咨询通告

中国民用航空局飞行标准司

编　　号：AC－121/135－FS－2008－26

下发日期：2008年4月29日

关于航空运营人安全管理体系的要求

关于航空运营人安全管理体系的要求

1. 依据和目的

本咨询通告依据中国民用航空规章《大型飞机公共航空运输承运人运行合格审定规则》（CCAR-121）和《小型航空器商业运输运营人运行合格审定规则》（CCAR-135）制定，目的是指导大型飞机公共航空运输承运人和小型航空器商业运输运营人（以下均简称“运营人”）建立符合要求的安全管理体系（SMS）。

2. 适用范围

本咨询通告适用于按照 CCAR-121 和 CCAR-135 运行的运营人。

3. 参考文献

本咨询通告的参考文献如下:

(1)《国际民用航空公约》 附件 6《航空器运行》

(2) 国际民用航空组织 Doc9859 《安全管理手册》

(3) FAA AC 120-92 《航空运营人安全管理体系介绍》

(4) FAA AC 120-59A 《航空承运人内部评估方案》

4. 撤销

（备用）。

5. 定义

过程——一组将输入转化为输出的相互关联或相互作用的活动。

程序——执行活动或过程的特定方法。

危险源——有可能导致人员受到伤害、疾病或死亡，或者系统、

设备或财产遭破坏或受损，或者环境受到破坏的任何现有的或潜在的状况。

风险——某一危险源可能导致潜在后果预计的可能性和严重性的综合。

衍生风险——作为风险控制结果无意中带来的新风险。

风险管理——安全管理体系内的一个正式过程，由系统和工作分析、危险源识别、风险分析、风险评价和风险控制组成。风险管理过程处于提供产品或服务的过程中，不是一个独立的或特殊的过程。

审核——定期、正式的评审、查证，以评价是否符合规章、政策、标准和合同要求。审核从组织的管理和运行着手，并扩展至组织的活动、产品和服务。

内部审核——由被审核组织或代表被审核组织的组织实施的审核。

外部审核——由被审核组织之外的组织执行的审核。

评估——对运营人政策、各程序和各系统进行的功能性独立的评审。当运营人自己完成此项工作时，应由运营人内独立于被评估部门的一个机构来完成。评估过程建立在审核和检查的基础上。评估与系统审核同义。

审核员——满足规定的经历条件、通过规定的培训胜任执行审核的人员。

安全保证——系统地为运营人的运输服务满足或超越安全要求而提供信心的过程管理功能。

安全管理体系——正式的、自上而下的、有条理的管理安全风险的做法。其包括安全管理的系统的程序、措施和政策（如本文所述的，

包括风险管理、安全政策、安全保证和安全促进）。

6. 背景和说明

2006 年 3 月，国际民航组织理事会通过了对附件 6《航空器运行》的第 30 次修订。该次修订增加了国家要求航空运营人实施安全管理体系的要求。附件 6 规定从 2009 年 1 月 1 日起，各缔约国应要求其航空运营人实施被局方接受的安全管理体系。

我国民航企业安全管理的纪录处于较为领先的水平，但是随着运输量的增长，如果不采取有效措施，事故的总次数将不为公众所接受，解决这个问题的最好办法就是将安全管理融入日常的运行管理中，并采取更为主动的安全管理模式降低事故率。

民航安全管理是随着人们对航空安全问题的研究和认识的深入而不断发展的。人们从最初重点关注航空器、空管及机场设备设施等硬件问题逐步过渡到关注人为因素问题，现在开始关注系统和组织对安全的影响。

运用系统方法管理安全可以使运营人通过科学地制定政策、目标，清楚地界定安全责任，鼓励全员参与，实施风险管理、安全保证、安全促进，有效地配备资源，在满足规章的基础上，不断提高运行水平。

7. 安全管理体系的本质构成

7.1 安全管理

现代安全管理和安全监督活动日益倾向于注重过程控制的系统方法，而不是仅仅努力地对最终结果开展检查和采取补救措施。理解安全管理体系概念的一个方法是简要地讨论三个词：安全、管理、系统。然后我们再讨论安全管理另一个必不可少的方面：安全文化。

(1) 安全：基于风险管理的要求

安全管理体系的目标是提供一个结构化的管理体系，以控制运行中的风险。有效的安全管理体系必须基于运营人影响安全的各过程的特点。有时安全被定义为没有潜在的危害，但对民航而言这是一个不切实际的目标。切合实际的做法是用后果严重性和可能性综合后的风险对安全进行描述。因此，安全可以被定义为人员伤害或财产损失的风险在可接受的水平或其以下的状态。我们可以识别、分析那些或多或少有可能使我们陷入事故以及其他相对严重后果的因素。对这些因素，我们可以设置系统要求，并采取措施来保证满足要求。从而，有效的安全管理就是风险管理。

(2) 管理：使用质量管理技术进行安全保证

本咨询通告中描述的安全管理过程始于组织过程的设计、实施，及航空运行中的风险控制程序。一旦这些控制措施付诸实施，质量管理技术可以被用来提供一个结构化过程，以保证其实现预定目标，并在不足之处加以改进。因此，安全管理可以被视为为实现安全目的，对安全相关的运行和支持过程进行的质量管理。

(3) 系统：关注系统作法

系统是指在特定环境下完成某使命或目标的人员和其他资源。系统活动的管理包含为实现组织目标的计划、组织、指挥和控制。系统及其过程的几个重要特性在被用于安全相关的运行和支持过程时被称为“过程属性”或“安全属性”。如果这些过程属性会产生需要的安全结果，则这些过程属性的设计必须有安全要求。这些属性包括：

(a) 完成所要求活动的职责及权力；

(b) 提供给组织内的人员供其遵守的、指令清楚的程序；

(c) 用于必需产生正确输出的过程中的活动的组织管理措施和监查控制措施;

(d) 对过程及其结果的测量;

(e) 明确组织内部每个人与其所在部门的关系，以及运营人与外委方、供应商、客户及其他有业务来往的组织间重要的相互关系或联系。

7.2 安全文化

一个组织的文化包括组织的价值观、信念、习惯、仪式、使命目标、绩效考核以及对员工、顾客、集体的责任感。除非组织内的员工共同努力促进安全运行，否则前面讨论的“安全”、“管理”、“系统”将不能实现它们各自的目标。安全文化包括心理的（人们怎么想）、行为的（人们怎么做）及组织的因素。组织因素大部分处于管理控制之下，其他两方面因素的结果则视其努力而定。因此，此咨询通告附录《航空运营人安全管理体系要求》（以下简称《要求》）中包括对政策（为安全管理体系提供框架）和组织（如：有效的员工安全报告和反馈系统及清晰的双向沟通安全事务的组织路线）的功能要求。

8. 运营人的运行、防护及其与局方安全监督管理的关系

8.1 运营人的运行与防护的关系

图 1 描述的是与安全相关的两个系统之间的关系。该图描述的是运营人内（与为顾客提供产品或服务有关的）技术、管理功能和与控制风险有关的功能之间的关系。

需要注意的是：图 1 是从功能角度，而不是从组织结构角度进行描述的。该图并不意味着安全管理只是“安全部门”或“安全总监”

的责任；事实上，安全管理体系强调管理“生产运行”过程的人员在安全管理中的角色。

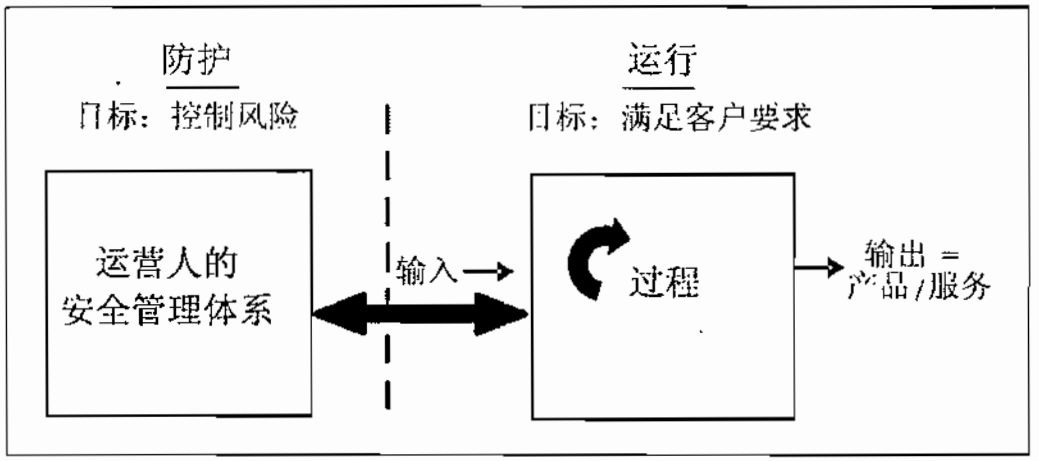

图 1　运行与防护的功能关系

8.1.1 运行

运行过程是指飞行运行、运行控制、维修、客舱安全、地面服务、货运等过程。由于运营人的运输服务是通过运行过程来完成的，所以有效的风险管理和安全保证应从彻底了解运行过程的结构和组织着手。相当数量的危险源、风险因素来自于过程设计不当或系统与运行环境不适宜。在这些情况下，影响运行安全的危险源可能不会被充分认识，因而得不到足够的控制。

8.1.2 防护

风险是伴随运行活动产生的。运营人的客户和员工是安全系统失效的潜在直接受害者。因此，运营人的首要职责是识别其管理过程和运行环境中存在的危险源，控制其风险。安全管理体系为运营人的管理提供了一个正式的管理体系以履行其义务，实现安全运行，保护客户及员工的利益。

8.2 运营人的运行及防护与局方安全监督管理的关系

运营人的运行过程、安全管理功能、局方安全监督管理功能之间的关系见图 2。局方的安全监督管理不仅包括对运营人的运行过程的安全监督管理，而且包括对运营人的安全管理体系的安全监督管理，从而形成又一层防护。

局方传统的监督管理注重符合技术标准，通常包括审定、持续监督、调查、规章的强制实施等。在继续保持传统监督管理方法的同时，局方将通过监督运营人的安全管理体系，逐步运用系统安全方法监督管理运营人整体安全状态。

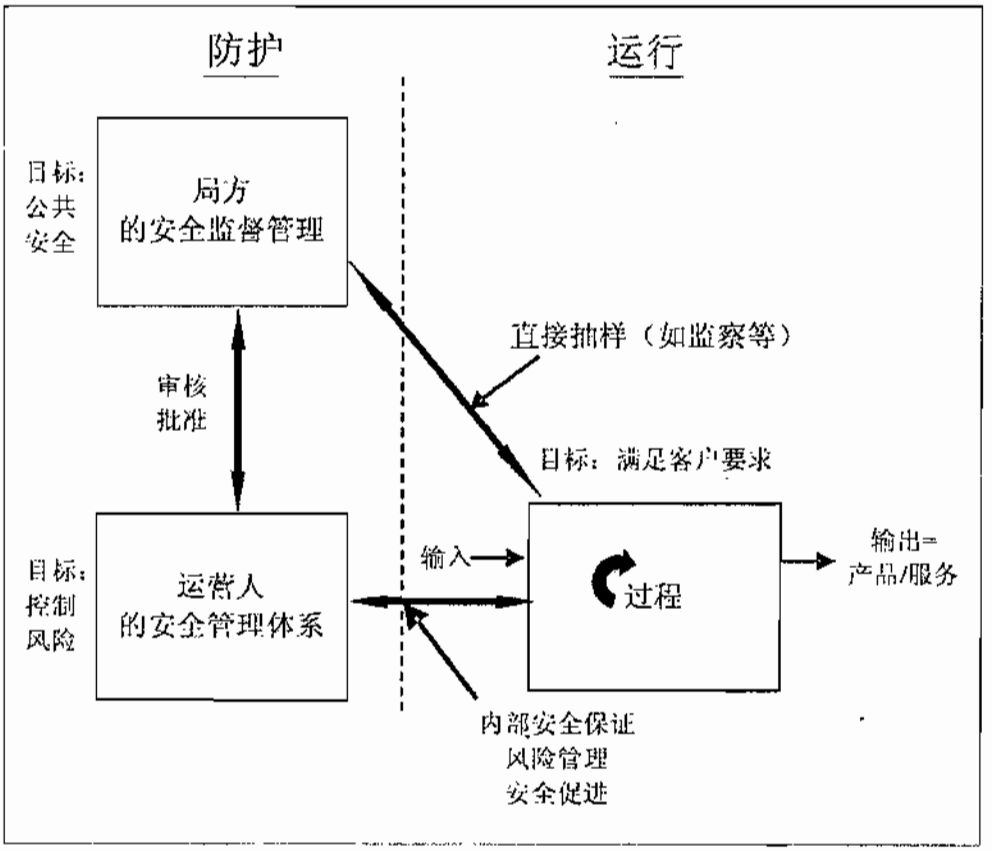

图 2　运营人的运行及防护功能与局方安全监督管理功能之间的关系

9.　《航空运营人安全管理体系要求》的几点说明

9.1 安全管理标准化的必要性

9.1.1 标准化

《要求》的制订参考了国际标准的条款结构，使用了与质量管理体系 ISO9001-2000 标准相似的模式，以便该体系与其他管理体系相互整合。

9.1.2 可审核性

《要求》以能够使组织本身、政府或其他第三方可用来进行审核的形式提出明确的功能要求。为了便于在系统审核时使用，《要求》尽最大可能使每一个条款都只单独规定一个要求。

9.2 结构和组成

9.2.1 功能性要求

由于需要适合各种类型和规模的运营人，所以《要求》是作为功能性要求文件制定的，它强调运营人应“做什么”而不是“怎么做”。这样可以为运营人的实施提供灵活性。

运营人在实施时应将《要求》中的要求转化成自己的具体做法。运营人应充分利用已经实施的各种安全管理过程，将安全管理体系的全部功能要求充分融入已有的管理体系之中，而不是重新建立一个独立的新体系。作为完整的安全管理体系，《要求》中的每一条功能要求都是必不可少的，但运营人不必对履行相同功能的现有项目重复建设。

9.2.2 安全管理体系的组成

安全管理体系的组成分为政策、风险管理、安全保证和安全促进四个部分。《要求》分四部分对各要素进行了功能性描述。

(1) 政策

所有的管理体系都必须明确政策、程序、组织结构以实现目标。其各要素的要求在《要求》中第 4 部分进行了描述。

(2) 风险管理

风险管理是将风险控制在可接受水平或其以下。其各要素的要求在《要求》中第 5 部分进行了描述。

(3) 安全保证

风险控制措施被确定后，运营人可利用安全保证功能，确保风险控制措施持续被执行并在不断变化的环境下持续有效。其各要素的要求在《要求》中第 6 部分进行了描述。

(4) 安全促进

运营人必须用支持良好安全文化的活动把安全作为核心价值进行促进。其各要素的要求在《要求》中第 7 部分进行了描述。

9.2.3 风险管理与安全保证的关系

风险管理与安全保证过程的关系见图 3。该图是功能关系图，而不是组织机构设置图。风险管理过程可用于初始的危险源识别和风险评价，当制定的风险控制措施能够使风险达到可接受水平时该措施就可被实施。此后，安全保证功能开始发挥作用，以确保风险控制措施被实施并持续达到预定目标。安全保证体系还可评估当运行环境变化时是否需要新的风险控制措施。

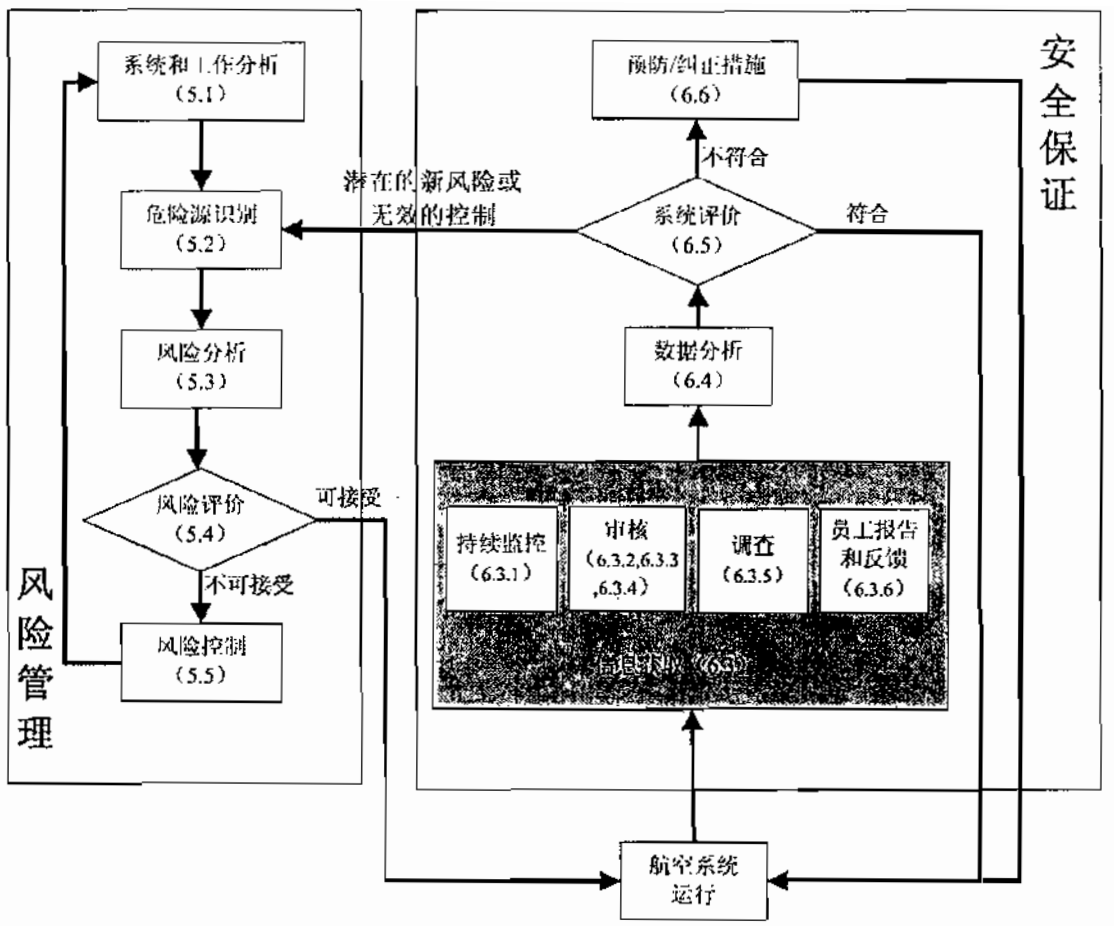

图 3 风险管理与安全保证功能的关系

10. 《航空运营人安全管理体系要求》的介绍

10.1 政策

10.1.1 安全政策

安全政策反映了运营人的安全管理理念以及对安全的承诺，是建立安全管理体系的基础，并为建设积极的安全文化提供了清晰的导向。

安全政策必须符合国家的相关规定，同时必须由最高管理者批准，并传达给全体员工。在制定安全政策的过程中，高层管理人员应与影响安全的相关领域的关键人员进行广泛地协商，以确保员工与安全政

策密切相关。

10.1.2 安全策划

安全策划是安全管理的一部分，致力于制定安全目标并具体规定必要的运行过程和相关资源以实现安全目标。

运营人在制定本单位的安全目标时，应注意：安全目标不应低于局方的要求；适合本单位的类型、规模和安全水平；是可测量的。

10.1.3 组织机构及职责

运营人应清晰地界定整个组织内的安全责任，包括高层管理人员的安全直接责任。最高管理者是安全管理的第一责任人，也是建立、实施并保持安全管理体系的最终责任人，应计划、组织、指导、控制员工的活动，分配安全相关活动所需的资源，以确保安全控制的有效性，并对整个组织的安全管理体系定期进行管理评审。虽然最高管理者必须对安全运行全面负责，但所有员工也都必须清楚自己的责任，并被准许参与安全事务。

安全总监作为建立、实施并保持有效的安全管理体系的负责人兼协调人，应独立于运行的组织和管理之外，直接向最高管理者汇报。

10.1.4 与法规和其他要求的符合性

法规和其他要求中的信息直接或间接影响运营人的安全管理体系，因此，运营人应建立正式的信息获取渠道，适时掌握现行有效的法规和其他要求，识别和了解运营人的安全管理体系受到相应法规和其他要求的影响，建立与安全相关法规和其他要求相符合的方法。

10.1.5 程序与控制

程序与控制是系统的两个关键属性。安全政策必须转化成程序以便应用，而且控制必须到位以保证关键步骤按设计完成。运营人应开

发程序、将程序文件化，并保持程序以落实安全政策、实现安全目标。《要求》还要求运营人确保员工理解自己的角色。而且，监查控制必须对程序的完成进行监视。

10.1.6 应急准备和响应

有效的应急响应方案可能会减轻事件和事故等不安全事件造成的后果，保证有序和有效地从正常运行过渡至紧急运行，并恢复至正常运行。应急响应方案以书面形式规定了不安全事件一旦发生后，运营人应该做些什么，以及每个行动由谁来负责。为了确保应急响应方案在实际运作时有效，应进行定期的训练和演练。进行演练还有助于验证方案的有效性，找出方案的不足，并进行改进。

10.1.7 文件及记录管理

文件的价值在于沟通意图、统一行动。因此，对文件的批准、评审与更新、标识、分发、作废等应进行控制，确保文件的适宜性、充分性和有效性。运行及安全管理中会生成大量的记录，这些记录可以提供符合要求和安全管理体系有效运行的证据。

安全管理手册（SMM）包括安全政策，安全目标，安全管理体系的要求，安全管理体系的程序和过程，安全管理体系的程序和过程所涉及的职责及权限，安全管理体系的程序和过程间的相互作用或接口。它是一个反映安全管理体系当前状态的、不断更新的文件，可以将运营人的安全管理做法传达给整个机构。

10.2 风险管理

风险管理过程常用于分析运营人的运行功能及其运行环境，以识别危险源，分析评价相关风险。风险管理过程处于运营人提供运输服务的过程中，不是一个独立的或特殊的过程。

10.2.1 系统和工作分析

风险管理始于系统设计。系统由组织结构、过程和程序，以及完成任务的人员、设备和设施构成。系统和工作分析应充分说明组成系统的硬件、软件、人员、环境相互间的影响，并详细到足以识别危险源和进行风险分析。系统需文件化，但没有特定的格式要求。系统文件一般包括运营人的手册系统、检查单、组织结构图和人员岗位说明等。运营人的运行及其支持过程建议分为：

(1) 飞行运行；

(2) 运行控制；

(3) 维修；

(4) 客舱安全；

(5) 地面服务；

(6) 货运；

(7) 训练等。

系统和工作分析只要详细到可用来进行危险源识别和风险分析即可，尽管有复杂的开发工具和方法可供使用，但是有管理者、监查人员和其他员工参加的简单的头脑风暴会议通常是更为有效的。

10.2.2 危险源识别

系统及其运行环境中存在的危险源必须被识别、记录和控制。确定危险源的分析过程应考虑系统的所有组成部分。在对系统及其运行的分析中，需要询问的关键问题是“如果……会发生什么?”。与系统和工作分析一样，问题的详尽程度应适当。尽管识别出每一个可能的危险源是不现实的，但运营人仍应在识别与其运行有关的重大的、可合理预见的危险源方面尽到应尽的责任。危险源样例参见表 1。

表 1　危险源样例

■ 航图中有些标注离所标注的点距离较远
■ 驾驶员持有现行有效的体检合格证，但执行飞行前其心理或生理状态较差
■ 航行情报发放现场的资料管理混乱
■ 装卸工缺乏危险品装卸知识
■ 机务维修人员遗忘工具
■ 搬运工装卸时装错舱位
■ 车辆在机坪超速行驶

10.2.3 风险分析和评价

风险分析和评价是采用传统的方法将风险分解为有害结果出现的可能性和该后果严重性。常用的工具是风险矩阵，图 4 是这种矩阵的一个样例。运营人应当建立一个最能体现其运行环境的矩阵，也可以为短期运行和长期运行分别建立具有不同风险接受标准的矩阵。

矩阵的定义和最终结构将由运营人自行设计。每个后果严重性和发生可能性等级的界定应以适用于具体运行环境的方式来确定，以保证每个运营人的决策工具与其运行和运行环境相关联。后果严重性和发生可能性等级界定的样例见表 2。各运营人对后果严重性和发生可能性等级的界定可以是定性的，但在可能的情况下，应尽量定量。

表 2　后果严重性和发生可能性等级界定的样例

后果严重性			发生可能性		
严重性等级	定义	参考值	可能性等级	定义	参考值
灾难性的	设备损毁。 多人死亡。	5	频繁的	可能会发生许多次	5
特别严重的	安全系数大大下降，身体压力或工作负荷已达到无法依靠操作人员精确或完全履行其任务的程度。 一定数量的人员严重受伤或死亡。 主要设备损坏。	4	偶尔的	可能会发生几次	4
严重的	安全系数明显下降，操作人员因工作负荷增加，或因影响其效率的条件，应付不利条件的能力下降。 严重事件。人员受伤。	3	极少的	不大可能，但或许会发生	3
轻微的	小麻烦；操作限制；启动应急程序；较小的事件。	2	不太可能的	很不可能发生	2
可忽略的	几乎没什么影响。	1	极不可能的	几乎不能想象事件会发生	1

运营人应制定风险接受程序，包括可接受标准以及风险管理决策中的权力和责任的分配。风险可接受程度可以使用风险矩阵（如图 4 所示）进行评估。示例矩阵说明了可接受程度的三个区域：不可接受的（黑色区域）、可接受的（白色区域）、缓解后可接受的（灰色区域）。

(1)　不可接受的（黑色区域）

如果风险处于黑色区域，则该风险是不可接受的，必须采取进一步干预行动来消除相关危险源，或控制可能导致更大风险（可能性或

严重性）的因素。

(2) 可接受的（白色区域）

如果风险处于白色区域，则该风险是可以接受的，不需进一步采取行动。但是，风险管理的目标应是无论评价显示风险是否在可接受范围内，都要将风险尽可能降至最低。这是持续改进的基本原则。

(3) 缓解后可接受的（灰色区域）

如果风险处于灰色区域，则在特定的缓解条件下该风险是可接受的。这种情况的一个例子就是对一个在最低设备清单中列明的失效航空器组件影响的评估。如果实施 MEL 中定义的操作（“O”）或维修（“M”）程序，就可使该风险从不可接受变为可接受，则制定 MEL 中的操作（“O”）或维修（“M”）程序就构成缓解行动。这些情况还应该在安全保证功能中持续特别地重点关注。

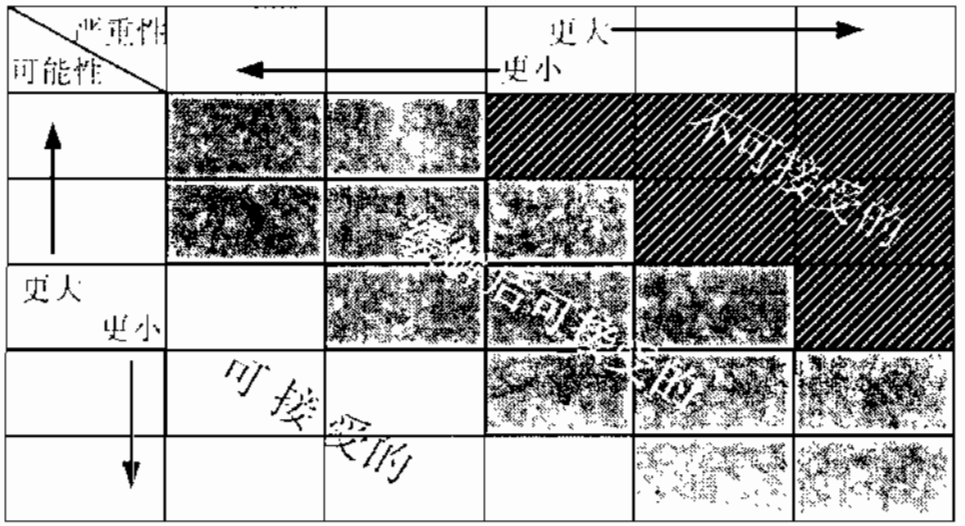

图 4 风险矩阵

其他一些风险评价工具也可用于飞行或运行的风险评价，如某些专业组织开发的用于飞行运行、运行控制和地面操作的风险评价方法。

10.2.4 原因分析

风险分析不仅应注重对严重性和可能性等级的界定，还应确定为何确定这些特定的等级。这也就是通常所说的“根原因分析”，这是制定有效控制措施，将风险降低至更低等级的第一步。一些已开发好的软件系统可用于进行根原因分析。然而在很多情况下，运营人的驾驶员、维修人员或签派员以及其他经验丰富的专家间进行的头脑风暴会议也是寻找降低风险途径的最有效和经济的方法。此方法的另外一个好处是可以使最终要去实施拟定的控制措施的员工参加到讨论会中。

10.2.5 风险控制

在完成以上步骤充分了解危险源和风险后，应进行风险控制措施的设计与实施。风险控制措施可以是增加或改变程序、增加新的监督控制措施、增加组织及软硬件的辅助、改进培训、增加或改装设备、调整人员或对系统所做的任何其他变化。

选择和设计控制措施的过程应以结构化的方式进行。系统安全技术和实践为我们提供了根据控制措施的有效性由高到低的分级方式。根据被彻查的危险源及其复杂程度，可采用的控制措施或策略可能不止一个。而且，根据必要措施的迫切性以及制定更有效措施的复杂性，可以在不同的时间实施这些控制措施。例如，在制定出更有效的危险源消除方法之前，先进行警告可能是十分恰当的。控制措施的分级包括:

(1) 从设计上消除危险源——修改系统（其中包括有危险源存在的硬件、软件系统和组织系统）;

(2) 物理防护或屏障——减少在危险源中的暴露或降低后果的严重性;

(3) 关于危险源的警告、通告或提示;

(4) 为避开危险源或降低相关风险可能性或严重性而做的程序修改;

(5) 为避开危险源或降低相关风险可能性而进行的培训。

即使采用了有效的控制措施，完全消除风险也几乎是不可能的。在这些控制措施设计完成后，系统投入使用前，必须评估控制措施是否有效及是否会对系统带来新危险源（后面这种情况被称为“衍生风险”）。图 3 中返回至图表顶端的环线指明可使用先前的系统和工作分析、危险源识别、风险分析和风险评价过程来确定经修改后的系统是否是可接受的。

10.3 安全保证

安全保证功能运用质量保证技术（包括内部审核和评估）判断设计于运营人的过程中的风险控制是否在被实施并按计划运行，以确保设计后的风险控制过程与要求持续符合，并在保持风险处于可接受水平内这一方面持续有效。这些保证功能也为持续改进打下了基础。质量保证技术是通过收集和分析客观证据，证实过程的要求是否已被满足。在安全管理体系中，体系的要求是基于对组织的运行或其生产的产品的风险的评价之上。

10.3.1 用以决策的信息

安全保证所使用的信息源很多，包括日常活动过程的持续监控，审核和评估，安全相关事件的调查，以及来自于员工安全报告和反馈系统的信息。由各种信息源在各运营人中都不同程度地存在，所以《要求》将每种信息源都写入信息获取中。这些信息源属于功能性要求，允许个别组织依据自身规模和类型进行调整。

10.3.2 持续监控

运营人应对运行数据进行持续监控。持续监控还提供了识别危险源、证实已采取的风险控制措施的有效性和持续评估系统绩效的方法。应监控的运行信息应来自于飞行记录器、值班日志、机组报告、工作卡、处理表单等。

10.3.3 生产运行部门内部审核

安全管理的主要责任落实在那些负责运营人技术过程的人员身上，技术过程是危险源直接出现的地方，是过程中的缺陷容易造成风险的地方，也是通过直接监管控制措施及资源分配能将风险降低至可接受水平的地方。因此，《要求》规定运营人各生产运行过程（图 1 和图 2 的运行这边）具有内部审核职责。内部审核可以为生产运行部门提供一种有计划的、有条理的评审和查证，其周期一般不应超过一年；当识别出不利趋势时，应及时增加专项审核。和其他要求一样，《要求》的审核要求是功能性的，审核可与组织的复杂程度相匹配。

(1) 管理者的责任

生产运行部门的经理对质量控制和确保其职责范围内的过程与设计一致直接负责。而且，生产运行部门拥有大量技术专家，对自己所在的技术过程最了解。因此，运营人应通过内部审核和评估大纲赋予生产运行部门经理监控这些过程、定期评价风险控制措施状况的职责。

(2) 审核工具

为促进体系的一体化，减少不必要的重复，运营人可考虑使用可用的技术系统的审核工具，例如局方的监察工具、第三方（如 IOSA）的工具。

10.3.4 内部评估

内部评估必须包含对运营人技术过程和安全管理体系特定功能的

评估。为此目的实施的审核必须由功能上独立于被评估的技术过程的个人或组织进行。通常内部评估可以由安全部门或最高管理者领导的其他下属机构来完成。对生产运行部门技术过程的评估可建立在生产运行部门内部审核基础上，除了对生产运行部门内部审核大纲的评估外，还应对其内部审核过程和结果进行评估和分析。内部评估需要审核及评估安全管理功能（政策制定、风险管理、安全保证及安全促进）。

内部评估的周期不应超过一年；当识别出不利趋势时，应及时增加专项评估。

10.3.5 外部审核

当有外部审核时，其审核结果也应作为信息输入进行分析、评价。对安全管理体系的外部审核可以由局方、独立的第三方、代码共享方或客户组织来进行。相对于运营人的内部审核，这些审核可以提供第二层保证系统。

10.3.6 调查

调查是一个以事故预防为目的过程，调查的结果也应作为信息输入进行分析、评价。调查应从关注找出“责任人”转向鼓励相关人员进行合作，找出系统和组织缺陷等信息。

10.3.7 员工安全报告和反馈系统

员工安全报告和反馈系统是获取信息的主要渠道之一。该系统不应只限于报告不安全事件，更应该用于报告安全相关问题。它还可帮助运营人识别运行中的危险源。

员工对报告系统的信任是保证所报告的数据的质量、精确度和实质性的基础。这种信任的建立可能需要较长的时间。但是，一旦这种信任遭到破坏就可能长期损害系统的有效性。要建立必要的信任，运

营人应在安全政策中鼓励员工报告，表明其对公开和自由地报告安全问题的态度，并明确说明可予接受或不可接受的工作表现，包括减免惩罚的条件。

10.3.8 分析和评价

只有将信息整理成为有意义的形式并得出结论，持续监控、审核、评估、调查和其他信息获取活动才能对管理起到作用。安全保证过程的首要目的是对风险控制措施的持续有效性进行评价。《要求》规定如果实施与控制措施有较大的偏离，应制定结构化、文件化的预防措施和纠正措施，使控制措施重回轨道。

10.3.9 纠正措施

安全保证过程应包括能保证对审核和评估发现的问题制定纠正措施，并校验其是否及时有效执行的程序。制定和实施纠正措施的职责应由被审核和评估证实存在问题的运行部门承担。如果发现新的危险源，应使用风险管理过程判断是否应制定新的风险控制措施。

10.3.10 监测环境

作为安全保证功能的一部分，分析和评估功能应能提醒组织注意运行环境的重大变化以及保持有效的风险控制所必需的系统改变需求。如图 3 所示，当这种情况出现时，根据评价的结果启动安全风险管理过程。

10.3.11 管理评审

最高管理者应按规定的时间间隔对风险管理的输出、安全保证的输出以及安全经验教训进行管理评审，评价是否需要改进运行过程和安全管理体系。管理评审的周期通常不应超过一年。

10.4 安全促进

即使机械地实施政策，运营人的安全努力仅靠强制命令无法获得成功。组织的文化将影响组织每个员工对待问题的态度和行为。组织的文化包括组织成员的价值观、信念、使命、目标和责任感。文化填补了组织政策、程序和过程的空隙，提供了安全努力方向的共识。

10.4.1 安全文化

文化包括心理的(人们如何思考、感受的)、行为的(人们或群体是如何行动、实施的)以及结构的(大纲、程序和组织机构)元素。尽管安全管理体系的政策、风险管理和安全保证部分中详细规定的许多过程为结构元素提供了框架，运营人还必须建立能让员工间及员工与管理层间进行沟通的渠道，尽全力就其目的、目标以及组织的行动和重大事件的现状进行沟通。同样，运营人应在开放的环境中提供自下而上的沟通手段。

10.4.2 沟通

系统安全理论强调“沟通文化”的重要性，组织必须尽全力培养员工为组织的知识库作贡献的意愿；系统安全理论强调“公正文化”的必要性，员工有信心当他们要对自己的行为负责任时，组织会公平对待他们。《要求》规定运营人必须提供员工沟通渠道以供员工及时提交安全缺陷的报告且不用担心受到报复。

《要求》规定运营人应保证所有人员完全了解安全管理体系、传达重要的安全信息、对为什么采取特殊的安全行动及为什么采取安全程序或对其进行修改做出解释。

10.4.3 培训

运营人应制定并保持安全培训大纲，保证人员得到相应的培训并能胜任履行安全管理体系的职责。

10.4.4 组织学习

组织安全文化的另一个原则是“学习文化”，如果不学习借鉴，那么报告、审核、调查、其他数据源内的信息是没有作用的。《要求》中已规定应对这些信息进行分析并与安全保证过程密不可分。《要求》中还规定应有一个分析过程、预防或纠正措施过程，以及当环境变化或识别出新危险源时，一个通向为了制定新安全控制措施的风险管理过程的渠道。《要求》进一步规定运营人向相关人员提供风险控制措施和安全经验教训的培训和沟通。

附录　航空运营人安全管理体系要求

1. 目的

本《要求》为运营人建立安全管理体系提供一个统一的要求。

2. 范围及适用性

(1) 本《要求》适用于运营人建立和实施安全管理体系。

(a) 本《要求》用于与运行和支持过程以及活动有关的航空安全，而不是职业健康安全、环境保护或服务质量。

(b) 运营人对外委的或购买的其他单位的服务或产品的安全负有责任。

(2) 本《要求》是可接受的最低要求。

3. 备用

4. 政策

4.1 总要求

(1) 安全管理应融入运营人的整个体系内，包括：

(a) 飞行运行；

(b) 运行控制；

(c) 维修；

(d) 客舱安全；

(e) 地面服务；

(f) 货运；

(g) 训练等。

(2) 安全管理体系过程应被:

(a) 文件化;

(b) 监控;

(c) 测量;

(d) 分析。

(3) 安全管理体系输出应被:

(a) 记录;

(b) 监控;

(c) 测量;

(d) 分析。

(4) 运营人应促进积极安全文化的建设(见 4.2 和 7.1)。

4.2 安全政策

(1) 最高管理者应确定运营人的安全政策。

(2) 安全政策应:

(a) 包括实施安全管理体系的承诺;

(b) 包括持续改进安全水平的承诺;

(c) 包括对风险进行管理的承诺;

(d) 包括遵守适用的法规要求的承诺;

(e) 包括鼓励员工进行安全问题报告且不受到报复的承诺;

(f) 包括不安全事件调查时注重识别系统和组织缺陷的承诺;

(g) 包括为安全政策的实施提供必要的人力和财务资源的明确声明;

(h) 建立清晰的可接受行为规范;

(i) 为设定安全目标提供管理指导;

(j) 为评审安全目标提供管理指导;

(k) 形成正式文件;

(l) 与全体员工和责任方进行沟通;

(m) 定期评审，以确保政策与组织相关和适宜;

(n) 明确管理层和员工在安全绩效方面的职责。

4.3 质量政策

最高管理者应确保运营人的质量政策与安全管理体系一致。

4.4 安全策划

运营人应建立并保持安全管理计划以实现安全目标。

4.5 组织机构及职责

4.5.1 最高管理者

(1) 最高管理者应是安全管理体系的最终负责人。

(2) 最高管理者应提供实施、保持安全管理体系的必要资源。

4.5.2 安全总监

最高管理者应任命一名独立于运行及其支持过程的安全总监,其应具备下列职责和权限:

(1) 确保建立、实施、保持安全管理体系需要的过程;

(2) 直接向最高管理者报告安全管理体系绩效和改进需求;

(3) 确保提高整个组织内对安全要求的认识。

4.5.3 安全相关的岗位、职责和权限

安全相关的岗位、职责和权限:

(1) 应被明确规定;

(2) 应文件化;

(3) 应在整个组织内得到沟通。

4.6 与法规和其他要求的符合性

(1) 安全管理体系应具有与安全相关法规和其他要求相符合的方法。

(2) 运营人应建立并保持程序以识别适用于安全管理体系的现行安全相关法规和其他要求。

4.7 程序与控制

(1) 运营人应建立并保持含有测量标准的各种程序以实现安全政策的目标。

(2) 运营人应建立并保持过程控制措施，以确保与安全相关的运行和活动遵守程序。

4.8 应急准备和响应

运营人应建立程序以:

(1) 识别潜在的事故和事件;

(2) 协调、策划运营人对事故和事件的响应;

(3) 对运营人的响应进行定期演练。

4.9 文件及记录管理

4.9.1 总则

运营人应以书面或电子形式建立并保持信息，以描述:

(1) 安全政策;

(2) 安全目标;

(3) 安全管理体系的要求;

(4) 安全相关的程序和过程;

(5) 安全相关的程序和过程的职责及权限;

(6) 安全相关的程序和过程间的相互作用或接口;

(7) 安全管理体系的输出。

4.9.2 安全管理手册

运营人应建立并保持安全管理手册，内容包括:

(1) 安全政策;

(2) 安全目标;

(3) 安全管理体系的要求;

(4) 安全管理体系的程序和过程;

(5) 安全管理体系的程序和过程的职责及权限;

(6) 安全管理体系的程序和过程间的相互作用或接口。

4.9.3 文件管理

(1) 文件应是:

(a) 易读的;

(b) 有日期标识的（包含修订日期）;

(c) 易于识别的;

(d) 有序保存的;

(e) 按运营人规定的期限进行保留，适用时，期限应经监管机构批准。

(2) 运营人应建立并保持程序，控制本《要求》所要求的所有文件，以确保:

(a) 文件易于查找;

(b) 文件:

① 被定期评审;

② 必要时进行修订;

③ 取得授权人员对其充分性的批准。

(c) 相关文件的最新版本可在所有会影响安全管理体系有效运转的运行实施场所获得;

(d) 过期文件应立即从所有正在使用的场所中收回，或采取其它措施防止误用。

4.9.4 记录管理

(1) 对于安全管理体系记录，运营人应建立并保持以下方面的程序:

(a) 标识;

(b) 维护;

(c) 处置。

(2) 安全管理体系记录应是:

(a) 易读的;

(b) 可识别的;

(c) 可追溯到实际相关活动的。

(3) 安全管理体系记录应按能达到下列要求的方式保持:

(a) 易找到的;

(b) 被保护的，以防:

① 损坏;

② 变质;

③ 丢失。

(4) 记录的保存期限应文件化。

5. 风险管理

(1) 风险管理应至少包括下列过程:

(a) 系统和工作分析;

(b) 危险源识别;

(c) 风险分析;

(d) 风险评价;

(e) 风险控制。

(2) 风险管理过程应被用于:

(a) 系统、组织和产品的初始设计;

(b) 运行程序的制定;

(c) 安全保证功能(如 6 中所述)识别出的危险源;

(d) 对运行过程的有计划的变更,以识别与这些变更相关的危险源。

(3) 运营人应建立与本《要求》6中所述的安全保证功能间的反馈环以评估风险控制措施的有效性。

(4) 运营人应确定风险可接受和不可接受的水平。

(a) 应建立下列方面的描述:

① 严重性等级;

② 可能性等级。

(b) 运营人应明确各管理层对风险可接受决策的权限;

(c) 运营人在制定和实施风险控制或缓解计划时,应为危险源明确短期内存在的可接受的风险。

(5) 除非每个识别出的危险源的风险被判定为是可接受的,否则,以下内容不得实施:

(a) 新的系统设计;

(b) 现有系统设计的更改;

(c) 新的作业或程序;

(d) 更改后的作业或程序。

(6) 风险管理过程不应妨碍运营人采取缓解现有风险的临时应急措施。

5.1 系统和工作分析

(1) 系统和工作描述应详细到足以识别危险源的程度。

(2) 系统和工作分析应考虑以下方面:

(a) 本系统与航空运输系统中的其他系统(如机场、空管等)间的相互作用;

(b) 本《要求》 4.1 (1)中的各领域的系统功能;

(c) 为完成本《要求》 5.1 (2) (b)中功能所需的员工工作;

(d) 在下列系统中必要的人的因素的考虑:

① 运行;

② 维修;

(e) 系统的硬件部分;

(f) 系统的软件部分;

(g) 为系统运行和使用提供指南的有关程序;

(h) 外界环境;

(i) 运行环境;

(j) 维修环境;

(k) 外委的和购买的产品和服务;

(l) 本《要求》5.1(2)的(b)-(j)各项的相互影响;

(m) 有关下列内容的任何假设:

① 系统;

② 系统的相互影响;

③ 现有的风险控制措施。

5.2 危险源识别

(1) 危险源应:

(a) 根据系统描述，在整个系统范围内进行识别;

(b) 文件化。

(2) 危险源信息应是:

(a) 可追溯的;

(b) 在整个风险管理过程中始终被管理。

5.3 风险分析

风险分析过程应包括:

(1) 现有的风险控制措施;

(2) 启动机制;

(3) 现有危险源的合理可能后果的风险，包括对下列方面的估计:

(a) 可能性;

(b) 严重性。

5.4 风险评价

(1) 各危险源的风险可接受性应使用本《要求》5 (4)中描述的风险可接受标准进行评价。

(2) 运营人应明确各管理层对风险可接受决策的权限。

5.5 风险控制

(1) 应为每个具有不可接受风险的危险源确定风险控制或缓解计

划；

(2) 风险控制措施应：

(a) 明确描述；

(b) 经过评估确保相关要求已被满足；

(c) 与其运行环境相适宜；

(d) 文件化。

(3) 在制定风险控制措施或缓解措施时应对衍生风险进行评价。

6. 安全保证

6.1 总要求

运营人应监测其各系统和运行以：

(1) 识别新危险源；

(2) 测量风险控制措施的有效性；

(3) 确保符合规章要求。

6.2 系统描述

安全保证功能应基于本《要求》5.1中的整体系统描述。

6.3 信息获取

运营人应收集证明运营人以下方面有效所必需的数据：

(1) 运行过程；

(2) 安全管理体系。

6.3.1 持续监控

(1) 运营人应监控运行数据（如：飞行记录器、值班日志、机组报告、工作卡、处理表单或来自于员工安全报告和反馈系统的报告）以：

(a) 评价与风险控制措施的符合性（如 5 中所描述的）；

(b) 测量风险控制措施的有效性（如 5 中所描述的）;

(c) 评价系统绩效;

(d) 识别危险源。

(2) 运营人应监控来自外委方的产品和服务。

6.3.2 生产运行部门内部审核

(1) 各生产运行部门经理应确保对运行过程（生产系统）的安全相关功能进行定期的内部审核，此职责应延伸至完成这些功能所涉及的任何外委方。

(2) 各生产运行部门经理应确保实施定期审核以:

(a) 确定与风险控制措施的符合性;

(b) 评价风险控制措施的绩效。

(3) 制定审核大纲应考虑:

(a) 被审核过程的安全重要性;

(b) 以前审核的结果。

(4) 审核大纲应包括:

(a) 审核的:

① 标准;

② 范围;

③ 频次;

④ 方法。

(b) 选择审核员的过程;

(c) 审核员不能审核自己工作的要求;

(d) 形成文件的程序，程序中包括:

① 职责;

② 关于下列内容的要求:

(i) 策划审核;

(ii) 实施审核;

(iii) 上报结果;

(iv) 保持记录。

(e) 对外委方和供应商的审核。

6.3.3 内部评估

(1) 运营人应按策划的时间间隔对运行过程和安全管理体系进行内部评估，以确保安全管理体系符合相关要求。

(2) 制定评估大纲应考虑:

(a) 被审核过程的安全重要性;

(b) 以前审核的结果。

(3) 评估大纲应包括:

(a) 评估的:

① 标准;

② 范围;

③ 频次;

④ 方法。

(b) 选择审核员的过程;

(c) 审核员不能审核自己工作的要求;

(d) 形成文件的程序，程序中包括:

① 职责;

② 对下列内容要求:

(i) 策划审核;

(ii) 实施审核;

(iii) 上报结果;

(iv) 保持记录。

(e) 对外委方和供应商的审核。

(4) 评估大纲应受最高管理者或安全总监的控制。

(5) 评估大纲应包括对本《要求》6.3.2中要求的大纲的评估。

(6) 对生产运行部门实施评估的个人或组织必须功能上独立于被评估部门。

6.3.4 安全管理体系外部审核

运营人应将外部审核方的审核结果纳入本《要求》6.4中的数据分析。

6.3.5 调查

(1) 运营人应收集以下数据:

(a) 事件;

(b) 事故。

(2) 运营人应建立下列程序:

(a) 调查事故;

(b) 调查事件;

(c) 调查潜在的不符合规章事件。

6.3.6 员工安全报告和反馈系统

(1) 运营人应建立并保持一个为报告人保密的员工安全报告和反馈系统(如7.1(5)中所述)。

(2) 员工应被鼓励使用员工安全报告和反馈系统(如4.2(2)(e)中

所述），且不会受到报复。

(3) 应监控来自员工安全报告和反馈系统的数据，以识别正在显露的危险源。

(4) 员工安全报告和反馈系统中收集的数据应被纳入本《要求》6.4的数据分析。

6.4 数据分析

(1) 运营人应分析本《要求》6.3所获得的数据，以证明以下方面的有效性:

(a) 运行过程中的风险控制措施;

(b) 安全管理体系。

(2) 通过数据分析，运营人应评估可从何处对以下方面进行改进:

(a) 运行过程;

(b) 安全管理体系。

6.5 系统评价

(1) 运营人应评价以下方面的绩效:

(a) 运行过程的安全相关功能相对于其要求;

(b) 安全管理体系相对于其要求。

(2) 系统评价应得出下列结论:

(a) 符合现行的风险控制措施或安全管理体系要求（包括规章要求）;

(b) 不符合现行的风险控制措施或安全管理体系要求（包括规章要求）;

(c) 发现的新危险源。

(3) 当评价发现有下列必要时，应启动风险管理过程：

(a) 新危险源的识别；

(b) 需要对系统进行变化。

(4) 运营人应按本《要求》4.9中的要求，保存评价记录。

6.6 预防措施和纠正措施

(1) 适当时，运营人应制定并按优先级实施：

(a) 对识别出的与风险控制措施不符合问题的纠正措施；

(b) 对识别出的与风险控制措施潜在不符合问题的预防措施。

(2) 在开展以下措施时，应考虑安全经验教训：

(a) 纠正措施；

(b) 预防措施。

(3) 运营人应基于调查发现的问题采取必要的纠正措施。

(4) 运营人应及时确定优先级并实施纠正措施。

(5) 运营人应及时确定优先级并实施预防措施。

(6) 应依据已建立的记录保存政策，对纠正和预防措施的实施和状态的记录进行保存。

6.7 管理评审

(1) 最高管理者应按规定的时间间隔对安全管理体系进行评审，包括：

(a) 风险管理的输出(第 5 部分)；

(b) 安全保证的输出(第 6 部分)；

(c) 安全经验教训(第 7.5 条)。

(2) 管理评审应包括评价运营人的以下方面是否需要改进：

(a) 运行过程;

(b) 安全管理体系。

6.8 持续改进

运营人应通过使用安全和质量的政策、目标、审核和评估结果、数据分析、预防纠正措施、管理评审等，持续改进安全管理体系和风险控制措施的有效性。

7. 安全促进

7.1 安全文化

最高管理者应通过以下方式，促进积极安全文化的成长:

(1) 发布向全体员工声明的高层管理人员对安全的承诺;

(2) 高层管理人员履行安全管理体系承诺的具体事例证明;

(3) 组织内人员安全责任沟通;

(4) 与全体员工就安全政策、目标、标准和绩效进行清晰、定期的沟通;

(5) 建立有效的、必要时可为报告人保密的员工安全报告和反馈系统;

(6) 使用能够提供易用且高效的信息获取手段的安全信息系统;

(7) 实施和保持安全管理体系所必要的资源的配置。

7.2 沟通与获知

(1) 适当时，运营人应向员工沟通安全管理体系输出。

(2) 运营人应依据法律法规或协议的要求，向有关机构提供获得其安全管理体系输出的渠道。

7.3 人员能力要求

(1) 运营人应将本《要求》4.5.3中的岗位的人员能力要求形成文件。

(2) 运营人应确保在本《要求》4.5.3中列出的岗位上的人员符合能力要求。

7.4 培训

运营人应制定并保持安全培训大纲，针对本《要求》4.5.3中的人员进行培训。

(1) 培训应包括:

(a) 初始培训;

(b) 复训。

(2) 员工应接受与他们的下列方面相对应的培训:

(a) 责任的等级;

(b) 对运营人的产品或服务的安全影响。

(3) 为保证培训现行有效，培训应定期进行:

(a) 评审;

(b) 更新。

7.5 安全经验教训

(1) 运营人应开发整理安全经验教训。

(2) 安全经验教训应被用于促进持续的安全改进。

(3) 运营人应沟通安全经验教训。