基础	通过所有在以前各个等级中观察到的管理实践的改进，持续改进级起到杠杆作用，然后强调维持这些收获的文化变迁

下述公共特征描述了为达到每个等级必需的安全工程成熟度的属性。这些公共特征以及定义它们的通用实践在附录C中描述。

等级1：

- 1.1 执行基本实践。

等级2：

- 2.1 计划执行；
- 2.2 规范执行；
- 2.3 验证执行；
- 2.4 跟踪执行。

等级3：

- 3.1 定义标准过程；
- 3.2 执行已定义过程；
- 3.3 协调实践。

等级4：

- 4.1 建立可度量的质量目标；
- 4.2 客观管理性能。

等级5：

- 5.1 改进组织能力；
- 5.2 改进过程有效性。

SSE-CMM®并不对通用实践的选择和执行有特殊要求。一个组织通常可以自由地采用自己选择的任何方式或者顺序来策划、跟踪、定义和改进自己的过程。不过，由于一些较高级别的实践依赖于较低级别的实践，因此鼓励组织在尝试达到较高级别之前最好先实施较低级别的通用实践。

5.2.4 能力等级

有多种方法可以将实践按照公共特征分组，或将公共特征按照能力等级分组。

公共特征的排序源于以下现象：一些实践的执行和制度化受益于其他实践的存在。如果实践得到妥善制定，这尤其正确。在一个组织能够有效地定义、裁剪和使用某个过程之前，单个项目应能积累一些管理该过程的经验。例如，在针对整个组织制度化某个具体的估计过程之前，这个组织应首先在某个项目中尝试使用这个估计过程。不过，过程执行和制度化的某些方面应一起（而不是按先后顺序）考虑，因为它们一起工作将会增强实际能力。

在执行评估和改进组织的过程能力时，公共特征和能力等级都重要。如果评估发现某个组织在某个特定过程的特定能力等级实施了一部分公共特征，那么这个组织通常是运行在该过程最低的已执行能力等级上。例如，假如某个组织没有实施某过程域2级的一个通用实践，应给这个组织定级为1级。如果一个组织在给定能力级别上实施了所有的公共特征，但是并没有实施较低能力级别的某个公共特征，那么这个组织不可能充分得到前者带来的收益。评估组在评估组织的各个过程的时候，应考虑这种情况。

在改进组织的过程能力时，为了提高某特定过程的能力，最好把实践按照能力等级进行分组，从而可为组织提供一幅“改进路线图”。因此，SSE-CMM®中的实践都归类到各个按能力等级排序的公共特征中。

应执行评估程序来判定每个过程的能力等级。不同的过程域根据其实际情况可能将处于不同能力等级。在判定后，组织可根据评估信息来改进其安全过程。组织应将安全过程改进的优先权和先后顺序纳入业务目标考虑范畴。

在解释一个模型，例如SSE-CMM®时，业务目标是原动力。但是，各项活动有它们的基本顺序，而

各项典型改进工作的逻辑顺序也有它的基本原理。这种活动顺序用 SSE-CMM® 体系结构能力等级的公共特征和通用实践表示。

SSE-CMM® 包括 5 个等级，如图 6 所示。

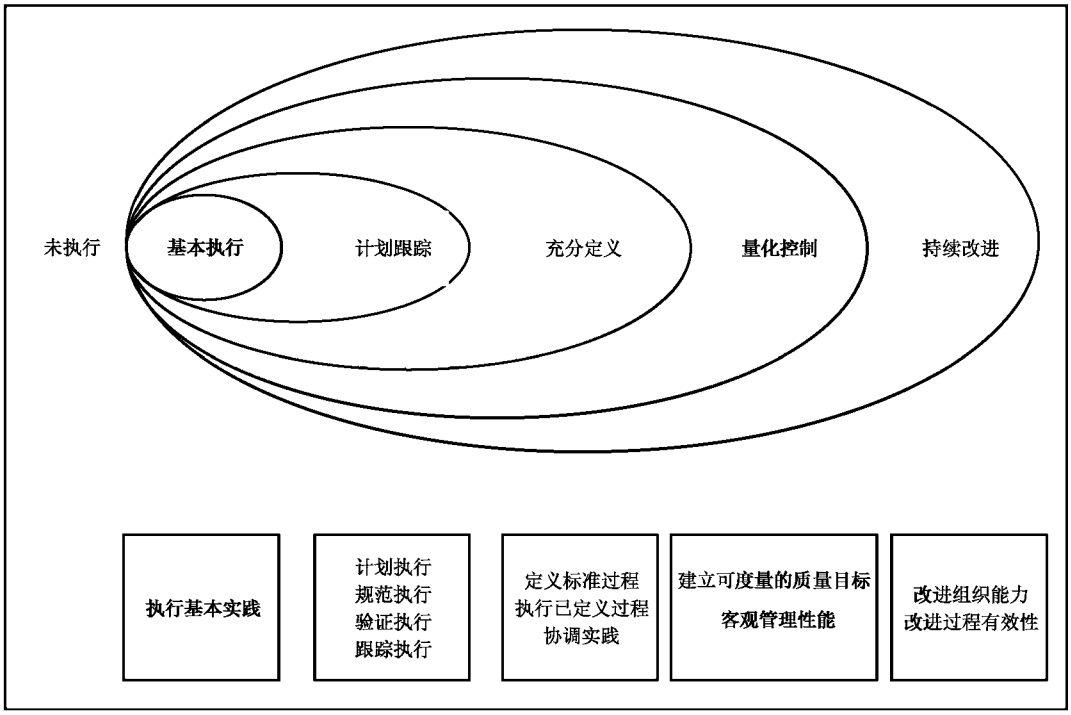

图 6　安全工程组织成熟度的能力等级

5.2.5　能力维/测量框架映射

由于均关注过程改进和能力成熟度评估，本标准与 ISO/IEC 33001、ISO/IEC 33020 等系列标准相关。相对而言，ISO/IEC 33001、ISO/IEC 33020 等系列标准偏向于关注软件过程，而 SSE-CMM® 则偏向于关注安全。SSE-CMM® 的能力维与 ISO/IEC 33020 的测量框架之间虽然在结构上存在差别，但是详细内容和目的方面的差别微乎其微。在 SSE-CMM® 中，能力维按“能力等级”分组，每个能力等级由若干个“公共特征”组成，每个公共特征又由一个或多个“通用实践”组成，见图 C.1。在 ISO/IEC 33020 中，测量框架由若干个“等级”组成，每个等级由若干过程属性组成。表 2 给出了 SSE-CMM® 的能力等级与 ISO/IEC 33020 的等级之间的映射关系。

表 2　能力维到测量框架之间的映射

SSE-CMM® 的能力维	ISO/IEC 33020 的测量框架
[在 SSE-CMM® 中没有明确地定义等级 0，而是隐含指出该等级]	等级 0：不完整的过程
能力等级 1 基本执行	等级 1：已执行过程
公共特征 1.1 执行基本实践	PA1.1 过程执行属性
能力等级 2 计划跟踪	等级 2：受管理过程
公共特征 2.1 计划执行 公共特征 2.4 跟踪执行	PA2.1 执行管理属性

表 2（续）

SSE-CMM® 的能力维	ISO/IEC 33020 的测量框架
公共特征 2.2 规范执行 公共特征 2.3 验证执行	PA2.2 工作产品管理属性
能力等级 3 充分定义	等级 3：已建立的过程
公共特征 3.1 定义标准过程 公共特征 3.2 执行已定义过程	PA3.1 过程定义属性
GP 2.1.1——分配资源 GP 2.1.2——指派责任 GP 2.1.5——确保培训	PA3.2 过程部署属性
公共特征 3.3 协调实践	[没有直接对应的内容]
能力等级 4 量化控制	等级 4：可预知的过程
公共特征 4.1 建立可度量的质量目标	PA4.1 定量分析属性
公共特征 4.2 客观管理性能	PA4.2 定量控制属性
能力等级 5 持续改进	等级 5：创新性过程
公共特征 5.1 改进组织能力	PA5.1 过程创新属性
公共特征 5.2 改进过程有效性	PA5.2 过程创新实施属性

5.2.6 与 ISO/IEC 15288 的关系

本标准和 ISO/IEC 15288 的基本概念和使用的方法都非常相似。但由于本标准与 ISO/IEC 15288 的开发环境不一样，所以两个标准的术语和详细内容之间存在区别。此外，本标准的目标是另一个不同的学科领域——系统安全工程，这也不可避免地导致标准间的差别。这些差别都不大，只是在应用时需要加以注意。

二者间关系的示例如下：

- 本标准的过程域直接对应到 ISO/IEC 15288 的过程；
- 本标准的基本实践直接对应到 ISO/IEC 15288 的活动；
- 本标准的工作产品直接对应到 ISO/IEC 15288 的成果；
- 本标准的过程描述与 ISO/IEC 15288 的过程描述相同。

下面的表 3 给出本标准的过程域和 ISO/IEC 15288 的过程之间的主要关系对照。

注 1：如果一行包含多个“X”，说明 ISO/IEC 15288 的这个特定过程被本标准中的多个过程域覆盖。

注 2：如果一列包含多个“X”，说明本标准的这个过程域被 ISO/IEC 15288 的多个过程覆盖。

表 3　本标准过程域和 ISO/IEC 15288 过程之间的关系

ISO/IEC 15288 过程	本标准过程域																						
	PA01	PA02	PA03	PA04	PA05	PA06	PA07	PA08	PA09	PA10	PA11	PA12	PA13	PA14	PA15	PA16	PA17	PA18	PA19	PA20	PA21	PA22	备注
采办																						X	
供应										X												X	
生存周期模型管理																	X	X					
基础设施管理																	X					X	
项目组合管理																							NRE
人力资源管理																					X		
质量管理	X											X							X	X			
知识管理																							
项目计划																X							
项目评估和控制															X								
决策管理										X													
风险管理														X									
配置管理													X										
信息管理						X	X																
测量		X																					
质量保证												X											
业务或使命分析										X													
相关方需要和需求定义										X													
系统需求定义			X						X	X	X												

表 3（续）

ISO/IEC 15288 过程	本标准过程域																						
	PA01	PA02	PA03	PA04	PA05	PA06	PA07	PA08	PA09	PA10	PA11	PA12	PA13	PA14	PA15	PA16	PA17	PA18	PA19	PA20	PA21	PA22	备注
架构定义									X														
设计定义									X														
系统分析									X														
实施																							NRE
集成																							NRE
验证											X												
移交																							NRE
确认											X												
运行								X											X				
维护	X								X														
弃置	X																						
备注				NRE	NRE																		
图例	X：过程和过程域之间有关系；NRC：没有实际相当的内容																						

5.3 汇总表

图 7 用关系表格抽象地表示了 SSE-CMM® 模型。需要注意的是：每个过程域都是由若干个基本实践组成，基本实践的描述参见第 6 章和附录 D；每个公共特征由若干个通用实践组成，通用实践的描述见附录 C。每个组织都可以选择适用的过程域的组合。

公共特征	过程域	PA01 管理安全控制	PA02 评估影响	PA03 评估安全风险	PA04 评估威胁	PA05 评估脆弱性	PA06 建立保障论据	PA07 协调安全	PA08 监视安全态势	PA09 提供安全输入	PA10 确定安全需要	PA11 验证和确认安全	PA12 确保质量	PA13 管理配置	PA14 管理项目风险	PA15 监督和控制技术工作	PA16 策划技术工作	PA17 定义组织系统工程过程	PA18 改进组织系统工程过程	PA19 管理产品线演化	PA20 管理系统工程支持环境	PA21 提供持续发展的技能和知识	PA22 与供方协调
5.2 改进过程有效性																							
5.1 改进组织能力																							
4.2 客观管理执行																							
4.1 建立可度量的质量目标																							
3.3 协调实践																							
3.2 执行已定义过程																							
3.1 定义标准过程																							
2.4 跟踪执行																							
2.3 验证执行																							
2.2 规范执行																							
2.1 计划执行																							
1.1 执行基本实践																							
		安全工程过程域											项目和组织过程域										

图 7 过程域与公共特征关系汇总

6 安全基本实践

6.1 安全基本实践概述

本章描述各项基本实践的内容，这些基本实践对指导基本安全工程至关重要。注意：各个过程域没有按照任何特定顺序编号，因为 SSE-CMM® 不规定具体的过程或者顺序。

一个组织可以按照任何一个单一的过程域或多个过程域的组合来接受评估。过程域组合在一起是为了覆盖安全工程中的所有基本实践，此时各个过程域之间存在多种交互关系。目前，SSE-CMM® 包含 11 个安全过程域，每个过程域包括若干个基本实践。下面各节中将讨论每个过程域的内容。

每个过程域描述的格式如图 8 中所示，其中“概要描述”简要概述了该过程域的作用。每个过程域被分解成若干个基本实践，这些基本实践是强制项（即，为了达到这些基本实践所支持的过程域的目的，它们应得到成功实施），每个基本实践在后面给出了详细描述；“目标”确定了希望通过执行该过程域达到的最终结果。

PA01——过程域标题(采用动词-名词形式)
概要描述——该过程域的概述
目标——表明实现该过程域的期望结果列表
基本实践列表——显示每个基本实践的编号和名称列表
过程域注释——关于该过程域的任何其他注释
BP.01.01——基本实践标题(采用动词-名词形式)
描述名——描述该基本实践的一句话
描述——该基本实践的概述
工作产品示例——说明某种可能输出的示例列表
注释——关于该基本实践的任何其他注释
BP.01.02……

图 8　过程域格式

6.2　PA01——管理安全控制

6.2.1　过程域

6.2.1.1　概要描述

“管理安全控制”的目的是确保系统运行时能实际达到系统预期安全,而这些系统预期安全是被集成到系统设计中的。

6.2.1.2　目标

正确地配置和使用安全控制。

6.2.1.3　基本实践列表

BP.01.01 建立安全控制的职责和可核查性,并且传达给组织中每个成员。
BP.01.02 管理系统安全控制的配置。
BP.01.03 管理针对所有用户和管理员的安全意识、培训和教育计划。
BP.01.04 管理安全服务和控制机制的定期维护和管理。

6.2.1.4　过程域注释

该过程域提出管理和维护针对开发环境和操作系统的安全控制机制所要求的活动。进一步地,随着时间的推移,这个过程域还将有助于确保安全等级不会下降。对新设施的控制措施的管理应和现有设施的控制措施管理结合在一起。

在跟踪本过程域的执行情况时,可以通过检查各基本实践的趋势来判断保障论据是否会被满足,具体参考 PA06“建立保障论据”。

6.2.2　BP.01.01——建立安全职责

建立安全控制的职责和可核查性,并且传达给组织中每个成员。

6.2.2.1　描述

安全的某些方面可通过通用的管理结构进行管理,而有些方面则需要更专业的管理。

该规程要求确保那些承担责任的人可被核查和对其授予行动权。无论采用什么安全控制，都要确保明确、一致地使用。此外，无论采用哪一种通信架构，都要确保传达给整个组织的成员，而不仅仅是该架构中的成员。

6.2.2.2 工作产品示例

- 组织安全架构图——确定与安全相关的组织成员和他们的角色；
- 描述安全角色的文档——描述每个与安全相关的组织的角色及其职责；
- 描述安全职责的文档——详细描述每个安全职责，包括期望的输出以及如何评审和使用它；
- 详细描述安全可核查性的文档——描述谁负责处理安全相关问题，确保有人负责所有的风险；
- 详细描述安全授权的文档——确定允许组织的每个成员做什么。

6.2.2.3 注释

组织可建立一个安全工程工作组来负责解决安全相关问题，也可通过指定安全工程领导，由他负责确保达到安全目标。

6.2.3 BP.01.02——管理安全配置

管理系统安全控制的配置。

6.2.3.1 描述

所有设备(或设施)的安全配置都要进行管理。这个基本实践认为系统安全在很大程度上依赖于许多有相互联系的部件(硬件、软件和规程)，并且常规的配置管理实践可能达不到安全系统所要求的相关依赖性。

6.2.3.2 工作产品示例

- 所有软件升级的记录——跟踪所有软件和系统升级软件的许可证、序列号和收据，包括日期、负责人和变更说明；
- 所有分发问题的记录——包括软件分发期间遇到的任何问题以及如何解决的描述；
- 系统安全配置——描述系统硬件、软件和通信的当前状态的数据库，包括它们的位置、逐个分配的情况以及相关的信息；
- 系统安全配置变更——记录系统安全配置变化的数据库，包括变更者姓名、变更内容描述、变更原因以及变更时间；
- 可信软件分发的定期总结——描述近期可信软件分发活动、难点以及分发内容；
- 要求的安全变更——跟踪因安全原因或安全影响在系统要求的任何变更，以便有助于确保这些变更及其影响是有意义的；
- 设计文档的安全变更——跟踪因安全原因或安全影响在系统设计的任何变更，以便有助于确保这些变更及其影响是期望的；
- 控制实现——描述系统内安全控制的实现，包括详细的配置内容；
- 安全评审——描述与预期的控制实现相关的系统安全控制的当前状态；
- 控制处置——描述移除或禁止安全控制的规程，包括过渡计划。

6.2.3.3 注释

如果需要，这个基本实践中可以包括建立安全控制配置，而安全控制配置的实际工作很可能在实施控制的时候才会执行。维护任何系统中安全控制配置的通用性是一项复杂任务，对于大的分布系统尤

其如此。配置本身的某些方面对于安全的维护来说是至关重要的。为实现有效的安全需要记录与组成系统的安全控制机制相关的而其他学科通常不用的特定信息。同样地，对现行系统提议的变更应加以评估，以确定它们对整个系统安全态势的影响。

为了确保某特定软件模块或应用软件模块的所有副本与对应的版本相同，组织应遵守相应的规程，特别是在分布式环境下。此外，尤其要确保在网络中分发软件时不发生错误。上述要求适用于所有的软件。

这个基本实践应确保：软件仅仅执行那些预期的功能、维护密封的参考版本、确保所有软件副本相同、确认升级软件，以及掌握和维护安全控制配置。

6.2.4 BP.01.03——管理安全意识、培训和教育计划

管理面向所有用户的安全意识、培训和教育计划。

6.2.4.1 描述

全体员工的安全意识、培训和教育要求按照与其他意识、培训和教育的管理方法相同的方法管理。

6.2.4.2 工作产品示例

- 安全培训材料用户评审结果——描述安全意识和培训材料的有效性、实用性和适用性；
- 已开展的意识、培训和教育的日志以及培训的结果——跟踪用户对组织和系统安全的理解情况；
- 用户团体关于安全的知识程度、意识和培训的定期复审结果——评审组织对安全的理解情况，以及确定将来可能关注的领域；
- 培训、意识和教育材料的目录——安全培训材料的汇集，这些培训材料可能还要在整个组织使用。可以与其他组织培训材料结合在一起。

6.2.4.3 注释

本标准中，“用户”不仅包括直接用该系统工作的个人，而且还包括所有直接或者间接从该系统接收信息的个人，以及所有管理部门。

使用户知道把安全放置在合适位置的原因以及采用某特定安全机制或者控制措施的原因是至关重要的。此外，使用户知道如何正确地使用这个机制或者控制措施也很重要。因此，当引进新的机制和控制措施的时候，用户需要从头开始学习、定期更新培训或参加修订会议。所有用户要求具有安全意识，部分用户要接受操作执行安全机制的培训，少数用户需要更深层次的安全知识。

6.2.5 BP.01.04——管理安全服务和控制机制

管理安全服务和控制机制的定期维护和管理。

6.2.5.1 描述

安全服务和机制的一般管理和其他服务和机制的管理类似，包括防止服务和机制无意或有意地被损坏，以及依据法律和政策要求进行合适的归档。

6.2.5.2 工作产品示例

- 维护和管理日志——关于对系统安全机制执行的维护、完整性检查和运行检查的记录；
- 定期维护和管理评审——包含近期系统安全管理和维护工作的分析；
- 管理和维护故障——跟踪系统安全管理和维护问题，以便识别哪些地方需要加强；

- 管理和维护异常情况——相对于正常管理和维护规程的异常情况的描述，包括异常情况的原因以及异常情况的持续时间；
- 敏感信息列表——系统中各种信息以及如何保护这些信息的描述；
- 敏感媒介列表——用来存储系统中信息的各种媒介以及如何保护这些媒介的描述；
- 脱敏、降级和处置——确保在降低某信息的敏感等级时或在对媒介实施脱敏或处置时不产生额外风险的规程。

6.2.5.3 注释

这类服务的例子包括：标识和鉴别、访问仲裁/控制，以及密钥管理。

每个安全服务应包含建立合适的安全参数、实现参数、监督和分析性能以及调整参数。

这类要求特别适用于某些安全服务，包括用户和鉴别数据维护用的“标识和鉴别服务”、许可维护用的“访问控制”服务等。

信息资产，作为资产的一个子集，被定义为隶属于某个组织的软件以及数据。部分信息资产可能要求剔除其中的敏感信息，以便剩下的信息可用于较不敏感的目的。脱敏确保只向需要知道信息的个体发布信息，可以通过降级信息或者有选择地剔除具体的敏感信息来实现。

在电子媒介上，即使用新信息进行覆盖，仍然能够保留残留的信息痕迹。某些媒介可能需要作净化后才可以用于较不敏感的目的。一旦磁媒介的使用寿命结束，应采用一种与残留信息的敏感度相对应的方式来处置，甚至需要销毁该媒介。有些团体不允许对敏感度较低的信息重复使用原来的媒介。脱敏、降级以及处置要求的具体细节取决于具体的团体和适用的规则。

6.3 PA02——评估影响

6.3.1 过程域

6.3.1.1 概要描述

评估影响的目的是识别与系统有关的影响，并评估发生影响的可能性。影响可能是有形的，例如税收或财务处罚；也可能是无形的，例如名声或信誉损失。

6.3.1.2 目标

识别系统的安全风险影响并且表述其特征。

6.3.1.3 基本实践列表

BP.02.01 识别和分析由系统支撑的运行、业务或使命能力，并且排列优先顺序。

BP.02.02 识别支持核心运行能力或系统安全目标的系统资产，并且描述其特征。

BP.02.03 选择用于评估的影响度量。

BP.02.04 必要时，识别选择用于评估的度量与度量转换因子之间的关系。

BP.02.05 识别影响并描述其特征。

BP.02.06 监视影响正在发生的变化。

6.3.1.4 过程域注释

影响是故意或意外引起的、影响资产的非期望事件的后果。此后果可能是某些资产的毁坏、IT 系统的损坏和保密性、完整性、可核查性、真实性或可靠性的丧失。可能的间接后果包括财务损失或对市场份额或组织形象造成影响。影响的度量可以影响非期望事件的结果和防止非期望事件的防护费用之间的平衡。应考虑非期望事件发生的频率，即使每次出现所引起的损害程度不大，但多次发生后的聚集

效应可能导致严重的损害，这一点特别重要。影响评估结果是风险评估和选用防护措施的一个重要的参考。

这个过程域所产生的影响信息将连同 PA04 的威胁信息和 PA05 的脆弱性信息用于 PA03。尽管涉及收集威胁、脆弱性和影响信息的活动已经分别归类到几个单独的过程域中，但是它们是相互依赖的。目的是发现威胁、脆弱性和影响的组合，并针对该组合判断是否需要采取行动。因此，在对影响进行研究时，应通过相应的威胁和脆弱性存在的情况，给予一定程度的指导。

由于影响总是变化的，为了确保通过实施这个过程域掌握的影响情况在任何时候都得到维护，应对它们定期监视。

在跟踪本过程域的执行情况时，可以通过检查各基本实践的趋势来判断保障论据是否会被满足，具体参考 PA06“建立保障论据”。

6.3.2 BP.02.01——排列能力优先顺序

识别和分析由系统支撑的操作、业务或使命能力，并且排列优先顺序。

6.3.2.1 描述

识别和分析操作、业务或任务指令，并且排列它们的优先顺序。应考虑业务策略的影响，这些将影响和缓解组织可能遭受到的影响。进而可能影响到其他基本实践和过程域中处理风险的顺序。因此，在检查潜在影响时，重要的是要考虑这些影响。本基本实践与 PA10“确定安全需要”的活动相关。

6.3.2.2 工作产品示例

- 系统优先权列表和影响调节因素；
- 系统能力轮廓——描述系统的能力及其对系统目标的重要性。

6.3.2.3 注释

可将功能和信息资产解释为它们在已定义环境中的价值和重要性。价值可以是操作重要性、分类、敏感等级，或者用于指定资产对系统预期运行和用途的感知价值的任何其他方法。在运行环境中某个起支撑作用的功能被损害、修改或者失去可用性的情况下，严重程度可以解释为对系统运行、人的生命、运行成本和其他关键因素的影响程度。资产的价值也可以用与之有关的、能应用的安全需求来定义，例如，定义为客户清单的保密性、办公室间沟通的有效性或工资单信息的完整性。与明确的资产相反，许多资产是无形的或隐含的。所选择的风险评估方法应提出如何评估能力和资产的价值，并排列它们的优先级。

6.3.3 BP.02.02——识别系统资产

识别支持核心运行能力或系统安全目标的系统资产，并且描述其特征。

6.3.3.1 描述

识别为支持系统的安全目标或核心能力(运行的、业务的或使命功能的)所必需的系统资源和数据。通过评估在已定义的环境中提供这种支持的每个资产的重要性，来定义每个资产。

6.3.3.2 工作产品示例

- 产品资产分析——产品资产及其对系统运行的重要性的标识；
- 系统资产分析——系统资产及其对系统运行的重要性的标识。

6.3.3.3 注释

从广义上说，资产包括系统中的人、环境、技术和基础设施。资产也包括数据和资源；不仅包括信息，还包括系统（例如通信、数据检索、应用软件或打印资源）。这些资产的重要性可以定义为它们在已定义环境中对所支持的能力的价值和关键程度的意义。在某些情况下，这个实践是对 PA09“提供安全输入”和 PA11“验证和确认安全”工作的评审。

6.3.4 BP.02.03——选择影响度量

选择用于评估的影响度量。

6.3.4.1 描述

为了测量一次事件的影响，可能要使用许多度量。最好针对所考虑的特定系统预先确定将使用哪些度量。

6.3.4.2 工作产品示例

- 所选择的影响度量。

6.3.4.3 注释

在处理有分歧的度量时，一组有限的、始终如一的度量可以将困难减到最小程度。有多种途径可以实现定量和定性地测量影响，例如：

- 制定财务费用；
- 规定严重程度经验等级，例如，1～10；
- 从预定义序列中选用修饰词，例如，高、中、低。

6.3.5 BP.02.04——识别度量关系

必要时，识别选择用于评估的度量与度量转换因子之间的关系。

6.3.5.1 描述

不同的影响可使用不同的度量进行评估。为确保整个影响评估中对所有暴露采用一致的方法，应建立不同度量之间的关系。“暴露”指威胁、脆弱性和影响的组合，它的可能造成重大损害。在某些情况下，有必要把若干度量组合，以产生成一个单一的结果。因此需要建立相应的整理合并方法。对于不同的系统，整理方法有所不同。使用定性度量时，应建立对应的规则，以指导合并阶段如何组合各个定性因素。

6.3.5.2 工作产品示例

- 影响度量关系列表——度量之间的关系描述；
- 影响度量组合规则——组合影响度量的规则描述。

6.3.5.3 注释

无。

6.3.6 BP.02.05——识别影响并描述其特征

使用多个度量或者（适当时）整理的度量来识别非期望事件的影响，并且描述其特征。

6.3.6.1 描述

以 BP.02.01 和 BP.02.02 中识别的资产和能力作为起点，识别可能导致损害的后果。对于每个资产而言，这些后果可能包括未授权的暴露、改变、丢失和(或)毁坏。对能力来说，影响可能包括中断、延迟或者弹性降低。

一旦建立相对完整的列表，就可以使用在 BP.02.03 和 BP.02.04 中识别的度量来描述这些影响的特征。这一步可能需要对保险精算表、历书或者其他资源有一定的研究。度量中的不确定性也应考虑，并且与每个影响进行关联。

6.3.6.2 工作产品示例

- 暴露影响列表——潜在的影响和相关度量的列表。

6.3.6.3 注释

影响评估的基础是 BP.02.03 中建立的影响度量，而影响组合的基础是 BP.02.04 中建立的规则。在大多数情况下，存在与测量相关的不确定性，以及在特定环境中发生特定影响的可能性。一般来说，保持不确定性因素的分离会更加有效，这样在采取措施提炼工作数据时可以看出提炼是针对数据本身还是数据的不确定性。

6.3.7 BP.02.06——监视影响

监视影响的持续变化。

6.3.7.1 描述

适用于任何地点和情况的影响是动态的。新的影响可能变得相关，而且现有影响的特征也会发生变化。因此，按照一定规则监视现有的影响和检查新的潜在影响很重要。这个基本实践与 BP.08.02 中一般性监视活动密切相关。

6.3.7.2 工作产品示例

- 影响监视报告——描述监视影响的结果；
- 影响变化报告——描述影响的变化。

6.3.7.3 注释

由于影响可能变化，因此影响评估活动应是迭代的，并且应在规定环境中多次进行。然而，影响评估的重复进行不应用来替代对影响监视。

6.4 PA03——评估安全风险

6.4.1 过程域

6.4.1.1 概要描述

“评估安全风险”的目的是识别、分析和评价某系统在已定义环境中的安全风险。该过程域关注的是根据所掌握的能力和资产易受威胁攻击的情况确定这些风险。具体来说，这项活动涉及识别和评估暴露发生的可能性。这组活动可能在系统生存周期内的任何时间执行，以便支持针对某个已知环境做出有关系统开发、维护或者运行相关的决策。

6.4.1.2 目标

- 了解该系统在已定义的环境中运行的安全风险；

- 按照已定义的方法排列风险的优先次序。

6.4.1.3 基本实践列表

BP.03.01 选择用于对已定义环境中系统的安全风险进行识别、分析、评价和比较的方法、技术和准则。

BP.03.02 识别威胁/脆弱性/影响三者组合(暴露)。

BP.03.03 评估与每个暴露的发生相关的风险。

BP.03.04 评估与暴露的风险相关的总的不确定性。

BP.03.05 按优先级排列风险。

BP.03.06 监视风险特征分布中正在发生的变化以及其特性的变化。

6.4.1.4 过程域注释

安全风险是非期望事件的影响将成为现实的可能性。虽然与涉及成本和进度的项目风险相关,但安全风险主要处理针对系统的资产和能力的影响。

风险估计总是包含不确定性因素,这个不确定性因素随具体环境而变。这就意味着安全风险的可能性只有在一定限制条件下才能够预测到。此外,由于非期望事件可能不按预期的发生,因此针对某特定风险评估的影响也有不确定性。总而言之,就安全风险因素预测的准确性而言,大部分因素存在不确定性。在很多情况下,这些不确定性可能很大,因此,规划和证明安全性都非常困难。

能够降低与特定环境相关的不确定性的任何事物都相当重要。因此,“保障”也很重要,因为它间接地降低系统风险。

这个过程域产生的风险信息依赖于从 PA04 得到的威胁信息、从 PA05 得到的脆弱性信息以及从 PA02 得到的影响信息。虽然这些有关收集威胁、脆弱性和影响信息的活动分别单独归类到几个单独的过程域中,但是,它们是相互依赖的。目的是发现威胁、脆弱性和影响的组合,并针对该组合判断是否需要采取行动。风险信息是 PA10 中确定安全需要和 PA09 中提供安全输入的基础。

由于风险环境是变化的,因此为了确保通过这个过程域掌握的风险始终得到维护,应定期监视风险环境。

在跟踪本过程域的执行情况时,可以通过检查各基本实践的趋势来判断保障论据是否会被满足。参考 PA06“建立保障论据”。

6.4.2 BP.03.01——选择风险分析方法

选择用于对已定义环境中系统的安全风险进行识别、分析、评价和比较的方法、技术和准则,并排定优先级。

6.4.2.1 描述

该基本实践包括定义用于识别已定义环境中系统的安全风险的方法,对于按照这种方法识别的安全风险可以进行识别、分析、评价和比校。这个方法应包括一个用于根据威胁、运行功能、已确定的系统脆弱性、潜在的损失、安全需求或者其他所关注的事项对风险进行分类和排列优先顺序的方案。

6.4.2.2 工作产品示例

- 风险识别方法——描述识别风险的方法;
- 风险评估方法——描述分析风险并进行评价的方法;
- 风险评估格式——描述使风险文档化并且可以跟踪的格式,包括格式描述、重要性和从属物。

6.4.2.3 注释

方法可以是现成的、经过裁剪的或者是专门供系统在已定义环境中运行时使用的。用于风险评估的方法应与选择用于威胁、脆弱性和影响评估的方法相互衔接。

6.4.3 BP.03.02——暴露识别

识别威胁/脆弱性/影响三者组合(暴露)。

6.4.3.1 描述

识别暴露的目的在于认识到有哪些威胁和脆弱性是应关注的,并且识别威胁和脆弱性发生的影响。在选择防护措施来保护系统时应考虑这些暴露。

6.4.3.2 工作产品示例

- 系统暴露列表——系统暴露的描述。

6.4.3.3 注释

该基本实践依赖于威胁、脆弱性和风险过程域的输出。

6.4.4 BP.03.03——评估暴露风险

评估与每个暴露的发生相关的风险。

6.4.4.1 描述

确定每种暴露的后果和发生的可能性,结合这些值来产生风险估值,并根据预先确定的标准来评价风险。

6.4.4.2 工作产品示例

- 暴露优先权表——计算出的风险的优先顺序表。

6.4.4.3 注释

暴露的可能性是威胁的可能性和脆弱性的可能性的组合。在多数情况下,可能影响的数量或者影响的严重性也应作为考虑因素。在所有情况下,都将会存在与度量相关的不确定性。一般来说,保持不确定性因素的分离会更加有效,这样在采取措施提炼工作数据时可以看出提炼是针对数据本身还是数据的不确定性。这往往影响到风险处理策略。这个基本实践要使用 BP.04.05“评估威胁可能性”和 BP.05.03 “收集脆弱性数据”中收集的数据以及 BP.02.05“识别影响并描述其特征”中收集的数据,既可以是多个度量,适当时也可以是经过合并的度量。

6.4.5 BP.03.04——评估总体不确定性

评估与暴露的风险相关的总的不确定性。

6.4.5.1 描述

每个风险都伴随有不确定性。总风险不确定性是所识别的各个不确定性的累积,包括针对威胁、脆弱性和影响的识别的不确定性,还包括由在 BP.04.05“评估威胁可能性”、BP.05.03“收集脆弱性数据”和 BP.02.05“识别影响并描述其特征”中描述的它们的特征识别的不确定性。该基本实践与 PA06“建立保

障论据”的所有活动密切相关，因为“保障”可以用于修改不确定性，并且在某些情况下还可以降低不确定的程度。

6.4.5.2 工作产品示例

- 带有不确定性的暴露风险——风险列表，显示风险以及相应的不确定性的测量。

6.4.5.3 注释

如果不把不确定性与暴露发生的可能性分开，那么防护措施的实施可能达不到预期效果，或者事实上不需要这样做，风险也可能缓解。

6.4.6 BP.03.05——排序风险

按优先级排列风险。

6.4.6.1 描述

已识别的风险应按照组织优先级、发生的可能性、与之相关的不确定性和可用资金进行排序。风险可以被缓解、避免、转移或接受，或者它们的组合。缓解措施涉及威胁、脆弱性、影响或者风险本身。应结合 PA10“确定安全需要”中所述的利益相关方的需要、业务优先权和整个系统的体系结构来选择所要采取的措施。

6.4.6.2 工作产品示例

- 风险优先权列表——风险优先顺序列表；
- 防护措施需求列表——有助于缓解风险的可能防护措施列表；
- 优先顺序理由——优先权方案的描述。

6.4.6.3 注释

这一步可能很复杂并且往往需要多次反复。防护措施可能涉及多种风险，或多种威胁、脆弱性和影响，这些因素会影响风险排序的效果。因此，这个过程域与 PA10“确定安全需要”和 PA09“提供安全输入”紧密相关。

6.4.7 BP.03.06——监视风险及其特性

监视风险特征分布的持续变化以及其特性的变化。

6.4.7.1 描述

适用于任何场所和情况的风险特征分布是动态的。新的风险可能更值得关注，并且现有风险的特征也可能改变。因此，按照一定规则监视现有的风险及其特征很重要。这个基本实践与 BP.08.02“监视变化”中的一般性监视活动紧密相关。

6.4.7.2 工作产品示例

- 风险监视报告——描述当前风险特征分布的报告；
- 风险变更报告——描述系统运行能力及其对系统目标的重要性。

6.4.7.3 注释

因为风险会发生改变，所以应在已定义环境中执行多次风险评估。然而，不能用重复的风险评估来

代替风险监视。

6.5 PA04——评估威胁

6.5.1 过程域

6.5.1.1 概要描述

“评估威胁”目的是识别安全威胁及其属性和特征。

6.5.1.2 目标

识别系统安全的威胁并且描述其特征。

6.5.1.3 基本实践列表

BP.04.01 识别由自然因素产生的适用的威胁。
BP.04.02 识别由人为因素(无意或有意)产生的适用的威胁。
BP.04.03 识别在特定环境中合适的度量单位和适用范围。
BP.04.04 针对人为因素产生的威胁,评估威胁方的能力和动机。
BP.04.05 评估威胁事件发生的可能性。
BP.04.06 监视威胁特征分布中发生的变化以及其特征的变更。

6.5.1.4 过程域注释

执行威胁评估的途径和方法很多。确定使用哪种方法的一个重要考虑因素是它将如何衔接所选的风险评估过程的其他部分。

该过程域产生的威胁信息,连同 PA05 的脆弱信息以及 PA02 的影响信息一起用于 PA03。虽然有关收集威胁、脆弱性和影响信息的活动分别归类到几个单独的过程域中,但是它们之间存在相互依赖关系。目标是发现威胁、脆弱性和影响的组合,以及针对该组合判断是否需要采取行动。因此,应根据相应的脆弱性和影响存在情况为发现威胁提供一定的指导。

由于威胁会变化,因此为了确保通过这个过程域掌握的情况始终得到维护,应对威胁情况定期监视。

在跟踪本过程域的执行情况时,可以通过检查各基本实践的趋势来判断保障论据是否会被满足,具体参考 PA06“建立保障论据”。

6.5.2 BP.04.01——识别自然威胁

识别由自然因素产生的适用的威胁。

6.5.2.1 描述

自然因素产生的威胁包括地震、海啸和龙卷风。注意,不是所有基于自然因素的威胁在所有地方都会发生,例如,海啸不可能发生在大陆中央。因此,重要的在于识别某个特定地方可能发生哪种基于自然因素的威胁。

6.5.2.2 工作产品示例

- 适用的自然威胁表格——形成文档的自然威胁的特征和可能性表格。

6.5.2.3 注释

评估所要求的大量信息可以从保险精算表和自然现象事件数据库获得。虽然这些信息是有价值

的，但由于它们可能是非常概括性的，因此应慎用，并且在涉及特定环境时可能需要解释。

6.5.3 BP.04.02——识别人为威胁

识别由人为因素（无意或有意）产生的适用的威胁。

6.5.3.1 描述

考虑人为因素产生的威胁时，应采用稍有不同的方法。主要有两类人为因素威胁：偶然因素和有意行为产生的威胁。某些人为因素威胁可能不适用于目标环境，在后面的分析过程中，应剔除它们，不予考虑。

6.5.3.2 工作产品示例

- 威胁场景描述——威胁发生状况的描述；
- 威胁严重程度估计——与威胁相关的可能性的测量。

6.5.3.3 注释

在某些情况下，可以设计描述威胁发生的场景，用于帮助理解有意威胁。当使用通用的人为因素威胁数据库时，应评估其完备性和关联性。

6.5.4 BP.04.03——识别威胁的度量单位

识别在特定环境中合适的度量单位和适用范围。

6.5.4.1 描述

多数自然威胁和许多人为威胁都有相应的度量单位。例如地震的里氏等级。在绝大部分情况下，度量单位的整个范围在某特定地区并不适用。因此，宜针对所考虑的特定位置设定可能发生威胁事件的数量或者频率的最大值和（在某些情况下的）最小值。

6.5.4.2 工作产品示例

- 有对应的度量单位和位置范围的威胁表格。

6.5.4.3 注释

如果还没有某特定威胁的度量单位，应专门针对该位置创建一个可接受的度量单位。应描述可测试项的范围（如果适用）和度量单位。

6.5.5 BP.04.04——评估威胁方能力

针对人为因素产生的威胁，评估威胁方的能力和动机。

6.5.5.1 描述

该过程域关注潜在对手对系统成功攻击的才能和能力，这里的才能指潜在对手的攻击知识（例如接受的培训/知识）；而能力是一个有才能的对手能够实际完成攻击的可能性的测度（例如，他们确实拥有资源）。

6.5.5.2 工作产品示例

- 威胁方描述——能力评估和描述。

6.5.5.3 注释

有意的人为威胁在很大程度上取决于威胁方的能力和威胁方所控制的资源。相对而言，一个缺乏经验的黑客在掌握了强大的黑客工具时很危险，但更有经验的黑客本人还是更加危险。当然，这个缺乏经验的黑客也可能在无意中造成的更大的损害。除了攻击者的能力外，应结合攻击者的行为动机评估其可用资源，攻击者对目标(资产)吸引力的评估可能影响他的行为。

为了达到预定目标，威胁方可能连续或同时发动多次攻击。应考虑连续或同时的多次攻击的效果，可使用场景设计来完成这个任务。

6.5.6 BP.04.05——评估威胁可能性

评估威胁事件发生的可能性。

6.5.6.1 描述

评估威胁事件发生的可能性。在进行这种评估时需要考虑的因素很多，其范围从自然事件发生的机会到个人的有意或无意行为。然而，所要考虑的许多因素可能并不纳入计算或测量范畴。此外，应采用一致的度量报告评估结果。

6.5.6.2 工作产品示例

- 威胁事件可能性评估报告——描述威胁事件的可能性的报告。

6.5.6.3 注释

由于许多因素涉及各种各样的可能性，评估威胁可能性是一个复杂的概率计算问题，因为许多因素涉及不同的概率。与任何可能性估计相关联的都是对某个不确定性因素的有效性和准确性的评估。为了减少可能的混淆，可能性评估的不确定性应单独报告。在所有情况下，度量和可能性估计都有不确定性。通常，更有效的做法是将不确定性因素(也是一个复合的表达式)分开，以便在采取措施提炼工作数据时，可以看出要提炼的是数据本身还是数据的不确定性。

6.5.7 BP.04.06——监视威胁及其特征

监视威胁特征分布中的持续变化及其特性的变化。

6.5.7.1 描述

适用于任何场所和情况的威胁特征分布是动态的。新的威胁可能更值得关注，并且现有威胁的特征也可能改变。因此，按照一定规则监视现有威胁及其特征很重要。这个基本实践与 BP.08.02“监视变化”中的一般性监视活动紧密相关。

6.5.7.2 工作产品示例

- 威胁监视报告——描述威胁监视工作结果的文档；
- 威胁变化报告——描述威胁特征分布变化的文档。

6.5.7.3 注释

因为威胁会发生改变，所以应在规定环境中执行多次威胁评估活动。不过，不能用重复的威胁评估来代替威胁监控。

6.6 PA05——评估脆弱性

6.6.1 过程域

6.6.1.1 概要描述

评估脆弱性的目的是识别系统脆弱性，并且描述其特征。这个过程域包括分析系统资产、定义具体的脆弱性和提供整个系统的脆弱性评估。与安全风险和评估脆弱性相关的术语在许多环境中用法不同。“脆弱性”指的是除了某个系统内很可能遭到威胁攻击的那些原始意图、弱项、安全漏洞，或实现缺陷外，能被特定意图所利用的系统的某个方面。这些脆弱性与任何特定威胁实例或攻击无关。这一系列活动可在系统生存周期的任何时候执行，以便支持在已知环境中开发、维护或运行系统的决定。

6.6.1.2 目标

了解已定义环境中的系统脆弱性。

6.6.1.3 基本实践列表

BP.05.01 选择用于识别已定义环境中的系统脆弱性并且描述其特征的方法、技术和准则。

BP.05.02 识别系统脆弱性。

BP.05.03 收集与脆弱性的属性相关的数据。

BP.05.04 评估系统脆弱性，并且把各个特定脆弱性以及这些特定脆弱性的各种组合聚集在一起。

BP.05.05 监视适用的脆弱性正在发生的变化，以及它们的特征的变化。

6.6.1.4 过程域注释

与这个过程域对应的分析和实践往往是“纸面研究”。通过主动工具和技术发现系统脆弱性是对脆弱性分析技术的补充，而不是替代。这些主动技术可以看成是脆弱性分析的一种专门形式，当试图确认在重要的系统升级之后的安全脆弱性，或者识别两个系统互联后的安全脆弱性时，此类分析可能很有用。在某些情况下，为了确认系统的安全状况和增加对现有的安全脆弱性的认识和理解，也需要主动脆弱性分析。主动脆弱性分析也称为渗透测试，它是安全工程师试图规避系统安全特征的过程。安全工程师一般工作在与普通用户一样的约束条件下，只不过有可能使用所有的设计和执行文档。攻击的过程不是穷尽的，它受到有限资源(时间、金钱、人力等)的限制。

这个过程域产生的脆弱性信息连同 PA04 的威胁信息和 PA02 的影响信息一起供 PA03 使用。虽然这些有关收集威胁、脆弱性和影响信息的活动分别单独归类到过程域中，但是，它们是相互依赖的。目标是发现威胁、脆弱性和影响的组合，以及针对该组合判断是否需要采取行动。因此，可根据相应的威胁和影响存在情况指导脆弱性研究。

由于脆弱性会发生变化，因此为了确保通过这个过程域掌握的情况始终得到维护，应对脆弱性情况定期监视。

在跟踪本过程域的执行情况时，可以通过检查各基本实践的趋势来判断保障论据是否会被满足。参考 PA06“建立保障论据”。

6.6.2 BP.05.01——选择脆弱性分析方法

选择用于识别已定义环境中的系统安全脆弱性并且描述其特征的方法、技术和准则。

6.6.2.1 描述

这个基本实践包括定义确定系统的安全脆弱性并且在某种程度上允许识别并描述其特征的方法。

这个方法可能包括一个方案，用于根据威胁及其可能性、运行功能、安全要求或者其他所关注的事项对脆弱性进行分类和排列优先顺序。识别分析的深度和广度，可以使安全工程师和客户决定目标系统是整个过程的一部分还是它的全部。应在预先安排和指定的时间里、在已知的并且记录在案的配置框架内执行分析。分析方法应包括预期的结果，具体分析目标应明确规定。

6.6.2.2 工作产品示例

- 脆弱性分析方法——识别发现和描述系统安全脆弱性的方法，包括分析、报告和跟踪过程；
- 脆弱性分析格式——描述脆弱性分析结果的格式，以确保使用标准化的方法；
- 攻击方法和基本原理——包括执行攻击测试的目标和方法；
- 攻击规程——执行攻击测试的详细步骤；
- 攻击计划——包括资源、进度、攻击方法描述；
- 渗透研究——以识别未知脆弱性为目标的攻击场景分析和实施；
- 攻击场景——将实施的特定攻击的描述。

6.6.2.3 注释

脆弱性分析方法可以是现有的、经过裁剪的，或是专门供系统在已定义环境中运行时使用的。它往往基于或依从 PA03“评估安全风险”中选择的风险分析方法。注意：有可能并不了解威胁、能力和价值，在这种情况下，分析方法应限制在比较窄的范围内或者采用一组适用的假设。

用来分析脆弱性的方法可以是定性的或者定量的。通常，脆弱性分析包括对脆弱性存在的可能性的反应。可以用书面报告传达攻击结果，但是也可以采用演示形式证明这些攻击。

对于脆弱性的识别，最少存在两种根本不同的途径。这两条途径，从它们的特征看，一个表现为以分析为基础，另一个表现为以测试为基础。基于测试的途径适合于鉴别现有的、在测试集中已经有其对应的已知威胁的脆弱性。基于分析的途径最适合于识别新的脆弱性以及那些虽然不会立即被当前爆发的问题利用，但是一旦另外一个问题爆发就会被利用的脆弱性。如果在选择脆弱性方法时包括基于定性的或者定量的途径，应考虑其他选项。此外，还应考虑控制分析或者测试的完整性的能力。

6.6.3 BP.05.02——识别脆弱性

识别系统安全脆弱性。

6.6.3.1 描述

系统的安全功能和非安全功能都有可能存在脆弱性。在很多情况下，支持安全功能或与安全机制系统工作的非安全功能也有可被利用的脆弱性。应适当遵循 BP.05.01 中设计攻击场景的方法，应记录又发现的系统脆弱性。

6.6.3.2 工作产品示例

- 描述引起各种攻击的系统脆弱性的列表；
- 包括攻击测试结果(例如脆弱性)的渗透轮廓图。

6.6.3.3 注释

在本实践中，脆弱性被看成是在不考虑任何威胁可能性的情况下的系统内在特性。这些脆弱性可以根据威胁分析结果排列优先顺序。不可重复读攻击使得制定对策变得很困难。

可以根据 PA03“评估安全风险”中的风险优先顺序和 PA10“确定安全需要”中的业务目标和优先顺序识别一部分脆弱性。此外，PA02 中提到的资产也需要考虑。

6.6.4 BP.05.03——收集脆弱性数据

收集与脆弱性的属性相关的数据。

6.6.4.1 描述

脆弱性有其相关的属性。此基本实践的目的是收集与这些属性相关联的数据。在某些情况下，脆弱性的度量单位可能与威胁的类似，参见 BP.04.03“识别威胁的度量单位”。还应确定和收集脆弱性可被利用的容易程度，以及脆弱性存在的可能性。

6.6.4.2 工作产品示例

- 脆弱性属性表格——产品或者系统的脆弱性特征的表格文档。

6.6.4.3 注释

这个活动期间收集到的许多数据将要在以后执行 PA03“评估安全风险”时使用。因此，采用适合 PA03 使用的格式来收集和存储数据是很重要的。在所有情况下，度量和可能性都存在不确定性。一般来说，保持不确定性因素的分离会更加有效。这样，在采取措施提炼工作数据时可以看出提炼是针对数据本身还是数据的不确定性。

6.6.5 BP.05.04——组合系统脆弱性

评估系统脆弱性，并且把各个特定脆弱性以及这些特定脆弱性的各种组合聚集在一起。

6.6.5.1 描述

分析哪些脆弱性或者脆弱性组合能够导致系统安全问题。分析应识别脆弱性的附加特征，例如脆弱性利用可能性和成功利用的机会。在分析结果中还可以包含关于解决这些合成脆弱性的处理建议。

6.6.5.2 工作产品示例

- 脆弱性评估报告——导致系统出现问题的脆弱性的定量或定性描述，包括攻击的可能性、成功攻击的可能性以及攻击的影响。
- 攻击报告——文档化结果和结果分析，包括发现的脆弱性、潜在的利用以及建议。

6.6.5.3 注释

需要识别和分析攻击演习的结果。为了使客户能做出对策决定，任何已发现的脆弱性及其潜在的利用有必要加以识别并且形成足够详细的文档。

6.6.6 BP.05.05——监视脆弱性及其特征

监视适用的脆弱性的持续变化，以及它们的特征的变化。

6.6.6.1 描述

适用于任何场所和情况的脆弱性特征分布是动态的。新的脆弱性可能更值得关注，并且现有脆弱性的特征也可能改变。因此，按照一定规则监视现有的脆弱性及其特征很重要。这个基本实践与 BP.08.02“监视变化”中的一般性监视活动紧密相关。

6.6.6.2 工作产品示例

- 脆弱性监视报告——描述脆弱性监视工作结果的文档；

- 脆弱性变化报告——描述新的或者已经变化的脆弱性的文档。

6.6.6.3 注释

由于脆弱性会改变，因此在已定义环境中应进行多次脆弱性评估活动。不过，脆弱性评估重复不应取代脆弱性监视。

6.7 PA06——建立保障论据

6.7.1 过程域

6.7.1.1 概要描述

“建立保障论据”的目的是清楚表明客户的安全需要得到满足。保障论据是一组得到保障证据支持的保障目标陈述，这些保障证据可能取自多个来源和抽象层次。

这个过程域包括识别和确定与保障相关的要求；作为产品的证据和分析活动；以及需要支持保障要求的补充证明活动。此外，需要收集、包装这些活动产生的证据，并作演示准备。

6.7.1.2 目标

工作产品和过程明确地提供客户的安全需要已得到满足的证据。

6.7.1.3 基本实践列表

BP.06.01 识别安全保障目标。

BP.06.02 定义安全保障战略，以提出所有的保障目标。

BP.06.03 定义用于监测安全保障目标的测量。

BP.06.04 识别和控制安全保障证据。

BP.06.05 执行安全保障证据的分析。

BP.06.06 提供证明客户的安全需要得到满足的安全保障论据。

6.7.1.4 过程域注释

建立保障论据所涉及的活动，包括识别、策划、保证和演示安全保障证据。

在跟踪本过程域的执行情况时，可以通过检查各基本实践的趋势来判断保障论据是否会被满足。

6.7.2 BP.06.01——识别保障目标

识别安全保障目标。

6.7.2.1 描述

由客户决定的保障目标确定了系统中必需的信任等级。系统安全保障目标规定了系统安全策略所强制的信任等级。目标的充分性由开发者、集成者、客户以及批准系统运行的人(如果有)来决定。

在识别新证据和修改现有证据时，安全保障目标要与工程组织内部的和外部的所有安全相关的组(例如客户、系统安全认证人员、用户)相协调。

更新安全保障目标，以反映各种变化。要求修改安全保障目标的变化示例包括：客户、系统安全认证人员或者用户的可接受风险等级发生改变，或者需求(或需求的解释)发生变化。

应无歧义地通报安全保障目标。如果必要，在通报这些目标时作适当解释。

6.7.2.2 工作产品示例

- 安全保障目标陈述——客户对系统安全特征中必需的信任等级的需求。

6.7.2.3 注释

在不强求遵循某特定声明的情况下，如果保证目标可以陈述或与达到或满足的具体保证声明有关，则是有益的，这有助于减少误解和歧义。

6.7.3 BP.06.02——制定保障战略

定义安全保障战略，以提出所有的保障目标。

6.7.3.1 描述

安全保障战略的目的是策划和确保安全目标得以恰当地实现和加强。在安全保障战略执行中产生的证据应提供一个可接受的信任等级，确保系统安全测量足以管理安全风险。通过开发和实施安全保障战略来达到对安全保障相关活动的有效管理。尽早识别和定义与保障相关的要求，对于产生必要的支持证据是至关重要的。通过持续的外部协调，理解并且监视客户安全保障需要的满意度，确保高质量的保障包。

6.7.3.2 工作产品示例

- 安全保障战略——描述满足客户安全保障目标的计划和识别各个负责团体。

6.7.3.3 注释

安全保障战略与 PA07“协调安全”中所定义的、所有受到影响的内部工程组和外部组（例如客户、系统安全认证人员或者用户）保持协调。

6.7.4 BP.06.03——定义安全测量

定义用于监测安全保障目标的测量。

6.7.4.1 描述

通过收集、分析和报告与绩效相关的数据，测量能够被用于促进决策和提高绩效和问责制。测量性能的目的是根据观察到的测量结果，应用安全措施来监控安全过程的状态，并促进过程的改进。措施将有利于监督完成保证战略和保证目标，因此也将会支持保障论据。

6.7.4.2 工作产品示例

- 与保证目标和保证策略相一致的测量项列表。

6.7.4.3 注释

本质上，测量需要是定量的，结果应是数字和实际数据。测量的项目成本需要在合理范围内，即收集数据的成本不应超过所收集到数据的价值。测量结果的一致性应由第三方评审人员进行验证。一些测量结果可能适用于趋势分析，并对影响的变化做出预期。所产生的测量结果应能够用于在所关注的项目工作的决策。它们应在尽可能低的级别收集，并且不能被分割成其他格式。最后，应使用频率、公式、证据和指标等特征来定义测量项。对于这个基本实践，最好能够理解组织外部因素（即政府、行业等）的测量需求。

6.7.5 BP.06.04——控制保障证据

识别和控制安全保障证据。

6.7.5.1 描述

按照安全保障战略中的定义收集安全保障证据，通过与所有安全工程过程域的交互，识别各个抽象层次的证据。对这类证据要加以控制，以确保与现有工作产品的流通以及与安全保障目标的关联。

6.7.5.2 工作产品示例

- 安全保障证据库——存储所有在开发、测试和使用期间产生的证据。可以采用数据库、工程笔记、测试结果或证据日志的形式。

6.7.5.3 注释

安全保障工作产品可以基于系统、体系结构、设计、实现、工程过程、物理开发环境以及物理运行环境等开发。

安全保障证据可用于测量安全的效率、有效性、能力和影响。识别和控制安全保障证据能够收集更高质量的数据，并将分析结果更有效地传达给更广泛的受众，从而提供一个客观的机制来持续地度量和改进整个安全过程的执行和结果。

6.7.6 BP.06.05——分析证据

执行安全保障证据的分析。

6.7.6.1 描述

应进行安全保障证据分析，以便提供所收集的证据满足安全目标的置信度，从而满足客户的安全需要。通过安全保障证据的分析，确定系统安全工程过程和安全验证过程是否足够充分和完整，以便做出安全特征和机制得到满意实施的结论。此外，通过分析证据，以确保有关基线系统的工程产品是完整的和正确的。在保障证据不充足或者不充分的情形下，该分析可能需要对系统、安全工作产品和支持安全目标的过程进行修改。

6.7.6.2 工作产品示例

- 保障证据分析结果——识别和总结证据库中证据的优缺点。

6.7.6.3 注释

部分保障证据只能够通过合并其他系统工程产品生成或者通过合并其他安全保障推断出。

6.7.7 BP.06.06——提供保障论据

提供证明客户的安全需要得到满足的安全保障论据。

6.7.7.1 描述

为了证明符合安全保障目标，要拿出全面的保障论据并且提供给客户。这种保障论据是得到保障证据的联合支持的一组保障目标陈述，且可能来自多个抽象层次。应针对证据表现的缺陷以及满足安全保障目标的缺陷评审保障论据。

6.7.7.2 工作产品示例

- 有支持证据的保障论据——得到各种保障证据支持的一组结构化保障目标。

6.7.7.3 注释

高层次安全保障论据可能是相关准则的目标已得到满足。其他保障论据可能涉及如何解决影响到系统资产的威胁。为了满足证明的适用标准，每个保障目标都得到相关的和足够的证据支持。保障论据可能被客户、系统安全认证人员以及用户使用。

6.8 PA07——协调安全

6.8.1 过程域

6.8.1.1 概要描述

协调安全的目的是确保所有团体都了解并且介入安全工程活动。此活动至关重要，因为安全工程不可能孤立地成功。这种协调包括所有项目人员与外部小组之间的公开沟通。可以使用各种各样的机制来协调和传达当事者之间的安全工程决策和建议，包括备忘录、文档、电子邮件、会议和工作组。

6.8.1.2 目标

- 项目组所有成员在履行其职责所需的范围内了解并介入安全工程活动；
- 通报和协调与安全相关的决策和建议。

6.8.1.3 基本实践列表

BP.07.01 明确安全工程协调目标和关系。

BP.07.02 识别安全工程协调机制。

BP.07.03 促进安全工程协调。

BP.07.04 运用已识别的机制来协调与安全相关的决策和建议。

6.8.1.4 过程域注释

这个过程域确保安全是整个工程工作中的一个完整组成部分。安全工程师应是所有主要的设计队伍和工作组中的一部分。特别重要的是，在系统生存周期的早期做出关键设计决策的时候，确立安全工程与其他工程队伍之间的关系。这个过程域可以等同应用于开发和运行组织。

在跟踪本过程域的执行情况时，可以通过检查各基本实践的趋势来判断保障论据是否会被满足。参考 PA06“建立保障论据”。

6.8.2 BP.07.01——定义协调目标

定义安全工程协调目标和关系。

6.8.2.1 描述

许多组需要了解并且介入安全工程活动。这些组的信息共享目标通过检查项目结构、信息需要和项目要求来确定。建立与其他组的关系和承诺。成功的关系有多种形式，但一定是所有涉及的团体公认的。

6.8.2.2 工作产品示例

- 信息共享协议——描述关于组间共享信息过程，识别涉及的团体、媒介、格式、期望和频率；
- 工作组成员资格和日程表——描述组织的工作组，包括它们的成员资格、成员的角色、目的、议程以及后勤保障；

- 组织标准——描述在各种工作组和客户之间交流与安全相关的信息的过程和规程。

6.8.2.3 注释

应在项目中尽早定义协调目标和关系，以确保建立良好的交流路线。所有工程组应定义安全工程师在日常运行（例如出席评审、参加培训、评审设计）中的角色。如果不这样做，将增加缺失安全关键点的风险。

6.8.3 BP.07.02——识别协调机制

识别安全工程协调机制。

6.8.3.1 描述

安全工程决策和建议可以通过多种方式在所有工程组间共享。本活动给出了在项目上协调安全的不同方式。

多名安全人员工作在同一个项目上的情况并不少见。如果属于这种情况，所有安全工程师应为一个共同理解的目标而工作。接口识别、安全机制选择、培训和开发工作需要按照这样的方式进行：当放置在运行的系统中时，每一个安全组件能确保按照预期目标运行。此外，为了将安全清楚地整合到系统中，所有的工程团队应了解安全工程工作和工程活动。客户也应了解安全相关事件和活动，以便确保恰当地识别和处理需求。

6.8.3.2 工作产品示例

- 沟通计划——包括共享的信息、会议次数以及工作组成员与其他组成员之间使用的过程和规程；
- 沟通所需的基础设施——工作组成员与其他组成员之间有效地共享信息所必需的基础设施和标准；
- 会议报告、消息和备忘录模板——确保标准化和有效工作的各种文档格式。

6.8.3.3 注释

无。

6.8.4 BP.07.03——促进协调

促进安全工程协调。

6.8.4.1 描述

成功的关系依赖于有效地促进。具有不同优先权的不同组之间的沟通可能会导致冲突。这个基本实践确保采用某种合适的建设性方式解决这些争论。

6.8.4.2 工作产品示例

- 解决冲突的规程——描述有效地解决组织单位内和组织单位间的冲突的方法；
- 会议日程、目标和活动项——描述会议期间讨论的主题，强调目标和所提出的活动项；
- 活动项跟踪——识别执行和解决某项活动项的计划，包括责任、进度和优先顺序。

6.8.4.3 注释

无。

6.8.5 BP.07.04——协调安全决策和建议

运用已识别的机制来协调与安全相关的决策和建议。

6.8.5.1 描述

这个基本实践的目的是在安全工程师、其他工程组、外部实体以及其他合适的团体中通报安全决策和建议。

6.8.5.2 工作产品示例

- 决策——通过会议报告、备忘录、工作组纪要、电子邮件、安全指南或者公告板向受影响的组通报与安全相关的决策。
- 建议——通过会议报告、备忘录、工作组纪要、电子邮件、安全指南或者公告板向受影响的组通报与安全相关的建议。

6.8.5.3 注释

无。

6.9 PA08——监视安全态势

6.9.1 过程域

6.9.1.1 概要描述

“监视安全态势”的目的是确保识别和报告所有对安全的破坏、试图破坏或者可能导致安全受到破坏的错误。应监视外部环境和内部环境中所有可能对系统安全构成影响的因素。

6.9.1.2 目标

- 检测和跟踪与内部和外部安全有关的事件；
- 按照策略对事件做出响应；
- 根据安全目标识别和处理安全态势的变化。

6.9.1.3 基本实践列表

BP.08.01 分析事态记录，确定事件原因、发展趋势以及可能的未来事件。

BP.08.02 监视威胁、脆弱性、风险和环境的变化。

BP.08.03 识别安全相关事件。

BP.08.04 监视安全防护措施的性能和功能效果。

BP.08.05 评审系统的安全态势，以识别必要的变更。

BP.08.06 管理对安全相关事件的响应。

BP.08.07 确保与安全监视相关的产品得到适当保护。

6.9.1.4 过程域注释

安全态势指出系统及其环境为了应付当前威胁、脆弱性和对系统及其资产的影响的准备情况。这个过程域涉及 PA03“评估安全风险”和 PA05“评估脆弱性”中的活动。对收集到的关于内部和外部环境的数据，既要就其所处的背景进行分析，也要就其与其他数据的关系进行分析；这些其他数据可能产生于正被讨论的某个事件发生之前、之后或同时发生的其他事件。这个过程域既提出了预定的系统目

标环境，也提出了系统开发环境。任何特定系统都应与可能影响其总体安全的现有系统协同工作，因此，这些现有系统也应纳入监视范围之内。

在跟踪本过程域的执行情况时，可以通过检查各基本实践的趋势来判断保障论据是否会被满足。参考 PA06“建立保障论据”。

6.9.2 BP.08.01——分析事态记录

分析事件记录，确定事件原因、发展趋势以及可能的未来事件。

6.9.2.1 描述

检查历史和事件记录以获取安全相关信息。应确定感兴趣的事件以及用于关联多个记录中的事件的因素。可把多个事件记录融合到一个单一事件记录中。

6.9.2.2 工作产品示例

- 每个事件的描述——识别每一个已发现的事件来源、影响和重要性；
- 日志记录的组成和来源——取自各种来源的安全相关事件记录；
- 事件识别参数——描述通过系统的各个组成部分要收集哪些和不收集哪些事件；
- 所有当前单一日志记录警报状态列表——识别所有基于单一日志记录的行动请求；
- 所有当前单一事件警报状态列表——识别所有基于(由多个日志形成的)事件的行动请求；
- 所有已发生的警报状态的定期报告——从多个系统合成警报列表，并做初步分析；
- 日志分析和小结——对最近发生的警报实施分析，并针对结果输出报告。

6.9.2.3 注释

许多审核日志很可能包含与某个同一事件相关的信息，在分布式/网络环境中尤其如此，一个事件往往在网络上的多个位置留下它的踪迹。为了确保单个记录是有价值的，并且有助于全面理解该事件及其行为，有必要把各个单独的日志记录组合或者融合到一个单一事件记录中。

可针对单个记录和多个记录进行分析。同类型多个记录的分析通常使用统计分析技术或趋势分析技术。虽然比较常见的是针对同类型事件进行多样事件记录分析，但是也可针对日志记录和事件(融合的)记录进行不同类型的多个记录分析。

警报，例如针对基于单一事件的行动请求的警报，应通过日志记录和已融合的事件记录这两者来确定。从开发环境中得到的日志和事件记录也应纳入分析范围之内。

6.9.3 BP.08.02——监视变化

监视威胁、脆弱性、影响、风险和环境的变化。

6.9.3.1 描述

注视任何可能对当前安全态势的有效性造成正面或负面影响的变化。

由于与其自身的内部和外部环境相关，任何系统实施的安全都应与威胁、脆弱性、影响和风险相关。这些都不是静态的，同时它们的变化将影响到系统安全的有效性和适当性。所有的变化都应得到监视和分析，以便评估它们对安全的有效性的重要程度。

6.9.3.2 工作产品示例

- 变化报告——识别任何可能影响到系统的安全态势的外部或内部变化；
- 变化重要程度的定期评估——对安全态势中的变化实施分析，以确定它们的影响以及所需的

响应。

6.9.3.3 注释

应检查内部和外部变化来源以及开发和运行环境。

当变化被注明需要触发某个响应时，通常是风险分析或其部分内容的评审。参见 PA03“评估安全风险”。

6.9.4 BP.08.03——识别安全事件

识别安全相关事件。

6.9.4.1 描述

确定是否已经发生安全相关事件，识别其详细内容，并且在必要时报告。可以使用历史事件数据、系统配置数据、完整性工具和其他系统信息，检测安全相关事件。由于一些事件的发生要经历一段较长的时间，因此这种分析可能涉及对整个时间里各种系统状态的比较。

6.9.4.2 工作产品示例

- 事件列表和定义——为了便于识别，识别普通安全事件并且描述它们；
- 事件响应说明——描述针对发生安全事件时的合适的响应；
- 事件报告——描述发生了什么事件以及所有相关的细节，包括事件起源、所有损害、所做出的响应以及所要求的下一步行动；
- 有关检测到的每个侵入事件的报告——描述每个检测到的侵入事件并且提供全部有关的细节，包括来源、所有损害、所做出的响应以及所要求的下一步行动；
- 定期事件总结——提供近期安全事件、趋势通告、可能要求提高安全的领域以及降低安全可能节约的成本的总结，牢记隐藏的新增风险。

6.9.4.3 注释

在开发和运行环境中都可能发生安全事件。这些事件可能以不同方式影响正在开发或运行的系统。防范黑客成熟的技术攻击或者恶意代码（病毒、蠕虫等）需要使用的与防止随机事件不同的方式。为了检测这些攻击，要求分析系统配置和状态。应拟订适当的响应方案，经过测试后投入使用。对于许多技术攻击要求迅速做出预定的响应，以便尽量缩小攻击危害的扩散范围。多数情况下，不协调的响应可能会导致情况更加恶化。在这种情况下，有必要确定和详细说明该响应（BP.08.06）。

6.9.5 BP.08.04——监视安全防护措施

监视安全防护措施的性能和功能效果。

6.9.5.1 描述

检查防护措施的性能，以便识别防护措施的性能变化。

6.9.5.2 工作产品示例

- 定期防护措施状况——描述现行防护措施状态，以便发现可能的错误配置或其他问题；
- 定期防护措施状态总结——提供现有防护措施状态、趋势通告、必要的改进以及降低安全可能节约的成本的总结。

6.9.5.3 注释

保护开发和运行环境的防护措施应受到监视。在使用之后，使许多防护措施可处于不合适的或者无效的状态。许多防护措施可以显示它们的当前状态、有效性和维护需求。所有这三个方面都需要进行定期评审。

6.9.6 BP.08.05——评审安全态势

评审系统的安全态势，以识别必要的变更。

6.9.6.1 描述

系统的安全态势会随威胁环境、运行要求和系统配置而变。这个实践再次检查为什么要适当考虑安全以及其他学科的安全需求。

6.9.6.2 工作产品示例

- 安全评审——包含当前安全风险环境、现有安全态势的描述以及二者是否协调一致的分析；
- 风险验收评审——由正式批准的权威机构做出的关于该系统的运行风险是可以接受的陈述。

6.9.6.3 注释

应根据当前运行环境和已经发生的变化进行安全态势评审。如果在上次评审之后发生的其他事件（例如，变化）没有引起全面安全评审，那么应根据时间间隔安排评审。按时间间隔安排的评审应与相应的策略和规则保持一致。该评审应引导到重新评估当前安全的充分性和当前可接受风险等级的适应性。这种评审应按照安全评估的组织方式，参见 PA03“评估安全风险”。按相同的方式评审运行环境，对于创建系统时所处的开发环境也应定期评审。事实上，开发环境可以被认为是系统开发用的运行环境。

6.9.7 BP.08.06——管理安全事件响应

管理对安全相关事件的响应。

6.9.7.1 描述

在很多情况下，系统的持续可用性是至关重要的。许多事件都不可能预防，因此对破坏做出响应的能力非常重要。应急计划需要识别系统不工作的最长时限、识别系统发挥作用的基本元素、识别并制定恢复战略和计划、测试计划和维护计划。

在许多情况下，系统的持续可用性至关重要。许多事件是无法预防的，因此应对中断的能力是必不可少的。应急计划需要识别系统的非功能性的最大周期；功能性系统的基本要素的识别；恢复策略和计划的识别和开发；计划的测试；以及计划的维护。

在某些情况下，突发事件可能包括事件响应和敌对代理人（如病毒、黑客等）的积极参与。

6.9.7.2 工作产品示例

- 系统恢复优先权列表——包含保护和某个事件导致失败的情况下恢复系统功能的某种顺序描述；
- 测试进度——包含系统定期测试的日程安排，以确保安全相关的功能和规程是可运行并且是熟悉的；
- 测试结果——描述定期测试结果和应采取的系统安全维持措施；

- 维护进度——包含所有系统的升级和预防性维护的日期安排，一般与测试进度合在一起；
- 事件报告——描述发生的事件和所有有关的细节，包括事件来源、所有的危害、做出的响应以及要求进一步采取的行动；
- 定期评审——描述执行系统安全定期评审的规程，包括涉及谁、将检查哪些内容以及输出的内容；
- 意外事故计划——识别可接受的系统最长停机时间、系统的基本元素、系统恢复的战略和计划、业务恢复、局势控制以及方案的测试和维护规程。

6.9.7.3 注释

未来的事件不可能预先确定，但是，一定要应对它们，除非它们不会造成混乱。如果情况超出了预先设想的场景的范围，那么把情况上交合适的业务管理决策层。

6.9.8 BP.08.07——保护安全监视产品

确保与安全监视相关的产品得到适当保护。

6.9.8.1 描述

如果监视活动的产品不能得到信任，这些产品就没有什么价值。这项活动包括密封和归档有关的日志、审核报告和有关的分析。

6.9.8.2 工作产品示例

- 所有归档日志和相关的保留期的列表——识别哪里是安全监视相关产品的存放地方和什么时间能够处置；
- 归档日志定期瑕疵检查结果——描述任何遗漏的报告，以及识别相应的响应；
- 归档日志的用途——指出归档日志的用户，包括访问的时间、目的和注释；
- 随机选择的归档日志的有效性和可用性的定期测试结果——分析随机选择的日志和确定它们是否完整、正确以及有用，以确保系统安全的充分监视。

6.9.8.3 注释

包括审核在内的大部分监视活动都产生输出。这类输出可能立即发挥作用，或者记录在案供以后分析和采取进一步行动。日志的内容设计应有助于了解事件期间发生了什么，以及便于探测变化趋势。输出日志应结合适用的策略和规则进行管理。日志应可靠存储并且要防止篡改或意外损害。日志填满后，应更换新的日志或者清空日志。更换日志后，任何不要求的记录都应删除，并且应执行所要求的其他缩减行动。日志应封存，以防止尚未发现的任何变化，并且应在禁用期间归档。

6.10 PA09——提供安全输入

6.10.1 过程域

6.10.1.1 概要描述

“提供安全输入”的目的是向系统设计师、设计人员、实施人员或用户提供他们所需要的安全信息。这类信息包括安全体系结构、设计或实施的候选方案和安全指南。根据 PA10“确定安全需要”中识别的安全需要，生成和分析这类输入，提供给合适的组织成员并与他们进行协调。

6.10.1.2 目标

- 针对所涉安全问题评审所有系统问题，并且根据安全目标解决；

- 项目组的所有成员了解安全，因此他们能够履行其职责；
- 解决方案反映了提供的安全输入。

6.10.1.3 基本实践列表

BP.09.01 与设计人员、开发人员和用户合作，以确保有关各方对安全输入需要达成共识。

BP.09.02 确定安全约束条件和注意事项，以便做出明智的工程选择。

BP.09.03 识别有关安全的工程问题的候选解决方案。

BP.09.04 运用安全约束条件和注意事项分析工程问题候选方案并且排列优先顺序。

BP.09.05 向其他工程组提供安全相关的指南。

BP.09.06 向运行系统的用户和管理员提供安全相关的指南。

6.10.1.4 过程域注释

这个过程域为支持系统设计和实现活动提供安全输入，其核心是如何使安全成为系统开发的一个组成部分，而不是独立的。每个基本实践都要使用整个工程组织的输入，产生特定的安全结果，并且把这些结果反馈给整个工程组织。已确定的过程适用于新系统的开发或者现有系统的运行和维护。

这个过程覆盖对开发（设计人员和实现人员）和操作（用户和管理员）的安全输入。此外，通过把设计和实现安全活动合并成一个单一的过程域，强调处于不同的抽象层次上的这些活动是非常相似的。候选解决方案的范围很广，从完整的系统体系结构到各个构件。安全要求的某些方面影响系统开发环境，而不是系统本身。

这个过程域中的所有基本实践都可能在系统生存周期的多个时间点迭代执行。

在跟踪本过程域的执行情况时，可以通过检查各基本实践的趋势来判断保障论据是否会被满足。参考 PA06“建立保障论据”。

6.10.2 BP.09.01——理解安全输入需要

与设计人员、开发人员和用户合作以确保有关各方对安全输入需要达成共识。

6.10.2.1 描述

与其他学科协调安全工程，以确定对这些学科有帮助的安全输入的类型。安全输入包括任何类型的、与其他学科应考虑的安全相关的指南设计、文档或想法。输入可以采用多种形式，包括文档、备忘录、电子邮件、培训和咨询。

这个输入是基于 PA10“确定安全需要”，例如，可能需要为软件工程师制定一组安全规则。有些输入与环境的关系比与系统的关系更密切。

6.10.2.2 工作产品示例

- 安全工程与其他学科之间的协议——安全工程如何向其他学科提供输入（例如文档、备忘录、培训、咨询）的定义；
- 所需输入的描述——提供安全输入的每种机制的标准定义。

6.10.2.3 注释

保障目标可能对特定安全需要有影响，特别是在从属性方面。这些目标还可能向安全需要提供其他的理由。在这种情况下，安全工程需要向其他学科就如何得到合适的证据提供指南。

6.10.3 BP.09.02——确定安全约束条件和考虑事项

确定安全限制条件和注意事项，以便做出明智的工程选择。

6.10.3.1 描述

这个基本实践的目的是识别做出明智的工程选择所必需的所有安全约束条件和注意事项。安全工程组要进行分析，确定关于需求、设计、实现、配置和文档编制的安全约束条件和注意事项。约束条件可以在系统生存周期的任何时候、在不同的抽象层次上识别。注意，约束条件可以是肯定性的(一定要这样做)或否定性的(绝不要这样做)。

6.10.3.2 工作产品示例

- 安全设计准则——为做出有关整个系统或者产品设计的决策所必需的安全约束条件和注意事项；
- 安全实现规则——适用于某个系统或者产品的实现(例如特殊机制的应用、编码标准)的安全约束条件和注意事项；
- 文档编制要求——为支持安全要求所必需的特定文档(例如管理员手册、用户手册、特定设计文档)的识别。

6.10.3.3 注释

这些约束条件和注意事项用来识别安全候选解决方案(BP.09.03)和提供安全工程指南(BP.09.05)。约束条件和注意事项的主要来源是 PA10“确定安全需要”中识别的安全相关的要求。

6.10.4 BP.09.03——识别安全候选方案

识别有关安全的工程问题的候选解决方案。

6.10.4.1 描述

这个基本实践的目的是识别与安全有关的工程问题的候选解决方案。这个过程要反复进行并且把安全相关要求转换成各种实现。这些解决方案可以采用多种形式提供，例如体系结构、模型和原型。这个基本实践涉及分解、分析和重写与安全相关的要求，直到有效的候选解决方案得到识别。

6.10.4.2 工作产品示例

- 系统体系结构的安全视图——在抽象层次上按照满足安全要求的方法描述系统体系结构各个要素之间的关系；
- 安全设计文档——包括系统中的资产和信息流的详细内容，以及将加强安全或与安全相关的系统功能的描述；
- 安全模型——系统强制的安全策略的正规演示；应识别一组用于调节某个系统如何管理、保护和分发信息的规则和实践；
- 安全体系结构——由于关系系统的安全，因此关注的是系统体系结构的安全方面的内容，描述相关原理、基本概念、功能和服务；
- 信任分析(防护措施之间的关系和依赖)——描述安全服务和机制是如何相互关联和相互依赖，从而产生整个系统的有效安全，识别可能需要额外的防护措施的领域。

6.10.4.3 注释

候选解决方案包括体系结构、设计和实现等的解决方案。当确定安全约束条件和考虑事项(BP.09.02)时，这些安全候选方案应与所识别的安全约束条件和注意事项相一致。这些候选方案也是权衡比较(BP.09.04)的一部分。这个活动与提供安全工程指南(BP.09.05)相关，一旦确定首选的候选解决方案

后，将要求对其他工程学科给予安全指导。

6.10.5 BP.09.04——分析工程候选解决方案的安全约束

运用安全限制条件和注意事项分析工程问题解决方案并且排列优先顺序。

6.10.5.1 描述

描述这个基本实践的目的是分析工程候选方案并且排列优先顺序。使用在 BP.09.02 中所识别的安全限制条件和注意事项，安全工程师能够评价每个工程候选方案并且向安全工程组提出建议。安全工程师还应从其他工程组的角度考虑工程指南。

这些工程候选方案并不只限于已识别的候选方案(BP.09.03)，还可能包括从其他学科的角度提出的候选方案。

6.10.5.2 工作产品示例

- 权衡分析研究结果和建议——包括对所有 BP.09.02 中提供的、考虑了安全约束条件和注意事项的工程候选方案进行的分析；
- 端到端的权衡分析研究结果——贯穿整个产品、系统或者过程的生存周期的各种决策结果，关注的是可以降低安全要求以满足其他目标(例如费用、功能)的领域。

6.10.5.3 注释

无。

6.10.6 BP.09.05——提供安全工程指南

向其他工程组提供安全相关的指南。

6.10.6.1 描述

这个基本实践的目的是开发与安全相关的指南并且提供给工程组。工程组使用安全工程指南来做出有关体系结构、设计和实现选择的决定。

6.10.6.2 工作产品示例

- 体系结构建议——给出支持开发满足安全要求的系统体系结构的原则或约束条件；
- 设计建议——给出指导系统设计的原则或约束条件；
- 实现建议——给出指导系统实现的原则或约束条件；
- 安全体系结构建议——给出定义系统安全特征的原则或约束条件；
- 保护原理——如何加强安全的高层次描述，包括自动的、物理的、人员的和行政管理的机制；
- 设计标准、原理、原则——有关如何设计系统的约束条件(例如最小的权限、安全控制的独立性)；
- 编码标准——有关如何实现系统的约束条件。

6.10.6.3 注释

所需的指南数量和详细程度取决于其他工程学科具备的安全知识、经验和熟悉程度。很多情况下，多数指南可能与开发环境有关，而不是与正在开发的系统有关。

6.10.7 BP.09.06——提供运行安全指南

向运行系统的用户和管理员提供安全相关的指南。

6.10.7.1 描述

本基本实践的目的是开发与安全相关的指南并且提供给系统用户和管理员。该指南告诉用户和管理员在以安全的方式安装、配置和运行系统以及使系统退役时应做什么。为此，应在系统生存周期的早期开始开发运行安全指南。

6.10.7.2 工作产品示例

- 管理员手册——在以安全方式安装、配置、运行和退役系统时系统管理员的作用和权限的描述；
- 用户手册——关于系统提供的安全机制及其使用指南的描述；
- 安全概述——安全环境(威胁，组织的策略)；安全目标(例如，将要对抗的威胁)；安全功能要求和安全保障要求；基本原理(开发的系统将满足这些目标要求的原理)；
- 系统配置说明书——为确保系统的运行将满足安全目标的系统配置说明书。

6.10.7.3 注释

所考虑的开发环境是用于系统开发的运行环境。

6.11 PA10——确定安全需要

6.11.1 过程域

6.11.1.1 概要描述

“确定安全需要”的目的是明确地识别有关系统安全的需要。“确定安全需要”涉及定义系统中的安全基础，以满足所有法律的、政策的和组织的安全要求。根据系统将来的运行安全背景、组织当前安全和系统环境来定制，并且确定一组安全目标。系统定义了一组与安全相关的需求，经批准后将成为系统安全的基线。

6.11.1.2 目标

所有各方(包括客户)之间对安全需要达成共识。

6.11.1.3 基本实践列表

BP.10.01 理解客户的安全需要。

BP.10.02 识别影响系统的法律、政策、标准、外部影响和约束条件。

BP.10.03 识别系统的目的，以便确定安全语境。

BP.10.04 捕获系统运行的高层次安全视图。

BP.10.05 捕获定义系统安全的高层次目标。

BP.10.06 明确一组一致的要求，用以规定将要在系统中实现的保护。

BP.10.07 就所规定的安全需求与客户需要相匹配达成协议。

6.11.1.4 过程域注释

这个过程域覆盖了整个信息系统的所有安全相关(例如物理的、功能的、程序的)的活动。这些基本实践提出如何识别安全需要以及如何把它们细化成一致的安全需求基线，供系统设计、开发、确认、运行和维护使用。在多数情况下，有必要考虑现有的环境和相关的安全需要。要收集通过这个过程域获得和产生的信息，进一步在项目中[特别是在“提供安全输入”(PA09)中]提炼、使用和更新，以确保客户需

求得到处理。

在跟踪本过程域的执行情况时，可通过检查各基本实践的趋势来判断保障论据是否会被满足。参考 PA06“建立保障论据”。

6.11.2 BP.10.01——理解客户安全需要

理解客户的安全需要。

6.11.2.1 描述

这个基本实践的目的是收集所有必要的信息，以便全面理解客户的安全需要。这些需要受安全风险对客户的重要程度影响。系统将在其中运行的目标环境也影响到客户对安全的需要。

6.11.2.2 工作产品示例

- 客户安全需要陈述——对客户所要求的安全的高层次描述。

6.11.2.3 注释

“客户”这一术语可能是指产品、系统或者服务的特定接受者，或者可能是指基于市场调查或者产品目标的一般接受者。可能需要识别和区别不同的用户群体。例如，普通客户可能有不同于管理员的需要。

6.11.3 BP.10.02——识别适用的法律、政策和约束

识别影响系统的法律、政策、标准、外部影响和约束条件。

6.11.3.1 描述

这个基本实践的目的是收集所有影响系统安全的外部影响。适用性的决定应识别那些支配系统的目标环境的法律、法规、政策和商业标准。应执行全球性的和本地的政策之间优先权的决定。应识别系统客户对系统的安全需求，并且揭示安全的含意。

6.11.3.2 工作产品示例

- 安全约束条件——法律、政策、规则和其他影响系统安全的约束条件；
- 安全轮廓——安全环境（威胁、组织的策略）；安全目标（例如将要对抗的威胁）；安全功能要求和安全保障要求；基本原理（针对这些要求开发的系统将满足目标的原理）。

6.11.3.3 注释

当系统跨越多重物理领域时，要求特殊的注意事项。在不同的国家和不同的业务类型中适用的法律和法规可能会发生冲突。在识别各个适用法律和法规的过程中，如果可能，冲突应尽可能小，并且设法解决。

6.11.4 BP.10.03——识别系统安全语境

识别系统的目的，以便确定安全语境。

6.11.4.1 描述

这个基本实践的目的是识别系统的环境如何影响安全。这涉及对系统目的的理解（例如，情报的、金融的、医疗的）。针对安全注意事项评估系统任务的处理和运行场景。在这个阶段，要求在高层次上

理解系统将要或可能经受的威胁。针对安全可能受到的影响，评估系统的性能要求和功能要求。还要从安全含义的角度评审各个运行约束条件。

为了定义系统的安全边界，环境本身也可能包括与其他组织或者系统的接口。接口元素可能在安全边界以内也可能在边界以外。

组织外部的许多因素也在不同程度上影响该组织的安全需要。这些因素包括政治定位和政治焦点、技术发展、经济影响、全球事件以及信息战活动中的变化。由于这些因素没有一个是静态的，所以要求对变化的潜在影响进行监视和定期评估。

6.11.4.2 工作产品示例

- 预期的威胁环境——对需要予以保护的系统资产的任何已知的或者假设的威胁；包括威胁方（专门技术、可用的资源、动机）、攻击（方法、被利用的脆弱性机会）、资产；
- 评价目标——要对其安全特征进行评价的产品或者系统的描述（类型、预期应用、一般特性、使用的局限性）。

6.11.4.3 注释

系统安全边界不必要与系统边界相同。例如安全边界可能包含系统所在设施和操作系统的人员，而系统边界可能仅限于在人机界面处。除了纯技术措施外，这个扩大的安全边界可以把物理措施作为访问控制的有效防护措施来考虑。

6.11.5 BP.10.04——捕获系统运行的安全视图

捕获系统运行的高层次安全视图。

6.11.5.1 描述

这个基本实践的目的是开发一个面向企业级高层次安全视图，包括角色、责任、信息流、资产、资源、人员保护和物理保护。这个描述应包括讨论企业如何在系统需求的约束条件下管理企业。系统的这种视图通常以运行安全概念的形式提供，同时应包括系统体系结构、规程和环境的高层次安全视图。有关系统开发环境的要求也应在这个阶段被识别。

6.11.5.2 工作产品示例

- 运行安全概念——系统的高层次安全视图（角色、责任、资产、信息流、规程）；
- 概念性安全体系结构——安全体系结构的概念性视图；见 BP.09.03“识别安全候选方案”。

6.11.5.3 注释

无。

6.11.6 BP.10.05——捕获高层次安全目标

捕获定义系统安全的高层次目标。

6.11.6.1 描述

这个基本实践的目的是识别应满足什么样的安全目标，从而为系统在其运行环境中提供足够的安全。PA06“建立保障论据”中确定的系统保障目标可能会影响到安全目标。

6.11.6.2 工作产品示例

- 运行/环境安全策略——在组织内外支配如何管理、保护和分配资产的规则、指示和实践；

- 系统安全策略——通过某个系统或产品支配如何管理、保护和分配资产的规则、指示和实践。

6.11.6.3 注释

安全目标应尽可能不依赖于任何具体的实现。如果具体的约束条件是根据现有环境提出的，那么在确定安全约束条件和注意事项以及支持做出基于可靠信息的工程选择时，应在 PA09“提供安全输入”中提出这些约束条件。安全目标至少应涉及系统和信息的可用性、可核查性、真实性、保密性、完整性和可靠性。

6.11.7 BP.10.06——明确安全相关要求

明确一组一致的要求，用以规定将要在系统中实现的保护。

6.11.7.1 描述

“明确安全相关要求”的目的是定义系统的安全相关要求。这个实践应确保每个要求与关于该系统的适用的政策、法规、标准、安全要求和约束条件保持一致。这些要求应全面定义系统的安全需要，包括那些通过非技术手段来提供的要求。宜定义或规定指定目标的逻辑或物理边界，以确保解决所有方面的问题。应将需求与系统目标相对照或联系，与安全有关的要求应明确而简洁，并且彼此之间不能矛盾。尽可能减少安全对系统功能和性能的影响。安全相关要求应为评估系统在其目标环境中的安全性奠定基础。

6.11.7.2 工作产品示例

- 安全相关要求——对系统的安全运行有直接影响或者促进符合规定的安全策略的要求；
- 可追踪性矩阵——安全需要与要求、解决方案（例如，体结构、设计、实现）及测试和测试结果的映射。

6.11.7.3 注释

许多要求适用于多种学科，只有少数是纯粹安全要求。本过程要求同其他学科大量协作，以便确切地提出系统要求。有关这种协调的活动在 PA07“协调安全”中描述。

6.11.8 BP.10.07——达成安全协议

就所规定的安全需求与客户需要相匹配达成协议。

6.11.8.1 描述

该基本实践的目的是获得有关安全要求的所有团体之间的合作。在针对的是一般性团体而不是某个特定客户的情况下，要求应满足设定的目标。规定的安全要求应全面并且一致地反映管理策略、法律和客户需要。应识别和反复提炼各个问题，直到达成共识。

6.11.8.2 工作产品示例

- 批准的安全目标——说明对抗所识别的威胁和（或）遵循所识别的安全策略（客户接受的）的意图；
- 安全相关的要求基线——在各个指定里程碑所有适用方（特定客户）达成协议的、一组最低限度的安全相关要求。

6.11.8.3 注释

确保协议内容真正得到所有有关各方理解和达成共识是很重要的。要特别注意确保安全要求对于

过程中涉及的所有人员传达同样的含义。

6.12 PA11——验证和确认安全

6.12.1 过程域

6.12.1.1 概要描述

“验证和确认安全”的目的是确保关于安全的解决方案得到验证和确认。针对安全要求、体系结构和设计，使用观察、示范、分析和测试来验证解决方案。针对客户的运行安全需要来确认解决方案。

6.12.1.2 目标

- 解决方案满足安全要求；
- 解决方案满足客户的运行安全需要。

6.12.1.3 基本实践列表

BP.11.01 识别要验证和确认的解决方案。

BP.11.02 定义验证和确认每个解决方案的方法和严格等级。

BP.11.03 验证解决方案是否实现了与更高层次的抽象相关联的要求。

BP.11.04 通过显示解决方案满足与以前的抽象层次相关联的需要，来验证其最终满足客户的运行安全需要。

BP.11.05 向其他工程组提供验证和确认结果。

6.12.1.4 过程域注释

该过程域是系统验证和确认的重要组成部分，应在所有抽象层次执行。安全体系结构宜分层次排列，每个后续的层次都提供了与前一个层次相关的更详细的设计。解决方案包括从运行概念、体系结构到实现，且横跨整个信息系统，包括环境和规程。

为了获得客观的结果，验证和确认组应独立于工程组，这个组要与各个工程组并肩工作。在解决方案生存周期中的任何时候都可以向各个工程组反馈验证和确认的结果。验证和确认有时与正确性和有效性概念相关。

在跟踪本过程域的执行情况时，可以通过检查各基本实践的趋势来判断保障论据是否会被满足。参考 PA06“建立保障论据”。

6.12.2 BP.11.01——识别要验证和确认的目标

识别要验证和确认的解决方案。

6.12.2.1 描述

该基本实践的目的是识别验证和确认活动的目标。验证证明解决方案得到正确实现，确认证明解决方案是有效的。这项活动在整个生存周期中可与所有工程组协调。

6.12.2.2 工作产品示例

- 验证和确认计划——验证和确认工作的定义（包括资源、日程安排、将验证和确认的工作产品等）。

6.12.2.3 注释

大量工作产品需进行验证和确认，包括要求、设计、体系结构、实现、硬件项、软件项以及测试计划

等。与系统的运行和维护相关的工作产品也可以被验证和确认，包括系统配置、用户文档、培训资料以及事件响应方案。

6.12.3 BP.11.02——定义验证和确认方法

定义验证和确认每个解决方案的方法和严格等级。

6.12.3.1 描述

该基本实践的目的是定义验证和确认每个解决方案的方法和严格等级。识别方法包括选择如何验证和确认每项需求；严格等级应指明验证和确认工作的详细程度，并且受从 PA06“建立保障论据”产生的保障战略的输出的影响。例如，有些项目可能只要求做粗略检查，看其是否符合需求，而另一些可能要求更加严格的查验。

这些方法还应包括维护可追踪性的某种手段：从客户的运行安全需要追踪到安全要求、到解决方案、直到解决方案的验证和确认结果。

6.12.3.2 工作产品示例

- 测试、分析、演示和观察计划——即将使用的验证和确认方法（例如测试、分析）和严格等级（例如正式的或非正式的方法）的定义；
- 测试规程——每个解决方案的测试中采用的步骤的定义；
- 追踪方法——验证和确认结果如何追踪到客户的安全需要和要求的描述。

6.12.3.3 注释

安全验证和确认方法应与整个系统的验证和确认方法一致。为此要求有效的协调和交互作用。有关协调的活动在 PA07“协调安全”中描述。

6.12.4 BP.11.03——执行验证

验证解决方案是否实现了与更高层次的抽象相关联的要求。

6.12.4.1 描述

该基本实践的目的是通过显示解决方案与更高层次的抽象相关联的要求（包括已识别的、作为 PA06“建立保障论据”的一个结果的保障要求），来验证解决方案正确与否。验证的方法很多，包括测试、分析、观察和演示。所用的方法参见 BP.11.02。

6.12.4.2 工作产品示例

- 从测试、分析、演示和观察得到的原始数据——由验证解决方案满足要求的过程中所使用的任何方法产生的；
- 问题报告——验证解决方案满足需求的过程中发现的不一致之处。

6.12.4.3 注释

无。

6.12.5 BP.11.04——执行确认

通过显示解决方案满足与更高层次的抽象相关联的需要，来验证其最终满足客户的运行安全需要。

6.12.5.1 描述

该基本实践的目的是确认解决方案满足与更高层次的抽象相关联的需要。确认证明解决方案有效地满足这些需要。确认这些需要是否已经得到满足的方法有很多，包括在设置的运行环境或有代表性的测试环境中测试解决方案。所使用的方法在 BP.11.02 中确定。

6.12.5.2 工作产品示例

- 问题报告——确认解决方案满足安全需要的过程中发现的不一致之处；
- 不一致处——解决方案不满足安全需要的地方；
- 无效解决方案——不满足客户安全需要的解决方案。

6.12.5.3 注释

这个实践与追踪性有关。

6.12.6 BP.11.05——提供验证和确认结果

向其他工程组提供验证和确认结果。

6.12.6.1 描述

该基本实践的目的是识别并提供验证和确认的结果。应采用易于理解和使用的方式提供验证和确认结果。这些结果应能被跟踪，以免丢失从需要到要求、到解决方案、到测试结果的可追踪性。

6.12.6.2 工作产品示例

- 测试结果——测试结果的文档；
- 可追踪矩阵——安全需要与需求、解决方案（例如体系结构、设计、实现）、测试和测试结果的对照。

6.12.6.3 注释

无。

附 录 A
（资料性附录）
本标准与 ISO/IEC 21827:2008 相比的结构变化情况

本标准与 ISO/IEC 21827:2008 具体章条编号对照情况见表 A.1。

表 A.1 本标准与 ISO/IEC 21827:2008 的具体章条编号对照情况

本标准章条编号	对应的 ISO/IEC 21827:2008 章条编号
3.12	—
3.13	—
3.14	3.12
3.15	3.13
3.16	3.14
3.17	3.15
3.18	3.16
3.19	3.17
3.20	3.18
3.21	3.19
3.22	—
3.23	—
3.24	3.20
3.25	3.21
3.26	3.22
3.27	3.23
3.28	3.24
3.29	3.25
3.30	—
3.31	3.26
3.32	3.27
3.33	3.28
3.34	3.29
3.35	3.30
3.36	3.31
3.37	3.32
3.38	3.33
3.39	3.34
3.40	3.35

表 A.1（续）

本标准章条编号	对应的 ISO/IEC 21827:2008 章条编号
3.41	3.36
3.42	3.37
3.43	3.38
3.44	3.39
4.1 第五段	4 第一段
4.1 第六段	4 第二段
4.1	4
—	4.3
—	5
4.2 第一段	6.1.1 第二段
4.3	6.1.3
4.4	6.1.4
4.5	6.1.5
4.6	6.1.6
5.1 第一段	6 第一段
5.1 第二段	6.2 第一段
5.1 第三段	6.2 第二段
5.1.1	6.2.1
5.1.2	6.2.2
5.1.3	6.2.3
5.2.1 第一段	6.3 第一、二段
5.2.1 第二段	6.3.1 第一段
5.2.1 第三段	6.3.1 第二段
5.2.1 第四段	6.3.1 第三、四段
5.2.1 第五段	6.3.1 第五段
5.2.2	6.3.2
5.2.3	6.3.3
5.2.4	6.3.4
5.2.5	6.3.5
5.2.6	6.3.6
5.3	6.4
6.1 第一、二、三段	7 第一、二、三段
6.2	7.1
6.3	7.2

表 A.1（续）

本标准章条编号	对应的 ISO/IEC 21827:2008 章条编号
6.4	7.3
6.5	7.4
6.6	7.5
6.7	7.6
6.8	7.7
6.9	7.8
6.10	7.9
6.11	7.10
6.12	7.11
附录 A	—
附录 B	—
附录 C	附录 A
附录 D	附录 B
附录 E	附录 C
附录 F	—
附录 G	—

附 录 B
（资料性附录）
本标准与 ISO/IEC 21827:2008 的技术性差异及其原因

表 B.1 给出了本标准与 ISO/IEC 21827:2008 的技术性差异及其原因。

表 B.1 本标准与 ISO/IEC 21827:2008 的技术性差异及其原因

本标准章条编号	技术性差异	原因
2	关于规范性引用文件，本部分做了具体技术性差异的调整，以适应我国技术条件，调整情况集中反映在第 2 章“规范性引用文件”中，具体调整如下： ——删除了原国际标准中已作废的 ISO/IEC 15504-2； ——增加了 GB/T 18336.1—2015、GB/T 25069—2010、GB/T 29246—2017、GB/T 30271—2013、ISO/IEC 15288、ISO/IEC 33020	适应我国技术条件。同时，增加了必要的规范性技术文件
3	增加了术语“基本实践”（见 3.12）、“能力”（见 3.13）、“信息安全事态”（见 3.22）、“信息安全事件”（见 3.23）、“过程域”（见 3.30）	助于标准理解，增加标准可操作性
4	修改 ISO/IEC 21827:2008 中 4.1（背景概述）和 4.2（安全工程的开发原因）合并为现在的 4.1（安全工程的开发背景）	适应我国标准结构和语言习惯
4	将 ISO/IEC 21827:2008 中 4.3（安全工程的重要性）与 ISO/IEC 21827:2008 中 6.1.1（安全工程描述）合并为现在的 4.2（安全工程的重要性）	适应我国标准结构和语言习惯，使标准语言更简洁明了，重点突出。原内容是从国际角度叙述的，我国不适用于这种叙述
4	调整 ISO/IEC 21827:2008 中 6.1.1 第二段为本标准 4.2 第一段	调整标准内容结构，突出内容含义表达
4	删除了 ISO/IEC 21827:2008 中 6.1.5 的“企业工程”、“测试工程”，6.1.6 中的“通信安全”“计算机安全”	加强我国相关学科的体系和术语的衔接
5	删除了 ISO/IEC 21827:2008 中第 5 章，将 ISO/IEC 21827:2008 中第 6 章、第 7 章调整为本标准的第 5 章、第 6 章	适应我国标准结构
5	修改了 ISO/IEC 21827:2008 中第 6 章第一段并入本标准 5.1	遵从 GB/T 1.1—2009 规则
5	修改了 ISO/IEC 21827:2008 中 6.3 第一、二段并入本标准 5.2.1	遵从 GB/T 1.1—2009 规则
5	增加了 5.2.1 中“域维具体内容在第 6 章中描述，能力维的通用实践和能力成熟度概念分别在附录 C 和附录 E 中描述”	明确标准内容结构关系
5	增加了 5.2.2 中“附录 F 中阐述了常见信息安全服务与过程域的映射关系”	明确标准内容结构关系

表 B.1（续）

本标准章条编号	技术性差异	原因
5	修改了 ISO/IEC 21827:2008 中 6.3.1 第三、四段内容	遵从我国标准语言表述形式
5	修改了 ISO/IEC 21827:2008 中 6.3.2 第一段中内容，把“129 个基本实践”修改为“130 个基本实践”	ISO/IEC 21827:2008 错误内容
6	修改了 ISO/IEC 21827:2008 中第 7 章第一、二、三段内容为本标准 6.1	遵从 GB/T 1.1—2009 规则
附录	增加了附录 A、附录 B	遵从 GB/T 20000.2—2009 规则
附录	修改了 ISO/IEC 21827:2008 中附录 A、附录 B、附录 C 的编号为本标准附录 C、附录 D、附录 E	本标准增加了附录 A、附录 B
附录	增加附录 F、附录 G	附录 F 更能便于行业对于本标准的利用，附录 G 便于本标准与上一版标准的对比

附 录 C
（规范性附录）
通 用 实 践

C.1 总则

本附录包含通用实践(即适用于所有过程的实践)。通用实践用于过程评估,以确定任一过程的能力。通用实践按公共特征和能力等级分组。通用实践分成以下能力等级:

- 能力等级 1——基本执行;
- 能力等级 2——计划跟踪;
- 能力等级 3——充分定义;
- 能力等级 4——量化控制;
- 能力等级 5——持续改进。

能力等级的通用格式如图 C.1 所示。概要描述包含能力等级简短概括。每个等级分成包含一组通用实践的若干公共特征。每个通用实践在随后的公共特征中详细描述。

能力等级 1——能力等级标题
概要描述——该能力等级描述
公共特征列表——每个公共特征的编号和名称列表
公共特征 1.1——公共特征标题
概要描述——该公共特征概述
通用实践列表——每个公共特征的编号和名称列表
GP1.1.1——通用实践标题
描述——该通用实践概述
注释——关于该通用实践的其他注释
关系——与该模型的其他部分的关系
GP1.1.2……

图 C.1 能力等级格式

C.2 能力等级 1——基本执行

C.2.1 能力等级公共特征

C.2.1.1 公共特征通用实践

C.2.1.1.1 概要描述

过程域基本实践的执行是普遍的。这些基本实践的执行可以不进行严格的计划和跟踪。具体的执行情况依靠个人的知识水平和努力程度。过程域的工作产品证实了它们的执行。组织里的人意识到应采取某项措施,并且普遍认为该措施会在需要的时候根据要求被执行。该过程中存在可识别的工作产品。

C.2.1.1.2 公共特征列表

能力等级由下列公共特征组成：

- 公共特征 1.1——执行基本实践。

C.2.2 公共特征 1.1——执行基本实践

C.2.2.1 公共特征通用实践

C.2.2.1.1 概要描述

该公共特征的通用实践仅仅确保该过程域的基本实践按某种方法执行。然而，由于缺乏控制，产生的工作产品的一致性或性能以及质量可能波动很大。

C.2.2.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 1.1.1——执行过程。

C.2.2.2 GP 1.1.1——执行过程

C.2.2.2.1 描述

执行实现该过程域的基本实践的过程，以便向需求方提供工作产品和(或)服务。

C.2.2.2.2 注释

这个过程可以称为“基本过程”。该过程域的需求方可以是组织内部的或外部的。

C.3 能力等级 2——计划跟踪

过程域中的基本实践是有计划且被跟踪执行的，工作产品符合规定的标准和要求。采取测量来跟踪过程域的执行，因此组织能够根据实际执行情况管理其活动。与等级 1“基本执行”的主要区别在于，该过程的执行是经过计划的和受到管理的。

C.3.1 能力等级公共特征

C.3.1.1 公共特征通用实践

C.3.1.1.1 概要描述

该能力等级由下列公共特征组成：

- 公共特征 2.1——计划执行；
- 公共特征 2.2——规范执行
- 公共特征 2.3——验证执行；
- 公共特征 2.4——跟踪执行。

C.3.2 公共特征 2.1——计划执行

C.3.2.1 公共特征通用实践

C.3.2.1.1 概要描述

这个公共特征的通用实践关注的是执行该过程域及其相应的基本实践进行的计划内容。因此，过

程文档复制、执行过程的合适工具的供给、过程执行的计划、过程执行中的培训、过程资源的分配和过程执行责任的指派等都要涉及。对于过程的规范执行，这些通用实践形成了一个至关重要的基础。

C.3.2.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 2.1.1——分配资源；
- GP 2.1.2——指派责任；
- GP 2.1.3——编制过程文档；
- GP 2.1.4——提供工具；
- GP 2.1.5——确保培训；
- GP 2.1.6——计划过程。

C.3.2.2 GP 2.1.1——分配资源

C.3.2.2.1 描述

为执行该过程域分配足够的资源(包括人员)。

C.3.2.2.2 注释

无。

C.3.2.2.3 关系

关键资源的识别在过程域 PA16“策划技术工作”中完成。

C.3.2.3 GP 2.1.2——指派责任

C.3.2.3.1 描述

为该过程域的工作产品开发和(或)服务提供指派责任。

C.3.2.3.2 注释

无。

C.3.2.3.3 关系

该实践与 PA16“策划技术工作”关系密切。

C.3.2.4 GP 2.1.3——编制过程文档

C.3.2.4.1 描述

把执行该过程域的方法编制成标准和(或)规程。

C.3.2.4.2 注释

执行过程的人(该过程的拥有者)参与编制过程文档，对于创建有用的过程描述非常重要。某个组织或项目的过程不必与本模型中的过程域一一对应。因此，覆盖某个过程域的过程可以用不止一种方法来描述[例如，方针、标准和(或)规程]，为了覆盖某个过程域，以及某个过程描述，可能横跨不止一个过程域。

C.3.2.4.3 关系

与其他通用实践的关系：这是等级 2 过程描述。该过程描述将随着过程能力的提高而演变（见 GP 3.1.1，GP 3.1.2，GP 5.1.2，GP 5.2.3 中该过程的描述）。

在这个等级上描述过程的标准和规程可能包括测量，因此可以用测量来跟踪执行（见公共特征 2.4）。这个实践与 PA17“定义组织系统工程过程”和 PA18“改进组织系统工程过程”有关。

C.3.2.5 GP 2.1.4——提供工具

C.3.2.5.1 描述

提供合适的工具以支持过程域的执行。

C.3.2.5.2 注释

所要求的工具随所执行的过程而变。执行该过程的个人可能很清楚执行该过程需要什么工具。

C.3.2.5.3 关系

与其他通用实践的关系：工具变更可能是过程改进的一部分（见有关过程改进的实践 GP 5.1.2，GP 5.2.3）。

关于工具的管理，见 PA20“管理系统工程支持环境”。

C.3.2.6 GP 2.1.5——确保培训

C.3.2.6.1 描述

确保执行该过程域的个人在如何执行过程方面得到合适的培训。

C.3.2.6.2 注释

由于执行和管理过程方式的变化，培训及其实施方式将随过程能力而改变。

C.3.2.6.3 关系

培训和培训管理的描述见 PA21“提供持续发展的技能和知识”。

C.3.2.7 GP 2.1.6——计划过程

C.3.2.7.1 描述

计划该过程域的执行。

C.3.2.7.2 注释

工程和项目类过程域的计划可以以项目计划的形式进行，而组织类过程域的计划可能是组织级的。

C.3.2.7.3 关系

项目策划在 PA16“策划技术工作”中描述。

C.3.3 公共特征 2.2——规范执行

C.3.3.1 公共特征通用实践

C.3.3.1.1 概要描述

这个公共特征的通用实践关注的是在过程上投入的总量控制。因此，过程执行计划的使用、过程按照标准和规程的执行以及对过程产生的工作产品的配置管理都要涉及。这些通用实践形成一个验证过程执行情况的重要基础。

C.3.3.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 2.2.1——使用计划、标准和规程；
- GP 2.2.2——实施配置管理。

C.3.3.2 GP 2.2.1——使用计划、标准和规程

C.3.3.2.1 描述

在实施过程域的过程中使用文档化的计划、标准和(或)规程。

C.3.3.2.2 注释

按过程描述执行的过程称为“已描述的过程”。应在标准、规程和计划中定义过程测量项。

C.3.3.2.3 关系

与其他通用实践的关系：使用的标准和规程在 GP 2.1.3 中形成文档，使用的计划在 GP 2.1.6 中形成文档。这个实践是 GP 1.1.1 的进化并将演化到 GP 3.2.1。

C.3.3.3 GP 2.2.2——实施配置管理

C.3.3.3.1 描述

合适时，将过程域的工作产品置于版本控制或配置管理下。

C.3.3.3.2 注释

无。

C.3.3.3.3 关系

在过程域 PA13“管理配置”中描述了配置管理学科中支持系统工程所需的典型实践。

过程域 PA13“管理配置”关注的是配置管理的通用实践，这个通用实践关注与正在调查研究的过程域的工作产品有关的这些实践的部署。

C.3.4 公共特征 2.3——验证执行

C.3.4.1 公共特征通用实践

C.3.4.1.1 概要描述

这个公共特征的通用实践关注的是证实过程是否已按预期目标执行。因此验证过程的执行是否符

合适用的标准和规程以及工作产品的审核都要涉及。这些通用实践形成跟踪过程执行情况能力的一个重要基础。

C.3.4.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 2.3.1——验证过程符合性；
- GP 2.3.2——审核工作产品。

C.3.4.2 GP 2.3.1——验证过程符合性

C.3.4.2.1 描述

验证过程是否符合适用的标准和(或)规程。

C.3.4.2.2 注释

无。

C.3.4.2.3 关系

与其他通用实践的关系：适用的标准和规程在 GP 2.1.3 中形成文档，在 GP 2.2.1 中使用。

质量管理和(或)保障过程在 PA12“确保质量”中描述。

C.3.4.3 GP 2.3.2——审核工作产品

C.3.4.3.1 描述

验证工作产品是否符合适用的标准和(或)要求。

C.3.4.3.2 注释

无。

C.3.4.3.3 关系

与其他通用实践的关系：适用的标准和规程在 GP 2.1.3 中形成文档，在 GP 2.2.1 中使用。

产品要求在过程域 PA10“确定安全需要”中得到提出和管理。在 PA11“验证和确认安全”中进一步讨论验证和确认。

C.3.5 公共特征 2.4——跟踪执行

C.3.5.1 公共特征通用实践

C.3.5.1.1 概要描述

这个公共特征的通用实践关注的是对项目执行过程的控制能力。因此涉及根据可度量的计划跟踪过程的执行情况，并且当过程的执行严重偏离计划时采取纠正措施。这些通用实践形成具备达到充分定义过程的能力的一个重要基础。

C.3.5.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 2.4.1——根据测量跟踪；

- GP 2.4.2——采取纠正措施。

C.3.5.2 GP 2.4.1——根据测量跟踪

C.3.5.2.1 描述

根据实施测量的计划来跟踪过程域的状态，包括时间表、费用或其他项目执行相关事项。

C.3.5.2.2 注释

建立测量历史是实施基于数据管理的基础，并且由此开始。跟踪测量为生成能力级别 3 的充分定义数据提供基础。整个项目可使用过程改进测量和信息安全测量。需要计入测量的数据应是可靠的，列入考虑的过程应是可测量的。只有持续的并可重复的过程才能考虑测量。

C.3.5.2.3 关系

与其他通用实践的关系：使用测量就意味着已在 GP 2.1.3 和 GP 2.1.6 中定义和选择了测量项，并且已在 GP 2.2.1 中收集了数据。

信息安全测量在过程域 PA06 中描述。

项目追踪在过程域 PA15“监督和控制技术工作”中描述。

C.3.5.3 GP 2.4.2——采取纠正措施

C.3.5.3.1 描述

当进展严重偏离计划时采取纠正措施。

C.3.5.3.2 注释

进展可能由于估计不准确而变化，执行情况受外部因素影响，或者作为计划基础的要求已改变。纠正措施可能涉及更改过程和(或)计划。

C.3.5.3.3 关系

与其他通用实践的关系：使用测量就意味着已在 GP 2.1.3 和 GP 2.1.6 中定义和选择了测量项，并且已在 GP 2.2.1 中收集了数据。

项目控制在过程域 PA15“监督和控制技术工作”中描述。

C.4 能力等级 3——充分定义

C.4.1 能力等级公共特征

C.4.1.1 公共特征通用实践

C.4.1.1.1 概要描述

根据已批准的充分定义过程、标准的裁剪版本和文档化过程执行基本管理。与等级 2“计划跟踪”的主要区别在于，在这个等级是使用组织级的标准过程来计划和管理过程。

C.4.1.1.2 公共特征列表

该能力等级组成了下列公共特征：

- 公共特征 3.1——定义标准过程；

- 公共特征 3.2——执行已定义过程；
- 公共特征 3.3——协调实践。

C.4.2 公共特征 3.1——定义标准过程

C.4.2.1 公共特征通用实践

C.4.2.1.1 概要描述

这个公共特征的通用实践关注的是组织标准过程的制度化。已制度化的过程的起源或基础可能是在某些特定项目中成功运用的类似的一个或多个过程。组织标准过程可能需要经过裁剪才适用于特定用途，所以也要考虑各种裁剪需要的开发。因此涉及编制组织标准过程文档和针对特定用途的标准过程的裁剪。这些通用过程形成执行已定义过程的一个至关重要的基础。

C.4.2.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 3.1.1——使过程标准化；
- GP 3.1.2——裁剪标准过程。

C.4.2.2 GP 3.1.1——使过程标准化

C.4.2.2.1 描述

编制本组织的标准过程或过程集合文档；这些文件描述如何实施该过程域的基本实践。

C.4.2.2.2 注释

通用实践 GP 2.1.3 和 GP 3.1.1(等级 2 和等级 3 的过程描述)间的关键区别在于方针、标准和规程的应用范围。在 GP 2.1.3 中，标准和规程可能仅用于过程的某种特定情况(如某个具体项目)。在 GP 3.1.1 中，方针、标准和规程是在组织级建立，供共同使用的，称为“标准过程定义”。

由于不要求组织里的过程与能力成熟度模型的过程域一一对应，因此，为了覆盖某个过程域可以定义不止一个标准过程描述；同理，某个已定义过程可能横跨多个过程域。SSE-CMM® 没有规定过程描述的组织或结构。因此，为了提出各个应用领域之间、需求方约束条件之间的差异，可以定义不止一个标准过程。这些标准过程合在一起称为“标准过程集合”。

C.4.2.2.3 关系

与其他通用实践的关系：等级 2 过程描述在 GP 2.1.3 中文档化。等级 3 过程描述在 GP 3.1.2 中裁剪。

开发过程描述的过程在过程域 PA17“定义组织系统工程过程”中描述。

C.4.2.3 GP 3.1.2——裁剪标准过程

C.4.2.3.1 描述

裁剪组织的标准过程集合，以创建提出某特定用途的具体需要的已定义过程。

C.4.2.3.2 注释

裁剪组织的标准过程创建“等级 3”过程定义。对于项目级的已定义过程，裁剪提出该项目的具体需要。

C.4.2.3.3 关系

与其他通用实践的关系：组织的标准过程在 GP 3.1.1 中文档化。裁剪的过程定义在 GP 3.2.1 中使用。

裁剪指南在过程域 PA17“定义组织系统工程过程”中定义。

C.4.3 公共特征 3.2——执行已定义过程

C.4.3.1 公共特征通用实践

C.4.3.1.1 概要描述

这个公共特征的通用实践关注的是充分定义过程的可重复执行。因此，涉及制度化过程的使用、过程的结果（即，工作产品）的缺陷评审，以及过程的执行数据和结果数据的使用。这些通用实践形成安全实践协调的一个重要基础。

C.4.3.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 3.2.1——使用充分定义过程；
- GP 3.2.2——执行缺陷评审；
- GP 3.2.3——使用充分定义数据。

C.4.3.2 GP 3.2.1——使用充分定义过程

C.4.3.2.1 描述

在实施过程域的过程中使用充分定义过程。

C.4.3.2.2 注释

一般是根据组织的标准过程定义裁剪“已定义过程”。充分定义过程是一种具有文档化的、一致的和完整的方针、标准、输入、准入准则、活动、规程、特定角色、测量项、确认、模板、输出和准出准则的过程。

C.4.3.2.3 关系

与其他通用实践的关系：组织的标准过程定义在 GP 3.1.1 中描述。已定义过程在 GP 3.1.2 中通过裁剪而建立。

C.4.3.3 GP 3.2.2——执行缺陷评审

C.4.3.3.1 描述

对该过程域相应的工作产品执行缺陷评审。

C.4.3.3.2 注释

无。

C.4.3.3.3 关系

无。

C.4.3.4 GP 3.2.3——使用充分定义数据

C.4.3.4.1 描述

使用在执行已定义过程的过程中产生的数据来管理该过程。

C.4.3.4.2 注释

在该点积极使用最初在等级 2 收集到的测量数据，将为下一个等级的定量管理奠定基础。

为了有助于跟踪效果和管理过程，测量需要提供随着时间变化的相关效果趋势，并指出可应用于问题领域的改进措施。测量应使用充分定义的数据。分析多个项目的测量标准可以识别趋势，并为组织提供更多关于业务影响的信息。

C.4.3.4.3 关系

与其他通用实践的关系：这是 GP 2.4.2 的演化；这里采取的纠正措施是基于充分定义过程的，该过程具备确定进展的客观准则(见 GP 3.2.1)。

C.4.4 公共特征 3.3——协调实践

C.4.4.1 公共特征通用实践

C.4.4.1.1 概要描述

这个公共特征的通用实践关注的是项目和组织中活动的协调。许多重要活动由项目中不同的组和代表项目的组织服务组执行。协调不足可能造成延误或者所得到的结果没有可比性。因此涉及组内、组间和外部活动的协调。这些通用实践形成具备量化控制过程能力的一个至关重要的基础。

C.4.4.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 3.3.1——执行组内协调；
- GP 3.3.2——执行组间协调；
- GP 3.3.3——执行外部协调。

C.4.4.2 GP 3.3.1——执行组内协调

C.4.4.2.1 描述

在工程学科内协调交流。

C.4.4.2.2 注释

这种类型的协调提出针对某个工程学科的需要，该工程学科通过意见一致的方式来确保有关技术问题(例如访问控制、安全测试)的决策都能实现。将相应的工程师的承诺、期望和责任形成文档并且在所涉及的人员之间达成一致。跟踪并解决工程问题。

C.4.4.2.3 关系

与其他通用实践的关系：这个通用实践与 GP 3.2.1 关系密切，在 GP 3.2.1 中各个过程要充分定义，才能实现有效协调。

协调对象和途径在 PA07“协调安全”中提出。

C.4.4.3 GP 3.3.2——执行组间协调

C.4.4.3.1 描述

在本组织内不同的组间协调交流。

C.4.4.3.2 注释

这种类型的协调解决工程师的需要，以确保在受影响的工程领域中各技术领域（例如风险评估、设计输入、安全测试）之间的关系得到解决。其目的是验证在 GP 3.3.1 中的数据收集工作与其他工程领域协调一致。

通过对组织内每个工程活动的承诺、期望和责任的共识，确立工程组之间的关系。这些活动和共识形成文档并且在整个组织内达成一致，并且提出在某个项目/组织内各个组之间的相互作用。在项目/组织里所有受到影响的工程组之间跟踪并解决工程问题。

C.4.4.3.3 关系

与其他通用实践的关系：这个通用实践与 GP 3.2.1 关系密切，在 GP 3.2.1 中各个过程要充分定义，才能实现有效协调。

协调对象和途径在 PA07“协调安全”中提出。确保及时而准确地向其他工程组提供输入的特定安全工程实践在 PA09“提供安全输入”中提出。

C.4.4.4 GP 3.3.3——执行外部协调

C.4.4.4.1 描述

与外部群体的协调交流。

C.4.4.4.2 注释

这种类型的协调解决请求或要求工程结果的外部组织（例如，消费者、认证活动、评价者）的需要。

通过对组织内每个工程活动的承诺、期望和职责的共识，确立与外部组（例如，需求方、系统安全认证师、用户）之间的关系。各个工程组要识别、跟踪并解决外部技术问题。

C.4.4.4.3 关系

与其他通用实践的关系：这个通用实践与 GP 3.2.1 关系密切，在 GP 3.2.1 中各个过程要充分定义，才能实现有效协调。

协调对象和途径在 PA07“协调安全”中提出。需求方的安全需要在 PA10“确定安全需要”中定义。需求方的保障需要在 PA06“建立保障论据”中提出。

C.5 能力等级 4——量化控制

C.5.1 能力等级公共特征

C.5.1.1 公共特征通用实践

C.5.1.1.1 概要描述

收集并分析执行的详细测量项。由此可以做到量化理解过程能力，并且具备提高预测执行的、已提高的能力。客观地管理执行和量化地理解工作产品的质量。与充分定义级的主要区别在于对已定义过程的量化理解和控制。

C.5.1.1.2 公共特征列表

该能力等级组成了下列公共特征：

- 公共特征 4.1——建立可度量的质量目标；
- 公共特征 4.2——客观管理执行。

C.5.2 公共特征 4.1——建立可度量的质量目标

C.5.2.1 公共特征通用实践

C.5.2.1.1 概要描述

这个公共特征的通用实践关注的是针对使用组织级的过程开发的工作产品所建立的可度量目标。因此涉及质量目标的建立。这些通用实践形成客观管理过程执行的一个重要基础。

C.5.2.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 4.1.1——建立质量目标。

C.5.2.2 GP 4.1.1——建立质量目标

C.5.2.2.1 描述

针对组织的标准过程集合的工作产品建立可度量的质量目标。

C.5.2.2.2 注释

可以把这些质量目标与组织的战略质量目标、需求方的具体需要以及优先顺序或项目的战术需要联系在一起。这里提到的测量不只是传统的最终产品测量。实际上其目的还在于充分了解那些可以用于设定和使用工作产品质量中间目标的过程。

C.5.2.2.3 关系

与其他通用实践的关系：在缺陷评审(GP 3.2.2)中收集的数据在设定工作产品质量目标时特别重要。

C.5.3 公共特征 4.2——客观管理执行

C.5.3.1 公共特征通用实践

C.5.3.1.1 概要描述

这个公共特征的通用实践关注的是确定过程能力的量化测量项，并且在过程管理中充分利用这些量化测量项。提出量化地确定过程能力和使用量化测量项作为纠正措施的基础。这些通用实践形成建立持续改进能力的一个至关重要的基础。

C.5.3.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 4.2.1——确定过程能力；
- GP 4.2.2——使用过程能力。

C.5.3.2 GP 4.2.1——确定过程能力

C.5.3.2.1 描述

量化地确定已定义过程的过程能力。

C.5.3.2.2 注释

这是基于充分定义(GP 3.1.1 和 GP 3.2.3)和测量过程(GP 2.4.1)的一个量化过程能力。测量项存在于过程中,并且应随着过程的执行而收集。

C.5.3.2.3 关系

与其他通用实践的关系:已定义过程通过 GP 3.1.2 中的裁剪来建立,并且在 GP 3.2.1 中执行。

C.5.3.3 GP 4.2.2——使用过程能力

C.5.3.3.1 描述

在过程的执行没有达到其过程能力的情况下采取适当的纠正措施。

C.5.3.3.2 注释

根据对过程能力的了解,已识别的特殊变化原因用户理解在何时、采取何种纠正措施是适当的。

C.5.3.3.3 关系

与其他通用实践的关系:这个实践是 GP 3.2.3 的演化,它给已定义过程补充了量化过程能力。

C.6 能力等级 5——持续改进

C.6.1 能力等级公共特征

C.6.1.1 公共特征通用实践

C.6.1.1.1 概要描述

在组织的业务目标基础上建立关于过程有效性和效率的量化的执行目标。通过执行已定义过程和尝试运用创新的想法与技术并得到量化反馈,能够做到按照这些目标的持续过程改进。与量化控制级的主要区别是,已定义过程和标准过程将在量化地理解变更对这些过程的影响的基础上得到持续精练和改进。

C.6.1.1.2 公共特征列表

该能力等级由下列公共特征组成:

- 公共特征 5.1——改进组织能力;
- 公共特征 5.2——改进过程有效性。

C.6.2 公共特征 5.1——改进组织能力

C.6.2.1 公共特征通用实践

C.6.2.1.1 概要描述

这个公共特征的通用实践关注的是比较标准过程在组织内的使用情况,以及不同的应用之间的区

别。在过程的使用中发现增强标准过程的机会，分析过程产生的缺陷，以识别标准过程的可能增强之处。因此，要建立过程有效性目标，识别标准过程的改进之处并进行分析，以确定标准过程的潜在变更。这些通用实践是形成改进过程有效性的一个至关重要的基础。

C.6.2.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 5.1.1——建立过程有效性目标；
- GP 5.1.2——持续改进标准过程。

C.6.2 GP 5.1.1——建立过程有效性目标

C.6.2.2.1 描述

在组织的业务目标和当前过程能力的基础上建立针对改进标准过程集合的过程有效性的量化目标。

C.6.2.2.2 注释

无。

C.6.2.2.3 关系

无。

C.6.2.3 GP 5.1.2——持续改进标准过程

C.6.2.3.1 描述

通过更改组织的标准过程集合，持续改进过程以增强其有效性。

C.6.2.3.2 注释

把管理单个项目的经验教训反馈给组织，供其他适用领域分析和推广使用。技术革新或渐进式的改进都可能促成对组织标准过程集合的更改。革新改进通常是由新技术这种外部因素驱动。渐进改进通常是内部因素驱动——在裁剪已定义过程中做出的改进。对标准过程的改进涉及解决共性变化原因。

C.6.2.3.3 关系

与其他通用实践的关系：变化的特殊原因在 GP 4.2.2 中得到控制。

组织过程改进在过程域 PA18“改进组织系统工程过程”中得到管理。

C.6.3 公共特征 5.2——改进过程有效性

C.6.3.1 公共特征通用实践

C.6.3.1.1 概要描述

这个公共特征的通用实践关注的是使标准过程处于受控的持续改进状态。因此提出消除标准过程产生缺陷的原因以及持续地改进标准过程。

C.6.3.1.2 通用实践列表

该公共特征由下列通用实践组成：

- GP 5.2.1——实施原因分析；
- GP 5.2.2——消除缺陷原因；
- GP 5.2.3——持续改进已定义过程。

C.6.3.2 GP 5.2.1——实施原因分析

C.6.3.2.1 描述

实施缺陷的原因分析。

C.6.3.2.2 注释

在此分析中，实施过程的人是典型的参与者。这既是一种前瞻性原因分析活动，也是一种反应式原因分析活动。先前具有类似属性的项目中的缺陷可以用于确定新工作的改进领域。

C.6.3.2.3 关系

与其他通用实践的关系：这些分析的结果在 GP 5.2.2、GP 5.2.3 中使用。

C.6.3.3 GP 5.2.2——消除缺陷原因

C.6.3.3.1 描述

有选择地消除造成已定义过程缺陷的原因。

C.6.3.3.2 注释

这个通用实践中暗示了变化的公共原因和特殊原因，每一种类型的缺陷可能导致不同的活动。

C.6.3.3.3 关系

与其他通用实践的关系：原因在 GP 5.2.1 中识别。

C.6.3.4 GP 5.2.3——持续改进已定义的过程

C.6.3.4.1 描述

通过更改已定义过程来持续地改进过程性能，以增强其有效性。

C.6.3.4.2 注释

改进可能基于渐进改进(GP 5.1.2)或革新改进，如新技术(可能作为前导测试的组成部分)。一般情况下，改进由 GP 5.1.1 中建立的目标驱动。

C.6.3.4.3 关系

与其他通用实践的关系：实践 GP 5.1.2 可能是改进的一个起源。目标在 GP 5.1.1 中建立。产品技术的引入在 PA19“管理产品线演化”中得到管理。

附 录 D
（规范性附录）
项目与组织基本实践

D.1 综述

SSE-CMM®包含项目类和组织类过程域。这些过程域源自 SSE-CMM®，并成为 SSE-CMM®的重要组成部分，并用于解释通用实践。

每个过程域包括“安全注意事项”，指出在安全工程的情况下使用该过程域的注意事项，并且还参考了相关的 SSE-CMM®过程域。

D.2 一般安全注意事项

除了作为每个过程域的特殊注意事项的解释清单外，以下各小节包括安全工程的一般注意事项适用于所有项目类和组织类过程域。

D.2.1 项目风险与安全风险

项目类和组织类过程域使用术语“风险”。在这些情况下，提及“项目风险”时，是指有关成功完成某个项目的风险，涉及成本和进度问题。系统安全工程过程域中，“安全风险”被看作是一种是否影响运行的活动，这取决于残留安全风险是否可以被接受。虽然项目类和组织类过程域并没有提出工程类过程域涉及的安全风险管理，但安全风险评估的结果可以提供输入并且影响项目风险管理活动。

D.2.2 运行阶段适用性

尽管项目类和组织类过程域的措辞似乎意味着只适用于开发阶段，但这些过程域同样适用于生存周期的运行和维护阶段。在针对适用于某个组织的过程域进行评估或改进时，需要解释这些过程域。在安全注意事项中很少做例外说明。

D.2.3 安全工程与系统工程

在所有项目类和组织类过程域（例如，“改进组织系统工程过程”）中都使用术语“系统工程”。不过这些过程域适用面很广。因此，当这些过程域应用于安全工程的情况时，术语“系统工程”应用术语“安全工程”取代。这些过程域也需要通过确保安全工程与其他工程学科的融合来完善和提升。

D.2.4 工程关系

在每个过程域中，都会指出系统工程和安全工程的关系。需要注意的是：在各种不同的过程域之间有许多关系（在这些章条中只标识出其主要关系）。

D.3 PA12——确保质量

D.3.1 过程域

D.3.1.1 安全注意事项

PA06“建立保障论据”与确保质量有关。保障可以看成是特殊类型的安全相关质量。

D.3.1.2 概要描述

“确保质量”的目的不仅涉及系统质量，而且还涉及用于创建系统的过程的质量以及项目遵循已定义过程的程度。这个过程域潜在的观念是：只有过程处于持续测量和改进质量的状态下，才可能始终如一地产生高质量系统。此外，应在整个系统生存周期里遵循这个过程。开发高质量系统的过程的关键内容就是测量、分析和纠正措施。

D.3.1.3 目标

- 定义和测量过程质量；
- 实现预期工作产品质量。

D.3.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.12.01 识别每个工作产品的质量要求；

BP.12.02 确保已定义的系统工程过程在系统生存周期中得到遵循；

BP.12.03 对照工作产品质量要求评价工作产品测量项；

BP.12.04 对项目使用的系统工程过程的质量进行测量；

BP.12.05 分析质量测量结果，以便提出关于质量改进或纠正措施的合理建议；

BP.12.06 使员工参与识别并报告质量问题；

BP.12.07 启动处理已发现的问题或质量改进机会的活动；

BP.12.08 建立一种或一系列收集关于对过程或产品采取纠正措施的需要的机制。

D.3.1.5 过程域注释

一个成功的质量程序要求质量工作始终与项目组以及各个支持元素相结合。有效的过程提供一种提高质量的机制，并且减少对最终产品检查的依赖并降低返工率。

这并不意味着单独由那些管理和(或)保障工作产品及过程质量的人负责工作产品输出的质量。相反，“提高”质量的主要责任落在创建者身上。质量管理过程有助于确保质量管理的所有各个方面在整个组织内得到认真考虑和执行，并且反映在产品中。其结果将增加开发者、管理层和客户对系统质量的信心。

这个过程域可能涉及的质量变化类型既包括技术内容，例如，派生的或分配的具体要求值；还包括形式问题，例如，对于产品使用说明书，客户喜欢纸面形式的还是电子形式的。成本超支和进度拖延也可以认为是缺陷，要像对待其他缺陷一样处理。

从期望值的角度来说，组织可能希望决定技术以及与组织进度承诺相符的增长过程中其他问题的变迁。例如，如果组织已承诺在指定的某周交付或首次展示某个产品，那么，明智的做法是通过测量每周的变化情况来测量或确定它的进度。

在跟踪此过程域的性能时，在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见过程域 PA06。

过程域 PA12 确保质量的主题和内容对应于 ISO/IEC 15288 的 6.3.2“项目评估和控制过程”。

D.3.2 BP.12.01——识别工作产品的质量要求

识别每个工作产品的质量要求。

D.3.2.1 描述

不同类型的工作产品和不同的特定工作产品可能有不同的质量要求。这些质量要求应在定义工作产品时予以识别。

D.3.2.2 工作产品示例

- 工作产品质量要求；
- 一般的工作产品质量要求列表。

D.3.2.3 注释

无。

D.3.3 BP.12.02——监视与已定义过程的一致性

确保已定义的系统工程过程在系统生存周期中得到遵循。

D.3.3.1 描述

确保项目的执行遵循已定义的系统工程过程。应按适当的时间间隔核查过程的符合性。应评估已定义过程的偏离以及这种偏离的影响，并且记录在案。

D.3.3.2 工作产品示例

- 已定义系统工程过程的偏离记录；
- 已定义系统工程过程的偏离产生的影响记录；
- 质量手册(纸面或在线形式)。

D.3.3.3 注释

对于已定义过程可以用多种方法监视。例如，某个自愿的审核/评审人员可以参与或观察全部(或一部分)过程活动，或者某个审核/评审人员可以监督全部(或一部分)过程中的工作产品。

D.3.4 BP.12.03——测量工作产品的质量

对照工作产品质量要求评价工作产品测量项。

D.3.4.1 描述

测量工作产品的特性(涉及需求与标准的一致性、正确性和时效性)，提出系统质量的标志。应设计一些测量项来评估工作产品是否能够满足客户和工程的要求。还应设计一些产品测量项，以帮助解决系统开发过程中的问题。

D.3.4.2 工作产品示例

- 产品质量评估；
- 产品质量认证。

D.3.4.3 注释

工作产品质量测量方法，包括：

- 在开发过程中不同点上产品测量项的统计过程控制；

- 依据要求对一系列完整的过程结果的测量，例如：

——规范值，
——计划值，
——接受范围，
——证实值，
——证实的技术变化，
——当前估计，
——预测的技术变化。

D.3.5 BP.12.04——测量过程质量

对项目使用的系统工程过程的质量进行测量。

D.3.5.1 描述

用来创建优质产品的过程与产品质量同样重要。有一个接受测量核查的系统开发过程是很重要，这样可以尽早识别正在恶化的状况，使得生产最终工作产品时能满足要求。因此，拥有这样一个可以测量的过程将减少浪费和提高生产率。

D.3.5.2 工作产品示例

- 过程质量认证。

D.3.5.3 注释

在测量过程中使用的工具实例包括：

- 过程流程图：可用于确定应测量哪些特性和识别潜在的变化根源，除此之外还用于定义过程；
- 对过程参数的统计过程控制；
- 实验设计。

D.3.6 BP.12.05——分析质量测量结果

分析质量测量结果，以便提出关于质量改进或纠正措施的合理建议。

D.3.6.1 描述

仔细检查产品、过程和项目执行情况的所有可用数据，可以揭示问题的根源。然后，可以利用这些信息改进过程和产品质量。

D.3.6.2 工作产品示例

- 偏离分析；
- 失效分析；
- 缺陷报告；
- 系统质量趋势；
- 纠正措施建议；
- 因果图。

D.3.6.3 注释

支持质量改进的测量实例包括：

- 趋势分析，例如识别引起产品参数缓慢蔓延的设备校准问题；
- 标准评价，例如确定在技术或过程变更的情况下某些特定标准是否依然适用。

D.3.7 BP.12.06——邀请参与

设法使员工参与识别并报告质量问题。

D.3.7.1 描述

使用得到遵循的质量过程开发优质的工作产品，要求所有相关人员关注。应鼓励改进质量的想法，需要有可供每个员工自由地提出过程质量问题的论坛。

D.3.7.2 工作产品示例

- 提高质量的环境；
- 从工作人员那里获得的输入和解决方案。

D.3.7.3 注释

可通过以下措施培育质量环境：

- 建立过程行动组；
- 建立质量保障组，这个小组的报告指挥链应独立于项目；
- 建立报告质量问题的独立通道。

D.3.8 BP.12.07——启动质量改进活动

启动处理已发现的问题或质量改进机会的活动。

D.3.8.1 描述

为了不断改进质量，应策划和执行具体的行动。具体到系统开发过程中，损坏产品或过程质量的具体内容需要进行识别和纠正。这将包括最小化繁琐的或不切实际的制度。

D.3.8.2 工作产品示例

- 改进系统工程过程的建议；
- 质量改进计划；
- 过程修订本。

D.3.8.3 注释

质量改进活动的有效实施要求工作产品组提供输入和接受改进。

D.3.9 BP.12.08——检测纠正措施的需要

建立一种或一系列收集关于对过程或产品采取纠正措施所需要的机制。

D.3.9.1 描述

这种机制应在产品的整个生存周期中(从开发、制造到客户使用)是可用的。这些机制可能包括：在线报告系统、专题讨论会、定期评审、以客户为中心的各种小组等。对于所有受影响的组，这些机制应是可用的，包括设计、制造、客户和客户支持等。

D.3.9.2 工作产品示例

- 不断更新的数据库或总库，包含已识别的各种需要、过程改进和产品改进数据；
- 为了把已识别的需要存入数据库或知识库中，要清楚地描述过程、方法和途径；
- 已识别的关于过程改进的需要；
- 已识别的关于产品改进的需要；
- 问题报告。

D.3.9.3 注释

这个基本实践对于在生存周期中的生产、运行和维护等阶段上有效运用系统工程是至关重要的。

在这个基本实践中查明针对纠正措施的需要。在“监督和控制技术工作”过程域(PA15)中引导执行各项纠正措施。问题报告也从“验证和确认安全”过程域(PA11)纳入这个基本实践。

D.4 PA13——管理配置

D.4.1 过程域

D.4.1.1 安全注意事项

在 BP.13.02 中确定系统/项目的配置单元层次时应考虑 PA06“建立保障论据”中保障目标所要求的细节层次。

“管理配置”为 PA06“建立保障论据”提供证据。此外，所选择的配置管理系统本身应按照 PA01“管理安全控制”进行管理。

D.4.1.2 概要描述

“管理配置”的目的是维护已识别的配置单元的数据和状态，并且分析和控制系统及其配置单元的变更。管理系统配置涉及向开发人员和客户提供正确的和最新的配置数据及状态。

这个过程域适用于所有置于配置管理下的工作产品，例如，包括硬件和软件的配置项、设计基本原理、需求、产品数据文件或趋势研究。

D.4.1.3 目标

维护对工作产品配置的控制。

D.4.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.13.01 确定合适的配置管理方法。

BP.13.02 确定不可分割的配置管理单元。

BP.13.03 维护工作产品基线库。

BP.13.04 控制对已建立的配置单元的变更。

BP.13.05 向受影响的组通报配置数据、变更建议以及访问信息的状态。

D.4.1.5 过程域注释

配置管理功能支持可跟踪性，允许在配置生存周期的任何时刻通过系统要求的层次结构追溯配置。可追溯性是 PA10 实践的一部分。

当此过程域的实践用于管理需求时，需要通过 PA10 迭代对这些需求的更改，以传达变更对客户或其代理的影响。

在跟踪此过程域的性能时，查看不同基本实践之间的趋势可能表明是否满足保证参数。参见 PA06。

PA13 的主题和内容在 ISO/IEC 15288 的配置管理过程中解决。

D.4.2 BP.13.01——确定配置管理方法

确定合适的配置管理方法。

D.4.2.1 描述

从均衡分析考虑，影响配置管理的结构和成本的主要因素有三点：

- 识别配置单元的详细程度；
- 配置单元置于配置管理下的时机；
- 配置管理过程要求的正规程度。

D.4.2.2 工作产品示例

- 识别配置单元的指南；
- 将配置单元置于配置管理下的时间安排；
- 选择的配置管理过程；
- 选择的配置管理过程描述。

D.4.2.3 注释

关于在合适的工作产品层次选择配置单元的准则（例如）包括：

- 需要在可管理的层次上维护接口；
- 特殊用户要求，例如范围可更换单元；
- 新设计与修改设计对比；
- 预期的变化率。

这些准则将影响设计工作的可视程度。

关于确定把工作产品置于配置管理下的时机的准则（例如）包括：

- 项目所在的开发生存周期阶段；
- 为了测试，系统元素是否准备就绪；
- 选择的正规化程度；
- 成本和进度限制；
- 客户需求。

关于选择配置管理过程的准则（例如）包括：

- 所在的开发生存周期阶段；
- 系统变更对其他工作产品的影响；
- 系统变更对采购的或分包的工作产品的影响；
- 系统变更对大纲进度资金安排的影响；
- 需求管理。

D.4.3 BP.13.02——确定配置单元

确定不可分割的配置管理单元。

D.4.3.1 描述

配置单元是作为配置管理中不可分割的单元对应的一个或多个工作产品。为配置管理选择工作产品应以选择配置管理战略时确定的准则为基础。选择配置单元时所考虑的层次应有利于开发者和客户，但不要给开发者增加不合理的管理负担。

D.4.3.2 工作产品示例

- 工作产品配置；
- 已识别的配置单元。

D.4.3.3 注释

需求管理领域中的配置单元可能从单个需求变化到需求组。

对于要求可以范围替换的系统，它的配置单元应是可以在范围替换这个层次的单元。

D.4.4 BP.13.03——维护工作产品基线

维护工作产品基线总库。

D.4.4.1 描述

这个实践涉及建立和维护关于工作产品配置的信息库。这个实践一般包括汇集数据或描述配置单元。此外还可能包括建立补充、删除和修改基线的规程以及跟踪/监视、审核和统计配置数据的规程。维护配置数据的另一目的是为从系统生存周期中任一点回溯到源文档提供审核轨迹。

D.4.4.2 工作产品示例

- 决策数据库；
- 配置基线；
- 可追踪性矩阵。

D.4.4.3 注释

在硬件配置单元情况下，配置数据包括规格说明书、图纸、趋势分析数据等等。配置数据最好能够用电子格式维护，这样便于对支持类文档的更新和变更。

软件配置单元一般包括资源代码文件、需求和设计数据以及测试计划和结果。

D.4.5 BP.13.04——控制变更

控制对已建立的配置单元的变更。

D.4.5.1 描述

维护对整个工作产品配置基线的控制。这包括跟踪每个配置单元的配置情况，批准新的配置，如有必要，更新基线。

分析已识别的工作产品问题或者对工作产品的变更请求，以确定工作产品、大纲进度和成本以及其他工作产品将发生的变更的影响。如果根据分析接受对工作产品的变更建议，要确定对工作产品和其他受影响领域实施变更的进度。

完成变更的配置单元，经过对配置变更的评审和正式批准后发布。在发布之前，变更不是正式的。

D.4.5.2 工作产品示例

- 新工作产品基线。

D.4.5.3 注释

变更控制机制可以裁剪来适应不同的变更类型。例如，部件变更的批准过程应短一些，以免影响其他部件。

D.4.6 BP.13.05——通报配置状态

向受影响的组通报配置数据、变更建议和访问信息的状态。

D.4.6.1 描述

一旦配置数据出现任何状态变化，就要通知受配置数据状态影响的组。状态报告应包括关于什么时候处理对配置单元实施被接受的变更的信息，以及受变更影响的相关工作产品的信息。应为开发人员、客户和其他受影响的组提供对配置数据和状态的访问。

D.4.6.2 工作产品示例

- 状态报告。

D.4.6.3 注释

配置状态通报活动(例如)包括：

- 向得到授权的用户提供访问许可；
- 为授权用户准备好基线副本。

D.5 PA14——管理项目风险

D.5.1 过程域

D.5.1.1 安全注意事项

“管理项目风险”提到的风险与项目的成功完成以及处理成本和进度问题有关。通过决定由于残留安全风险所引起的运行影响是否可以容忍，安全工程域提出“安全风险”活动。安全风险活动的结果可能为项目风险管理活动提供输入并且影响到项目风险管理活动。

为了确保安全问题得到说明和解决，PA07“协调安全”应作为考虑的范围。

D.5.1.2 概要描述

“管理项目风险”的目的是识别、评估、监视和缓解成功执行系统工程活动和整个技术工作的风险。这个过程域贯穿整个项目生存周期。与“策划技术工作”(PA16)和“监督和控制技术工作”(PA15)过程域类似，这个过程域的范围包括系统工程活动和整个技术项目工作，因为只有整个技术工作成功，项目系统工程工作才可能被认为是成功的。

D.5.1.3 目标

识别、理解和缓解项目的风险。

D.5.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.14.01 拟订风险管理活动计划；它是识别、评估、缓解和监视项目生存周期中风险的基础。

BP.14.02 通过检查项目目标（关于候选目标和限制条件）和确定可能出现什么差错，识别项目风险。

BP.14.03 评估风险和确定风险发生的可能性以及风险发生的后果。

BP.14.04 正式承认项目风险评估。

BP.14.05 执行风险缓解活动。

BP.14.06 监视风险缓解活动，以确保获得预期结果。

D.5.1.5 过程域注释

所有系统开发工作都有内部风险，其中一些不容易识别。特别是在早期，应搜寻已知风险的可能性和未知风险的存在。不良的风险管理往往是造成客户不满意、成本超预算或进度被拖延的主要原因。及时发现和缩减风险将避免在系统开发比较成熟的状态时才缩减风险造成的成本增加。

说明风险的类型、分析和管理方法之间的区别是很重要的。优秀的风险管理在三维空间运行。例如，分析开发人员风险主要涉及管理方法，如利润和市场开拓；分析用户风险主要涉及风险类型和分析，如使命和目标满意度。

在跟踪此过程域的性能时，在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见过程域 PA06。

过程域 PA14 的主题和内容对应于 ISO/IEC 15288 的 6.3.4“风险管理过程”。重要的是要理解，无论是过程域 PA14 还是 ISO/IEC 15288 的风险管理过程都不涉及安全风险，而只关注项目执行过程中出现的风险。

D.5.2 BP.14.01——开发风险管理方法

拟订风险管理活动计划；它是识别、评估、缓解和监控项目生存周期中风险的基础。

D.5.2.1 描述

这个基本实践的目的是拟订有效的计划来指导项目的风险管理活动。计划的元素应包括：风险管理团队成员的身份证明以及他们的职责；常规的风险管理活动的进度表、方法以及风险识别和缓解中使用的工具；以及跟踪和控制风险缓解活动的方法。该计划还应规定风险管理结果的评估。

D.5.2.2 工作产品示例

- 风险管理计划。

D.5.2.3 注释

风险管理方法的例子包括：

- 螺旋管理法——定期说明和文档化下一个周期的目标和整个项目的目标；
- 在每个周期开始时正式识别和评审风险，并且提出缓解方法；
- 在每个周期结束时评审关于缓解每一个风险的缓解进度。

D.5.3 BP.14.02——识别风险

通过检查项目目标（关于候选目标和限制条件）和确定可能出现什么差错，以识别项目风险。

D.5.3.1 描述

按某种顺序检查项目目标、项目计划（包括活动或事件的依赖关系）和系统需求，以便识别可能有困

难的地方以及这些地方可能出现什么差错。在识别潜在风险时应考虑基于以往经验的风险来源。这个活动在“策划技术工作”(PA16)中规定。建立关键开发依赖关系以及提供跟踪和纠正措施的活动在“监督和控制技术工作”过程域(PA15)中执行。

D.5.3.2 工作产品示例

- 已识别的风险列表。

D.5.3.3 注释

风险识别活动(例如)包括:

- 制定一个通用的风险分类方案或风险分类法,用于分类风险。这种分类法包含每类风险的历史,包括风险发生的可能性(哪些系统元素最可能有风险)、风险发生的估计成本以及缓解策略。这个实践在改进风险估计和重用成功的风险缓解措施中非常有用。
- 关注与那些最有可能产生风险的系统元素有关的风险缓解资源和控制。
- 收集所有详细说明项目和系统工程目标、候选的技术策略、限制条件和成功准则的信息。确保清楚地定义项目和系统工程工作的目标。针对每个满足这些目标的、建议的候选方法,把那些可能阻挠目标实现的事项形成文档;这些事项就是风险。根据这个规程产生每个候选方法的一份风险列表。注意,有些风险是所有候选方法共有的。
- 为了揭示导致风险的假设和决定,访问技术人员和管理人员。使用从相似项目中获得的历史数据来查明在相似的情况下导致问题发生的地方。

D.5.4 BP.14.03——评估风险

评估风险和确定风险发生的可能性以及风险发生的后果。

D.5.4.1 描述

假如以前识别的风险发生了,估计潜在损失(或获益)的机会及其后果。分别分析各个风险并且了解不同的单个风险之间的关系。所用的分析方法应考虑诸如由于技术成熟度和复杂度导致的失败可能性之类因素。

D.5.4.2 工作产品示例

- 风险评估。

D.5.4.3 注释

评估风险的活动(例如)包括:

- 制定估计风险发生可能性和风险发生后产生的成本的标准。这些标准的可能范围从简单的高-中-低定性尺度到以货币和可能性(接近某个百分数的十分之一)计算的定量尺度。
- 根据项目规模、持续时间、全面风险暴露、系统域以及客户环境,建立实用的标准。

D.5.5 BP.14.04——评审风险评估

正式承认项目风险评估。

D.5.5.1 描述

评审风险评估的充分性,并且根据风险做出关于推进、修改或取消某工作的决定。这种评审活动应包括评审潜在的风险管理工作以及这些工作成功的可能性。

D.5.5.2 工作产品示例

- 风险缓解战略。

D.5.5.3 注释

评审风险评估的活动(例如)包括：

- 举行公司内部的所有项目共利益者会议，介绍风险评估。为了有助于沟通对风险控制的理解，要介绍每个风险的可能的缓解策略。
- 对于风险估计的合理性和没有忽视明显的风险缓解策略得到与会者一致同意。

D.5.6 BP.14.05——执行风险缓解活动

执行风险缓解活动。

D.5.6.1 描述

风险缓解活动可能涉及降低风险发生的可能性或降低风险发生时引起破坏的程度。对于那些需要特别关注的风险，可能要同时启动若干风险缓解活动。

D.5.6.2 工作产品示例

- 风险缓解计划。

D.5.6.3 注释

缓解风险的活动(例如)包括：

- 处理所交付的系统将不满足某个特定性能要求的风险，构造可以针对该要求进行测试的系统原型或模型。这类缓解战略降低了风险发生的可能性。
- 处理交付进度将由于子系统不能按时用于集成而造成拖延的风险，针对有风险的子系统拟订具有不同集成时间安排的候选集成方案。如果风险发生(如子系统没有按时准备好)，风险对总进度的影响比较小。这类缓解战略降低了风险发生后造成的影响。
- 使用预定的基线(风险指示物)来触发风险缓解活动。

D.5.7 BP.14.06——跟踪风险缓解活动

监视风险缓解活动，以确保获得预期结果。

D.5.7.1 描述

按常规检查已经实施的风险缓解的结果，以便测量这些结果，并且确定缓解是否成功。

D.5.7.2 工作产品示例

- 风险状态；
- 风险分类法。

D.5.7.3 注释

对于开发进度大约为 6 个月的项目，每两周重新评估一次风险。重新估计每个风险发生的可能性及其后果。

D.6 PA15——监督和控制技术工作

D.6.1 过程域

D.6.1.1 安全注意事项

在开发工作期间和系统运行期间都需要考虑 PA08“监视安全态势”和 PA01“管理安全控制”。

应考虑 PA07“协调安全”,以确保安全问题得到处理。

D.6.1.2 概要描述

“监督和控制技术工作”的目的是为了提供实际进度和风险的足够透明度。当性能明显偏离计划时,这种透明度促进及时采取纠正措施。

“监督和控制技术工作”包括指导、跟踪和评审项目的完成、结果和风险,这是与项目的文档化估计、承诺和计划相对的。文档化的计划用作跟踪活动和风险、沟通状态和修订计划的基础。

D.6.1.3 目标

监督和控制技术工作。

D.6.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素:

BP.15.01 按照技术管理计划指导技术工作。

BP.15.02 对照技术管理计划跟踪资源的实际使用情况。

BP.15.03 对照已确定的技术参数跟踪性能。

BP.15.04 针对技术管理方案评审项目性能。

BP.15.05 分析由跟踪和评审的技术参数所产生的问题,以确定纠正措施。

BP.15.06 当技术参数表明将出现问题或当实际结果偏离计划时采取纠正措施。

D.6.1.5 过程域注释

与“策划技术工作”过程域(PA16)类似,这个过程域适用于项目技术活动以及系统工程工作。当所选择的工作产品完成时和在所选择的里程碑处时,判断工作进展的主要方式是通过对照实际工作、工作产品规模、成本和计划的进度表。当确定计划没有得到满足时,采取纠正措施。这些措施可能包括修改计划,以反映实际完成情况和重新策划剩余工作,或者采取措施提高效率或减少风险。

在跟踪此过程域的性能时,在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见过程域 PA06。

过程域 PA15 的主题和内容对应于 ISO/IEC 15288 中的 6.3.2“项目评估和控制过程”。

D.6.2 BP.15.01——指导技术工作

按照技术管理计划指导技术工作。

D.6.2.1 描述

执行在“策划技术工作”过程域中创建的技术管理计划。这个实践涉及项目的所有工程活动的技术指导。

D.6.2.2 工作产品示例

- 责任矩阵;
- 工作授权。

D.6.2.3 注释

有效的技术指导包括使用适当的沟通机制和及时向所有受影响的团体发布技术信息。应汇集所有的技术指导，以便作为决策和行动的基础予以保留。

D.6.3 BP.15.02——跟踪项目资源

对照技术管理计划跟踪资源的实际使用情况。

D.6.3.1 描述

在项目实施期间提供当前资源的使用情况，将有助于在必要时调整工作和工作计划。

D.6.3.2 工作产品示例

- 资源用途。

D.6.3.3 注释

跟踪成本包括对比实际成本和项目计划中的估计成本，以便识别潜在的超支和欠支。

D.6.4 BP.15.03——跟踪技术参数

对照已确定的技术参数跟踪性能。

D.6.4.1 描述

通过测量技术管理计划中确定的技术参数来跟踪项目及其产品的实际性能。把这些测量值与技术管理计划中确定的阈值相比较，以便向管理层通报问题警告。

D.6.4.2 工作产品示例

- 技术性能管理轮廓。

D.6.4.3 注释

下面是一个性能跟踪场景的例子。

示例练习：针对每个技术参数，定义一个将用于获得测量值的基准活动。由该项目经理控制范围之外的人员执行这个基准活动，确保得到客观的测量值。定期执行这个基准活动，并且把实际测量值与预定的参数值相比较。

D.6.5 BP.15.04——评审项目性能

针对技术管理方案评审项目性能。

D.6.5.1 描述

定期评审项目及其产品的性能，此外，当超过技术参数阈值时也进行这种评审。结合其他技术性能标志评审技术性能测量值的分析结果，并且批准纠正措施计划。

D.6.5.2 工作产品示例

- 对技术管理计划的变更请求；
- 批准的纠正措施。

D.6.5.3 注释

性能评审活动(例如)包括:

- 举行组织内项目所有共利益者的会议,介绍性能分析情况和提出的纠正措施建议;
- 编写形成项目评审会议基础的状态报告。

D.6.6 BP.15.05——分析项目问题

分析由跟踪和评审的技术参数所产生的问题,以确定纠正措施。

D.6.6.1 描述

新的项目问题会在整个项目生存周期里频繁出现。及时识别、分析和跟踪这些问题,对于控制项目性能是至关重要的。

D.6.6.2 工作产品示例

- 项目性能问题的分析;
- 批准的纠正措施。

D.6.6.3 注释

把新的信息与历史项目数据整合。结合暗示项目成功的风险的新问题,识别危害项目的趋势。必要时,针对那些尚未做结论的问题和趋势收集更详细的数据。分析工作往往要求建模和仿真工具以及外部专家意见。

D.6.7 BP.15.06——采取纠正措施

当技术参数表明将出现问题或当实际结果偏离计划时采取纠正措施。

D.6.7.1 描述

当批准纠正措施时,通过重新分配资源、改变方法和规程,或者加强对现行计划的遵循执行纠正措施。当有必要变更技术管理计划时,使用"策划技术工作"(PA16)的实践来修改该计划。

D.6.7.2 工作产品示例

- 资源重新分配;
- 改变方法和规程;
- 改变顺序。

D.6.7.3 注释

这个基本实践涵盖所有为防止出现预计的问题或者纠正已经发现的问题所必需的措施。在这个基本实践下可能采取的措施种类多、数量大。

D.7 PA16——策划技术工作

D.7.1 过程域

D.7.1.1 安全注意事项

应考虑"协调安全"(PA07),特别是在项目整个生存周期里"识别技术活动"(BP.16.05)以及为支持

与需求方和提供方的有效交互“定义项目接口”(BP.16.06)的执行过程中。

D.7.1.2 概述

“策划技术工作”的目的是制定计划,这些计划是进度安排、成本核算、实施控制、跟踪和协商在系统开发、制造、使用和处理中涉及的技术工作的范围和性质的基础。这些技术工作。应把系统工程活动整合到整个项目的综合性技术策划中。

“策划技术工作”涉及估计所要执行的工作、从彼此接口的组获得必要的承诺以及拟订执行该工作的计划。

D.7.1.3 目标

全面策划技术工作。

D.7.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素:

BP.16.01 识别从技术上确保项目成功的关键资源。

BP.16.02 估计影响项目的规模和技术灵活性的因素。

BP.16.03 制定项目所需的所有技术资源的成本估算,是针对项目要求的所有技术资源估计成本。

BP.16.04 确定项目将使用的技术过程。

BP.16.05 识别项目的整个生存周期中的技术活动。

BP.16.06 定义特定的过程,以支持与需求方和提供方有效交互。

BP.16.07 制定整个项目生存周期的技术进度。

BP.16.08 为项目和系统建立具有阈值的技术参数。

BP.16.09 使用在策划活动中收集的信息制定技术管理计划,这个计划将作为跟踪项目和系统工程工作各个重点部分的基础。

BP.16.10 与所有受影响的组和个人共同评审技术管理计划,并且获得组的承诺。

D.7.1.5 过程域注释

策划从了解所要执行的工作的范围和相应的制约条件、风险以及定义和限定项目的目标开始。策划过程包括几个步骤:估计工作产品规模,估计所需资源,拟订进度,考虑风险和协商承诺。可能需要反复执行这些步骤,以便制定在质量、成本和进度目标之间求得平衡的计划。

在跟踪此过程域的性能时,在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见过程域 PA06。

过程域 PA16 的主题和内容对应于 ISO/IEC 15288 的 6.3.1“项目规划过程”。

D.7.2 BP.16.01——识别关键资源

识别从技术上确保项目成功的关键资源。

D.7.2.1 描述

关键资源是对项目成果至关重要的并且可能不是项目现成可用的资源。关键资源可能包括具有特殊技能的人员、工具、设施或数据。关键资源可以通过分析项目任务和进度,以及与类似项目对比来识别。

D.7.2.2 工作产品示例

- 识别的关键资源。

D.7.2.3 注释

实践示例：检查项目进度并且设想每个时间点所要求的资源的类型。列出不容易获得的资源列表。通过设想为合成系统和工作产品所要求的工程技能，检查和补充这个列表。

D.7.3 BP.16.02——估计项目范围

估计影响项目的规模和技术灵活性的因素。

D.7.3.1 描述

可以通过把系统分解成与其他项目组件类似的元素来估计项目的范围和规模。然后可以针对某些因素（例如复杂度或其他参数的差别）调整规模估计值。

历史资料往往是启动规模估计的最佳可用信息。随着现有系统的可用信息的增加，可以精练这些估计值。

D.7.3.2 工作产品示例

- 系统范围估计值；
- 源代码行数；
- 电子插件数量；
- 大型锻件数量；
- 要移动的材料的立方码数。

D.7.3.3 注释

实践示例：分析可用项目文档，访问项目工作人员，以便确定主要的技术制约条件和假设。识别可能的最高水平技术途径和可能阻碍项目或系统工程工作成功的因素。识别主要技术参数并估计每个参数的可接受范围。

D.7.4 BP.16.03——估计项目成本

针对项目要求的所有技术资源估计成本。

D.7.4.1 描述

对于优秀的项目管理，项目成本的详细估计非常重要，无论客户是否要求。根据进度和已识别的工作范围，通过确定劳动力成本、材料成本以及分包成本做出项目成本的估计。直接成本和间接成本（如工具、培训、特殊测试和支持的成本）都包括在内。对于劳动力成本，可以利用历史参数或成本模型，根据工作复杂程度、工具、可用技能和经验、进度以及直接费率和管理费率，把时间（小时）数转换为货币数量。根据标识的风险，设立适当的储备。

D.7.4.2 工作产品示例

- 以技能水平和进度计的全部劳动力成本；
- 以项目、销售商和进度计的材料成本；
- 以销售商和进度计的分包成本；
- 工具成本；
- 培训成本；
- 支持理由。

D.7.4.3 注释

相当数量的项目数据，例如范围、进度和材料项等，应在估计成本之前收集。其他项目的核查表和历史数据可以用来识别可能被忽略的成本项。各种各样的报告和“经验总结”文档是这类信息的典型的良好来源。

D.7.5 BP.16.04——确定项目过程

确定项目将使用的技术过程。

D.7.5.1 描述

在最高层次上，技术过程应遵循以项目特征、组织特征和组织的标准过程为基础的生存周期模型。典型的生存周期模型有：瀑布型、螺旋发展型和增量型。在过程定义中，包括过程活动、输入、输出、序列以及过程和工作产品的质量测量项。

D.7.5.2 工作产品示例

- 为项目选择的系统工程过程。

D.7.5.3 注释

制定并维护综合性的管理计划，这个计划规定项目与所有执行技术工作的内部和外部组织（如分包方）的交互。包括为项目选择的项目生存周期模型和具体的项目活动。

D.7.6 BP.16.05——识别技术活动

识别项目的整个生存周期中的技术活动。

D.7.6.1 描述

可以从适用标准、已知的行业部门最佳实践、参考模型（例如 SSE-CMM®）、本组织的历史经验中选择项目和系统工程活动。

D.7.6.2 工作产品示例

- 识别的技术活动。

D.7.6.3 注释

在可能的情况下，利用类似项目的历史记录来制定活动列表，并且确信列表是完整的信任度。使用“滚动式”方法进行计划。“滚动式”方法被常用于定义近期活动比用于定义项目后期开始的活动更精确。

例如：直到每项活动大约持续两周，才把系统工程活动分解为针对今后三个月策划的活动。从第 3 到第 12 月的活动应按照每项活动大约持续一个月来策划。一年以后启动的活动可以在很高的层次上描述，每项活动大约持续两个月。对于非系统工程技术活动，按照“提供安全输入”（PA09）过程域与其他学科一起推进时，可以使用相同的策划方法。

D.7.7 BP.16.06——定义项目接口

定义特定的过程，以支持与客户的供方有效交互。

D.7.7.1 描述

项目接口包括那些对项目的成功执行必要的组织和个人，可能是项目组内部的也可能是外部的。交互的类型包括信息交换、任务分配以及工作产品交付。确定的交互方法和过程（包括控制）适合参加交互的各方。

D.7.7.2 工作产品示例

- 为项目接口定义的过程。

D.7.7.3 注释

针对项目识别需要与项目交互的组织内部和外部的组，以便成功实现交互。针对每个组，执行“提供安全输入”过程域（PA09）的基本实践，以便交互机制、交互频率以及问题解决机制定义和实施每个借口。

D.7.8 BP.16.07——制定项目进度计划

制定整个项目生存周期的技术进度。

D.7.8.1 描述

项目进度包括系统和组件开发、获得已完成的项、培训，以及准备工程支持环境。进度是基于针对确定的任务的可验证工作模型或数据，并且这些进度应支持任务的相互依赖性和已完成的项的可用性。进度还应包括适合于已识别的风险的宽松时间。所有受影响的团体都应评审和承诺进度。

D.7.8.2 工作产品示例

- 项目进度。

D.7.8.3 注释

进度一般都包括客户和技术的里程碑。

实践示例：在项目限制条件（合同要求、投放市场时间、客户提供的输入等）内，规定系统的增长与全部技术方法一致。从用户角度看，每一个新的增量都应提供更多的系统能力。针对每个新的增量，需要估计额外的员工工时开销。

为了建立按一定比率使用的资源的某个进度，要选择完成每一步增长的日期，它与相应的开发工作量成比例。通过从增长的开始排列各项活动的顺序并且考虑活动之间的依赖关系，可以派生出每一步增长中各项技术活动的详细进度。

对于事件驱动的进度，其实施一般不是平坦的。对于非关键路径活动，为了避免出现不可以接受的资源需求峰值，可能有必要调整活动的持续时间、活动顺序、活动开始日期。

D.7.9 BP.16.08——建立技术参数

为项目和系统建立具阈值的技术参数。

D.7.9.1 描述

建立关键技术参数，它们可以在整个项目生存周期中被跟踪，并且将充当满足最终技术目标的进展指示符。可以通过与客户的交互、客户需求、市场调查研究、原型、识别的风险或类似的项目的历史经验等来识别关键技术参数。每个被跟踪的技术参数应有一个阈值或容忍限度，超过了它就要采取某种纠

正措施。应预先安排在项目进度的适当点对关键技术参数进行评估。

D.7.9.2 工作产品示例

- 技术参数；
- 技术参数阈值；

技术参数的示例包括：

- 防火墙的吞吐量、每秒新建会话数、最大并发连接数；
- 入侵检测的特征库数量；
- 扫描器的漏洞库数量、扫描速度；
- 异常流量阈值。

D.7.9.3 注释

实践示例：识别系统中系统性能的主要驱动因素。在开发系统期间，制定针对每一项随着时间的流逝能够被跟踪的内容的度量。

D.7.10 BP.16.09——制度技术管理计划

使用在策划活动中收集的信息制定技术管理计划；这个计划将作为跟踪项目和系统工程工作各个重点部分的基础。

D.7.10.1 描述

制定并维护综合管理计划。这个计划规定项目与执行技术工作的内部和外部组织（如分包方）的交互。

D.7.10.2 工作产品示例

- 技术管理计划。

D.7.10.3 注释

典型技术管理计划包括：

- 系统开发计划；
- 与开展技术工作的其他组织（如分包方）交互的计划。

D.7.11 BP.16.10——评审和批准项目计划

与所有受影响的组和个人共同评审技术管理计划，并且获得组的承诺。

D.7.11.1 描述

项目计划评审的目标是确保取得整个项目中受影响的组和个人对过程、资源、进度和信息需求的透彻的共识。请求所有项目成员和负责的组织单位为项目计划提供输入。只要可能，就要纳入这些输入，构造团队拥有的计划。如果输入被拒绝或修改，要反馈给提供输入的个人。临时和正式的项目计划都要分发供评审。应从组成项目团队的所有组得到项目计划的承诺。

D.7.11.2 工作产品示例

- 学科/组之间的接口问题；
- 风险；

- 项目计划输入；
- 项目策划问题和解决方案。

D.7.11.3 注释

受影响的群体和个人一般包括：

- 软件工程；
- 硬件工程；
- 制造；
- 管理；
- 客户；
- 用户；
- 合作伙伴；
- 分包方。

活动示例：识别问题并回答问题，将这部分作为评审的一部分（对于不同的组，问题可能不同）。通报各个组将如何进行评审。向各个组提供技术管理计划并且按照预先的安排开会讨论各个组的意见。根据评审者的意见列出问题列表，逐一处理并解决这些问题。

D.8 PA17——定义组织系统工程过程

D.8.1 过程域

D.8.1.1 安全注意事项

这个过程域使用术语“系统工程”。不过，这个过程域适用范围很广，在评估组织的安全工程能力时，术语“系统工程”可以用术语“安全工程”代替。

这个过程域的基本实践涉及安全工程与系统工程和其他学科的整合。因此，当定义组织的安全工程过程时，应考虑 PA07“协调安全”。

D.8.1.2 概要描述

“定义组织系统工程过程”的目的是创建和管理组织的标准系统工程过程。随后可以由项目对它进行裁剪，以形成开发系统或产品进程所遵循的唯一过程。

“定义组织系统工程过程”包括定义、收集和维护满足组织业务目标的过程，以及设计开发系统工程过程资产并且将其形成文档。这些资产包括过程示例、过程片段、过程相关文档、过程体系结构、过程裁剪规则和工具，以及过程测量项。

D.8.1.3 目标

为本组织定义标准系统工程过程。

D.8.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.17.01 根据组织业务目标建立组织系统过程的目标。

BP.17.02 收集和维护系统工程过程资产。

BP.17.03 开发本组织的妥善定义的标准系统工程过程。

BP.17.04 制定组织标准系统工程过程的裁剪指南，用于项目开发定义的过程。

D.8.1.5 过程域注释

这个过程域涵盖收集和维护过程资产(包括组织标准系统工程过程)所要求的初始活动。过程资产和组织标准系统工程过程的改进由“改进组织系统工程过程”(PA18)覆盖。

在跟踪此过程域的性能时,在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见PA06“建立保障论据”。

PA17 的主题和内容对应于 ISO/IEC 15288 的两个过程中,即 6.2.1“生存周期模型管理过程”和资源管理过程的一些活动。

D.8.2 BP.17.01——建立过程目标

根据组织业务目标建立组织系统工程过程的目标。

D.8.2.1 描述

系统工程过程是在业务背景下运行的,为了制度化组织的标准实践,应明确认识到这一点。过程目标应考虑财政、质量、人力资源和对业务成功举足轻重的市场问题。

D.8.2.2 工作产品示例

- 组织系统工程过程的目标;
- 对组织标准系统工程过程的要求;
- 对组织过程资产库的要求;
- 过程资产库的要求;
- 过程资产库。

D.8.2.3 注释

建立目标可能包括根据“时机-市场”、质量以及生产率等业务问题确定关于过程性能的准则判据。

D.8.3 BP.17.02——收集过程资产

收集和维护系统工程过程资产。

D.8.3.1 描述

过程定义活动产生的组织级和项目级的信息保存(例如,存放在过程资产库里),使用介入过程设计的裁剪工作的人可以访问它们,并维护这些信息,保持其最新。

D.8.3.2 工作产品示例

- 过程资产使用说明;
- 过程资产库设计规范;
- 过程资产。

D.8.3.3 注释

过程资产库的目的是存储过程资产,并可供使用。各个项目将发现这些资产对定义系统开发过程是有用的。过程资产库包含一些已定义的过程示例和过程测量项。组织标准系统工程过程已被定义时,应添加到过程资产库中,同时添加的还有关于项目在定义本项目的过程时裁剪这个组织标准系统工程过程的指南。

过程资产一般包括：

- 组织标准系统工程过程；
- 推荐的或批准的开发生存周期；
- 项目过程和在这些过程执行期间收集的测量值；
- 组织的标准系统工程过程的裁剪指南和准则；
- 过程相关的参考文档；
- 项目过程测量项。

D.8.4 BP.17.03——开发组织系统工程过程

开发本组织的妥善定义的标准系统工程过程。

D.8.4.1 描述

使用过程资产库的设备开发组织标准系统工程过程。在开发过程中新的过程资产可能是必需的并且应把这些新资产添加到过程资产库中。组织标准系统工程过程应放置在过程资产库中。

D.8.4.2 工作产品示例

- 组织标准系统工程过程；
- 培训输入；
- 系统工程过程改进输入。

D.8.4.3 注释

标准系统工程过程应包括与本组织其他已定义过程的接口。此外，应引述和维护用来定义系统工程过程的参考文件(例如，军用标准、IEEE 标准)。

为了开发标准系统工程过程，组织可能要识别该组织系统工程的所有过程元素或活动。组织一定要对输入和输出的一致性、冗余的活动以及遗漏的活动，评价各个过程元素。应解决过程元素与针对合适的顺序和验证特征的预防措施之间的不一致性。最后得到的过程应是妥善定义的。

妥善定义的过程定义包括：

- 准备就绪准则；
- 输入；
- 标准和规程；
- 验证机制：
  - 同行评审；
  - 输出；
  - 完整准则。

D.8.5 BP.17.04——制定裁剪指南

制定组织标准系统工程过程的裁剪指南，用于项目开发项目定义的过程。

D.8.5.1 描述

由于组织标准系统工程过程可能不适合每个项目的情况，因此需要裁剪这些过程的指南。裁剪指南应适合于各种情况，同时不允许项目放弃那些应予以遵循的标准或者由组织方针指出的那些基本的和重要的实践。

D.8.5.2 工作产品示例

- 组织标准系统工程过程裁剪指南。

D.8.5.3 注释

这些指南应使组织标准系统工程过程能被裁剪，以便处理各种情况变量，例如：项目领域、成本、进度和质量均衡关系，项目工作成员的经验，客户的性质，项目的技术难度等。

D.9 PA18——改进组织系统工程过程

D.9.1 过程域

D.9.1.1 安全注意事项

在“改进组织系统工程过程”中，使用术语“系统工程”，这个过程域适用范围很广，因此，当评估组织的安全工程能力时，术语“系统工程”代之以术语“安全工程”。此外，这个过程域的基本实践涉及安全工程与各个系统工程学科的整合。

D.9.1.2 概要描述

“改进组织系统工程过程”的目的是通过持续改进本组织使用的系统工程过程的效率和效果获得竞争优势，它涉及使组织过程在本组织业务目标背景中得到理解，分析过程性能，以及明确策划和部署针对这些过程的改进。

D.9.1.3 目标

策划并实施对标准系统工程过程的改进。

D.9.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.18.01 评估组织中正在执行的现行过程，了解它们的强项和弱项。

BP.18.02 根据分析潜在改进对实现过程目标的影响，策划组织过程的改进。

BP.18.03 变更组织标准系统工程过程，以反映已确定为目标的改进。

BP.18.04 适当时，向现在的项目的其他受影响的组通报过程改进情况。

D.9.1.5 过程域注释

这个过程域覆盖持续的活动，以便测量和改进组织中系统过程的性能。组织过程资产的初始收集和组织标准系统工程过程的定义，由“定义组织系统工程过程”过程域(PA17)覆盖。

改进标准过程的指南有多种来源，包括过去的经验教训、通用实践应用以及对照 SE-CMM® 对标准过程的评估。对照各个过程域的能力等级轮廓将指出最需要改进的领域。把通用实践纳入这些过程域将是很有用的。

在跟踪此过程域的性能时，在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见 PA06“建立保障论据”。

PA18 的主题和内容对应于 ISO/IEC 15288 的 6.2.1“生存周期模型管理过程”的其余活动。

D.9.2 BP.18.01——评估过程

评估组织中正执行的现行过程，了解它们的强项和弱项。

D.9.2.1 描述

评估组织中正在执行的现有过程，了解它们的强项和弱项。

D.9.2.2 工作产品示例

- 过程成熟度轮廓；
- 过程性能分析；
- 评估发现；
- 差距分析。

D.9.2.3 注释

评价场景示例：使用 SE-CMM® 及其他相应的评估方法评估组织的现行系统工程过程。使用评估的结果来建立或更新过程性能目标。

如果现行系统工程过程的执行中出现拖延和等候现象，那么为了缩短周期时间，组织可能从开始点关注这些现象。按照重新核查诸如准备就绪准则、输入验证机制之类的过程特征。

D.9.3 BP.18.02——策划过程改进

根据分析潜在改进对实现过程目标的影响，策划组织过程的改进。

D.9.3.1 描述

评价过程提供变更动力。应在策划那些将为组织业务目标提供最大回报的改进中利用这种动力。改进计划替代一个利用评估过程中产生的动态的框架。该计划应包括提升目标，这些提升目标将产生高的回报率。

组织可以利用这个机会来“防止误解”过程和清除浪费工作。使过程稳定，也就是说，每个人都一致地执行过程是很重要的。过程部署通常是一个挑战。在实施改进中，要注意避免由于局部优化而导致其他方面出问题。

D.9.3.2 工作产品示例

- 过程改进计划。

D.9.3.3 注释

对照估计的周期时间里的回报率、生产率以及质量，对建议的过程改进进行均衡分析。使用 PA09“提供安全输入”的技术。

D.9.4 BP.18.03——变更标准过程

变更组织标准系统工程过程，以反映已确定为目标的改进。

D.9.4.1 描述

对组织标准系统工程过程的改进，以及对过程资产库里裁剪指南的必要变更，将保护改进的过程并且鼓励各个项目把这些纳入新产品开发中。

D.9.4.2 工作产品示例

- 组织标准系统工程过程；

- 组织标准系统工程过程的裁剪指南。

D.9.4.3 注释

随着标准系统工程过程的改进的实施和评价，组织应采用各项成功改进对标准系统工程过程作永久性变更。

D.9.5 BP.18.04——交流改进情况

适当时，向现有的项目和其他受影响的组通报过程改进情况。

D.9.5.1 描述

对于现有的项目，某些过程改进可能是有用的，并且根据项目的状态，这些项目可以把有用的改进吸收到他们的项目过程中。过程改进情况还应通知其他负责培训、质量保证、测量等人员。

D.9.5.2 工作产品示例

- 过程资产库使用说明书；
- 组织标准系统工程过程的裁剪指南；
- 逐一列出对系统工程过程的变更及其理由；
- 实施过程变更的进度。

D.9.5.3 注释

过程改进，以及变更的理由和预期效益应通报给所有影响的项目和组。组织应制定一个部署计划，用于更新过程和监督部署计划的一致性。

D.10 PA19——管理产品线演化

D.10.1 过程域

D.10.1.1 安全注意事项

由安全产品组成的产品线有特殊要求，包括：应严格遵守的配置管理实践，对安全代码开发的人员许可证要求及安全产品的认证和认可。所有人这些要求将加长产品开发周期和加大生存周期成本。

PA06“建立保障论据”与确保新的或修改的产品持续满足客户的安全需要有关。

D.10.1.2 概要描述

“管理产品线演化”的目的是在产品线向其终极目标发展的过程中引入服务、设备和新技术、从而在产品演化、成本、进度和性能方面得到最佳效益。

组织应首先确定产品的演化，然后应做出以下决策：如何设计和构造这些产品，包括关键构件划算的工具，以及高效的和有效的过程。

D.10.1.3 目标

产品线向终极目标发展。

D.10.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.19.01 定义所要提供的产品类型。

BP.19.02 识别那些将有助于组织获取、开发和应用技术来提高竞争优势的新产品技术或基础设施。

BP.19.03 在产品开发周期中做必要变更，以支持新产品的开发。

BP.19.04 确保关键构件是可用的，以便支持已策划的产品演化。

BP.19.05 在产品开发、营销和制造中引入新技术。

D.10.1.5 过程域注释

之所以需要“管理产品线演化”，是由于“为了确保产品开发工作集中实现战略业务目的，以及创建和改进为长期支持研究和开发具有竞争力的产品所需的能力”。

这个过程域覆盖的实践与产品线管理相关，而不是产品本身的工程。

在跟踪此过程域的性能时，在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见PA06“建立保障论据”。

PA19 的主题和内容对应于 ISO/IEC 15288 的两个过程，即环境管理过程和 6.4.12“操作过程”的一些活动。

D.10.2 BP.19.01——定义产品演化

定义所要提供的产品类型。

D.10.2.1 描述

定义支持组织的战略构想的产品线。

考虑组织的强项和弱项、竞争情况、潜在的市场规模和可用的技术。

D.10.2.2 工作产品示例

- 产品线定义。

D.10.2.3 注释

定义的产品线使更有效的重用方法和给投资带来很高的潜在回报率成为可能。

D.10.3 BP.19.02——识别新产品技术

识别那些将有助于组织获取、开发和应用技术来提供竞争优势的新产品技术或基础设施。

D.10.3.1 描述

识别有可能引入产品线中的新产品技术。建立和维护识别新技术的基础设施改进（例如设备或维护服务）的来源方法。

D.10.3.2 工作产品示例

- 产品线技术评审；
- 过程小组的改进建议。

D.10.3.3 注释

这个实践涉及识别、选择、评价和试用测试新技术，通过维护对技术创新的关注，以及系统地评价和实验新技术，组织能够选择合适的技术来提高自己的产品线的质量以及工程和制造活动的生产率。对

于那些新的和未经验证的技术，在它们投入产品线之前，通过试用加以评估。诸如设备升级或增强分布链的服务能力之类基础设施的改进，也可以为推动产品线向未来目标发展提供机会。

D.10.4 BP.19.03——调整开发过程

在产品开发周期中做必要变更，以支持新产品的开发。

D.10.4.1 描述

调整组织的产品开发过程，以便利用那些打算将来使用的构件。

D.10.4.2 工作产品示例

- 调整的开发过程。

D.10.4.3 注释

这个实践包括建立可重用构件库，其中包括识别的检索构件的机制。

D.10.5 BP.19.04——确保关键构件的可用性

确保关键构件是可用的，以便支持已策划的产品演化。

D.10.5.1 描述

组织应确定产品线的关键构件并且针对它们的可用性进行策划。

D.10.5.2 工作产品示例

- 产品线构件。

D.10.5.3 注释

可以把关于关键构件的未来使用事宜纳入产品需求中，从而确保这些构件的可用性。组织应分配合适的资源，用于持续维护这些构件。

D.10.6 BP.19.05——引入产品技术

管理产品线的新技术引入。

D.10.6.1 描述

管理产品线的新技术引入，包括修改现有的产品线构件和引入的新构件。识别和管理与产品设计变更相关的风险。

D.10.6.2 工作产品示例

- 新产品线定义。

D.10.6.3 注释

这个实践的目标是改善产品质量、提高生产率、降低生存周期成本和缩短产品开发周期。

D.11 PA20——管理系统工程支持环境

D.11.1 过程域

D.11.1.1 安全注意事项

在通信安全和可信的软件开发环境中的产品开发将在 BP.20.02、BP.20.03、BP.20.04 中提出唯一要求，例如安全保障需要明确的人员和监管链。

“安全工程支持环境”应包括在 PA03“评估安全风险”的各项活动中。应通过正确管理的“安全工程支持环境”来确认 PA06“建立保障论据”。

D.11.1.2 概要描述

“管理系统工程支持环境”的目的是为开发产品和执行过程提供所需的技术环境。开发和过程技术在尽可能少地中断开发活动的前提下引入环境中，从而升级到可以使用新技术。

随着时间的推移，组织的技术需要发生变化，同时，由于需要的演变，该过程域中描述的工作应重新执行。

D.11.1.3 目标

系统工程支持环境尽可能提高过程效率。

D.11.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.20.01 维持支持组织目标的技术意识；

BP.20.02 根据组织的需要确定对组织系统工程支持环境的需求。

BP.20.03 通过使用“分析候选解决方案”过程域中的实践，获得满足在“确定支持需求”(BP.20.02)中建立的需求的系统工程支持环境。

BP.20.04 针对个别项目需要裁剪系统工程支持环境。

BP.20.05 根据组织的业务目标和项目的需要把新技术引入系统工程支持环境中。

BP.20.06 维护系统工程支持环境，以持续支持依赖该环境的项目。

BP.20.07 监视系统工程支持环境以寻求改进机会。

D.11.1.5 过程域注释

在项目级和组织级，这个过程域涉及的问题与系统工程支持环境相关。支持环境的元素由系统工程活动的所有外围环境组成，包括：

- 计算资源；
- 通信频道；
- 分析方法；
- 组织的结构、策略和规程；
- 机械修理店；
- 化学处理设备；
- 环境应力设备；
- 系统工程仿真工具；
- 软件生产工具；

- 系统工程专有工具；
- 工作空间。

在跟踪此过程域的性能时，在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见 PA06。

PA20 的主题和内容对应于 ISO/IEC 15288 的环境管理过程的其余活动。

D.11.2 BP.20.01——维持技术意识

维持支持组织目标的技术意识。

D.11.2.1 描述

技术的当前状态或实践状态的意识是评估改进机会的一个必要元素。因此，为了引入新技术，应表明本组织有足够的新技术意识。这种意识可以是内部维持的，也可以是获取的。

D.11.2.2 工作产品示例

- 支持环境技术评审。

D.11.2.3 注释

维护意识可以通过阅读行业期刊、参加专业协会以及建立和维护技术图库来实现。

D.11.3 BP.20.02——确定支持要求

根据组织的需要确定对组织系统工程支持环境的需求。

D.11.3.1 描述

组织的需要主要通过评估竞争性问题来确定。例如，组织的支持环境影响了组织的竞争地位吗？组织支持环境的每个主要元素允许系统工程以足够的速度和准确度运行吗？

D.11.3.2 工作产品示例

- 对系统工程支持环境的要求。

D.11.3.3 注释

确定组织对计算机网络性能、改进的分析方法、计算机软件和过程改组的需要。

D.11.4 BP.20.03——获得系统工程支持环境

通过使用 PA10 确定安全需要中的实践，获得满足在“确定支持需求”(BP.20.02)中建立的需求的系统工程支持环境。

D.11.4.1 描述

确定适合于所需的系统工程支持环境的评价准则和候选解决方案。然后使用 PA10 确定安全需要中的实践选择方案。最后，获得并实现所选择的系统工程支持环境。

D.11.4.2 工作产品示例

- 系统工程支持环境。

D.11.4.3 注释

系统工程支持环境可能包括下列内容中的大部分：软件生产工具；系统工程仿真工具；内部专用工具；商业化定制工具；特殊测试设备和新设备。

D.11.5 BP.20.04——裁剪系统工程支持环境

针对个别项目需要裁剪系统工程支持环境。

D.11.5.1 描述

全部支持环境从总体上代表组织的需求。不过，个别项目可能对于所选的环境元素有自己的特殊需要。这种情况下，裁剪系统工程支持环境元素可以使项目更加有效的运行。

D.11.5.2 工作产品示例

- 裁剪的系统工程支持环境。

D.11.5.3 注释

裁剪允许个别项目定制自己的系统工程支持环境。例如，项目 A 不涉及信号处理，所以可以从这个项目的成套自动化工具中裁剪掉（即不提供）自动信号处理工具。相反，项目 B 是组织里唯一需要自动需求跟踪项目，所以要在这个项目的自动化成套工具里裁剪进（即补充提供）适当的工具。

D.11.6 BP.20.05——引入新技术

根据组织的业务目标和项目的需要把新技术引入系统工程支持环境中。

D.11.6.1 描述

随着新技术的出现，以及发现他们支持组织的业务目标和项目需要，应使用它们来更新组织系统工程支持环境。

对于系统工程支持环境中新技术的使用应提供培训。

D.11.6.2 工作产品示例

- 新的系统工程支持环境。

D.11.6.3 注释

向组织的支持环境中引入新技术时有一些困难。为了尽可能弱化这些困难，要遵循以下步骤：

1） 彻底测试新技术
2） 决定是在整个组织还是在组织的某些部分引入改进。
3） 对那些将受到影响的人员尽早地提醒即将发生的变更。
4） 提供适合新技术的，任何必要的“如何使用”的培训。
5） 监督新技术的接受情况。

D.11.7 BP.20.06——维护环境

维护系统工程支持环境，以持续支持依赖该环境的项目。

D.11.7.1 描述

维护系统工程支持环境，使其性能水平与所期望的水平一致。维护活动可能包括计算机系统管理、

培训、热线支持、专家的可用性、发展/扩展技术数据库等。

D.11.7.2 工作产品示例

- 针对系统工程支持环境的性能报告。

D.11.7.3 注释

实现系统工程支持环境的维护有多种方式，包括：

- 雇佣或培训计算机系统管理者；
- 发展使用所选自动化工具的专家；
- 发展可以应付各种项目的方法学专家；
- 发展可以应付各种项目的过程专家。

D.11.8 BP.20.07——监视系统工程支持环境

监视系统工程支持环境以寻求改进机会。

D.11.8.1 描述

确定影响系统工程支持环境有用性的因素，包括任何新引入的技术。监视新技术和整个系统工程支持环境的接受情况。

D.11.8.2 工作产品示例

- 系统工程支持环境中使用技术的评审。

D.11.8.3 注释

把某些监视措施设计为自动化的背景活动，使得用户在使用支持环境时不需要有意识地提供数据。也向系统工程支持环境的用户提供一种有意识地就当前系统工程支持环境的有用性提供输入和改进建议的方法。

D.12 PA21——提供持续发展的技能和知识

D.12.1 过程域

D.12.1.1 安全注意事项

需要在组织上的安全工程过程中提供培训。

D.12.1.2 概要描述

“提供持续增长的技能和知识”的目的是确保项目的组织拥有必要的知识和技能去实现项目和组织目标。为确保这些显然只有取自于人的关键资源的有效应用，有必要识别组织内的知识和技能需求以及项目的或组织的具体需要(例如有关新出现的程序或技术，以及新的产品、过程和策略的需要)。

所需的技能和知识可以通过组织内培训和及时从组织外部获取的方式提供。获取技能和知识的外部来源可能包括客户资源、临时雇佣、新雇佣、咨询和分包方。

D.12.1.3 目标

组织拥有为实现项目和组织目标所需要的必要技能。

D.12.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素：

BP.21.01 使用项目的需要、组织战略规划以及员工的现有技能做指导，识别整个组织对技能和知识的改进需要。

BP.21.02 评价和选择有关培训或其他来源的、获取知识或技能的适合模式。

BP.21.03 确保适当的技能和知识可供系统工程工作使用。

BP.21.04 根据已确定的培训需要准备培训材料。

BP.21.05 培训人员、使其掌握必要的技能和知识，以履行分配给他们的岗位职责。

BP.21.06 评估培训效果，以满足已识别的培训需要。

BP.21.07 维护培训和测验的记录。

BP.21.08 维护可访问库中的培训材料。

D.12.1.5 过程域注释

为所需要的技能和知识选择内部培训还是外部来源，往往根据培训专家的可用性、项目进度和业务目标确定。成功的内部培训计划来源于组织的承诺。此外，培训计划的管理采用一种优化学习过程的、并且是可重复的、可评估的以及容易变更以满足组织新的需要的方法。内部培训不限于在“教室”里进行：它包括很多支持技能增强和知识提升的培训手段。如果由于进度或培训资源的可用性问题，内部培训的方式不可行时，可以从外部购买必要的技能和知识来源。

在跟踪此过程域的性能时，在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见PA06“建立保障论据”。

PA21 的主题和内容对应于 ISO/IEC 15288 资源管理过程的一些活动。

D.12.2 BP.21.01——确定培训需要

使用项目的需要、组织战略规划以及员工的现有技能做指导，识别整个组织对技能和知识的改进需要。

D.12.2.1 描述

这个基本实践确定组织内对技能和知识改进的需要。根据现行计划、组织的战略规划以及员工现有技能综合情况来确定这些需要。项目提供情况有助于识别现有的不足，它们可以通过培训或其他方式获取技能和知识来补救。组织战略规划有助于识别新生技术，而现有的技能水平用于评估当前能力。

在识别对技能和知识的需要时，还应确定相应的培训，以便达到提高培训的效果和通过组织内公共工具的使用来加强交流的目的。应在组织系统工程过程中和针对具体项目裁剪过程时提供培训。

D.12.2.2 工作产品示例

- 组织的培训需要；
- 项目技能或知识。

D.12.2.3 注释

D.12.3 BP.21.02——选择知识或技能获取模式

组织应识别由评估发现确定的和通过缺陷预防过程识别的其他培训需要。应根据文档化的规程制定和修订组织的培训计划。每个项目应制定和维护规定自己的培训需要的培训计划。评价和选择有关

培训或其他来源的、获取知识或技能的合适模式。

D.12.3.1 描述

这个实践的目的是确保选择最有效的方法，使项目及时得到所需要的技能和知识。分析项目和组织需要，利用“PA09 提供安全输入”的方法在各种候选方案（例如咨询师、分包方、从确定的主题专家处获取知识或培训等）中进行选择。

D.12.3.2 工作产品示例

- 所需要的技能和知识的调查结果；
- 指出获取技能或知识的最有效方式的趋势研究结果。

D.12.3.3 注释

可以用于确定获取技能或知识的最有效方式的准则（例如）包括：

- 项目实施准备的可用时间；
- 业务目标；
- 内部专家的可用性；
- 培训的可用性。

D.12.4 BP.21.03——确保技能和知识的可用性

确保适合的技能和知识可供系统工程工作使用。

D.12.4.1 描述

这个实践涉及一定要可供项目系统工程工作使用的所有技能和知识的获取。通过精心评估和准备，可以制定和执行相应的计划，使所要求的各种知识和技能可供使用。这些知识和技能包括：功能性工程技能，应用问题领域的知识，人际交往技能，多学科技能以及过程相关技能。在识别所需的知识和技能，可以使用对知识或技能获取方式的评价结果来选择最有效的方式。

D.12.4.2 工作产品示例

- 按技能类别划分的、所需的技能类型的评估；
- 项目知识获取计划；
- 培训计划；
- 确定的和可用的主题专家列表。

D.12.4.3 注释

使用针对工作分解结构的每个元素的知识类型（例如功能工程、问题领域等）核查表，可以处理各种知识和技能类型的合适覆盖问题。

例如，为了确保相应的应用问题领域知识（例如，卫星天气数据处理）的可用性，可能要拟订一个计划，结合需求解释或系统设计访问所识别的主题专家。当组织确定没有所要求的专门技术可用时（在一条新的业务线里推动第一项计划时），这种方法也适用。

D.12.5 BP.21.04——准备培训材料

根据已识别的培训需要准备培训材料。

D.12.5.1 描述

针对正在开发的和适合本组织人员的每类培训编制培训材料，或者针对正在购买的每类培训索取培训材料。

D.12.5.2 工作产品示例

- 课程描述和要求；
- 培训材料。

D.12.5.3 注释

培训课程描述应包括：

- 预期听众；
- 参与培训前准备；
- 培训目标；
- 培训时间；
- 课程计划；
- 判断学员圆满结业的准则。

准备：

- 定期评价培训效果和特殊考虑事项的规程，例如培训课程的试点和范围测试；
- 进修培训的需求，和跟随培训的机会；
- 对于将作为过程组成部分的特定实践进行培训的材料（例如，方法技术）；
- 过程培训材料；
- 过程技能培训材料，例如统计技术、统计过程控制、质量工具和技术，过程描述建模、过程定义和过程测量；
- 与部分或者全部后续的教育专家、主题专家和试点计划中安排的学员一起评审培训材料。

D.12.6 BP.21.05——培训人员

培训人员，使其掌握必要的技能和知识，以履行分配给他们的岗位职责。

D.12.6.1 描述

按照培训计划和开发的材料培训人员。

D.12.6.2 工作产品示例

- 经过培训的人员。

D.12.6.3 注释

及时提供培训（适时培训），以确保保持最佳状态和可能的最高技能水平。

- 应存在一个在接受培训之前确定雇员的技能水平的规程，以便确定培训是否合适（例如，对于雇员来说，免于培训或者相似情形是否应得到管理）；
- 存在提供鼓励和激励学院参与培训的某种规程；
- 在线培训/定制的教学模块适应不同的教学风格和文化背景，除此之外还传递较小的知识单元。

D.12.7 BP.21.06——评估培训效果

评估培训效果，以满足已识别的培训需要。

D.12.7.1 描述

培训的一个关键内容是确定它的效果。需要结合培训计划的制定和培训材料的编写处理评价培训的方法。在某些情况下，这些方法有必要作为培训材料的一个完整组成部分。应及时报告评价结果，以便对培训做出调整。

D.12.7.2 工作产品示例

- 培训效果分析；
- 培训调整。

D.12.7.3 注释

应具备相应的规程，用于确定雇员接受培训后的技能水平，以判断培训成功与否。这种规程可以通过正规测试、工作中技能实证，或者嵌入在课件中的评价机制来实现。

D.12.8 BP.21.07——维护培训记录

维护培训和测验的记录。

D.12.8.1 描述

维护记录，以跟踪每个雇员接受的培训以及雇员的技能和能力。

D.12.8.2 工作产品示例

- 培训和测验记录。

D.12.8.3 注释

保存所有成功完成每个培训课程或其他批准的培训活动的学员的记录。同时，在委派职员和管理人员的过程中，成功完成培训的记录可用作考虑因素。

D.12.9 BP.21.08——维护培训材料

维护可访问库中的培训材料。

D.12.9.1 描述

课件材料在一个库中维护，以便雇员将来访问，并且维护课程材料中变更的可追踪性。

D.12.9.2 工作产品示例

- 基线培训新材料；
- 培训材料修订本。

D.12.9.3 注释

维护培训材料库，并使之可供所有雇员使用。（例如，组织的资料室可能提供使用图书、笔记本、录像带等；软拷贝培训材料可以使用公共文件服务器维护）把经验教训纳入培训材料和培训计划。随着过

程的变更和改进不断更新过程培训材料。

D.13 PA22——与供方协调

D.13.1 过程域

D.13.1.1 安全注意事项

当供方执行 PA10“确定安全需要”时，被评估组织充当客户的角色。

D.13.1.2 概要描述

“与供方协调”的目的是为了提出组织的需要，以有效管理由其他组织执行的产品工作部分。作为该过程域的一部分的决策，应与已定义过程一致。使用通用术语“供方”来识别开发、制造、测试、支持系统的某组成部分等的组织。供方可以是销售商、分包方、合作伙伴等，随业务组织的授权而定。

除了对进度、过程和工作产品交付的协调外，各个受影响的组织还应共享某种工作关系。这类关系可能的形式有：集成开发商/供方产品团队，主承包方/分包方，或者销售商等等。组织和供方之间的成功关系取决于组织的能力以及对关系和期望的共识。

D.13.1.3 目标

选择和使用有效的供方。

D.13.1.4 基本实践列表

下面包括的基本实践是优秀系统工程的基本元素；

BP.22.01 识别应由其他/外部组织提供的、必要的系统构件或服务。

BP.22.02 识别已经显示出在已识别的领域具有专业知识的供方。

BP.22.03 按已定义的过程选择供方。

BP.22.04 向供方提出关于将要交付的系统构件或服务的需要、期望和组织所掌握的有效性测量项。

BP.22.06 与供方保持及时的双向沟通。

D.13.1.5 过程域注释

当供方交付的产品不满足组织需要时，组织可做如下选择：换用其他供方，降低自己的标准和接受已交付的产品，或者帮助供方或销售商满足本组织的需要。

当供方执行“确定安全需要”过程域(PA10)时，被评估组织充当客户的角色。组织应帮助供方充分理解客户需要和期望。如果供方确实没有实施该过程域的过程，那么组织应知道供方得到必要信息。

在跟踪此过程域的性能时，在可能表明是否满足保证参数的不同基本实践之间查看趋势。参见 PA06。

PA22 的主题和内容分布在 ISO/IEC 15288 的三个过程中，特别是 6.1.1“采购过程”，6.1.2“供应过程”的一些活动以及 6.3.1“项目规划过程”的一些活动。

D.13.2 BP.22.01——识别系统构件或服务

识别应由其他/外部组织提供的必要的系统构件或服务。

D.13.2.1 描述

一个组织确实很少制作系统的全部构件。采用“制作与购买”分析和决策方法来确定将采购哪些

项。通常本组织缺乏专业知识和不太感兴趣的系统需求，由外部组织满足的系统需要。

D.13.2.2 工作产品示例

- 制作与购买间的权衡；
- 系统构件列表；
- 由外部组织处理的系统构件子集；
- 潜在供方列表；
- 所需工作完成的开始准则。

D.13.2.3 注释

实际做法（例如）包括：

- 执行趋势研究；
- 检查本组织，确定是否缺乏为处理系统需求所需的专业知识。

D.13.3 BP.22.02——识别胜任的供方或销售商

识别已经显示出在已识别的领域具有专业知识的供方。

D.13.3.1 描述

供方的能力应是组织的能力补充并且与组织的能力兼容。可能关注的问题包括胜任的开发过程、制造过程、验证责任、按时交付、生存周期支持过程，以及有效的远距离沟通能力（电视电话会议、电子文件传送、电子邮件等）。

D.13.3.2 工作产品示例

- 供方列表；
- 每个供方的优缺点；
- 与供方远距离工作的潜在方式。

D.13.3.3 注释

实际做法（例如）包括：

- 阅读商业期刊；
- 使用可用的图书馆服务；
- 使用组织的知识库（可能是在线系统）。

D.13.4 BP.22.03——选择供方或销售商

按已定义的过程选择供方。

D.13.4.1 描述

按照合乎逻辑的、公正的方法选择供方，以满足产品目标。确定供方的那些作为本组织能力的最佳补充的特性，并且识别有资格的候选对象。

D.13.4.2 工作产品示例

- 组织的脆弱点可以由供方减弱；
- 所希望的与供方建立的工作关系的特点；

- 供方需求；
- 将提供给供方的客户需求；
- 所选择的供方；
- 识别选择供方的理由。

D.13.4.3 注释

供方选择中的一个重要考量是期望的工作关系。这种关系的表现形式可能从高度集成的产品队伍到传统的“满足需求”关系。选择准则可能不同，取决于所期望的关系。

D.13.5 BP.22.04——提出期望

向供方提出关于将要交付的系统构件或服务的需要、期望和组织所掌握的有效性测量项。

D.13.5.1 描述

主承包组织应清楚地识别和排列其需要和期望，同时，明确指出对供方的任何限制条件。组织与供方密切合作，就产品需求、责任以及将应用于思想计划目标的过程达成共识。

D.13.5.2 工作产品示例

- 需要陈述；
- 技术性能参数；
- 验证规范。

D.13.5.3 注释

向供方或销售商提供需要、期望和效果测量项的技术和论坛（例如）包括：

- 趋势研究；
- 正式合同；
- 过程中评审；
- 联合会议；
- 支付里程碑。

D.13.6 BP.22.05——保持沟通

与供方保持及时的双向沟通。

D.13.6.1 描述

组织和供方对所期望的和所需要的沟通达成共识。所要确立的沟通特征包括公开考虑的、不受任何限制的信息的类型、受限制的信息的类型（例如策略或合同关系）、所期望的信息请求和响应的时间安排、沟通用的工具和方法、安全性、隐私以及分布期望。对“面对面”沟通和“远距离”沟通的需要，以及关于归档沟通情况的需要机制等也要考虑。

D.13.6.2 工作产品示例

- 合同要求的沟通；
- 沟通计划；
- 沟通分布列表。

D.13.6.3 注释

组织和供方之间存在一个有效的沟通环境是必要的。电子邮件和语音邮件工具对于不要求双向沟通的简单沟通而言是很有效的。

对于影响进度成本或范围的沟通应仅限于得到授权的单位。

附 录 E
（资料性附录）
能力成熟度模型概念

E.1 概述

本附录的目的是综述 SSE-CMM® 中使用的概念和结构。其中给出关于指导 SSE-CMM® 设计的需求信息、体系结构描述，还有一条介绍一些有助于理解该模型的关键概念和术语。这一章充当第 5 章中模型详细讨论的前导。

SSE-CMM® 提供了一种团体范围（政府和行业）标准衡量尺度，用于建立安全工程并且引导它成为一门成熟的可度量的学科。对于那些将遭遇硬件、软件、系统、企业安全问题的工程工作，模型及其评价方法确保安全性成为整个工程工作的有机组成部分。该模型定义了安全工程过程的特征。这种安全工程过程在所有工程工作类型中明确加以定义、管理、测量和控制，并且在其中发挥作用。

E.2 过程改进

过程是针对给定目的执行的一系列步骤。它是任务、支持工具以及介入生产和某些最终结果（例如产品、系统、或服务）发展演变的人员构成系统。认识到过程是产品成本、进度和质量（涉及人和技术）的决定因素之一，因此各种工程团体都已经开始把他们的关注焦点投放到改进他们的生产产品和服务的过程上。

过程能力指的是组织的潜力。它是组织可望达到的一个范围。过程性能是对某特定项目实际执行结果的测量，它可能在上述范围内也可能在这个范围以外。

“在某制造厂里，某经理观察某条生产线的问题。他发现人们在生产线上制造了大量有缺陷的制品，他的第一倾向也许是以这些工人太辛苦、太快作为辩解理由。但是实际上，他收集了数据并绘制出缺陷制品所占百分比。所绘制的图形表明，缺陷制品的数量和每天的变化率是可以预计的。”[戴明 86]

这个例子说明一个处于统计过程控制中的系统。也就是说，它的能力限定在特定范围内，并且能力变化的极限值是可以预计的。存在一个会产生缺陷制品的、稳定的系统。这个例子说明，把系统置于统计过程控制下并不意味着没有缺陷制品。

然而，它表明以大致相同的方法重复工作将生产出大致相同的结果。重要之点在于，为了找到可以有效实施改进之处，需要建立过程的统计控制。许多组织已经使用 CMM® 作为指南来协助他们实现统计过程控制。

另一概念，过程成熟度，指出某特定过程明确定义、管理、测量、控制和有效的程度。过程成熟度意味着能力成长的潜力，并且指出组织过程的丰富程度以及在整个组织应用的一致程度。

戴明（Deming）与日本人合作把统计过程控制的概念应用到工业活动中。在《软件过程特征化：成熟框架》中，瓦茨·汉弗莱（Watts Humphrey）描述了一个软件过程成熟度框架。该框架就软件开发过程解释了戴明（Deming）的成就。

汉弗莱（Humphrey）声言：“尽管（应用领域之间）存在重要区别，但是这些概念就像它们适用于汽车、照相机、手表和钢铁领域一样，也适用于软件领域。处于统计控制下的软件开发过程在预定的成本、进度和质量限制范围内将得到所希望的结果。”通过把统计过程控制下的软件开发过程，汉弗莱（Humphrey）描述了几个过程成熟度等级。这些等级引导组织以较小的递增步骤不断改进他们的过程能力，他描述的这些成熟度等级成为软件工程研究所的软件 CMM® 的基础。

CMM®是工程组织从一个缺乏组织性的、效率低下的特别状态到高度结构化的高效率状态的发展框架。组织把这种模型作为一种手段，把组织的实践行为带到统计过程控制下，从而不断提高组织的过程能力。作为对软件应用CMM®的结果，许多软件组织已经显示了在成本、生产率、进度和质量方面的满意结果。SSE-CMM®按预期开发。统计过程控制概念在安全工程中的应用将促进安全系统和可信产品在预期的成本、进度和质量限制范围内开发。

E.3 预期结果

E.3.1 概述

基于软件和其他行业的类似情况，可以预计过程和产品改进的一些结果。这些在下面讨论。

E.3.2 改进可预计性

作为组织成熟度第一项预期改进是可预计性。随着能力增长，各个项目的目标结果和实际结果之间的差别将相应降低。例如，处于等级1的组织往往在很大的范围内错过他们最初规定的交付日期，而那些处于比较高的成熟度等级的组织应能够预计项目的成本开销和进度，并且预计准确度将随着成熟度等级的增高而增高。

E.3.3 改进控制

作为组织成熟度第二项预期改进是控制。随着过程能力增长，可以把渐次增加的结果用于建立经过修改的更准确目标。可以根据该过程和其他项目过程结果的经验评价各种纠正措施，以便选择应用最佳的控制措施。因此，能力成熟度较高的组织，在可接受的范围内，它对性能的控制也更有效。

E.3.4 改进过程有效性

作为组织成熟度第三项预期改进是过程有效性。目标结果将随着组织成熟程度的增长而改进。随着组织趋于成熟，它的成本将降低，开发时间将缩短，生产率和质量将提高。在处于等级1的组织中，可能由于纠正错误而应执行的返工量很大而导致开发时间很长。相反，具有较高成熟程度的组织可以通过提高过程效率和减少返工，缩短全部开发时间。

E.4 常见误解

E.4.1 概述

下面的陈述反映了一些有碍于CMM®使用的共同之点。本节旨在澄清这些常见误解。

E.4.2 CMM®定义工程过程

一个常见错误概念是："CMM®定义具体过程"。实际上，组织定义他们自己的过程，然后改进这些过程，而CMM®是开展这些活动的指南。这个指南的适用性与所执行的具体过程无关。CMM®描述的是，为了有助于定义、管理、监视和改进组织的过程应执行"什么"活动，而不是描述应"如何"具体执行这些特定的活动。

针对特定学科的CMM®，例如SSE-CMM®，要求应实现一定的基础工程活动作为相应学科的工程过程的一部分，但是它们没有规定这些工程活动应"如何"具体执行。

CMM®所依据的基本原理是使工程组织能够开发出对它们最有效的工程过程并且不断改进这些过程。为此需要以下基本能力：定义工程过程、把它们形成文档的实施管理，并且使整个组织的过程标

准化。这种原理并不聚焦于任何特定的开发生存周期、组织结构、工程技术。

E.4.3 CMM®是手册或培训指南

CMM®旨在指导组织改善它们执行特定过程(例如安全工程)的能力。CMM®不是那些帮助个人改善其工程技能的手册或培训指南。目标是使一个组织接受CMM®中描述的原理和使用CMM®中描述的技术作为指导和改进工程过程的指南。

E.4.4 SSE-CMM®是产品评价的替代物

对照CMM®做出的组织等级评定不可能替代产品评价或系统认证。不过,(实施评价或认证的)第三方在进行分析时可以适当关注那些已经通过CMM®评价指出其薄弱之处的领域。把过程置于统计过程控制下并不意味着不存在缺陷。实际上,这样做是提高对缺陷的可预计性,因此一些分析形式的抽样仍然是必要的。

任何可能从使用SSM-CMM®中得到的收益都基于对SEI的软件CMM®使用经验的解释,为了声明SSE-CMM®对评价和认证有贡献,安全工程团体需要就安全工程要什么成熟程度达成一致。如同在SEI软件CMM®所做的那样,这类声明需要随着SSE-CMM®在本团体中的持续使用不断加以研究。

E.4.5 要求文档编制太多

阅读CMM®,很容易被其中隐含的、过量的过程和计划淹没。CMM®包含许多关于使过程和规程文档化并且确保这些过程和程序文档得到执行的要求。尽管CMM®中调用大量过程、计划和其他类型的文档,但是并不指定要编制的文档和数量。也许一份安全计划就满足许多过程域的要求。CMM®只指出所要形成的信息类型。

E.5 关键概念

E.5.1 引言

本附录介绍的术语和概念在SSE-CMM®中有特定含义。本条详细说明的一些概念对于恰当理解、解释和使用SSE-CMM®很关键。有些概念是专门针对这类模型的,如"通用实践"和"基本实践",在与之有关的各个模型描述的章条中定义和讨论。本条讨论的概念是:

- 组织;
- 项目;
- 系统;
- 工作产品;
- 客户;
- 过程;
- 过程域;
- 角色独立性;
- 过程能力;
- 制定化;
- 过程管理;
- 能力成熟度模型。

E.5.2 组织和项目

SSE-CMM®中使用的与组织结构里的用法不同的两个术语是组织(organization)和项目(project)。

业务实体里还有其他结构，例如团队(team)，但是还没有在所有业务背景里普遍接受的术语。选择这两个术语是因为SSE-CMM®的大部分预期读者普遍使用/理解它们。

E.5.2.1 组织

就SSE-CMM®而言，组织定义为公司里的一个单位、整个公司或其他实体(例如，政府机构或服务部门)，它负责监管多个项目。一个组织内的所有项目一般都共享顶层报告结构上的公共策略。一个组织的各个项目和支持性基础设施可能共处一地也可能分散在各处。

E.5.2.2 项目

项目是工作和其他资源的汇聚点，它关注的是开发和(或)维护某个特定产品或提供某项服务。产品可能包括硬件、软件和其他构件。一般，一个项目有它自己的资金投入、成本核算和交付进度。项目可能构成它自己组织实体，也可能以团队、特别任务组或其他实体形式组建，由组织用于产生产品或提供服务。

SSE-CMM®范畴内的过程域划分为工程、项目和组织三类。组织和项目类一般按拥有关系区分。SSE-CMM®对项目和组织类的区分是：把项目定义为关注特定产品的，对于组织类，则强调包含一个或多个项目。

E.5.3 系统

在SSE-CMM®中，系统指的是：

- 人员、产品、服务和为满足需要或目标提供能力的过程等的综合体[MIL-STD-499B]；
- 构成某个单一复杂整体的若干事物或组成部分的组合体(例如，组织起来完成某个或某组特定功能的构件集合)；
- 从功能角度考虑的各个元素的互动组合。
- 一个系统可能是某个产品，它可能是纯粹的硬件、硬件/软件组合、纯粹的软件，也可能是一项服务。在整个模型中，术语“系统”用于指出将要交付给客户或用户的产品的总和。如果把某产品看成系统，是认为需要按照某种规范的、系统化的方法来处理产品的所有元素及其接口，以便实现正在开发产品的业务实体的全部成本、进度和性能(包括安全)目标。

E.5.4 工作产品

工作产品是执行任何过程生成的所有文档、报告、文卷、数据等，SSE-CMM®没有针对每个过程域一一列出各个工作产品，而是给出特定基本实践的“工作产品示例”，用于进一步说明基本管理的范围。所列出的案例只是说明性的，用于反映组织和产品背景的范围。他们不是“强制性的”工作产品。

E.5.5 客户

客户是接受所开发的产品或所提交的服务的个人或实体，是使用该产品或服务的个人或实体。

在SSE-CMM®背景中，客户既可以是协议的也可以是非协议的。协议客户是指按其提出的规范就某个或某组特定产品的生产与另一个实体签订合同的个人或实体。非协议客户，或市场驱动的客户，是对某产品有现实需要或意识到的需要的众多个人或实体的一个。客户可代理，例如营销部门或产品集中部门，也可以代表客户。

在大部分情况下，SSE-CMM®按照语法习惯以单数形式使用术语customer(客户)。然而，SSE-CMM®并不排斥多个客户的情况。

注意，在SSE-CMM®背景下，使用产品或服务的个人或实体也在客户概念范围内。这对于经过协商的客户而言是相关的，因为向其交付产品的实体并不总是实际使用该产品或服务的实体或个人。考

虑到安全工程功能的责任，SSE-CMM® 中术语“客户”的概念和用途涉及客户的整体概念，即包括用户。

E.5.6 过程

过程是为实现给定目的而执行的一系列活动。这些活动可以反复地、循序地和(或)并行地执行。一些活动可以将输入工作产品转换为其他活动需要的输出工作产品。所执行的活动的可能序列受到输入工作产品和资源的可用性的限制，并且由管理者控制。妥善定义的过程包括活动、每个活动的输入和输出制品以及控制活动执行的机制。

SSE-CMM® 中提及的过程类型包括“已定义”的和“已执行”的。已定义过程是组织正式描述的或者由组织的安全工程师描述提供组织使用的。例如，这种描述可以包含在某个文档里或者放置在过程资产数据库里。已定义过程是支持组织的安全工程师展开工作的过程。已执行过程是安全工程师实际开展工作的过程。

E.5.7 过程域

过程域(PA)是一组已定义的、相关的安全工程过程特征，这些特征在一起实施时，可以达到规定的目的。

过程域由基本实践组成。这些基本实践是强制性特征，一个组织只有使它已实施的安全工程过程里具备这些基本管理，它才可以声明满足了某给定的过程与要求。这些概念在定义模型体系结构的章条里进一步展开。

E.5.8 角色独立性

SSE-CMM® 的过程域是按组实践的，并且合在一起实践以实现某个共同的目的。但是，这种分组并不意味着过程域的所有基本实践应由一个人或一个角色执行。所有基本实践都以动-宾格式(即不带具体主体)书写，从而使某个实践“属于”某特定角色的意识被尽量弱化。这是模型采用的一种造句方法，它支持模型在广泛的组织背景范围里使用。

E.5.9 过程能力

过程能力定义为可以量化的预期结果的范围，通过遵循该过程可能得到这个范围里的结果。SSE-CMM® 评价方法(系统安全工程能力成熟度模型评价方法)的基础是系统过程控制概念，按照这种概念定义过程能力的使用。系统安全工程能力成熟度模型评价方法可以用来确定项目或组织内每个过程的能力等级。SSE-CMM® 的能力维反映这些概念并且为改进在 SSE-CMM® 的域维中提到的安全工程实践行为的过程能力提供指南。

组织的过程能力有助于预测项目满足目标的能力。在低能力的组织里，项目在实现成本、进度、功能和质量目标方面的变动范围很大。

E.5.10 制度化

制度化是构筑建立各种方法、实践和规程的基础设施和社团文化的过程，即使是那些当初规定这些方法、实践和程序的人离开了也没有影响。SSE-CMM® 的过程能力方面通过实践支持机构化，并倾向于定量管理和持续改进。因此，SSE-CMM® 断言：组织需要明确支持过程定义、管理和改进。对于一个显示出可靠的安全工程特征的过程，制度化将为从该过程取得的最大效益开辟通道。

E.5.11 过程管理

过程管理是一种活动和基础设施，它们用于预测、评价和控制过程的性能。过程管理就意味着要定义某个过程(因为未定义的过程是不能用于预测和控制的)。过程管理的焦点意味着在策划、执行、评

价、监视和采取纠正措施等活动中，项目或组织既要考虑产品相关的因素也要考虑过程相关的因素。

E.5.12 能力成熟度模型

能力成熟度模型(CMM®)，例如 SSE-CMM®，描述若干阶段，过程经过这些阶段予以定义、管理和改进。这种模型提供一种通过确定特定过程的当前能力和识别特定域里最关键的质量和过程改进问题来选择过程改进策略的指南。CMM®可以以参考模型的形式用于开发和改进已定义的成熟过程的指南。

CMM®也可以用来评价那些实施所引用的实践的已定义过程的现状和制度化情况。能力成熟度模型覆盖了用于执行规定领域(例如安全工程)任务的各个过程。CMM®还可以覆盖用于确保有效开发和使用人力资源以及把适当技术引入产品和生产工具的过程。后者还没有形成关于安全工程应用的详细说明。

附 录 F
（资料性附录）
信息安全服务与安全工程过程域对应表

信息安全服务与安全工程过程域对应表见表 F.1。

表 F.1 信息安全服务与安全工程过程域对应表

过程域	专业咨询服务	建设实施服务	运行维护服务
PA01——管理安全控制	管理体系咨询服务		
PA02——评估影响	评估业务影响服务		评估业务影响服务
PA03——评估安全风险	风险评估服务		风险评估服务
PA04——评估威胁	受攻击面分析服务； 威胁建模服务	受攻击面分析服务； 威胁建模服务	威胁情报服务； 识别安全态势服务
PA05——评估脆弱性	评估系统安全性服务	分析系统可行性服务	评估系统安全性服务
PA06——建立保障论据	建立、分析咨询服务论据	建立、分析安全集成、安全加固服务保证论据	建立、分析安全运维服务保证证据
PA07——协调安全	咨询服务组内、组外间协调	安全实施协调	安全运维协调
PA08——监视安全态势	安全态势监控咨询服务		安全巡检服务； 安全态势监控服务； 网站安全监控服务
PA09——提供安全输入	安全集成咨询服务	实施安全集成服务	
PA010——确定安全需要	安全设计服务； 等级保护差距分析服务	安全集成实施调研	
PA11——验证和确认安全	系统测评服务	安全集成、加固服务证实系统安全性	检验系统安全性服务

附 录 G
（资料性附录）
GB/T 20261—XXXX 与 GB/T 20261—2006 主要变化对比表

GB/T 20261—XXXX 与 GB/T 20261—2006 主要变化对比见表 G.1。

表 G.1 GB/T 20261—XXXX 与 GB/T 20261—2006 对比主要变化

本标准章名	变化内容
标题	修改为：信息安全技术 系统安全工程 能力成熟度模型
1 范围	按照 GB/T 1.1—2009 要求对范围语言进行规范，对标准段落进行调整，将第三段调整为第二段，且删除原第三段开头“尽管”
	增加一个列项：在“本标准适用于”增加列项“系统安全工程的需求方、提供方和评估方”
	因 ISO/IEC 15504 已经作废，相关内容由 ISO/IEC 33001、ISO/IEC 33020 等系列标准替代，故把“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® 则偏向于关注安全。”修改为“由于均关注过程改进和能力成熟度评估，本标准与 ISO/IEC 33001、ISO/IEC 33020 等系列标准相关。相对而言，ISO/IEC 33001、ISO/IEC 33020 等系列标准偏向于关注软件过程，而 SSE-CMM® 则偏向于关注安全。”，并入 5.2.5
2 规范性引用文件	ISO/IEC 33020 替代了 ISO/IEC 15504-1、ISO/IEC 15504-2、ISO/IEC 15504-4
	增加了 GB/T 30271—2013、GB/T 29246—2017、ISO/IEC 33001、ISO/IEC 33020
	修改了 ISO/IEC 15288、GB/T 18336.1 的引用版本为最新版本
	从规范性引用文件中删除 GB/T 11457、GB/T 9378.2、GB/T 2000.1、GB/T 19715、ISO/IEC 15504-1、ISO/IEC 15504-2、ISO/IEC 15504-4
3 术语和定义	增加了术语：基本实践、能力、信息安全事态、信息安全事件、过程域
	修改了术语定义：保障、工程组、工作产品
	“残留风险”修改为“残余风险”，对“风险管理”进行重新定义
	将引用已废止标准 GB/T 19715.1—2005 的术语和定义修改为 GB/T 25069—2010、GB/T 18336.1—2015、GB/T 29246—2017 相关术语定义
4 系统安全工程概述	原章标题“4 背景”修改为“系统安全工程概述”
	删除了 GB/T 20261—2006 的 4.3
	将原 6.1 的内容移至第 4 章，将原 6.1.3～6.1.6 改为现在的 4.3～4.6
	将原 4 中的第 1、2 自然段和 4.1 合并为现在的 4.1（条标题名称改为：安全工程的开发背景）
	原 4.2 与原 6.1.2 内容修改合并为现在的 4.2
	删除了原 6.1.4（安全工程和其他学科）和 6.1.5（安全工程专业）中一些国内不存在的学科名称

表 G.1（续）

本标准章名	变化内容
5 模型体系结构	删除了原第 5 章
	修改了原第“6”章为第“5”章
	原第 6 章中内容“SSE-CMM® 是若干广为人知的安全工程惯例的汇编。为了便于理解这个模型，要求一些安全工程背景知识。这部分提供安全工程的高层次描述，然后说明模型的体系结构如何反映这种基本认识”修改为“ SSE-CMM® 是安全工程最佳实践的汇编。本章提供安全工程的高层次描述，然后说明模型的体系结构如何反映这种基本认识。”，并入5.1
	原 6.1.1 与 6.1.2 内容合并，并入 5.1
	将原 6.2.1 第 2 段中内容“风险管理是评估和量化风险并且为组织确定合理风险级别的过程。”修改为“风险管理是所有需要协调去指引和控制一个组织风险管理工作的活动，它包括建立组织可接受的风险水平，并相应地识别、分析、评估和处置风险。”，并入 5.1.1
	将原 6.3.4 第 3 段中“如果一个组织在某个公共特征的实施上是到位的，但是其他公共特征处于较低能力等级，那么这个组织不可能充分得到前者带来的收益。”修改为“如果一个组织在任何给定能力级别上的公共特征的实施上是到位的，但是较低能力级别的公共特征没有实施，那么这个组织不可能充分得到前者带来的收益。”，并入 5.2.4
	原 6.3.5 内容涉及本标准与 ISO/IEC 15504-2 的映射关系，由于 ISO/IEC 15504-2 已经废止，修改为与 ISO/IEC 33020 的映射内容。调整后的条号为 5.2.5
	原 6.3.6 内容涉及与 ISO/IEC 15288 的映射关系，由于 ISO/IEC 15288 已经更新至 2015 版，本标准修改为与 ISO/IEC 15288：2015 的映射内容，调整后条号为 5.3.5
6 安全基本实践	修改了原第“7”章为第“6”章
	原 7.2.1.4 第 2 自然段中“目标是为了寻找威胁、脆弱性和影响的组合，认为该组合可证明行动的合理性是非常危险的。” 修改为“目标是发现威胁、脆弱性和影响的组合，针对该组合判断是否需要采取行动。”，内容调整后并入 6.3.1.4 第 2 自然段
	原 7.2.7.1 中“BP.07.02”修改为“BP.08.02”，内容调整后并入 6.3.7.1
	原 7.3.1.4 中第 4 自然段“PA01”修改为“PA10”，“PA02”修改为“PA09”，内容调整后并入 6.4.1.4
	原 7.3.7.1 中“BP.07.02”修改为“BP.08.02”，内容调整后并入 6.4.7.1
	原 7.4.7.1 中“BP.07.02”修改为“BP.08.02”，内容调整后并入 6.5.7.1
	原 7.6.1.3 中增加“BP.06.03 定义用于监测安全保障目标的测量”，内容调整后并入 6.7.1.3
	增加“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，内容调整后为 6.7.4
	原 7.8.3.3 中“PA05”修改为“PA03”，内容调整后并入为 6.9.3.3
	原 7.8.4.3 中“BP.07.06”修改为“BP.08.06”，内容调整后并入 6.9.4.3
	原 7.9.3.3 中“BP.02.03”修改为“BP.09.03”，“BP.02.05”改为“BP.09.05”，内容调整后并入 6.10.3.3

表 G.1（续）

本标准章名	变化内容
6 安全基本实践	原 7.9.4.3 中“BP.02.02”修改为“BP.09.02”，“BP.02.04”改为“BP.09.04”，“BP.02.05”改为“BP.09.05”，内容调整后并入 6.9.4.3
	原 7.9.5.1 第一段中“BP.02.02”修改为“BP.09.02”，内容调整后并入 6.10.5.1
	原 7.9.5.1 第二段中“BP.02.03”修改为“BP.09.03”，内容调整后并入 6.10.5.1
	原 7.9.5.2 中“BP.02.02”修改为“BP.09.02”，内容调整后并入 6.10.5.2
	原 7.10.1.4 第一段中“PA02”修改为“PA09”，内容调整后并入 6.11.1.4
	原 7.10.5.2 中“BP.02.03”修改为“BP.09.03”，调整后并入 6.11.5.2
	原 7.10.6.3 中“PA02”修改为“PA09”，内容调整后并入 6.11.6.3
	原 7.11.4.1 中“BP.03.02”修改为“BP.11.02”，内容调整后并入 6.12.4.1
	原 7.11.5.1 中“BP.03.02”修改为“BP.11.02”，内容调整后并入 6.12.5.1
附录 C（规范性附录）通用实践	修改了图 C.1 能力等级格式，纠正原标准内容当中的错误信息
	附录 C 为与 GB/T30271—2013 等有关能力成熟度的标准保持一致，将 GB/T 20261—2006 中“能力等级 1——非正式执行”“能力等级 2——策划和跟踪”“能力等级 3——妥善定义”“能力等级 4——定量控制”“能力等级 5——持续改进”，统一修改为“能力等级 1——基本执行”“能力等级 2——计划跟踪”“能力等级 3——充分定义”“能力等级 4——量化控制”“能力等级 5——持续改进”；同时，将全文中所有“惯例”一词改为“实践”，“客户和供方”改为“需求方和提供方”
	原 A.3.2.4.3 中“见 GP 3.1.1，GP 3.1.2，GP 5.2.3 中该过程的描述”，修改为“见 GP 3.1.1，GP 3.1.2，GP 5.1.2，GP 5.2.3 中该过程的描述”，内容调整后并入 C.3.2.4.3
	原 A.3.2.5.3 中“见有关过程改进的实践 5.2.3”，修改为“见有关过程改进的实践 GP 5.1.2，GP 5.2.3”，内容调整后并入 C.3.2.5.3
	原 A.5.3.2.2 中“(GP 3.1.1)和测量过程”，修改为“(GP 3.1.1 和 GP 3.2.3)和测量过程(GP 2.4.1)”，内容调整后并入 C.5.3.2.2
	原 A.6.3.4.2 中内容“基于渐进改进(GP 5.2.2)”，修改为“基于渐进改进(GP 5.1.2)”，内容调整后并入 C.6.3.4.2
	原 A.6.3.4.3 中内容“实践 GP 5.2.2 可能是改进的一个起源”，修改为“实践 GP 5.1.2 可能是改进的一个起源”，内容调整后并入 C.6.3.4.3
附录 D（规范性附录）项目与组织基本实践	原 B.6.1.1 中“PA07”修改为“PA08”，“PA09”修改为“PA07”，内容调整后并入 D.6.1.1
	原 B.7.7.3 中“综合学科”过程域(PA04)，修改为“提供安全输入”过程域(PA09)，内容调整后并入 D.7.7.3
	原 B.9.3.3 中“分析候选解决方案”过程域 5)”修改为“PA09 提供安全输入”，调整后内容并入 D.9.3.3
	原 B.11.1.1 中“PA05 评估运行安全风险”，修改为“PA03 评估安全风险”，调整后内容并入 D.11.1.1

表 G.1（续）

本标准章名	变化内容
附录 D（规范性附录）项目与组织基本实践	原 B.11.4 中“利用‘分析候选解决方案’的方法”，修改为“PA10 确定安全需要”，调整后内容并入 D.11.4
	原 B.11.4.1 中“利用‘分析候选解决方案’的方法”，修改为“PA10 确定安全需要”，调整后内容并入 D.11.4.1
	原 B.12.3.1 中第 2 行内容“利用‘分析候选解决方案’的方法”，修改为“PA10 提供安全输入”，调整后内容并入 D.12.3.1
附录 F（资料性附录）信息安全服务与安全工程过程域对应表	增加，主要描述安全基本实践与信息安全服务内容间的映射，用于提高信息安全服务机构开展相关信息安全服务的便利性
附录 G（资料性附录）GB/T 20261—XXXX 与 GB/T 20261—2006 对比主要变化表	增加，主要为补充说明标准前言内容

参 考 文 献

[1] GB/T 8566—2007 信息技术 软件生存周期过程(ISO/IEC 12207:1995,MOD)

[2] ISO/IEC 33001:2015 Information technology—Process assessment—Concepts and terminology

[3] ISO/IEC TR 33014:2013 Information technology—Process assessment—Guide for process improvement

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 系统安全工程
能力成熟度模型
GB/T 20261—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2020年11月第一版
*
书号:155066·1-66282

GB/T 20261-2020