ICS 35.240.40
CCS A 11

中华人民共和国国家标准

GB/T 40473.7—2021

银行业应用系统　非功能需求
第7部分:安全性

Banking application system—Nonfunctional requirement—Part 7:Security

2021-07-20 发布　　2022-02-01 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。

本文件是GB/T 40473《银行业应用系统　非功能需求》的第7部分。GB/T 40473已经发布了以下部分：

——第1部分：描述框架；

——第2部分：功能适宜性；

——第3部分：性能效率；

——第4部分：兼容性；

——第5部分：易用性；

——第6部分：可靠性；

——第7部分：安全性；

——第8部分：可维护性；

——第9部分：可移植性。

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。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会(SAC/TC 180)归口。

本文件起草单位：中国人民银行科技司、中国农业银行股份有限公司、中国外汇交易中心暨全国银行间同业拆借中心、中国人民银行清算总中心、中国建设银行股份有限公司、交通银行股份有限公司、农信银资金清算中心有限责任公司、中国金融电子化公司。

本文件主要起草人：李伟、杨富玉、曲维民、李宽、王鹏、马骏、王锋、杨明英、葛洪慧、崔婉旻、赵刘韬、叶旻、梁军、景芸、王灿雍、陆原鹏、杨倩、谢彦丽、刘书元、王思源。

引　言

GB/T 40473 给出了银行业应用系统非功能需求的描述框架和各类银行业应用系统非功能需求的模板，旨在提高银行业应用系统非功能需求的编制质量和效率，降低编制银行业应用系统非功能需求的门槛和成本，由九个部分组成。

——第 1 部分：描述框架。目的在于明确银行业应用系统的范畴，确立银行业应用系统非功能需求的描述框架，阐明银行业应用系统非功能需求的标识和描述，给出银行业应用系统非功能需求的定制包与定制轮廓，提出对银行业应用系统非功能需求的技术管理与评价，并给出银行业应用系统非功能需求的 XML 描述的方法，是其余各部分阅读和应用的基础。

——第 2 部分：功能适宜性。目的在于给出包括功能完整性、功能正确性和功能适合性的功能适宜性需求，这些需求从严谨的需求分类看，可以看作是功能需求，但在银行业应用系统的研发中，往往被视作非功能需求。

——第 3 部分：性能效率。目的在于给出包括时间特性、资源利用和容量的性能效率需求。

——第 4 部分：兼容性。目的在于给出包括共存性和互操作性的兼容性。

——第 5 部分：易用性。目的在于给出包括可辨识性、易学性、易操作性、用户差错防御性、用户界面舒适性和易访问性的易用性。

——第 6 部分：可靠性。目的在于给出包括成熟性、可用性、容错性和易恢复性的可靠性。

——第 7 部分：安全性。目的在于给出包括保密性、完整性、抗抵赖性、可核查性和真实性的安全性。

——第 8 部分：可维护性。目的在于给出包括模块性、可重用性、易分析性、易修改性和易测试性的可维护性。

——第 9 部分：可移植性。目的在于给出包括适应性、易安装性和易替换性的可移植性。

当不考虑缩写和编号含义时，本领域的技术人员基于本领域的专业知识，可基本正确地理解本文件的实质性内容。但在如下典型的情况下，本文件的应用者宜先阅读并理解 GB/T 40473.1—2021：

——编制应用系统的非功能需求；

——评审应用系统的非功能需求；

——对应用系统按照非功能需求开发的系统进行验证和确认；

——对应用系统按照非功能需求开发的系统进行静态和动态测试。

对按照本文件编制的非功能需求，若以 GB/T 40473.1—2021 给出的 XML 形式描述，会对非功能需求带来传输和处理上更大便利。

银行业应用系统　非功能需求
第7部分:安全性

1　范围

本文件界定了银行业应用系统安全性的概念,规定了安全性元素与组件层次及描述方式、安全性类保密性族、完整性族、抗抵赖性族、可核查性族和真实性族非功能需求模板。

本文件适用于银行业各类应用系统对安全性类非功能需求的描述。与银行业应用系统进行信息交换的应用系统,根据需要可参照使用。

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 40473.1—2021　银行业应用系统　非功能需求　第1部分:描述框架

3　术语和定义

GB/T 40473.1—2021界定的以及下列术语和定义适用于本文件。

3.1

信息安全性　security

产品或系统保护信息和数据的程度,以使用户、其他产品或系统具有与其授权类型和授权级别一致的数据访问度。

注1:信息安全性不仅适用于存储在产品或系统中的数据或者通过产品或系统存储的数据,也适用于传输中的数据。

注2:存活性(在受到攻击时,产品或系统及时提供必要的服务,继续履行其任务的程度)包含在易恢复性中。

注3:免疫性(产品或系统抗攻击的程度)包含在完整性中。

注4:信息安全性有助于可靠性。

[来源:GB/T 25000.10—2016,4.3.2.6]

3.2

保密性　confidentiality

产品或系统确保数据只有在被授权时才能被访问的程度。

[来源:GB/T 25000.10—2016,4.3.2.6.1]

3.3

完整性　integrity

系统、产品或组件防止未授权访问、篡改计算机程序或数据的程度。

[来源:GB/T 25000.10—2016,4.3.2.6.2]

3.4

抗抵赖性　non-repudiation

活动或事件发生后可以被证实且不可被否认的程度。