ICS 35.110
CCS L 70

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T XXXX—202X
［代替 YD/T］

网络空间安全仿真　安全技术效能评估方法

Cybersecurity emulation — Efficiency assessment of security technical

（报批稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国工业和信息化部　发布

前　言

本文件按照GB/T 1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：华中科技大学、鹏城实验室、广州大学网络空间先进技术研究院、北京天融信网络安全技术有限公司、中国电子信息产业集团有限公司第六研究所、哈尔滨工业大学（深圳）、北京奇安信科技有限公司、北京神州绿盟科技有限公司、郑州信大捷安信息技术股份有限公司、中国电信集团有限公司、中国信息通信研究院。

本文件主要起草人：邹德清、贾焰、李树栋、王伟豪、龙翔、韩兰胜、韩伟红、田志宏、殷丽华、吴晓波、陶莎、柳扬、廖清、王帅、燕玮、刘子健、谢玮、孟楠、何婧瑗、李清波、孙海丽、孙润华、刘为华、杨圣峰、田尚君、王龑。

网络空间安全仿真　安全技术效能评估方法

1　范围

本文件规定了安全技术效能评估的技术要求、系统要求以及评估指标。

本文件适用于网络空间安全仿真平台中所涉及的各项安全技术的效能评估。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20984-2022　信息安全技术　信息安全风险评估方法

GB/T 25069-2022　信息安全技术　术语

GB/T 30279-2020　信息安全技术　网络安全漏洞分类分级指南

3　术语和定义

GB/T 20984-2022、GB/T 25069-2022、GB/T 30279-2020界定的以及下列术语和定义适用于本文件。

3.1

效能评估　efficacy assessment

依据某种特定的准则对某一事物或过程的某种能力进行测定和评价。

3.2

安全技术　security technique

网络安全的参与者为实现攻击或防御战术所使用的具体手段。

3.3

战术　tactic

网络安全的参与者为达到攻击或防御目的所使用的所有策略。

4　效能评估概述

安全技术效能评估是网络安全仿真平台分析能力的重要组成部分，旨在发现攻防中存在的不足和短板，帮助后续改进提高。

安全技术效能反映了安全技术在网络攻防过程中的攻击或防御能力，这些能力是通过安全技术的期望效用及其获得成功的概率来体现的，也应通过这两个方面来进行评估。其中，安全技术的期望效用由其收益及成本共同决定，获得成功的概率则主要与使用情况相关。为了量化安全技术的收益、成本及成功概率，应从安全技术自身及其使用情况两个角度出发来对网络攻防情况进行评估。

对安全技术自身的评估是一种静态效能评估，主要包括安全技术可能带来的收益及其研发或维护成本。安全技术的原理、功能设计及实现方法等反映了开发者或使用者对其能力的预期，决定了该技术的收益及成本，针对这些方面的评估是必要的。所有的安全技术效能评估均应至少包含安全技术的静态效能评估。

对安全技术使用情况的评估则是一种动态效能评估，主要包括安全技术在攻防过程中获得成功的概率及其使用时的开销。攻防参与者对安全技术的选择是否合理、配置是否正确、使用是否充分等都会影响攻防的最终结果，对这些方面的评估体现了基于特定攻防技术的不同攻防战术的效能。条件允许时

应尽量开展安全技术的动态效能评估，并将评估结果与静态效能评估结果一起，共同构成安全技术效能评估的结果。在条件不具备等特殊情况下，也可以不进行动态效能评估，仅以静态效能评估的结果作为安全技术效能评估的最终结果。

安全技术效能评估的基本原理如图1所示。

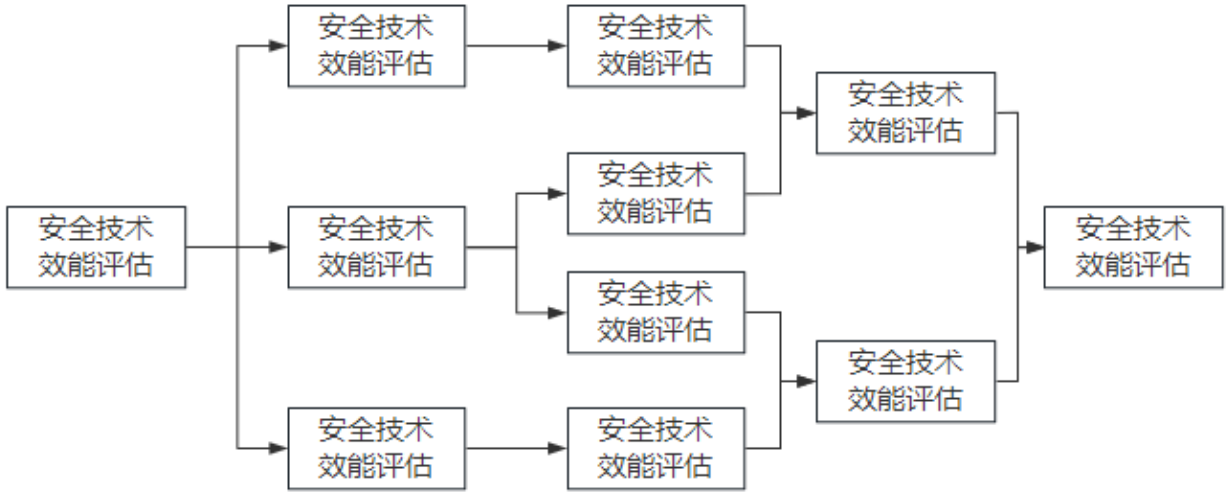

图 1　安全技术效能评估原理

5　指标体系

根据安全技术效能评估的基本原理，安全技术的静态及动态效能应分别由若干个特性来进行量化，每种特性又应进一步细分为若干个子特性，这些特性及子特性应体现出安全技术的普遍要求，无论这些技术是用于攻击的还是防御的。子特性应根据不同安全技术的特点进一步细分为若干个评估指标，评估指标不具有通用性，不同类型的安全技术（如攻击技术与防御技术）或功能不同的同类型安全技术（如防火墙与数据恢复），其评估指标一般不能通用，功能相近的同类型安全技术可以有部分评估指标相同或重叠。特性、子特性及评估指标之间的关系如图2所示。

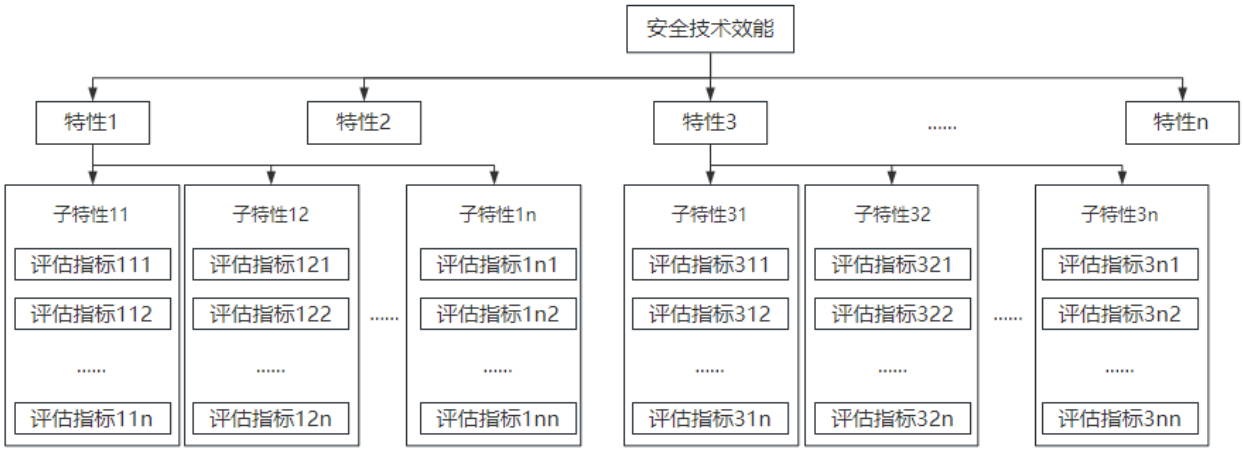

图 2　安全技术效能特性、子特性及评估指标关系图

根据安全技术效能评估的实际情况，应从功能性、可用性、适应性、合理性、维护开销、运行开销共6个方面的特性入手进行效能评估，并进一步细分子特性。具体的特性及其子特性见表1。

表1　安全技术效能特性及子特性

分类	特性	子特性	含义
静态效能	功能性	恰当性	安全技术的功能设计是否恰当、合理。
		正确性	安全技术的预期功能是否被正确地实现。
		完备性	安全技术的功能实现是否全面、完善。
		操作性	安全技术是否便于操作，易于使用。
	可用性	成熟性	安全技术的理论及实现基础是否成熟、有效。
		稳定性	安全技术的收益或效果是否稳定、一致。
		可靠性	安全技术的收益或效果是否可靠、可信。
		兼容性	安全技术在各类软硬件环境下正常使用。
		可配置性	安全技术能否根据使用环境进行自定义配置。
		自我保护性	安全技术能否进行有效的自我保护，尤其是在对抗环境下。
	维护开销	更新开销	安全技术是否需要更新，是否便于更新。
		技术支持开销	安全技术是否需要技术支持或文档支持，相应的工作量如何。
动态效能	适应性	匹配性	攻防过程中选择该安全技术是否考虑了攻防场景，技术与场景是否匹配。
		针对性	攻防过程中选择该安全技术是否考虑了对抗情况，有无针对性。
		灵活性	攻防过程中选择该安全技术是否考虑了偶然因素，有无灵活性。
	合理性	必要性	攻防过程中对安全技术的使用是否必要，有没有用力过猛的情况。
		充分性	攻防过程中对安全技术的使用是否充分，有没有发挥出全部作用。
		规范性	攻防过程中对安全技术的使用是否规范，有没有造成不良的后果。
	运行开销	时间开销	攻防过程中使用该安全技术所需的时间或造成的时延。
		空间开销	攻防过程中使用该安全技术所需的内存或磁盘存储空间。
		计算资源开销	攻防过程中使用该安全技术所需的 CPU、GPU、FPGA 及网络带宽等资源。

一个完整的效能评估指标体系应完整包括特性、子特性和评估指标。根据安全技术类型及评估目标的不同，效能评估所侧重的特性、子特性和评估指标也有所不同，评估时应根据具体情况对上述特性、子特性进行适当的取舍或补充，并在此基础上确定具体的评估指标。效能评估指标根据其重要性及必要性可以分为3类：

1）Ⅰ类：基本评估指标，反映安全技术基本效能的评估指标，是必须进行评估的指标，无特殊情况皆应采用，例如功能性中的正确性指标；

2）Ⅱ类：可选评估指标，反映安全技术可选效能的评估指标，这些评估指标可能仅在某些情况下才需要评估，或评估它们所需要的数据仅在某些情况下才可以获得，例如运行开销中的计算资源开销评估指标“FPGA资源开销”，当且仅当评估场景中具有FPGA资源时才需要评估该指标；

3）Ⅲ类：非常规可选评估指标，与安全技术的常规效能评估无关，但可能与一部分特殊的安全技术效能评估相关，或可能是为了实现某个评估目标需要专门进行评估的指标，例如可用性中的自我保护性指标“数据可回滚”，当且仅当用于极特殊场景的安全技术才需要评估该指标。

附录A给出了一个安全技术效能评估指标体系的示例。

6 评估方法

6.1 评估流程

根据安全技术效能评估的基本原理及指标模型，效能评估流程应包含以下5个阶段：

a）效能评估准备。效能评估准备是安全技术效能评估有效性的基础，在真正开始进行效能评估前应对评估对象进行调研，以掌握其基本情况，同时对本次评估的目标进行明确。

b）评估指标确定。评估指标确定是整个安全技术效能评估过程中最重要的工作之一，是效能评估准确和有效的必要保证。评估指标应根据评估对象的情况及评估目标来选取，并应为每项指标分配合理的权重。

c）数据测定。数据测定关系到安全技术效能评估指标数据是否准确，决定了最终得到的效能评估结果是否可信，是安全技术效能评估的关键。所有的安全技术效能评估在进行数据测定时均应至少包含静态数据测定，在开展动态效能评估时还应进行动态数据测定。

d）效能计算。效能计算根据效能评估指标及数据测定的结果得到最终的安全技术效能，计算方法的科学性直接影响到效能评估结论的合理性，是安全技术效能评估的另一个关键。进行效能计算时应先计算单一安全技术的效能，再计算完整攻防过程的整体效能。

e）文档记录。文档记录是安全技术效能评估流程中不可缺少的步骤，应至少包括评估过程文档和评估结果文档。

安全技术效能评估流程如图3所示，安全技术效能评估的完整案例见附录B。

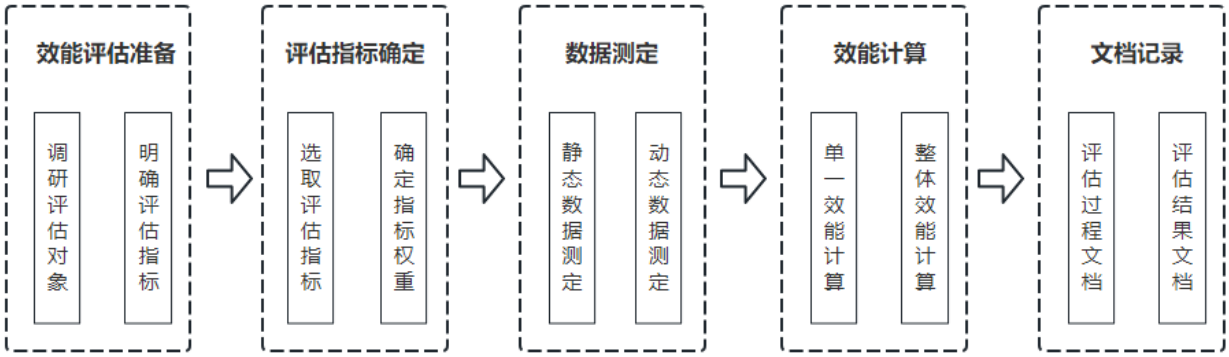

图 1 安全技术效能评估流程

6.2 效能评估准备

6.2.1 调研评估对象

对评估对象进行调研能够为效能评估指标的确定和数据的测定提供依据，调研的内容应包括：

a）安全技术原理及架构；

b）安全技术功能及特点；

c）安全技术安装及配置说明；

d）安全技术操作及使用说明；

e）安全技术涉及的数据和文档；

f）效能评估依托的安全仿真环境；

g）其它需要了解的信息。

调研评估对象时应采取资料阅读、问卷调查、现场沟通等方法中的一种或多种组合。

6.2.2 明确评估目标

对评估目标进行明确有助于根据需要确定评估指标及其权重，从而使效能评估结果更为准确、实用。安全技术效能评估的目的包括测定安全技术的有效性或危害性、发现攻防技战术中的不足或短板、对网络攻防能力进行量化分析、对重要安全事件进行复盘及定损、协助评估重要信息系统的风险情况等。不同的评估目标所侧重的评估指标不同，应在此基础上对效能评估的特性及子特性进行适当的取舍或补充，并最终确定评估指标及其权重。

6.3 评估指标确定

6.3.1 选取评估指标

根据安全技术效能特性及子特性，结合安全技术自身的特点和效能评估的目标，至少应按照下面的原则来选取评估指标：

a）能充分体现该类型安全技术的特性及子特性；

b）可度量性好；

c）指标数据易测定且其测定开销较小；

d）评估指标之间独立或不相关。

进行效能评估时还可根据需要增加其它评估指标选取原则。选取的评估指标应根据重要性及必要性进行分类，分类原则见本文件第5部分。

6.3.2 确定指标权重

安全技术效能评估指标体系为层次结构，效能由多个特性来量化，每个特性可细分为多个子特性，每个子特性又可细分为多个评估指标，因此必须为特性、子特性及评估指标分配合理的权重。分配指标权重时应按照下列步骤依次进行：

a）选定方法：采取经验数据法、专家评估法或优序法等方法中的一种或多种组合，同时参考效能评估的目标；

b）逐层评分：根据选定的方法，按照特性层、子特性层和评估指标层的顺序分别进行权重评分。以专家评估法为例，首先进行特性层权重评分，规定静态效能特性和动态效能特性的满分各为10分，请5名专家对两类特性逐一评分并收集评分结果；接着进行子特性层权重评分，规定隶属于同一个特性的子特性满分为10分，请5名专家对子特性逐一评分并收集评分结果；评估指标的权重评分以此类推；

c）数据处理：按照特性层、子特性层和评估指标层的顺序对权重评分结果进行归一化处理，确保同类效能特性之间、隶属于同一个特性的子特性之间和隶属于同一个子特性的评估指标之间权重之和为1，最终得到各个评估指标的权重。

6.4 数据测定

6.4.1 静态数据测定

静态数据测定应按照下列步骤依次进行：

a）功能性测试：根据安全技术的文档或使用说明，通过实际操作，分别测试安全技术的恰当性、正确性、完备性及操作性指标；

b）可用性测试：设计测试用例若干，分别测试安全技术的成熟性、稳定性、可靠性、兼容性、可配置性和自我保护性指标；

c）维护开销测试：通过资料收集、现场确认、调查走访等方法，获取安全技术的更新升级情况及技术支持情况；

d）数据处理：测试结束后，根据评估指标对获取的所有静态数据进行分析和处理，其中数值类型的数据统计其数量，比值类型的数据计算其比率，布尔类型的数据统一采用1或0来表示，最终得到各项指标的测定值。

6.4.2 动态数据测定

动态数据测定应按照下列步骤依次进行：

a）部署数据探针：在安全仿真平台上部署必要的数据采集探针，这些探针可以根据需要采集系统状态数据、行为数据、流量数据、日志数据等；

b）评估资产状态：利用数据探针对攻防过程中涉及到的目标资产状态进行评估，例如攻击方控制的资产及其权限、防御方控制的资产及其脆弱性等；

c）记录操作行为：利用数据探针对攻防双方使用的安全技术及其配置、操作、结果等进行记录；

d）采集网络流量：利用数据探针对攻防过程中产生的网络流量进行采集；

e）获取各类日志：利用数据探针获取攻防过程中产生的系统日志、应用日志、资源使用日志等；

f）根据需要重复步骤b至e；

g）数据处理：攻防结束后，根据评估指标对获取的所有动态数据进行分析和处理，其中数值类型的数据统计其数量，比值类型的数据计算其比率，布尔类型的数据统一采用1或0来表示，最终得到各项指标的测定值。

6.5 效能计算

6.5.1 单一效能计算

单一安全技术的效能应按照下列步骤依次进行计算：

a）对评估指标进行加权求和，得到子特性的效能值，计算公式如下：

$$E_{ij} = \sum E_{ijk} \times W_{ijk}$$

其中，E_{ij}为子特性的效能值，E_{ijk}为评估指标的测定值，W_{ijk}为该评估指标所对应的权重，$i \in \{1,2,3,4,5,6\}$为特性的标识，$j \in \{1,2,3,\dots,n\}$为子特性的标识，$k \in \{1,2,3,\dots,n\}$为评估指标的标识；

b）对子特性进行加权求和，得到特性的效能值，计算公式如下：

$$E_i = \sum E_{ij} \times W_{ij}$$

其中，E_i为特性的效能值，E_{ij}为子特性的效能值，W_{ij}为该子特性所对应的权重，$i \in \{1,2,3,4,5,6\}$为特性的标识，$j \in \{1,2,3,\dots,n\}$为子特性的标识；

c）分别对单一安全技术的静态效能特性和动态效能特性进行加权求和，得到其静态效能值和动态效能值，计算公式如下：

$$E = \sum E_i \times W_i$$

其中，E为安全技术的效能值，E_i为特性的效能值，W_i为该特性所对应的权重，i为特性的标识。当$i \in \{1,2,3\}$时$E = E_S$为静态效能值，$i \in \{4,5,6\}$时$E = E_D$为动态效能值。

6.5.2 整体效能计算

根据安全技术效能评估的基本原理，在计算出单一安全技术的效能后，应通过下面的范式得到攻防过程的整体效能：

$$E_O = \mathrm{F}(U,P) \tag{1}$$

其中，E_O表示攻防过程整体效能，F表示整体效能计算函数，U表示安全技术期望效用，P表示安全技术在攻防过程中的成功概率。范式中的三个关键环节应按照以下原则来计算：

a）计算安全技术期望效用U

安全技术的期望效用是由其收益及成本决定的，在效能评估指标体系中由静态效能来体现，即：

$$U = \mathrm{U}\left(E_S^1, E_S^2, \dots, E_S^i, \dots, E_S^n\right)$$

其中，E_S^i为单一安全技术的静态效能，n为本次评估的攻防过程中某一参与者所使用的安全技术的总数，U为不同安全技术的静态效能之间的函数关系。在具体的计算过程中，应综合考虑攻防参与者的情况来确定函数关系U。

b）计算安全技术在攻防过程中的成功概率P

安全技术的成功概率主要与攻防参与者的具体使用情况相关，在效能评估指标体系中由动态效能来体现，即：

$$P=\begin{cases}\mathrm{P}\left(E_D^1,E_D^2,\ldots,E_D^j,\ldots,E_D^n\right), & \text{进行动态效能评估时}\\ 1, & \text{不进行动态效能评估时}\end{cases}$$

其中，E_D^j为单一安全技术的动态效能，n为本次评估的攻防过程中某一参与者所使用的安全技术的总数，P为不同安全技术的动态效能之间的函数关系。在具体的计算过程中，应综合考虑攻防参与者的情况来确定函数关系P。

c）计算攻防过程整体效能E_O

根据计算出的安全技术期望效用及它们在攻防过程中的成功概率，即可根据范式(1)计算攻防过程整体效能E_O。在具体的计算过程中，应根据实际情况选择适当的计算函数或计算方法，如相乘法或矩阵法等。在附录B给出的安全技术效能评估案例中展示了利用相乘法计算攻防过程整体效能的过程。

6.6 文档记录

6.6.1 评估过程文档

评估过程文档是指在安全技术效能评估过程中产生的、用于记录效能评估的具体实施情况的文档，其中应至少包含下列内容：

a）效能评估计划：记录本次评估的目标、平台、人员、时间和地点安排等；

b）评估对象清单：记录效能评估对象的范围、数量、详细信息和调研情况等；

c）效能评估模型：记录本次评估所用的指标模型，包括特性、子特性、评估指标及其分类、指标权重等；

d）效能评估数据：记录本次评估过程中所测定的原始数据、指标数据及数据处理方式。

所有的评估过程文档应符合以下要求：

a）文档的形式及详略程度由效能评估的组织管理部门决定；

b）文档的发布或修订是得到批准的；

c）文档的标识、储存、检索、保护、保存期限及处置方式是可以控制的；

d）文档不会被非预期地使用。

6.6.2 评估结果文档

评估结果文档是反映安全技术效能评估的最终结果的文档，旨在总结安全技术和安全攻防过程中存在的不足和短板，帮助提高安全问题的发现和处理能力。

评估结果文档应至少包含一份详细的安全技术效能评估报告，对本次安全技术效能评估的情况和结果进行说明，包括评估对象、评估指标、数据测定、效能计算的大致情况，单一静态效能、单一动态效能和攻防过程整体效能的数值结果及意义，对评估结果的统计、对比和分析等内容。评估结果文档的要求与评估过程文档相同。

如有必要，评估结果文档还可包含对单一安全技术或对基于多种安全技术的战术的效能等级评定报告，以体现不同安全技术或战术的有效性或危害性。对安全技术的效能等级评定应以单一静态效能为主要评定依据，对战术的效能等级评定应以攻防过程整体效能为主要评定依据，具体的效能等级划分方式则应根据具体场景来制定或调整。效能等级较高的安全技术或战术可以在安全攻防实践中优先使用，效能等级较低的安全技术或战术则需要弃用或改进，评估结果文档宜包含对安全技术或战术的使用或改进建议。

附 录 A
（资料性）
安全技术效能评估指标体系示例

以网络安全仿真中常见的红蓝对抗演练仿真为例，考虑这类对抗演练的特点，对安全技术效能评估指标体系进行细化和补充，得到如表A.1所示的效能评估指标体系，指标类型I类为基本评估指标，II类为可选评估指标，III类为非常规可选评估指标。

表 A.1 红蓝对抗演练效能评估指标体系

效能分类	特性	子特性	评估指标	指标类型
静态效能	功能性	恰当性	功能设计的合理性	I
			功能设计的逻辑性	II
			功能设计的稳定性	III
			功能设计的连贯性	III
		正确性	功能预期的符合性	I
			功能接口的正确性	II
			数据项的正确性	III
		完备性	功能实现的完整性	I
			完整实现的覆盖率	II
		操作性	使用的复杂性	I
			功能的易识别性	I
			消息的易理解性	II
			文档的易理解性	II
	可用性	成熟性	工作原理的有效性	I
			潜在失效率	III
			累计有效服务时间	III
			有效服务时间占比	III
		稳定性	结果的一致性	I
			功能的稳定性	II
			接口的稳定性	II
			无故障率	II
			容错性	II
		可靠性	误报率	I
			漏报率	I

效能分类	特性	子特性	评估指标	指标类型
			可重复验证性	II
		兼容性	硬件适应性	I
			操作系统适应性	II
			支撑软件适应性	II
			数据适应性	II
			通信适应性	III
		可配置性	配置的复杂性	I
			操作的可定制性	II
			默认值的可定制性	II
			界面的可定制性	III
			快捷方式的可定制性	III
		自我保护性	访问的可控制性	I
			访问的可审核性	II
			数据的安全性	I
			数据的保密性	II
	维护开销	更新开销	更新的复杂性	I
			更新的频繁性	II
			更新的可还原性	III
		技术支持开销	技术支持的复杂性	II
			远程技术支持的复杂性	III
			人工技术支持的复杂性	III
动态效能	适应性	匹配性	当前场景下的可行性	I
			效果预期的符合性	I
		针对性	对抗成功率	I
			防躲避能力	III
			逃逸能力	III
		灵活性	安装灵活性	II
			配置灵活性	II
			卸载灵活性	III
	合理性	必要性	实际操作次数	I
			实际操作次数占比	I
			操作可替代性	III
		充分性	使用功能个数	I
			使用功能个数占比	I
			应使用而未使用功能个数	III