ICS 03.100.01
A 02

中华人民共和国国家标准

GB/T 24353—2009

风险管理　原则与实施指南

Risk management—Principles and guidelines on implementation

2009-09-30 发布　　2009-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准是风险管理系列标准中的指导性标准。

本标准参考 ISO/DIS 31000《风险管理　原则与实施指南》编制而成。

本标准由全国质量管理与质量保证标准化技术委员会(SAC/TC 151)提出。

本标准由全国风险管理标准化技术委员会(SAC/TC 310)归口。

本标准起草单位:中国标准化研究院、第一会达风险管理科技有限公司、中国航空综合技术研究所、北京理工大学、中国科学院科技政策与管理科学研究所、北京大学。

本标准主要起草人:高晓红、吕多加、汤万金、杨颖、汪邦军、刘铁忠、李建平、刘新立。

引　言

任何类型和规模的组织都面临风险，组织的所有活动也都涉及风险。风险会影响组织目标的实现，这些目标可能关系到组织中从战略决策到运营的各种活动，包括各个过程和具体项目，表现在领导、战略、经营、财务、环境、社会、声誉等各个方面。

风险管理通过考虑不确定性及其对目标的影响，采取相应的措施，为组织的运营和决策及有效应对各类突发事件提供支持。风险管理适用于组织的全生命周期及其任何阶段，其适用范围包括整个组织的所有领域和层次，也包括组织的具体部门和活动。

风险管理旨在保证组织恰当地应对风险，提高风险应对的效率和效果，增强行动的合理性，有效地配置资源。有效的风险管理应当融入到整个组织的理念、治理、管理、程序、方针策略以及文化等各方面。风险管理意识应当是整个组织文化的一部分。

虽然风险管理在长期的实践中得到了发展，并在许多行业满足了不同的需要，但是目前还缺乏一个一般性的方法，用来保证风险管理一致、有效的实施。本标准提供了风险管理的原则和实施的通用指南，有助于组织在任何范围和具体环境中以透明和可靠的方式实施风险管理。

本标准有助于组织做到：

——提高风险管理意识；

——有效配置和使用风险管理资源；

——实施主动的、前瞻性的管理；

——改进对机会和威胁的识别；

——遵守相关法律法规及国际规范的要求；

——改善内部控制；

——改进财务报告；

——改善公司治理；

——改善运营效果和效率；

——提高利益相关者的信心和信任；

——为计划和决策奠定可靠的基础；

——提高健康、安全和环保水平；

——改进对事故的预防和处理；

——减少损失；

——提高组织的学习能力；

——增强组织的生存和持续发展能力。

本标准的预期使用者是组织的利益相关者，如：

——组织的决策者；

——组织内部负责制定风险管理政策的人员；

——组织或活动中实施风险管理的人员；

——需要对组织的风险管理实践进行评估的人员；

——组织中负责制定有关风险管理的标准、指南、程序、应用准则的人员；

——股东、董事会、高级管理人员、员工、债权人、供应商、顾客、银行、监管机构、合作伙伴等，以及其他需要确保组织管理其风险的人员。

考虑到风险的性质、重要程度和复杂性等方面的多样性，在实际应用时，组织可使用本标准提供的方法，识别具体的风险管理环境，以确保风险管理的合理性和适用性。

许多组织在现有的管理实践和过程中已经实施了风险管理，或者已经对某些特定风险或具体领域采用了正式的风险管理过程，如内部控制。管理层可对照本标准对现有的风险管理实践和过程进行检查。

本标准是通用标准，旨在协调现有的和将来的标准中有关风险管理的内容。本标准提供通用的方法，为制定具体风险或具体行业的标准提供支持，而不是为了替代这些标准。

风险管理　原则与实施指南

1　范围

本标准提供了风险管理的原则和通用的实施指南。

本标准适用于各种类型和规模的组织，适用于组织的全生命周期及其各阶段，也适用于组织的各种活动，包括流程管理、职能行为、项目管理以及与产品、服务、资产、运作和决策等有关的各项活动。

本标准提供实施风险管理的通用指南，但风险管理的具体实施取决于组织的实际需要和具体实践。

2　规范性引用文件

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

GB/T 23694　风险管理　术语

3　术语和定义

GB/T 23694 确立的术语和定义适用于本标准。

4　风险管理原则

为有效管理风险，组织在实施风险管理时，可遵循下列原则：

a)　控制损失，创造价值

以控制损失、创造价值为目标的风险管理，有助于组织实现目标、取得具体可见的成绩和改善各方面的业绩，包括人员健康和安全、合规经营、信用程度、社会认可、环境保护、财务绩效、产品质量、运营效率和公司治理等方面。

b)　融入组织管理过程

风险管理不是独立于组织主要活动和各项管理过程的单独的活动，而是组织管理过程不可缺少的重要组成部分。

c)　支持决策过程

组织的所有决策都应考虑风险和风险管理。风险管理旨在将风险控制在组织可接受的范围内，有助于判断风险应对是否充分、有效，有助于决定行动优先顺序并选择可行的行动方案，从而帮助决策者做出合理的决策。

d)　应用系统的、结构化的方法

系统的、结构化的方法有助于风险管理效率的提升，并产生一致、可比、可靠的结果。

e)　以信息为基础

风险管理过程要以有效的信息为基础。这些信息可通过经验、反馈、观察、预测和专家判断等多种渠道获取，但使用时要考虑数据、模型和专家意见的局限性。

f)　环境依赖

风险管理取决于组织所处的内部和外部环境以及组织所承担的风险。需要特别指出的是，风险管理受人文因素的影响。

g)　广泛参与、充分沟通

组织的利益相关者之间的沟通，尤其是决策者在风险管理中适当、及时的参与，有助于保证风险管理的针对性和有效性。

利益相关者的广泛参与有助于其观点在风险管理过程中得到体现，其利益诉求在决定组织的风险偏好时得到充分考虑。利益相关者的广泛参与要建立在对其权利和责任明确认可的基础上。

利益相关者之间需要进行持续、双向和及时的沟通，尤其是在重大风险事件和风险管理有效性等方面需要及时沟通。

h) 持续改进

风险管理是适应环境变化的动态过程，其各步骤之间形成一个信息反馈的闭环。随着内部和外部事件的发生、组织环境和知识的改变以及监督和检查的执行，有些风险可能会发生变化，一些新的风险可能会出现，另一些风险则可能消失。因此，组织应持续不断地对各种变化保持敏感并做出恰当反应。组织通过绩效测量、检查和调整等手段，使风险管理得到持续改进。

5 风险管理过程

5.1 概述

风险管理过程是组织管理的有机组成部分，嵌入在组织文化和实践当中，贯穿于组织的经营过程。风险管理过程由5.2到5.5所描述的活动组成，即明确环境信息、风险评估、风险应对、监督和检查，如图1所示。其中，风险评估包括风险识别、风险分析和风险评价等三个步骤。

沟通和记录，应贯穿于风险管理过程的各项活动中，5.6将对其进行详细说明。

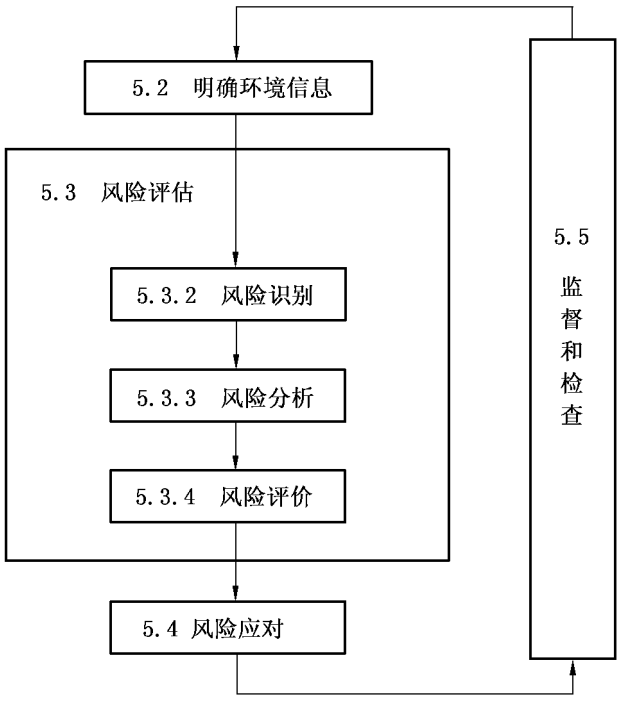

图1 风险管理过程

5.2 明确环境信息

5.2.1 概述

通过明确环境信息，组织可明确其风险管理的目标，确定与组织相关的内部和外部参数，并设定风险管理的范围和有关风险准则。

5.2.2 外部环境信息

外部环境信息是组织在实现目标过程中所面临的外界环境的历史、现在和未来的各种相关信息。

为保证在制定风险准则时能充分考虑外部利益相关者的目标和关注点，组织需要了解外部环境信

息。外部环境信息以组织所处的整体环境为基础，包括法律和监管要求、利益相关者的诉求和与具体风险管理过程相关的其他方面的信息等。

外部环境信息包括但不限于：

——国际、国内、地区及当地的政治、经济、文化、法律、法规、技术、金融以及自然环境和竞争环境；

——影响组织目标实现的外部关键因素及其历史和变化趋势；

——外部利益相关者及其诉求、价值观、风险承受度；

——外部利益相关者与组织的关系等。

5.2.3 内部环境信息

内部环境信息是组织在实现目标过程中所面临的内在环境的历史、现在和未来的各种相关信息。

风险管理过程要与组织的文化、经营过程和结构相适应，包括组织内影响其风险管理的任何事物。组织需明确内部环境信息，因为：

——风险可能会影响组织战略、日常经营或项目运营等各个方面，从而进一步会影响组织的价值、信用和承诺等；

——风险管理在组织的特定目标和管理条件下进行；

——具体活动的目标和有关准则应放到组织整体目标的环境中考虑。

内部环境信息可包括：

——组织的方针、目标以及经营战略；

——资源和知识方面的能力（如资金、时间、人力、过程、系统和技术）；

——信息系统、信息流和决策过程（包括正式的和非正式的）；

——内部利益相关者及其诉求、价值观、风险承受度；

——采用的标准和模型；

——组织结构（包括治理结构、任务和责任等）、管理过程和措施；

——与风险管理实施过程有关的环境信息等。

其中，风险管理过程的环境信息根据组织的需要而改变，它包括但不限于：

——所开展的风险管理工作的范围和目标，以及所需要的资源；

——风险管理过程的职责；

——应执行的风险管理活动的深度和广度；

——风险管理活动与组织其他活动之间的关系；

——风险评估的方法和使用的数据；

——风险管理绩效的评价方法；

——需要制定的决策；

——风险准则等。

5.2.4 确定风险准则

风险准则是组织用于评价风险重要程度的标准。因此，风险准则需体现组织的风险承受度，应反映组织的价值观、目标和资源。有些风险准则直接或间接反映了法律和法规要求或其他需要组织遵循的要求。风险准则应当与组织的风险管理方针一致。具体的风险准则应尽可能在风险管理过程开始时制定，并持续不断地检查和完善。

确定风险准则时要考虑以下因素：

——可能发生的后果的性质、类型以及后果的度量；

——可能性的度量；

——可能性和后果的时限；

——风险的度量方法；

——风险等级的确定；

——利益相关者可接受的风险或可容许的风险等级；

——多种风险的组合的影响。

通过对以上因素及其他相关因素的关注，将有助于保证组织所采用的风险管理方法适合于组织现状及其所面临的风险。

5.3 风险评估

5.3.1 概述

风险评估包括风险识别、风险分析和风险评价三个步骤。

5.3.2 风险识别

风险识别是通过识别风险源、影响范围、事件及其原因和潜在的后果等，生成一个全面的风险列表。识别风险不仅要考虑有关事件可能带来的损失，也要考虑其中蕴含的机会。

进行风险识别时要掌握相关的和最新的信息，必要时，需包括适用的背景信息。除了识别可能发生的风险事件外，还要考虑其可能的原因和可能导致的后果，包括所有重要的原因和后果。不论风险事件的风险源是否在组织的控制之下，或其原因是否已知，都应对其进行识别。此外，要关注已经发生的风险事件，特别是新近发生的风险事件。

识别风险需要所有相关人员的参与。组织所采用的风险识别工具和技术应当适合于其目标、能力及其所处环境。

5.3.3 风险分析

风险分析是根据风险类型、获得的信息和风险评估结果的使用目的，对识别出的风险进行定性和定量的分析，为风险评价和风险应对提供支持。风险分析要考虑导致风险的原因和风险源、风险事件的正面和负面的后果及其发生的可能性、影响后果和可能性的因素、不同风险及其风险源的相互关系以及风险的其他特性，还要考虑现有的管理措施及其效果和效率。

在风险分析中，应考虑组织的风险承受度及其对前提和假设的敏感性，并适时与决策者和其他利益相关者有效地沟通。另外，还要考虑可能存在的专家观点中的分歧及数据和模型的局限性。

根据风险分析的目的、获得的信息数据和资源，风险分析可以是定性的、半定量的、定量的或以上方法的组合。一般情况下，首先采用定性分析，初步了解风险等级和揭示主要风险。适当时，进行更具体和定量的风险分析。

后果和可能性可通过专家意见确定，或通过对事件或事件组合的结果建模确定，也可通过对实验研究或可获得的数据的推导确定。对后果的描述可表达为有形或无形的影响。在某些情况下，可能需要多个指标来确切描述不同时间、地点、类别或情形的后果。

5.3.4 风险评价

风险评价是将风险分析的结果与组织的风险准则比较，或者在各种风险的分析结果之间进行比较，确定风险等级，以便做出风险应对的决策。如果该风险是新识别的风险，则应当制定相应的风险准则，以便评价该风险。

风险评价的结果应满足风险应对的需要，否则，应做进一步分析。有时，根据已经制定的风险准则，风险评价使组织做出维持现有的风险应对措施，不采取其他新的措施的决定。

5.4 风险应对

5.4.1 概述

风险应对是选择并执行一种或多种改变风险的措施，包括改变风险事件发生的可能性或后果的措施。风险应对决策应当考虑各种环境信息，包括内部和外部利益相关者的风险承受度，以及法律、法规和其他方面的要求等。

风险应对措施的制订和评估可能是一个递进的过程。对于风险应对措施，应评估其剩余风险是否可以承受。如果剩余风险不可承受，应调整或制定新的风险应对措施，并评估新的风险应对措施的效果，直到剩余风险可以承受。执行风险应对措施会引起组织风险的改变，需要跟踪、监督风险应对的效

果和组织的有关环境信息，并对变化的风险进行评估，必要时重新制订风险应对措施。

可能的风险应对措施之间不一定互相排斥。一个风险应对措施也不一定在所有条件下都适合。风险应对措施可包括下列各项：

——决定停止或退出可能导致风险的活动以规避风险；

——增加风险或承担新的风险以寻求机会；

——消除具有负面影响的风险源；

——改变风险事件发生的可能性的大小及其分布的性质；

——改变风险事件发生的可能后果；

——转移风险；

——分担风险；

——保留风险等。

5.4.2 选择风险应对措施

选择适当的风险应对措施时需考虑很多方面，比如：

——法律、法规、社会责任和环境保护等方面的要求；

——风险应对措施的实施成本与收益（有些风险可能需要组织考虑采用经济上看起来不合理的风险应对决策，例如可能带来严重的负面后果但发生可能性低的风险事件）；

——选择几种应对措施，将其单独或组合使用；

——利益相关者的诉求和价值观、对风险的认知和承受度以及对某一些风险应对措施的偏好。

风险应对措施在实施过程中可能会失灵或无效。因此，要把监督作为风险应对措施的实施计划的有机组成部分，以保证应对措施持续有效。

风险应对措施可能引起次生风险，对次生风险也需要评估、应对、监督和检查。在原有的风险应对计划中要加入这些次生风险的内容，而不应将其作为新风险而独立对待。为此需要识别并检查原有风险与次生风险之间的联系。当风险应对措施影响到组织内其他领域的风险或影响到其他利益相关者时，要评估这些影响，并与有关利益相关者沟通，必要时调整风险应对措施。

决策者和其他利益相关者应当清楚在采取风险应对措施后的剩余风险的性质和程度。

5.4.3 制定风险应对计划

在选择了风险应对措施之后，需要制定相应的风险应对计划。风险应对计划中应当包括以下信息：

——预期的收益；

——绩效指标及其考核方法；

——风险管理责任人及实施风险应对措施的人员安排；

——风险应对措施涉及的具体业务和管理活动；

——选择多种可能的风险应对措施时，实施风险应对措施的优先次序；

——报告和监督、检查的要求；

——与适当的利益相关者的沟通安排；

——资源需求，包括应急机制的资源需求；

——执行时间表等。

风险应对计划要与组织的管理过程整合。

5.5 监督和检查

组织应明确界定监督和检查的责任。

监督和检查可能包括：

——监测事件，分析变化及其趋势并从中吸取教训；

——发现内部和外部环境信息的变化，包括风险本身的变化、可能导致的风险应对措施及其实施优先次序的改变；

——监督并记录风险应对措施实施后的剩余风险，以便在适当时做进一步处理；

——适用时，对照风险应对计划，检查工作进度与计划的偏差，保证风险应对措施的设计和执行有效；

——报告关于风险、风险应对计划的进度和风险管理方针的遵循情况；

——实施风险管理绩效评估。

风险管理绩效评估应被纳入到组织的绩效管理以及组织对内、对外的报告体系之中。

监督和检查活动包括常规检查、监控已知的风险、定期或不定期检查。定期或不定期检查都应被列入风险应对计划。

适当时，监督和检查的结果应当有记录并对内或对外报告。

5.6 沟通和记录

5.6.1 沟通

组织在风险管理过程的每一个阶段都应当与内部和外部利益相关者有效沟通，以保证实施风险管理的责任人和利益相关者能够理解组织风险管理决策的依据，以及需要采取某些行动的原因。

由于利益相关者的价值观、诉求、假设、认知和关注点不同，其风险偏好也不同，并可能对决策有重要影响。因此，组织在决策过程中应当与利益相关者进行充分沟通，识别并记录利益相关者的风险偏好。

5.6.2 记录

在风险管理过程中，记录是实施和改进整个风险管理过程的基础。

建立记录应当考虑以下方面：

——出于管理的目的而重复使用信息的需要；

——进一步分析风险和调整风险应对措施的需要；

——风险管理活动的可追溯要求；

——沟通的需要；

——法律、法规和操作上对记录的需要；

——组织本身持续学习的需要；

——建立和维护记录所需的成本和工作量；

——获取信息的方法、读取信息的容易程度和储存媒介；

——记录保留期限；

——信息的敏感性。

6 风险管理的实施

6.1 概述

组织实施风险管理过程(见第5章)需要一个风险管理体系，包括相关方针、组织结构、工作程序、资源配置、信息沟通机制以及相关的技术手段等基础设施，以便将风险管理嵌入到组织的各个层次和活动之中。通过在组织的不同层次和特定环境内实施风险管理过程，风险管理体系帮助组织有效地管理风险。组织的风险管理体系可能由在各层次和特定环境内实施风险管理过程的子体系构成，如内部控制体系等。风险管理体系应当保证风险管理过程中的风险信息的充分沟通，并且在相关的组织层次范围内作为决策和问责的依据使用。组织要在检查的基础上，做出如何改进风险管理体系、方针和风险应对计划的决策，从而引导组织的风险管理和风险管理文化的改进。

风险管理体系的要素主要包括：

——风险管理方针；

——适当的制度和程序，使风险管理嵌入到组织的所有活动和过程中；

——与组织结构相关的职责，及有关的与组织的绩效指标一致的风险管理绩效指标；

——资源分配；

——与所有利益相关者沟通风险管理的机制；

——技术手段、方法、工具等。

6.2 风险管理方针

风险管理方针应明确下列事项：

——组织的风险管理理念；

——组织的最高管理者对风险管理的承诺；

——组织的风险管理目标；

——组织的风险偏好；

——风险管理方针与组织的目标及其他方针之间的关系；

——风险管理的职责分配；

——管理风险的程序和方法；

——风险管理的资源配置；

——测量和报告风险管理绩效的方式；

——建立风险管理体系的计划；

——持续改进的承诺。

组织应就风险管理方针同内部和外部利益相关者进行充分沟通。

6.3 风险管理工作程序

组织应当设计适当的制度和行为规范，建立风险管理工作程序，特别是整个组织层面的风险管理计划，以保证风险管理嵌入到组织的所有活动和过程之中，尤其是组织的战略规划、运营过程以及变革管理之中。

6.4 风险管理相关组织结构

组织可通过以下方法保证风险管理的责任认定和授权，从而能够执行风险管理过程，并保证风险管理的充分性和有效性：

——明确风险管理体系的制定、实施和维护人员的职责；

——明确执行风险应对措施、维护风险管理体系和报告相关风险信息人员的职责；

——建立批准、授权制度；

——建立绩效测量及相应的合适的奖励、惩罚制度；

——建立对内对外的报告机制等。

6.5 风险管理资源配置

组织需根据风险管理计划制定可行的方法，为风险管理分配适当的资源。具体要考虑下列各项：

——人员、技术、经验和能力；

——风险管理过程每一阶段所需要的资金及各种资源；

——数据记录的过程和程序步骤；

——信息和知识管理系统。

6.6 沟通和报告机制

6.6.1 内部沟通和报告机制

组织要建立内部沟通和报告机制，以保证：

——风险管理体系的关键组成部分及其调整得到适当的沟通；

——在组织内部充分报告风险应对计划实施的效果和效率；

——在适当的层次和时间提供风险管理的相关信息；

——建立与内部利益相关者协商的程序。

内部沟通和报告机制还包括在考虑到组织敏感程度的基础上，适当整合从各内部渠道得到的风险信息的程序。

6.6.2 外部沟通和报告机制

组织需建立与外部利益相关者沟通的机制。这种机制应当保证：

——组织的对外报告符合法律、法规和公司治理要求；

——组织与外部利益相关者保持有效的信息沟通；

——在外部利益相关者中建立对组织的信心；

——在发生突发事件、危机和紧急状况时与利益相关者沟通；

——为组织提供外部利益相关者的报告和反馈。

参 考 文 献

[1] ISO/DIS 31000,Risk management—Principles and guidelines on implementation

[2] GB/T 20000.4—2003 标准化工作指南 第4部分:标准中涉及安全的内容

[3] GB/T 19000—2008 质量管理体系 基础和术语

[4] GB/T 16856.1—2008 机械安全 风险评价 第1部分:原则

[5] GB/T 16856.2—2008 机械安全 风险评价 第2部分:实施指南和方法举例

[6] GB/T 15706.1—2007 机械安全 基本概念与设计通则 第1部分:基本术语和方法

[7] GB/T 24050—2004 环境管理 术语

[8] ISO 13702:1999,Petroleum and natural gas industries—Control and mitigation of fires and explosions on offshore production installations—Requirements and guidelines

[9] ISO 14971:2007,Medical devices—Application of risk management to medical devices

[10] ISO 15265:2004,Ergonomics of the thermal environment—Risk assessment strategy for the prevention of stress or discomfort in thermal working conditions

[11] ISO 15544:2000,Petroleum and natural gas industries—Offshore production installations—Requirements and guidelines for emergency response

[12] ISO 17776:2000,Petroleum and natural gas industries—Offshore production installations—Guidelines on tools and techniques for hazard identification and risk assessment

[13] ISO 13215-3:1999,Road vehicles—Reduction of misuse risk of child restraint systems—Part 3:Prediction and assessment of misuse by Misuse Mode and Effect Analysis (MMEA)

[14] ISO 13232-5:2005,Motorcycles—Test and analysis procedures for research evaluation of rider crash protective devices fitted to motorcycles—Part 5: Injury indices and risk/benefit analysis

[15] ISO/IEC 15408-1:2005,Information technology—Security techniques—Evaluation criteria for IT security—Part 1:Introduction and general model

[16] ISO/IEC 15408-2:2005,Information technology—Security techniques—Evaluation criteria for IT security—Part 2:Security functional requirements

[17] ISO/IEC 15408-3:2005,Information technology—Security techniques—Evaluation criteria for IT security—Part 3:Security assurance requirements

[18] ISO 16312-1:2006,Guidance for assessing the validity of physical fire models for obtaining fire effluent toxicity data for fire hazard and risk assessment—Part 1:Criteria

[19] GB/T 7826—1987 系统可靠性分析技术 失效模式和效应分析(FMEA)程序

[20] IEC 60300-1:2003,Dependability management—Part 1:Dependability management systems

[21] IEC 60300-2:2004,Dependability management—Part 2:Guidelines for dependability management

[22] IEC 61508-2:2000,Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2:Requirements for electrical/electronic/programmable electronic safety-related systems

[23] IEC 61882:2001,Hazard and operability studies (HAZOP studies)—Application guide

[24] GB/T 20032—2005 项目风险管理 应用指南

[25] IEC 62305-2:2006,Protection against lightning—Part 2:Risk management