

ICS 13.110

CPI

E 92

团体标准

T/CPI XXXX—2023

石油钻采设备设计安全技术规范

Safety Technical Specification for Design of Petroleum
Drilling and Production Equipment

(征求意见稿)

202X-XX-XX 发布

202X-XX-XX 实施

中国石油和石油化工设备工业协会

目 次

前 言..... III

引 言..... IV

1 范围.....5

2 规范性引用文件.....5

3 术语和定义.....5

4 石油钻采设备安全设计的风险评估和风险减小策略..... 8

 4.1 总则..... 8

 4.2 风险评估和风险减小的策略.....8

 4.3 采用评估组方式..... 12

5 风险评估.....13

 5.1 概述..... 13

 5.2 风险评估信息..... 13

 5.3 石油钻采设备限制的确定..... 14

 5.4 危险识别..... 15

 5.5 风险估计..... 16

 5.6 风险评价..... 16

6 安全要求和风险减小措施.....17

 6.1 风险减小原则..... 17

 6.2 本质安全设计措施..... 18

 6.3 防护装置和保护装置的选择和使用.....26

 6.4 防护装置和保护装置的设计要求.....30

 6.5 通过安全防护减少排放.....32

 6.6 补充保护措施..... 32

 6.7 安全要求和风险减小措施的符合性验证.....34

 6.8 可容许风险的实现..... 34

7 使用信息.....35

 7.1 起草使用信息..... 35

 7.2 预定使用信息..... 35

 7.3 使用信息的形式.....36

 7.4 使用信息的位置和属性.....36

 7.5 信号和警告装置.....36

 7.6 标志、符号（象形图）和书面警告.....36

 7.7 随行文件..... 37

8 风险评估和风险减小的文件..... 39

9 采用合适的产品安全标准.....39

 9.1 概述..... 39

 9.2 遵循的步骤..... 40

参 考 文 献.....	42
--------------	----

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。

本文件由中国石油和石油化工设备工业协会提出并归口。

本文件起草单位：大庆石油管理局有限公司装备制造分公司、大庆油田有限责任公司、烟台杰瑞石油装备技术有限公司、苏州道森钻采设备有限公司、上海神开石油设备有限公司、渤海石油装备制造有限公司研究院、北京石油机械有限公司、中海油研究总院有限责任公司钻采研究院、宝鸡石油机械有限责任公司、大庆油田采油工艺研究院。

本文件主要起草人：王敬平、宋艳春、高大鹏、金岩松、贾子凯、陈晶、彭芳庆、姜磊、陈健、董思、袁浩天、孟静宇、靳明恂、张树立、崔启利、裘伟斌、詹良斌、金祖国、邹祥城、李德伟、周家齐、杨向前、孙娟、钱坤、赵怀洲、邵宏宇、李春龙

本文件为首次发布。

引 言

本文件的目的是为石油钻采设备的设计者提供框架和决策指南，使其在开发阶段能够设计出在预定使用范围内具备安全性的石油钻采设备。本文件也为标准制定者提供一种策略，以便制定一致和适当的专业安全标准。

石油钻采设备安全的概念考虑了在风险已被充分减小后，在其生命周期内执行其预定功能的能力。本文件是石油钻采设备安全标准体系中的基础标准，石油钻采设备安全标准体系的结构如下：

石油钻采设备基础安全标准，给出适用于所有石油钻采设备的基本概念设计原则和一般特征；

石油钻采设备通用安全标准，涉及石油钻采设备的一种安全特征或使用范围较宽的一类安全装置，包括特定的安全特定（如安全距离、表面温度、噪声等）标准；安全装置（如双手操控装置、联锁装置、压敏装置、防护装置等）标准；

石油钻采设备安全专业标准（本文件中的产品安全标准），对一种特定的石油钻采设备或一组石油钻采设备规定出详细的安全要求的标准。

当石油钻采设备安全专业标准的内容与本文件或者其他通用安全标准的一个或多个技术规定不一致时，以石油钻采设备安全专业标准的技术规定为准。

本文件从设计者角度，提供石油钻采设备整体设计策略，使石油钻采设备设计能够充分地减小风险，使其达到可接受的水平，同时本文件并未对一种特定的设备或一组设备的详细安全要求予以规定。

石油钻采设备设计安全技术规范

1 范围

本文件规定了石油钻采设备设计过程中需进行的风险评估和评价，安全要求和风险减小措施，以及验证方法等内容。

本文件适用于石油钻采设备的设计。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

石油钻采设备 petroleum drill and production equipment

用于对陆地和海洋的石油、天然气等开采所需的专用设备。包括石油、天然气钻采专用设备及石油钻采工具及配件，本文件中提到的设备指石油钻采设备。

3.2

安全 safety

除去不可接受风险的状态。

注1：改写自GB/T 20002.4—2015 的定义。

3.3

危险 hazard

潜在的伤害源。

注2：可由其起源（例如：石油钻采设备机械危险和电气危险），或其潜在伤害的性质（例如：电击危险、切制危险、中毒危险和火灾危险）进行限定。

注3：本定义中的危险包括在设备的预定使用期间，始终存在的危险（例如：危险运动部件的运动、焊接过程中产生的电弧、不利于健康的姿势、噪声排放，高温等）和意外出现的危险（例如：爆炸、意外启动引起的挤压危险、破裂引起的喷射、加速减速引起的坠落等）。

3.4

重大危险 significant hazard

已识别为相关危险，需要设计者根据风险评价采用特殊方法去消除或减小的风险。

3.5

危险事件 zard

能够造成伤害的事件。

注4：危险事件的发生过程可以是短时间的，也可以是长时间的。

3.6

风险 risk

伤害发生的概率与伤害严重程度的组合。

3.7

剩余风险 residual risk

采取设计保护措施之后仍然存在的风险。

注5：本文件区分了设计者采取保护措施后的剩余风险和已采取所有的保护措施后仍然存在的剩余风险。

3.8

风险估计 risk estimation

确定伤害可能达到的严重程度和伤害发生的概率。

3.9

风险分析 risk analysis

石油钻采设备限制的确定、危险识别和风险估计的组合。

3.10

风险评价 risk evaluation

以风险分析为基础，判断是否已达到减小风险的目标。

3.11

风险评估 risk assessment

包括风险分析和风险评价在内的全过程。

3.12

保护措施 protective measure

用于实现风险减小的措施。

3.13

本质安全设计措施 inherently safe design measure

通过改变石油钻采设备设计，而不是使用防护装置或保护装置来消除危险或减小与危险相关的风险保护措施。

3.14

安全防护 safeguarding

使用安全防护装置保护人员的措施，使人员远离那些不能合理消除的危险或者通过本质安全设计措施无法充分减小的风险。

3.15

使用信息 information for use

由信息载体（如文本、文字、标记、信号、符号、图表）组成的保护措施，可单独或组合使用这些载体向使用者传递信息。

3.16

可合理预见的误用 reasonably foreseeable misuse

不是按设计者预定的方法而是按照常理可预见的人类习惯来使用设备。

3.17

安全防护装置 safeguard

防护装置或保护装置。

3.18

固定式防护装置 fixed guard

以一定方式（如采用螺钉、螺母、焊接）固定的，只能使用工具或破坏其固定方式才能打开或拆除的防护装置。

3.19

活动式防护装置 movable guard

不使用工具就能打开的防护装置。

3.20

连锁防护装置 interlocking guard

与连锁装置联用的防护装置，同石油钻采设备控制系统一起实现以下功能：

- a) 在防护装置关闭前，其“遮蔽”的危险的设备功能不能执行；
- b) 在危险设备功能运行时，如果打开防护装置，则发出停机指令；
- c) 在防护装置关闭后，防护装置“遮蔽”的危险的设备功能可以运行。防护装置本身的关闭不会启动危险设备功能。

3.21

带防护锁定的连锁防护装置 interlocking guard with guard locking

与连锁装置、防护锁定装置联用的防护装置，同石油钻采设备控制系统一起实现以下功能：

- a) 在防护装置关闭和锁定前，其“遮蔽”的危险的设备功能不能执行；
- b) 在防护装置“遮蔽”的危险的设备功能所产生的风险消失之前，防护装置保持关闭和锁定状态；
- c) 在防护装置关闭和锁定后，被防护装置“遮蔽”的危险的设备功能可以运行。防护装置本身的关闭和锁定不会启动危险设备功能。

3.22

带启动功能的连锁防护装置 interlocking guard with a start function

带控制功能的防护装置 control guard

特殊连锁防护装置，一旦其到达关闭位置，便发出触发石油钻采设备危险功能的命令，无需使用单独的启动控制。

3.23

保护装置 protective device

防护装置以外的安全防护装置。

3.24

联锁装置 interlocking device

联锁 interlock

用于防止危险设备功能在特定条件下(通常是指只要防护装置未关闭)运行的机械、电气或者其他类型的装置。

3.25

限制装置 limiting device

防止石油钻采设备或危险设备状态超过设计限度(如空间限度、压力限度、荷载力矩限度等)的装置。

3.26

失效 failure

产品完成要求功能能力的中断。

4 石油钻采设备安全设计的风险评估和风险减小策略

4.1 一般要求

石油钻采设备设计应遵循计划阶段、方案设计阶段、技术设计阶段等三个流程,所有阶段应考虑安全因素,在确保安全运行以及操作人员安全的前提下进行设计。石油钻采设备安全设计旨在对各种各样的设备的复杂性以及潜在危害方面进行风险评估,风险评估的目的是识别危险、估计和评价风险、以便能减小风险。只要采取了从危险识别到风险减少的系统方法,即考虑了所有风险要素。在设计阶段对设备进行更改并采取相应安全措施,更为经济和有效。

4.2 风险评估和风险减小的策略

4.2.1 石油钻采设备在进行安全设计时,在设计计划阶段、方案计划阶段、技术设计阶段等设计过程中进行风险评估和风险减小,设计完成后在每个设计阶段进行重复迭代。

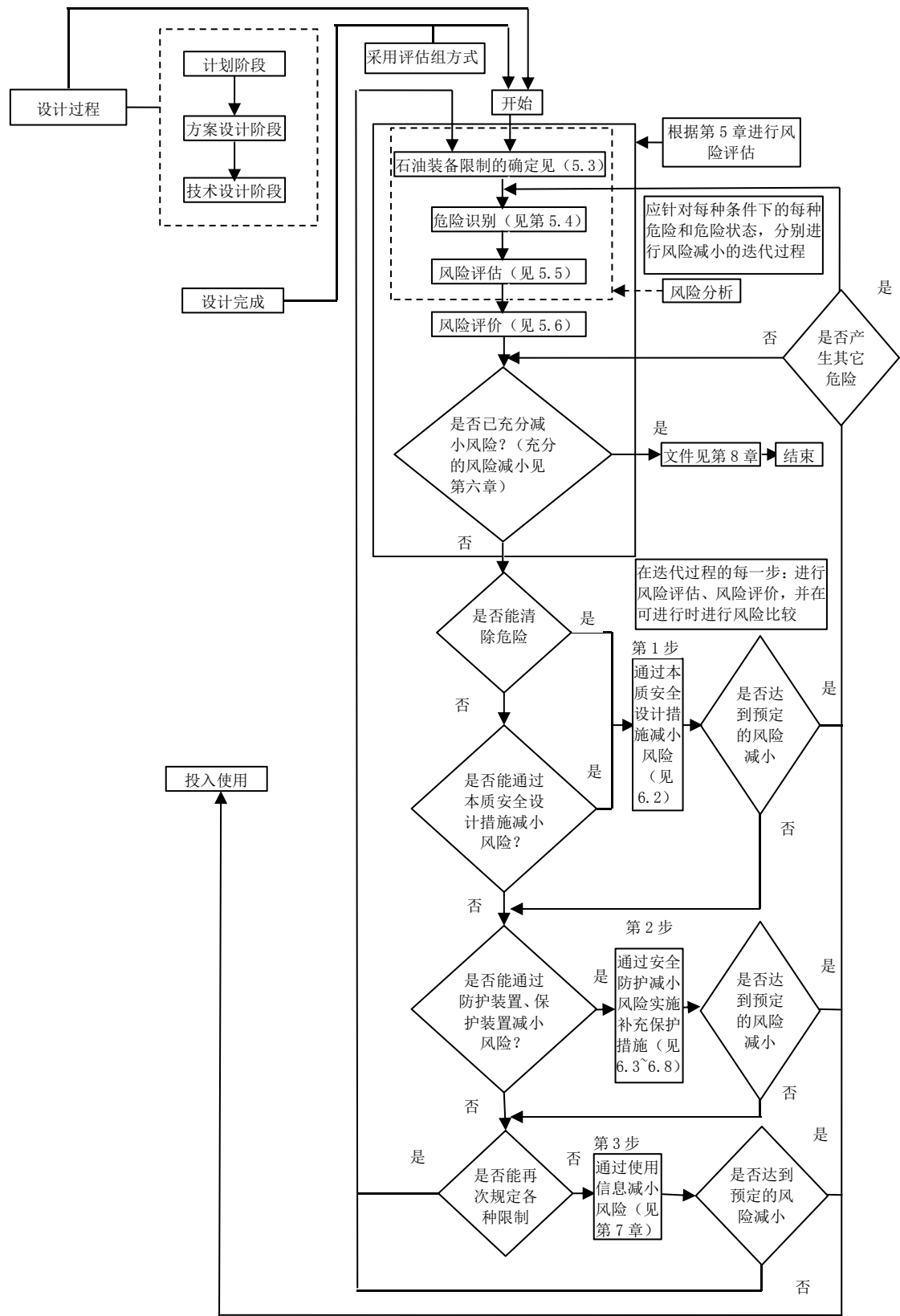
a) 在设计完成后进行风险评估和风险减小,并按下列顺序依次采取措施(见图1)。

- 1) 确定设备的各种限制,包括预定使用 and 任何可合理预见的误用;
- 2) 识别危险及其伴随的危险状态;
- 3) 对每一种识别出的危险和危险状态进行风险估计;
- 4) 评价风险并决定是否需要减小风险;
- 5) 采取保护措施消除危险或减小危险伴随的风险措施。

b) 当设计的石油钻采设备可以使用相似设备的经验时,设计者可以依次采取以下措施:

- 1) 确定相似设备的限制和设计用途;
- 2) 确定相似设备的危险和危险情况;
- 3) 为每个危险和危险情况估计风险;

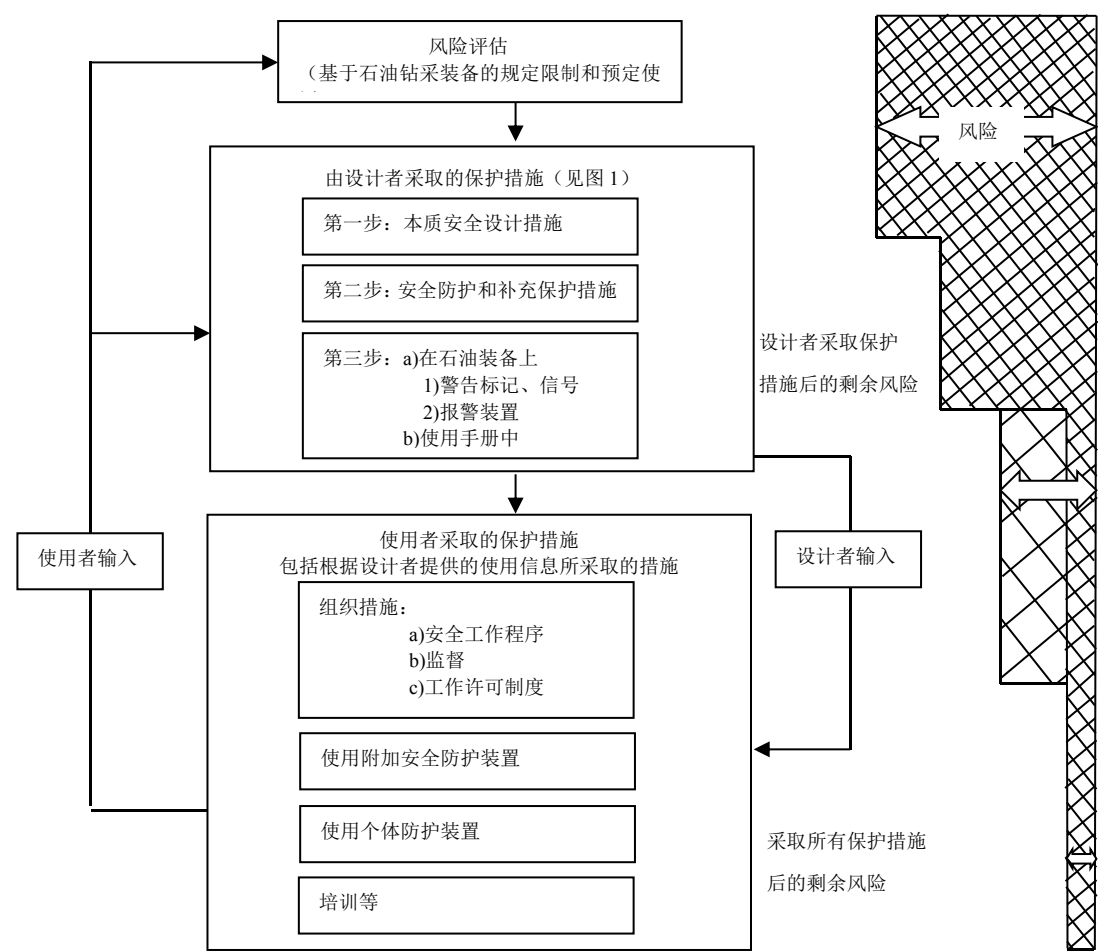
- 4) 对设备进行风险评估，做出风险减小的决定；
- 5) 通过保护措施消除危险或减小风险。



*用初始风险评估结果回答初次问题

图 1 石油钻采设备安全设计风险减小过程迭代三步法

4.2.2 风险评估是以系统方法对与石油钻采设备有关的风险进行分析和评价的一系列逻辑步骤。必要时，风险评估之后需要进行风险减小。为了尽可能通过采取保护措施消除危险或充分减小风险，有必要重复进行该过程。假如设备上存在危险且不采取保护措施，则迟早会造成伤害。GB/T 15706—2012 附录 B 给出了危险的示例。保护措施是设计者和使用者根据图 2 所采取的措施的组合。在设计阶段采取的措施优于在使用阶段由使用者采取的措施，而且通常更有效。



*提供合适的使用信息是设计者从设计角度减小风险的一个步骤，但其相关的保护措施只有在使用者实施后才能发挥作用。

*用户输入是指设计者从预定使用石油钻采设备的一般或特殊用户群体得到的信息。

*使用者采用的各种保护措施是没有层次之分的。这些保护措施不在本文件范围之内。

*这类装置用于机器预定使用没有预见的特殊工艺，或者设计者不能控制的特殊安装条件。

图 2 通过设计减小风险的过程

4.2.3 为了最大程度的减小风险，应考虑下述四种因素。图 1 中的流程图表示了本章规定的策略。过程本身是迭代的，并且为了达到减小风险的目的，应充分利用现有技术连续数次应用该过程。实施该过程时，应按下列优先次序考虑这四种因素：

a) 设备在生命周期所有阶段内的安全；

- b) 设备执行其功能的能力;
- c) 设备的易用性;
- d) 制造、使用和拆卸设备的成本。

注1:对这些原则的最佳应用需要掌握石油钻采设备的使用、事故历史和健康记录、可用的风险减小技术以及有关设备使用的法律体制方面的知识。

注2:当技术发展后出现了风险更低的等效石油钻采设备设计,则在特定时间内可接受的设备设计可能不再合理。

4.3 采用评估组方式

4.3.1 一般要求

组成评估组进行风险评估通常是比较彻底和有效的。随着下列条件的不同,评估组的规模也不同:

- a) 选择的风险评估方法;
- b) 石油钻采设备的复杂程度;
- c) 使用石油钻采设备的过程。

评估组应由具备不同学科知识、各种经验和专业技能的专家组成。但是,评估组太大可能会导致难以保持意见一致或达成共识。根据具体问题所要求的专业技能不同,风险评估过程中评估组的组成可以有变化。宜明确实施项目的评估组领导,因为风险评估的成功与否取决于其技能。风险估计应由一个团队完成并且达成共识,不同的团队针对相似的情况的分析所形成的详细结果不一定完全相同。然而,实际工作中不一定总是要建立风险评估组,因为有些石油钻采设备的危险已被充分认知。

注3:通过咨询其他具有如 4.3.2 所述的知识和专业技能的人员,并通过另外的合格人员对风险评估的检查,能够提高该风险评估结果的可信度。

4.3.2 评估组成员的组成和作用

评估组宜有组领导,组领导宜保证对进行风险评估的符合第 8 章要求的在计划中、执行过程中和编制的文件中涉及的所有任务全面负责,并将评估结果和(或)建议报告给合适的人员。

宜根据风险评估需要的技能和专业知识选择评估组成员。评估组中宜包括下列人员:

- a) 能回答关于石油钻采设备设计和功能方面技术问题的人员;
- b) 具备石油钻采设备操作、调试、保养、维修等实际经验的人员;
- c) 了解此类石油钻采设备事故历史的人员;
- d) 熟悉有关法规、标准,特别是所评估石油钻采设备有关的具体安全问题的人员;
- e) 了解人为因素的人员。

4.3.3 方法和工具的选择

本文件旨在用于对复杂性和潜在危险程度差异很大的石油钻采设备进行风险评估,用于进行风险评估的方法和工具也很多(见 GB/T 16856—2015 第 6 章)。当选择一种方法或工具进行估计风险时,宜考虑设备危险的可能性质和风险评估的目的。还宜考虑风险评估的评估组的技能、经验和对特定方法的喜好。GB/T 16856—2015 第 5 章提供了风险评估过程每一步选择适当方法和工具的准则的附加信息。

4.3.4 风险评估信息的来源

风险评估所需信息在 5.2 列出。该信息可以通过诸如技术图样图表照片、影像资料、使用信息[包括维护记录和标准操作程序（SOP）]等各种各样形式的载体获取。如果可行，相类似的石油钻采设备或设计成的样机常常也是有用的。

5 风险评估

5.1 概述

风险评估包括风险分析与风险评价（见图 1）。

风险分析，包括：

- a) 石油钻采设备各种限制的确定（见 5.3）；
- b) 危险识别（见 5.4 和 GB/T 15706—2012 附录 B）；
- c) 风险估计（见 5.5）；

风险评价（见 5.6）。风险分析提供了风险评价所需的信息，最终判断是否需要减小风险；这些判断应借助于对石油钻采设备存在危险的有关风险进行的定性估计或适当的定量估计。

注 1：当可获得有效数据时，定量法可能是适当的。但是，定量法受到可获得的有效数据和/或风险评估人员资源有限性的限制，因此，在许多应用场合只能进行定性的风险估计。应按照第 8 章对风险评估进行文件记录。

5.2 风险评估信息

风险评估信息宜包括下列信息：

- a) 关于石油钻采设备的描述：
 - 1) 使用说明书；
 - 2) 设备的预期说明，包括设备整个生命周期各阶段的描述、设计图或确定设备特性的其他方法以及所要求的能源及其提供方式；
 - 3) 类似设备的先前设计方面的文件；
 - 4) 可获得的设备使用信息。
- b) 法规、标准及其他适用的文件：
 - 1) 适用法规；
 - 2) 相关标准；
 - 3) 相关技术规范；
 - 4) 相关安全数据表。
- c) 使用经验：
 - 1) 现有的或类似石油钻采设备的任何事故、事件或故障历史；
 - 2) 由排放物（噪声、振动、粉尘、烟雾、爆炸等）、使用的化学品或设备加工物料等所引起的损害健康的历史记录；
 - 3) 用户关于类似设备的经验，并尽可能与潜在用户进行信息交流。

注 2：一次已发生并导致伤害的事件可认为是一次“事故”。相反，一次已发生但没有导致伤害的事件，可认为是一次“未遂事故”或“危险事件”。

- d) 有关人类工效学的原则：应随着设计的发展或石油钻采设备的修改更新信息。

只要能获取不同类型设备相关的类似危险状态中的危险环境和事故环境的足够信息，在上述类似危险状态之间进行比较通常是可能的。只要确信其适用性，数据库、手册、实验室或制造商技术说明书中的数据可用于定量分析。在文件中应指明这些数据的不确定性（见第 8 章）。

注3：在缺乏事故历史记录的情况下，不宜采用少量事故或严重程度低的事件作为推测出低风险根据。

5.3 石油钻采设备限制的确定

5.3.1 概述

作为评价对象的石油钻采设备，是在有限范围内为一定的应用目的服务的，即石油钻采设备限制。风险评估从石油钻采设备限制的确定开始，考虑设备生命周期的所有阶段。意味着宜根据5.3.2到5.3.5给出的使用限制识别一个完整过程中石油钻采设备或系列设备的特征和性能、相关的人员环境和产品。

5.3.2 使用限制

使用限制包括预定使用和可合理预见的误用，应考虑以下几个方面：

- a) 不同的石油钻采设备运行模式和使用者的不同干预程序，包括设备失灵时所需的干预；
- b) 性别、年龄、优势手或身体能力限制（如听力或视力损伤、身高、体力等）不同的人员使用石油钻采设备；
- c) 包括下列使用者的预期培训水平、经验或能力水平：
 - 1) 操作人员；
 - 2) 维护人员或技师；
 - 3) 实习人员或学徒；
 - 4) 一般群众。
- d) 暴露于可合理预见的与石油钻采设备有关危险的其他人员，包括：
 - 1) 非常了解具体危险的人员，如邻近设备的操作人员；
 - 2) 不太了解设备危险但非常了解现场安全规程、准行路线等情况的人员，如管理人员；
 - 3) 基本不了解设备危险或现场安全规程的人员，例如参观者或者包括儿童在内的一般公众。

如果无法获得b)中的具体信息，宜考虑预期用户群体的一般信息（如适当的人体测量数据）。

5.3.3 空间限制

应考虑以下几个方面：

- a) 运动范围；
- b) 人机交互的空间要求，如运行和维修期间；
- c) 人员交互方式，例如“人机”界面；
- d) “石油钻采设备—动力源”接口。

5.3.4 时间限制

应考虑以下几个方面：

- a) 考虑石油钻采设备的预定使用和可合理预见的误用时，设备某些组件（如工具、易损的部件、机电组件）的寿命限制；
- b) 推荐的维修保养时间间隔。

5.3.5 其他限制

其他限制的示例包括：

- a) 被加工物料的特性；
- b) 符合清洁水平要求的保养；
- c) 环境—推荐的最低和最高温度，石油钻采设备是否能在室内或室外、干燥或潮湿气候中运行，是否能在太阳直射条件下运行，是否能耐受粉尘和潮湿环境等。

5.4 危险识别

5.4.1 在确定设备限制后，任何石油钻采设备风险评估的基本步骤是系统识别在设备生命周期所有阶段可合理预见的危险（永久性危险和意外突发危险）、危险状态和/或危险事件。石油钻采设备生命周期的阶段包括：

- a) 运输、装配和安装；
- b) 试运转；
- c) 使用；
- d) 拆卸、停用以及报废。

5.4.2 只有当危险已经被识别后才能采取措施消除危险或减小风险。为了实现危险识别，有必要识别石油钻采设备完成的动作和与其相互作用的操作人员执行的任务，同时考虑包括不同的部件、设备的机构或功能待加工物料以及使用环境。

5.4.3 设计者识别危险时应考虑以下因素：

a) 设备生命周期内人与设备的相互作用。任务识别宜考虑 5.4.1 中列出的所有阶段的相关任务，还宜考虑但并不限于下面的任务类型：

- 1) 设定；
- 2) 测试；
- 3) 示教/编程；
- 4) 过程/工具转换；
- 5) 启动；
- 6) 所有的运行模式；
- 7) 设备进料；
- 8) 从设备上取下产品；
- 9) 停机；
- 10) 急停；
- 11) 由卡滞或锁定到恢复运行：非计划停机后的重新启动；
- 12) 故障查找/故障排除（操作者干预）；
- 13) 清洁和保养；
- 14) 预防性维护；
- 15) 校正性维护。

应识别所有与各种任务相关的可合理预见的危险、危险状态或危险事件。GB15706—2012 附录 B 给出了危险、危险状态和危险事件的示例。目前已有几种可用于系统识别危险的方法，也可见 GB/T16856—2015。另外，应识别与任务不直接相关的可合理预见的危险、危险状态或危险事件。

示例：地震、雷电、过大的冰雪载荷、噪声、石油钻采设备断裂、液压软管爆裂。

b) 设备的可能状态：

- 1) 石油钻采设备执行预定功能（设备正常运转）；
- 2) 由于各种原因，设备不能执行预定功能（即失灵），这些原因包括：
被加工材料或工件的性能或尺寸变化，设备的一个（或多个）部件或辅助装置

失效，外部干扰（如冲击振动电磁干扰）、设计错误或缺陷（如软件错误），动力源扰动以及环境条件（如损坏的工作地面）等。

c) 非预期的操作者条件反射行为或设备可合理预见的误用，包括：

- 1) 操作者对设备失去控制（特别是手持式或移动式石油钻采设备）；
- 2) 设备在使用过程中发生失灵、事故或失效时，人员的条件反射行为；
- 3) 精神不集中或粗心大意导致的行为；
- 4) 工作中不按规程操作导致的行为；
- 5) 为保持石油钻采设备在所有情况下运转所承受的压力导致的行为；
- 6) 特定人员的行为（如儿童、残疾人等）。

注4：识别石油钻采设备危险时，检查已有设计文件是一种实用的方法，特别是那些与运动部件（如电机、液压缸）相关的危险。

5.5 风险估计

5.5.1 概述

危险识别后，应通过确定 5.5.2 中给出的风险要素，对每种危险状态进行风险估计。在确定这些要素时，应考虑5.5.3 中规定的几个方面。

5.5.2 风险要素

与特定危险状态相关的风险取决于以下要素：

- a) 估计危险可能造成危害的严重程度；
- b) 估计伤害发生的概率，它取决于人员在危险中的暴露情况（例如，频次、持续时间）、危险事件发生的概率以及避免或限制伤害的技术和人为可能性。

5.5.3 风险估计过程中应考虑方面

- a) 暴露人员；
- b) 暴露的类型、频次和持续时间；
- c) 暴露与影响之间的关系；
- d) 人的因素；
- e) 保护措施适用性；
- f) 废弃保护措施或避开保护措施的可能性；
- g) 维持保护措施的能力；
- h) 使用信息。

5.6 风险评价

5.6.1 概述

风险估计之后，应进行风险评价，以便确定：

- a) 是否需要风险减小；
- b) 是否已达到风险减小的目标。

如果需要减小风险，则应选用适当的保护措施（见第6章）。应在采用第6章所述风险减小三步法的每个步骤后确定是否达到充分的风险减小。作为该迭代过程的一部分，设计者还应检查采用新的保护措施时是否引入了额外的危险或增加了其他风险。如果出现了额外的危险，则应把这些危险列入已识别的危险清单中，并提出适当的保护措施。

风险充分减小目标的实现和实际可行的风险比较结果，都可以作为风险已被充分减小的证据。

5.6.2 充分的风险减小

实现充分风险减小的基本要求是采用6.1中所描述的三步法。

采用三步法之后，当满足以下条件时，可认为实现了充分的风险减小：

- a) 考虑了所有的运行条件和干预程序；
- b) 已消除危险，或风险减小到可行的最低水平；
- c) 已正确处理保护措施产生的新危险；
- d) 已向使用者充分告知和警告了剩余风险（见6.1中的第三步）；
- e) 所采取的保护措施相互匹配；
- f) 已充分考虑到为专业/工业用设计的机器用于非专业/非工业场合时产生的后果；
- g) 保护措施不会对操作者的工作条件或机器的易用性产生不利影响。

5.6.3 风险比较

只要下列准则适用，作为风险评价过程的一部分，所评价石油钻采设备或其部件的风险能够与类似设备或其部件的风险相比较：

- a) 类似设备符合相关的设备安全专业标准；
- b) 两种机器的预定使用、可合理预见的误用及它们的设计和制造方法都是可比的；
- c) 危险和风险要素是可比的；
- d) 技术规范是可比的；
- e) 使用条件是可比的。

使用这种比较方法并不排除还需要针对特定使用条件进行本文件所规定的风险评估过程。例如：用于切割钢材的带锯机与用于切割尼龙的带锯机比较时，应评估与不同材料有关的风险。

5.6.4 风险减小目标的确定

根据危险识别和估计，应进行以下步骤：

- a) 根据伤害严重程度和/或发生概率的减小，规定风险减小的目标；
- b) 识别出GB/T 15706—2012中适用于每种重大危险、危险状态或危险事件的相关条款；
- c) 针对每种重大危险，确定引用其他标准的安全要求和/或风险减小措施是否足够，或者是否需要采用特殊的安全要求和/或风险减小措施。

6 安全要求和风险减小措施

6.1 风险减小原则

通过消除危险，或通过分别或同时减小下述决定相关风险的两个因素，可以实现风险减小：即所考虑危险产生伤害的严重程度和伤害发生的概率。

所有预定用于达到此目标的保护措施应按照下列顺序进行，即“三步法”：

- a) 本质安全设计；
- b) 安全防护和/补充保护措施；
- c) 使用信息。

6.2 本质安全设计措施

6.2.1 概述

本质安全设计措施是指通过适当选择设备的设计特性和/或暴露人员与设备的交互作用来消除危险或减小风险。本质安全设计措施是风险减小过程中的第一步,也是最重要的步骤。这是因为尽管所采取的保护措施作为设备固有特征可能是有效的,然而经验表明即使设计得再好的安全防护也可能失效或被破坏,使用信息也有可能不被遵循。

注1:如果仅通过本质安全设计措施不足以减小风险时,可采用实现减小风险目标的安全防护和补充措施。

6.2.2 几何因素和物理特性的考虑

6.2.2.1 几何因素

几何因素包括:

- a) 石油钻采设备外形的设计使得在控制位置上对工作区和危险区的直接观察范围最大,如减少盲点考虑人类的视觉特点,在必要的地方选择和安装间接观察装置,尤其是安全操作需要操作者持续进行直接控制时,例如:
 - 1) 移动式设备的行走和工作区域;
 - 2) 提升载荷或提升人员的设备轿厢运行区;
 - 3) 物料处理时,手持式或手导式设备的工具接触区域。

石油钻采设备的设计应使得在主控制位置上的操作者能确保危险区内没有暴露人员。

- b) 设备的形状和相对位置:例如,通过加大运动部件之间的最小间距来避免挤压和剪切危险,使得人体的相应部位可以安全的进入,或通过减小间距使人体的任何部位不能进入(见GB/T 12265和GB/T 23821);
- c) 避免锐边、尖角和凸出部分:在不影响其功能的情况下,可接近的设备部件不应出现可能造成危害的锐边、尖角、粗糙面、凸出部位、以及可使人体部位或衣服“陷入”的开口。特别是对金属薄板,其边缘应除去毛刺、进行折边或倒角,并且对可能造成“陷入”的管口端,应进行覆盖;
- d) 设备外形的设计应获得合理的操作位置并提供可接近的手动控制器(执行器)。

6.2.2.2 物理特性

物理特性包括:

- a) 将制动力限制到足够低,使得被致动的部件不会产生机械危险;
- b) 限制运动部件的质量和/或速度,从而限制其动能;
- c) 根据排放源特性限制排放,采取措施减小:
 - 1) 排放源的噪声排放(见GB/T 25078.1);
 - 2) 振动源的振动,如重新分配或增加质量并改变过程参数;
 - 3) 有害物质的排放,包括使用更安全的物质或使用降低粉尘的工艺(用颗粒代替粉末、用铣代替磨等);
 - 4) 辐射排放,例如:避免使用有害辐射源,在满足设备正常功能的情况下将辐射功率限制在最低水平;通过设计使辐射源射线束集中于目标之上;加大辐射源和操作者之间的距离或提供远程操作石油钻采设备的装置(可见GB/T 26118.1和GB/T 26118.3)。

6.2.3 石油钻采设备设计的通用技术知识

通用技术知识可从设计技术规范（标准、设计规范、计算规则等）中得到，这些知识宜涵盖：

- a) 机械应力，例如：
 - 1) 对螺栓连接装配和焊接装配等，通过采用正确计算、构造和紧固方法限制应力；
 - 2) 借助过载保护（防爆膜、限压阀、断裂点、力矩限制装置等）限制应力；
 - 3) 避免交变应力（特别是循环应力）下零件产生疲劳；
 - 4) 回转件的静平衡和动平衡。
- b) 材料及其性质，例如：
 - 1) 耐腐蚀、抗老化、抗磨蚀和抗冲蚀；
 - 2) 硬度、强度、塑性、韧性、弹性；
 - 3) 均匀性；
 - 4) 毒性；
 - 5) 易燃、易爆性。
- c) 下列项目的排放值：
 - 1) 噪声；
 - 2) 振动；
 - 3) 有害物质；
 - 4) 辐射。

如果特定部件或者装配件的可靠性对安全起关键作用（如用于提升载荷或人员的绳、链条、提升附件），则其应力限值应乘以适当的工作系数。

6.2.4 适用技术的选择

对于具体的应用，通过技术的选用可消除一种或多种危险，或者减小风险，例如：

- a) 预定用于爆炸性环境中的设备，采用：
 - 1) 经适当选择的气动或液压控制系统及设备执行器；
 - 2) 本质安全的电气设备（见GB/T 3836.4）。
- b) 对特定的待加工产品（如溶剂），使用确保温度远远低于溶剂燃点的设备；
- c) 使用可避免高噪声的替代设备，例如：
 - 1) 以电气设备代替气动设备；
 - 2) 在某些条件下，用水切割设备代替机械加工设备。

6.2.5 采用直接机械作用原则

如果一个石油钻采设备零件运动不可避免的使另一个零件通过直接接触或通过刚性连接件随其一起运动，这就实现了直接机械作用。电路中开关装置的直接打开操作是其中一个示例（见GB/T 14048.5—2001和GB/T 18831—2002）。

注2：如果一个机械部件的运动造成第二个部件自由运动（如因为重力、弹簧力），则前者对后者不存在直接机械作用。

6.2.6 稳定性的规定

设备的设计应使其具有足够的稳定性，并使其在规定的使用条件下可以安全使用。需要考虑的因素包括：

- a) 底座的几何形状；
- b) 包括载荷在内的重量分布；
- c) 由于设备部件、设备本身或设备所夹持部件运动引起的，且能够产生倾覆力矩的

动态力；

- d) 振动；
- e) 重心的摆动；
- f) 石油钻采设备行走或不同安装地点（如地面条件、斜坡）的支承面的特性；
- g) 外力，如风力、人力。

在石油钻采设备生命周期的各个阶段内，包括搬运、运输、安装、使用、拆卸、停用和报废，都应考虑设备的稳定性。

6.2.7 维修性的规定

设计石油钻采设备时，应考虑以下使设备可维护的维修性因素：

- a) 可接近性，考虑环境和人体测量尺寸，包括工作服和所使用工具的尺寸；
- b) 易于搬运，考虑人的能力；
- c) 专用工具和设备的数目限制。

6.2.8 遵循人类工效学原则

6.2.8.1 设计石油钻采设备时应考虑人类工效学原则，以减轻操作者心理、生理压力和紧张程度。在初步设计阶段，分配操作者和设备的功能（自动化程度）时，应考虑这些原则。这样也能改善操作性能和可靠性，从而降低在设备所有使用阶段内的出错概率。应考虑石油钻采设备预定使用人群的人体尺寸、力量和姿势、运动幅度、动作重复频率（见GB/T 15241和GB/T 15241.2）。

6.2.8.2 人机界面的所有元件，如控制装置、信号或数据显示元件，其设计应易于理解，使操作者和设备间的相互作用尽可能清楚、明确。（见GB/T 18209.1）。

6.2.8.3 设计者在设计时，尤其应注意以下人类工效学要求：

- a) 避免操作者在设备使用过程中采用紧张姿势和动作的必要性（如提供按照不同操作者调节设备的装置）。
- b) 设备，尤其是手持式和移动式设备的设计，应考虑人力的可及范围、控制机构的操动，以及人的手、臂、腿等解剖学结构，使其容易操作。
- c) 尽可能限制噪声、振动、热效应（如极端温度）。
- d) 避免操作者的工作节奏与自动连续循环之间的联系。
- e) 当设备和/或其防护装置的结构特征使得环境照明不足时，应在设备上或设备内部提供对工作区和调整、设定与经常维护区的局部照明。应避免引起风险的闪动、眩光、阴影和频闪效应。如果不得不调整光源或光源的方位，则光源的位置不应调整者造成任何危险。
- f) 手动控制装置（执行器）的选用、位置和标记应满足以下要求：
 - 1) 清晰可见、可识别，必要处适当加标志（见7.6）；
 - 2) 可毫不迟疑的或立刻进行安全操作，且作用明确（如控制装置采用标准布局，可降低操作者由一台设备转到另一台具有相同运行模式的同类型设备上工作时出错的概率）；
 - 3) 位置（对按钮）和运动（对手柄和手轮）与它们的作用一致（见GB/T 18209.3）；
 - 4) 操作不能引起附加风险。

注3：当所设计和制造的控制装置执行几种不同动作时，即它们不是一一对应的（如键盘等），则所执行的动作应清晰的显示出来，并且必要时应经过确认。应根据人类工效学原则，使控制装置的布局、行程和操作阻力与所执行的动作相匹配。应考虑由于采用必要的或预计使用的个体防护设备（如鞋、手套等）所带来的约束。

- g) 指示器、刻度盘和视觉显示单元的选择、设计与位置应使得：
 - 1) 它们在人员能觉察的参数和特征范围之内，
 - 2) 对操作者的要求和预定使用面言，显示的信息应便于察看，识别和理解，即耐久、清晰、含义确切、易懂；
 - 3) 操作者在操作位置能觉察到它们。

6.2.9 电气危险

对于石油钻采设备电气设备的设计，GB/T 5226.1 给出了关于电路断开与接通以及防电击保护的一般规定有关特定设备的要求，见相应的 IEC 标准（如IEC 61029）。

6.2.10 气动与液压危险

设备的气动和液压设备的设计应使得：

- a) 不能超出回路的最大额定压力《如通过限压装置》；
- b) 不能因压力波动或升高、压力损失或真空导致危险；
- c) 不能因为泄漏或部件失效而导致危险的流体喷射或软管突发危险运动（如甩动）；
- d) 储气罐、蓄气瓶或类似容器（如充气蓄能器）符合相关的设计标准规则或法规；
- e) 设备的所有元件，尤其是管路和软管有防止受到外部有不利影响的保护措施；
- f) 当设备与动力源断开后，储气罐等类似容器（如充气蓄能器）尽可能自动卸压。

如果无法实现，则提供隔离、局部卸压及压力显示的措施（见 GB/T 19670—2005 中第5章）；

- g) 所有在设备与动力源断开后仍保持压力的元件，配备有清晰标识的排空装置，以及对设备进行任何设定或维护前必需对这些元件进行卸压的警告牌。

6.2.11 爆炸危险

爆炸危险场所中使用的石油钻采设备及其防护系统，应从整体防爆安全的观点考虑并设计。应做到：

- a) 首先，如果可能，防止设备及其防护系统自身产生或释放可燃性物质可能形成爆炸性环境；
- b) 考虑每一电气和非电气点燃源的性质，防止点燃爆炸性环境；
- c) 如果仍然发生爆炸，能直接或间接地危害人员、财产安全时，立即阻止爆炸和/或将爆炸火焰和爆炸压力限制在足够安全的水平之内。

石油钻采设备及其防护系统的设计和制造应在对可能存在的运行故障进行适当分析之后进行，以期尽可能地排除危险状况。应考虑任何能合理地预先采取措施以防错误使用的情况。

6.2.12 对控制系统应用本质安全设计措施

6.2.12.1 概述

控制系统设计措施的选用应使其有关安全的性能可减小足够的风险（见GB/T 16855.1 或IEC 62061）。设备控制系统的正确设计可避免无法预料的或潜在的设备危险状况。

6.2.12.2 导致设备危险状况的典型原因

- a) 控制系统逻辑的设计或修改不合适（无意的或有意的）；
- b) 控制系统的一个或几个部件暂时或永久的缺陷或失效；

- c) 控制系统动力源的变化或失效;
- d) 控制装置的选用、设计和位置不当。

6.2.12.3 设备危险状况的典型例子

- a) 意外启动;
- b) 没有控制的速度变化;
- c) 运动部件无法停止;
- d) 设备部件或设备夹紧的工件掉落或飞出;
- e) 保护装置不起作用(被废弃或失效)造成的设备动作。

6.2.12.4 控制系统设计方法

为了防止设备危险状况并实现安全功能,控制系统的设计应符合 6.2.12和6.2.13中提出的原则和方法。根据具体情况,这些原则和方法可以单独使用,也可以联合使用。控制系统的设计应便于操作者与设备进行安全互动。这要求采取以下一种或多种方法:

- a) 对启动和停止条件进行系统分析;
- b) 提供特定运行模式(如正常停机后启动、运行过程中断后或急停后重新启动、卸下装在设备上的工件,在设备的一个元件失效的情况下操作设备的一个部件;
- c) 清晰的显示故障;
- d) 采取措施防止意外产生的意外启动指令(如启动装置加装护罩)造成石油钻采设备危险状况;
- e) 保持停机指令(如联锁)以防止可能产生设备危险状况的重新启动。

6.2.12.5 多台设备的组合

多台设备的组合可能分为多个区域,用于急停、用于保护装置作用时的停止和/或用于隔离与能量耗散。应明确界定不同的区域,以及属于不同区域的石油钻采设备部件。同时,还应明确属于各个区域的控制装置(如急停装置、动力源断开装置)和/或保护装置。各区域之间接口的设计使得一个区域内的功能不会在其他因干预而停止的区域产生危险。

6.2.12.6 控制系统的安全设计

控制系统的安全设计应将设备的部件、设备本身、设备夹持的工件或载荷的运动限定在安全设计参数(如范围、速度、加速、减速、载荷能力)以内,应留有动态效应(如载荷摆动等)的余量。例如:

- a) 非远程控制的移动式步进控制设备,其移动速度应与步行速度保持一致;
- b) 用于提升人员的载人轿厢和载人工具的运动范围、速度、加速和减速应限定在无危险的数值范围内,并考虑操作者和设备的总反应时间;
- c) 用于提升载荷的设备部件,其移动范围应限制在规定限度以内。

如果石油钻采设备包含可单独操作的不同元件,则控制系统的设计应能防止因缺乏协调造成的危险(如防碰撞系统)。

6.2.12.7 启动内部动力源/接通外部能源供应

启动内部动力源或接通外部能源供应不应导致危险状态。例如:

- a) 内燃机启动不应导致移动式的运动;
- b) 接通主电源不应导致设备工作部件的启动。

6.2.12.8 机构的启动/停止

- a) 用于机构启动或加速运动的主要动作宜通过施加或增大电压或流体压力来实现。或者，如果考虑采用二进制逻辑元件，则通过由0 状态变到1状态来实现（其中1代表最高能态）。
- b) 用于机构停止或减速运动的主要动作宜通过去除或降低电压或流体压力来实现。或者，如果考虑采用二进制逻辑元件，则通过由1状态变到0状态来实现（其中1代表最高能态）。
- c) 在某些应用中，如高压开关装置，不能遵循此原则，此时宜采取其他措施来实现同等置信等级的停止或减速。
- d) 如果为了使操作者能保持对减速的持久性控制而未遵循此原则（如自行式移动设备的液压制动装置）时，则在石油钻采设备上应配备主制动系统（失效时用于减速或停止的装置）。

6.2.12.9 动力中断后重新启动

如果动力中断后重新接通时，石油钻采设备自发的重新启动可能产生危险，则应防止这种启动（如采用自持式继电器接触器或阀门）。

6.2.12.10 动力源中断

石油钻采设备的设计应防止因动力源中断或波动过大造成的危险状态。至少应满足以下要求：

- a) 应保持设备的停机功能；
- b) 对于为了安全而需要持久操作的所有装装置，应以有效的方式操作来保持安全（如锁紧、夹紧装置、冷却或加热装置、自行式移动设备的动力辅助导向）；
- c) 因势能可能产生运动的设备部件或设备所夹持的工件和/或载荷，应能保留允许其安全降低势能所需的必要时间。

6.2.12.11 使用自动监控

- a) 如果执行功能的部件或元件的能力被削弱或因工艺条件变化产生危险，自动监控用于确保安全功能或由保护措施执行的功能不会失效。
- b) 在下一安全功能启动之前，自动监控可以即时检测故障或者可以通过周期性检查来检测故障。在这两种情况下，保护措施可立即被触发或被延迟到特定事件发生时触发（如设备循环开始时）。
- c) 保护措施可以是：危险过程的停止、失效引起首次停机后防止此过程重新启动、警报触发等。

6.2.12.12 可编程电子控制系统执行的安全功能

6.2.12.12.1 一般要求

含有可编程电子设备（如可编程控制器）的控制系统在适当时可用于执行石油钻采设备的安全功能。如果采用可编程电子控制系统，有必要考虑与安全功能要求有关的性能要求。可编程电子系统的设计应充分降低对安全相关控制功能的性能造成不利影响的随机硬件失效概率和系统失效的可能性。如果可编程电子控制系统用于监控功能，则应考虑故障检测的系统性能（更多指南见 GB/T 20438 系列标准）。

可编程电子控制系统的安装与确认宜确保每种安全功能已达到规定的性能[如GB/T 20438中的安全完整性等级(SIL)]。确认包括试验和分析(如静态、动态或失效分析),用于证明所有部件能够相互正确作用,执行安全功能,且不会发生非预期的功能。

注4:专门针对石油钻采设备安全的GB/T 16855.1和IEC 62061两项标准提供了适用于可编程电子控制系统的指南。

6.2.12.12.2 硬件方面

硬件(包括传感器、执行器、逻辑运算器等)的选择、设计和安装应同时满足待执行的安全功能和性能要求,特别是通过以下方式来实现:

- a) 结构约束(如系统结构、硬件的容错能力、硬件的故障检测性能);
- b) 选择和/或设计具有适当硬件随机危险失效概率的设备和装置;
- c) 将避免系统性失效和控制器系统性故障的措施和技术纳入硬件中。

6.2.12.12.3 软件方面

软件包括内部操作软件(或系统软件)和应用软件在内的软件,其设计应符合安全功能的性能规范(见GB/T 20438.3)。

应用软件不宜由用户进行重新编程。这可通过在不可重新编程的存储器中使用嵌入式软件[如微控制器、专用集成电路(ASIC)]来实现。需要用户重新编程时,宜限制访问涉及安全功能的软件(如设置密码)。

6.2.12.13 有关手动控制的原则

应遵守以下原则:

- a) 手动控制装置的设计和定位应符合6.2.8中给出的有关人类功效学原则。
- b) 每个启动控制装置附近均应配置一个停止控制装置。如果启动/停止功能通过保持运行控制方式实现,则当保持运行控制装置释放后不能发出停止指令而造成风险时,应提供单独的停止控制装置。
- b) 除某些有必要位于危险区的控制器之外,如急停控制器或示教盒,手动控制器应位于在危险区内能触及的区域之外。
- d) 控制装置和控制位置的定位应尽可能使操作者能观察到工作区或危险区。
 - 1) 除了从其他位置可以更安全地控制功能之外,骑乘式移动石油钻采设备的驾驶员应能从驾驶位置驱动设备运行所需要的所有控制装置。
 - 2) 在预定用于提升人员的设备上,用作升降的控制器以及适当情况下用作移动轿厢的控制器,通常应位于轿厢内。如果安全操作需要将控制器置于轿厢外,则应向轿厢内的操作者提供防止轿厢危险运动的方法。
- e) 如果几个控制器可能启动同一危险元件,则控制回路的布置应使得在给定时间只能有一个控制装置是有效的。这尤其适用于由操作者携带便携式控制单元(如示教盒)等进入危险区内进行手动控制的装置。
- f) 控制执行器的设计或防护应使其在有风险的场合只有通过主动操作才能起作用。
- g) 对于依靠操作者持久、直接操控才能安全运行的功能,应采取措施确保操作者处于控制位置上(如通过控制装置的设计和位置)。
- h) 对于无线控制装置,在没有接收到正确的控制信号,包括失去联络时,应执行自动停机功能。

6.2.12.14 设定、示教过程转换、故障查找、清洗或维护的控制模式

对石油钻采设备的设定、示教、过程转换、故障查找、清洗或维护，当不得不开或拆除防护装置和/或使一保护装置不起作用，以及为了进行这些操作而有必要使石油钻采设备或某些部件运转时，应采用同时满足下列要求的特殊控制模式来实现操作者的安全：

- a) 使其他所有控制模式不起作用；
- b) 只有通过连续驱动使能装置（与启动控制一起使用且只有连续操作时才能使设备运行的附加手动操作装置）、双手操纵装置或保持运行控制装置，才允许危险元件运转；
- b) 只有在风险已被减小的条件下（如已利用有限运动控制装置等逐步减速、降低动力 / 力），才允许危险元件运转；
- d) 通过设备的传感器检测有意或无意的动作防止任何危险功能运行。

注5：对一些特殊石油钻采设备，可能有其他更合适的保护措施。

此控制模式应与下列一项或多项措施相结合：

- a) 尽可能限制进入危险区；
- b) 急停控制器位于操作者立刻可触及的范围内；
- c) 便携式控制单元（示教盒）和/或现场控制装置能看到被控元件。

6.2.12.15 控制和运行模式的选择

如果石油钻采设备的设计和制造允许用于几种需要不同保护措施和/或工作流程要求的控制或运行模式（如允许调整、设定、维护、检查），则应配备一个能锁定在每个位置的模式选择器。选择器的每个位置都应清晰无疑并对应一种操作或控制模式。

选择器可能被另一种选择方式所代替，这种选择方式限定只有某些操作者才能使用石油钻采设备的某些功能（如用于某些数控功能的访问口令）。

6.2.12.16 采取措施实现电磁兼容（EMC）

关于电磁兼容的指南，见GB/T 5226.1和IEC 61000—6。

6.2.12.17 辅助故障查找的诊断系统

控制系统中宜含有辅助故障查找的诊断系统，以便无需使任何保护措施不起作用

注6：这类诊断系统不仅改善石油钻采设备的实用性和可维修性，还可以减少维护人员在危险区的暴露。

6.2.13 最大程度降低安全功能失效的概率

6.2.13.1 概述

石油钻采设备的安全不仅取决于控制系统的可靠性，而且还取决于设备所有部件的可靠性。安全功能的持续运行对石油钻采设备的安全使用至关重要。这可以通过采取 6.2.13.2～6.2.13.4 给出的措施来实现。

6.2.13.2 使用可靠的组件

“可靠的组件”是指在预定使用条件下（包括环境条件），在固定的使用期限或操作次数内，能够经受住与设备使用有关的所有干扰和应力，且产生危害设备失灵的失效概率小的组件。组件的选择应考虑上述所有因素（也可见6.2.14）。

注7：“可靠的组件”不等于“经验证的组件”。

注8：需要考虑的环境条件包括冲击、振动、冷、热、潮湿、粉尘、腐蚀和/或磨蚀材料、静电、电磁场，由此产生的干扰包括绝缘失效、控制系统组件的功能暂时或永久失效。

6.2.13.3 使用“定向失效模式”组件

“定向失效模式”组件或系统是指主要失效模式已事先知道，并且能预知使用时石油钻采设备功能发生此类失效的影响的组件或系统。

注9：在有些情况下，有必要采取附加措施限制这类失效的负面影响。

宜始终考虑使用这类元件，特别是在未采用冗余时（见 6.2.13.4）。

6.2.13.4 组件或子系统加倍（或冗余）

设计石油钻采设备安全相关部件时，可能使元件加倍（或冗余），以便当一个组件失效时，另一个组件或其他多个组件能继续执行各自的功能，从而保证安全功能继续有效。为了允许触发正确的动作，应通过自动监控（见 6.2.12.11）或在某些情况下通过定期检查（假如定期检查的间隔小于组件的预期寿命）来检测组件的失效。

可采用多样化的设计和/或技术来避免共因失效（如由于电磁干扰）或共模失效。

6.2.14 提高设备的可靠性

石油钻采设备各组成部件可靠性的提高可降低发生需要干预的事故频率，从而减少暴露在危险中的情况。这同样适用于石油钻采设备的动力系统、控制系统、安全功能以及其他功能。应采用可靠性已知的安全相关组件（如某些传感器）。防护装置和保护装置的元件应特别可靠，因其失效会使人员暴露在危险中，且由于可靠性差还会鼓励人员废弃这些装置。

6.2.15 加载（装料）/卸载（卸料）操作的机械化或自动化

石油钻采设备加载/卸载以及更为普遍的（工件、材料、物资等的）搬运操作的机械化和自动化可减少人员在操作点暴露在危险中的情况，从而限制由这些操作产生的风险。可通过机器人、搬运装置、传送机构、鼓风设备等实现自动化。可通过进料滑道、推杆和手动分度工作台等实现机械化。

自动装料和卸料装置虽然更能预防石油钻采设备操作者发生事故，但在进行故障校正时也可能产生危险。应注意保证使用这些装置不会引发更多的危险，如在装置与石油钻采设备部件或被加工的工件材料之间的陷入或挤压。如果不能保证，应提供合适的安全防护装置（见6.3）。在全面研究整个设备的所有控制与运行模式中如何执行所有安全功能之后，应使用自身带有控制系统的自动装料和卸料装置与石油钻采设备相关的控制系统相互连接。

6.2.16 将设定和维护点的位置放在危险区之外

应将维护、润滑和设定点放在危险区之外，从而最大程度减少人员进入危险区的需求。

6.3 防护装置和保护装置的选择和使用

6.3.1 一般要求

根据运动部件的性质（见图3）和进入危险区的需求，本条给出了选择和使用防护装置和保护装置的指南。采用这些装置的主要目的是防止运动部件对人员产生危险。对特定石油钻采设备的安全防护装置的正确选用，应基于该设备的风险评估结果。为特定类型的石油钻采设备或危险区选用合适的安全防护装置时，应铭记固定式防护装置是简单的装置，并且用在设备正常运行（无失灵运行）期间不需要操作者进入危险区的场合。随着需要进入危险区

的频次增加，不可避免的导致固定式防护装置无法回到原处。这需要使用其他保护措施（活动式联锁防护装置、敏感保护设备），有时可能需要使用安全防护装置的组合。

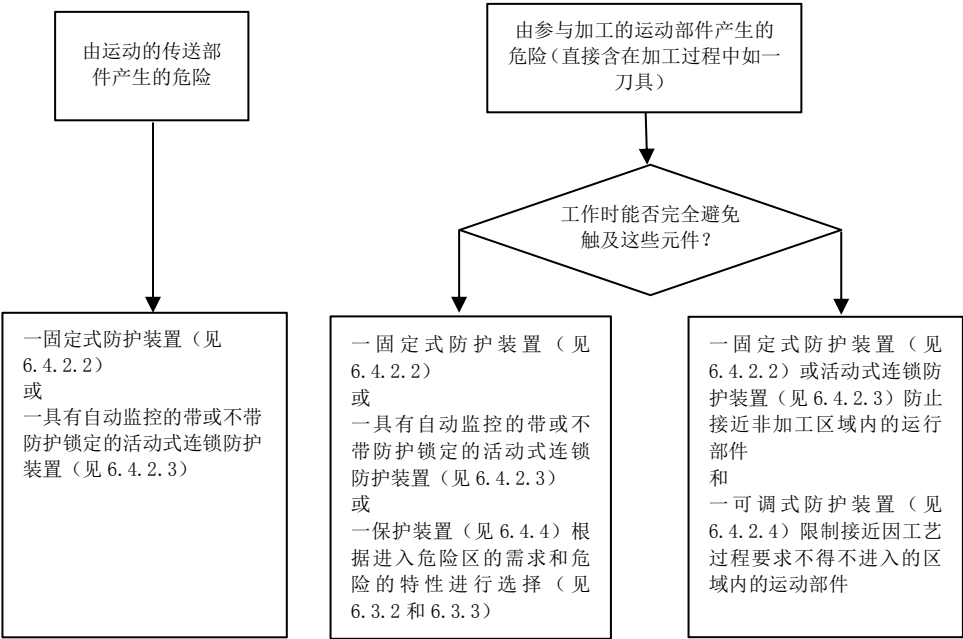


图3 选择安全防护装置防止由运动部件产生的危险的指南

应考虑封闭控制位置或干涉区域，以提供针对多种危险的组合保护，这些危险包括：

- a) 通过落物保护结构（FOPS）等予以保护的坠落或弹射物体产生的危险；
- b) 排放危险（防止噪声、振动、辐射、有害物质对健康的危害等）；
- c) 因环境造成的危险（如防止热、冷、恶劣天气等）；
- d) 通过滚翻保护结构或倾翻保护结构（ROPS和TOPS）等予以保护的机械滚翻或倾翻产生的危险。

对封闭式工作站，如室和舱的设计，应考虑与能见度、照明、大气条件、进入途径、姿势等相关的人类工效学原则。

6.3.2 正常运行期间不需要进入危险区

石油钻采设备正常运行期间不需要进入危险区时，宜选用下列安全防护装置：

- a) 固定式防护装置（见GB/T 8196-2018）；
- b) 带或不带防护锁定的联锁防护装置；
- c) 自关闭式防护装置（见GB/T 8196—2018 中3.3.2）；
- d) 敏感保护设备，如电敏保护设备（见IEC 61496）或压敏保护装置（见 GB/T 17454）。

6.3.3 正常运行期间需要进入危险区

石油钻采设备正常运行期间需要进入危险区时，宜选用下列安全防护装置：

- a) 带或不带防护锁定的联锁防护装置（也可见 GB/T 18831、GB/T 8196-2018）；
- b) 敏感保护设备，如电敏保护设备（见IEC 61496）；
- c) 可调式防护装置；
- d) 自关闭式防护装置（见GB/T 8196—2018中3.3.2）；

- e) 双手操纵装置（见GB/T 19671）；
- f) 带启动功能的联锁防护装置（带控制功能的防护装置）。

6.3.4 石油钻采设备设定、示教、过程转换、故障查找、清洗或维护时需要进入危险区

石油钻采设备的设计应尽可能使用保护生产操作人员的安全防护装置，在不妨碍进行设定、示教过程转换、故障查找、清洗或维护的人员执行任务的前提下，保护他们的安全。此类任务应在风险评估中作为石油钻采设备的使用部分进行识别和考虑（见5.2）。

注10：在进行一些无需石油钻采设备与其动力源保持连接的工作任务（特别是维护和修理任务）时，动力源的隔离和设备停止后的能量耗散可确保最高等级的安全水平。

6.3.5 敏感保护设备的选择和使用

6.3.5.1 选择

由于敏感保护设备检测功能所基于技术的多样性，因此所有类型的敏感保护设备用于安全用途时的适合程度存在很大差异。以下条款为设计者针对各种应用选择最合适的装置提供了准则。

- a) 敏感保护设备的类型包括：光幕、扫描装置，如激光扫描器、压敏垫、边沿开关及拉绳开关等。
- b) 敏感保护设备可：
 - 1) 用于触发；
 - 2) 用于存在感应；
 - 3) 用于触发和存在感应；
 - 4) 重新启动设备的运行，此做法需要满足严格的条件。

注11：有些类型的敏感保护设备既不适用于存在感应，也不适用于触发。

- c) 尤其对于具有下列特征的石油钻采设备不能单独使用敏感保护设备：
 - 1) 可能存在材料或零部件弹射；
 - 2) 不得不防止排放（噪声、辐射、粉尘等）；
 - 3) 无规律的或过长的设备停机时间；
 - 4) 设备不具备在工作循环过程中停机的能力。

6.3.5.2 实施

- a) 宜考虑以下因素：
 - 1) 检测区域的大小，特征和位置（见GB/T 19876，该标准涉及某些类型的敏感保护设备的定位），装置对故障状态的反应（电敏保护设备见 IEC 61496）；
 - 2) 被避开的可能性；
 - 3) 检测能力及其随时间的变化（如由于对反射表面、其他人工光源、日光或空气杂质等这类不同环境条件的敏感性而造成的结果）。
- b) 敏感保护设备应集成到操作部分中，并且与石油钻采设备的控制系统相连接，从而使得：
 - 1) 一旦检测到人员或人体部位就立即给出指令；
 - 2) 撤回被检测到的人体或人体部位不会自动重新启动危险功能，从而使控制系统在给出新的指令之前维持敏感保护设备发出的指令；
 - 3) 危险功能的重新启动是操作者主动驱动位于操作者可观察到的危险区之外的控制装置的结果；

- 4) 除抑制阶段外,敏感保护设备的检测功能被中断时,设备不能运转;
- 5) 检测区域的位置和形状,可能和固定防护装置一起防止人或人体部位在未被探测到的情况下进入或处于危险区。

注12:抑制是指安全功能被控制系统有关安全部件临时自动暂停(见GB/T 16855.1)。

6.3.5.3 对于循环启动的敏感保护设备的附加要求

在此类特殊应用中,石油钻采设备工作循环的启动由被检测到的人体或人体部位从敏感保护设备检测区撤出引起,且不需要任何额外的启动指令,因此不符合上述 6.3.5.2 中b)的第二项要求。但是,接通动力源后或敏感保护设备的触发功能已经使设备停机时,设备的工作循环应只能通过主动驱动启动控制装置才能启动。

由敏感保护设备引起的循环启动应满足以下条件:

- a) 只应使用符合IEC 61496系列标准的有源光电保护装置(AOPDs);
- b) AOPD 用做触发和存在感应装置(见IEC 61496)时的要求得到满足—特别是位置、最小距离(见GB/T 19876)检测能力可靠性以及对控制和制动系统的监控;
- c) 设备的循环时间短,并且感应区一旦清空,设备重新启动的时间被限制在与单个正常循环相匹配的周期内;
- d) 进入AOPD的感应区或开启联锁防护装置是进入危险区的唯一途径;
- e) 如果有多个AOPD用于设备的安全防护,则其中只能有一个具有循环再启动的能力;
- f) 对于自动循环启动产生的较高风险,AOPD 和与其相关的控制系统应比正常工作条件下具有更高的安全相关性能。

注13:上述d)中所指的危险区是指由清空感应区而触发的危险功能(包括辅助设备和传送元件)所在的任何区域。

6.3.6 稳定性的保护措施

如果不能通过重量分布(见 6.2.6)等本质安全设计措施实现稳定性,则有必要采取措施保持石油钻采设备的稳定性,例如:

- a) 地脚螺栓;
- b) 锁定装置;
- c) 运动限制器或机械式停机装置;
- d) 加速或减速限制器;
- e) 载荷限制器;
- f) 接近稳定性极限或倾覆极限时发出警告的警报器。

6.3.7 其他保护装置

- a) 当石油钻采设备需要操作者连续操控(如移动式设备、起重机),且操作者的错误能产生危险状态时,则应为该设备配备必要的、使其运行保持在规定限度内的装置,特别是:
 - 1) 当操作者不能充分观察到危险区时;
 - 2) 当操作者对安全相关参数(距离、速度、质量角度等)的实际值缺乏了解时;
 - 3) 当危险是由操作者控制之外的运行引发时。
- b) 必要的装置包括:
 - 1) 限制运动参数(距离、角度、速度 加速度)的装置;
 - 2) 过载和力矩限制装置;

- 3) 防止与其他石油钻采设备冲突或干涉的装置;
- 4) 防止对移动式设备的步行操作者或其他行人产生危险的装置;
- 5) 防止组件和成套件应力过大的扭矩限制装置或断裂点;
- 6) 限制压力或温度的装置;
- 7) 监控排放的装置;
- 8) 防止操作人员不在控制位置时运行的装置;
- 9) 防止稳定衡器不在其位置时进行提升操作的装置;
- 10) 限制设备在斜面上倾斜的装置;
- 11) 确保组件在移动之前处于安全位置的装置。

上述装置触发的自动保护措施(如危险运动的自动停止)使石油钻采设备的运行超过了操作者的控制范围,因此,宜预先发出或同时发出警告信号,使操作者能采取适当的措施。

6.4 防护装置和保护装置的设计要求

6.4.1 一般要求

防护装置和保护装置的设计应适用于预定使用,并考虑相关的石油钻采设备危险和其他危险。防护装置和保护装置应与设备的工作环境协调,且其设计应使其不易被废弃。为减少其被废弃的诱因,应将防护装置和保护装置对石油钻采设备运行期间和设备生命周期其他各阶段的各种动作的干涉降至最低程度。

防护装置和保护装置应:

- a) 结构坚固耐用;
- b) 不增加任何附加危险;
- c) 不容易被绕过、拆卸、移走或使其无法操作;
- d) 与危险区有足够的距离(见GB/T 19876 和 GB/T 23821);
- e) 对观察生产过程的视野障碍最小;
- f) 只允许进入不得不进行操作的区域,进行工具的安装和/或更换及维修等必要的工作,且尽可能不移除防护装置或使保护装置不起作用;
- g) 不应出现漏保护区。

注14: 防护装置的开口,见GB/T 23821。

6.4.2 防护装置的要求

6.4.2.1 防护装置的功能

防护装置能实现的功能如下:

- a) 防止进入被防护装置封闭的空间;
- b) 容纳或捕获由石油钻采设备抛出或掉下的材料、工件、切屑、液体,减少由石油钻采设备产生的排放(噪声、辐射、有害物质,如粉尘、烟雾、气体等)。

此外,防护装置可能还需要具有与电、温度、火、爆炸、振动、能见度(见 GB/T 8196-2018)以及操作者位置人类工效学(如易用性、操作者的运动、姿势、重复运动)相关的独特特征。

6.4.2.2 固定式防护装置的要求

固定式防护装置应采用以下方式保持其位置:

- a) 永久固定(如通过焊接);
- b) 通过紧固件(螺钉、螺母)固定,使得不使用工具不可能将其移除/打开;没有紧固件时,固定式防护装置不宜保持关闭(见 GB/T 8196-2018)。

注15：固定式防护装置可采用铰接辅助打开。

6.4.2.3 活动式防护装置的要求

活动式防护装置用于防止由运动的传动部件产生的危险时，要求打开时尽可能固定在设备或其他结构上（一般通过铰链或导轨），同时是联锁的（必要时带防护锁定）（见GB/T 18831）。

活动防护装置用于防止运动的非传动部件产生的危险时，应将其设计成与石油钻采设备控制系统相连，从而使得：

- a) 运动部件在操作者可触及的范围内时不能启动，并且一旦运动部件启动，操作者就触及不到，这可通过采用联锁防护装置来实现，必要时可带防护锁定；
- b) 只有通过有意识的动作才能对防护装置进行调整，如使用工具或钥匙；
- c) 防护装置的某一组件缺失或失效可防止运动部件启动或停止运动部件，这可通过自动监控来实现（见GB/T 18831）。

6.4.2.4 可调式防护装置的要求

只有因操作需要而不能完全封闭危险区时，才可采用可调式防护装置。可调式防护装置的可调或活动部分在特定操作期间应保持固定，自锁状态不得因为机器振动而发生位移或脱落。手动可调式防护装置，应符合以下要求：

- a) 设计上应保证在给定的操作期间，调整后的状态保持恒定；
- b) 不使用工具就容易调整。

6.4.2.5 带启动功能的联锁防护装置（带控制功能的防护装置）的要求

只有满足以下条件才能使用带启动功能的联锁防护装置：

- a) 满足联锁防护装置的所有要求（见GB/T 18831）；
- b) 设备的工作循环时间短；
- c) 将防护装置打开的最长时间预先设定为较低的值（如等于循环时间），并且一旦超过该时间，通过关闭带启动功能的联锁防护装置不能触发危险功能，并在重新启动设备前有必要进行复位；
- d) 防护装置关闭时，设备的尺寸或形状不允许人员或人体部位停留在危险区内或危险区与防护装置之间（见GB/T 8196-2018）；
- e) 其他所有防护装置，无论是固定式（可拆卸式）还是活动式均为联锁防护装置；
- f) 与带启动功能的联锁防护装置相连的联锁装置，其设计应使得在位置检测器加倍以及使用自动监控等方法时（见6.2.12.11），其失效不能导致非预期的启动/意外启动；防护装置安全可靠的保持打开状态（如通过弹簧或配重），使其不能因其自身重量掉下而触发启动。

6.4.3 防护装置产生的危险

应注意防止可能由以下因素带来的危险：

- a) 防护装置的结构（锐边或尖角、材料、噪声排放等）；
- b) 防护装置的运动（由动力驱动的防护装置和由容易掉下的重型防护装置产生的剪切或挤压区）；
- c) 防护装置出现故障，失效丧失保护功能。

6.4.4 保护装置的技术特征

保护装置的选择或设计以及与控制系统的连接，应确保能正确执行其安全功能。保护装置的选择应符合相应的产品标准（如关于有源光电保护装置的IEC 61496）或者应根据GB/T 16855.1或IEC 62061所规定的一项或多项原则进行设计。保护装置的安装以及其与控制系统的连接应使其不能轻易被废弃。

6.4.5 提供其他类型的安全防护装置

由于待完成工作范围的原因而不得不改变安全防护装置时，宜提供便于安装其他类型的安全防护装置的措施。

6.5 通过安全防护减少排放

6.5.1 一般要求

如果6.2.2.2 中减少排放源排放的措施不够，则应为石油钻采设备提供补充保护措施。

6.5.2 噪声

防止噪声的补充保护措施包括：隔声罩（见GB/T 19886）、安装在石油钻采设备上的隔声屏、消声器（见GB/T 20431）等。

6.5.3 振动

防止振动的补充保护措施包括：

- a) 隔振器，如置于振源和暴露人员之间的减震装置；
- b) 弹性架；
- c) 悬浮座椅。

6.5.4 有害物质

防止有害物质的补充保护措施包括：

- a) 石油钻采设备的密封（带负压的外壳）；
- b) 带过滤的局部排气通风；
- c) 用液体加湿；
- d) 石油钻采设备区域内特殊通风（气幕、操作舱）。

6.5.5 辐射

防止辐射的补充保护措施包括：

- a) 采用过滤和吸收；
- b) 使用衰减屏或防护装置。

6.6 补充保护措施

6.6.1 概述

根据石油钻采设备预定用途及可合理预见的误用，可能不得不采用既不是本质安全设计措施、安全防护（使用防护装置和/或保护装置），也不是使用信息的保护措施。这类措施可参考GB/T 15706—2012 6.3.5中的内容。需要明确的是这些措施并不局限于这些描述。

6.6.2 实现急停功能的组件和元件

如果根据风险评估,设备需要安装实现急停功能的组件和元件,以避免正在发生或即将发生的紧急状态时,应满足下列条件:

- a) 执行器应容易识别、清晰可见且随手可及;
- b) 应尽快停止危险过程,且不产生额外的危险,但如果这不可能实现或不能降低风险,则宜考虑执行急停功能是否为最佳解决方法;
- c) 急停控制器应触发或允许触发某些必要的安全防护装置的运动。

一旦执行急停指令后急停装置的有效动作已经停止,应维持该指令的作用直至其复位为止。只有在触发急停指令的位置,才有可能复位。急停装置的复位不应重新启动设备,而仅是允许设备重新启动。

6.6.3 被困人员逃生和救援措施

被困人员被困人员逃生和救援的措施可能主要是指:

- a) 在可能使操作者陷入危险的设施中的逃生通道和躲避处;
- b) 供急停后人工移动某些元件的安排;
- c) 用于某些元件反向运动的布置;
- d) 下降装置的锚定点;
- e) 受困人员的呼救通讯方式。

6.6.4 隔离和能量耗散的措施

石油钻采设备应具备通过采取以下措施实现隔离动力源和耗散储存能量的技术手段:

- a) 将设备(或指定的部件)与所有动力供应隔离(脱开分离);
- b) 将所有隔离单元锁定(或采用其他方式固定)在隔离位置;
- c) 耗散能量,如果不可能或不可行,抑制(遏制)任何可增大危险的储存能量;
- d) 通过安全工作程序验证按照上述三项所采取的措施是否已达到预期效果。

6.6.5 提供方便且安全搬运机器及其重型零部件的装置

无法移动或无法用手搬运的机器及其零部件应配备或能够配备适当的附属装置,用于通过提升机构搬运。这些附属装置可能是:

- a) 带吊索、吊钩、吊环螺栓或用于固定的螺纹孔的标准提升装置;
- b) 当不可能从地面安装附属设备时,采用带起重吊钩的自动抓取装置;
- c) 通过叉车搬运的设备的叉臂定位装置;
- d) 集成到设备内的提升和装载机构和装置。

对操作中可通过手动拆除的设备部件,应提供安全移除和更换的方法。

6.6.6 安全进入设备的措施

石油钻采设备的设计应使得操作及与安装和/或维护相关的所有常规作业尽可能由人员在地面完成。如果无法实现,为了执行这些任务,设备应提供安全进入的机内平台、阶梯或其他设施;但是,宜注意确保这类平台或阶梯不会使操作者接近设备的危险区。

在工作条件下,步行区应尽量采用防滑材料防滑,并且根据步行区距离地面的高度提供适当的护栏。在大型自动化设备中,应特别注意给出安全进入的途径,如通道、输送带过桥或跨越点。进入位于一定高度的设备部件的设施应提供防止跌倒的措施(如楼梯、阶梯及平台的护栏和/或梯子的安全护笼)。必要时,还应为防止人员从高处跌倒的个体防护装置提供锚定点(如在用于提升人员的机械轿厢中或带升降的控制站)。

只要有可能，开口都应朝向安全的位置，其设计应防止因意外打开产生的危险。应提供必要的进入辅助设施（台阶、把手等）。控制装置的设计和位置应防止其被用作进入时的辅助设施。如果提升货物和/或人员的机械包含固定高度的停层，则应配备连锁防护装置防止某一停层没有平台时发生人员跌落。当防护装置打开时，应防止提升平台运动。

6.7 安全要求和风险减小措施的符合性验证

对于识别并确定的每种安全要求和/或风险减小措施可通过下述方法进行验证（不证自明的除外）：

- a) 通过试验（例如，双手控制装置的功能试验、防护装置的强度试验、稳定性试验）；
- b) 通过测量（例如，噪声排放的测量）；
- c) 通过计算（例如，重心的位置）；
- d) 如果试验和计算不够充分，则通过其他方法验证（例如通过目视检查）。

6.8 可容许风险的实现

6.8.1 将风险降低到可容许程度采用的步骤

降低风险到可容许的程度宜采用下列步骤（见图 4）：

确定石油钻采设备产品的预期使用，评定产品的可合理预见的误使用；确定设备产品、过程或服务包括安装、维护、修理和销毁或报废时所有阶段和条件下产生的每个危险（源）（包括危情况和伤害事件）；

预测和评价已确定的危险（源）对各个已确定的使用或接触的群体引起的风险（见图4）如果判定结果表明，风险达到了可容许的程度（例如，通过对同类的产品、过程或服务的比较）则终止；如果判定结果表明，风险未达到可容许的程度，则再降低风险直至达到可容许的程度。

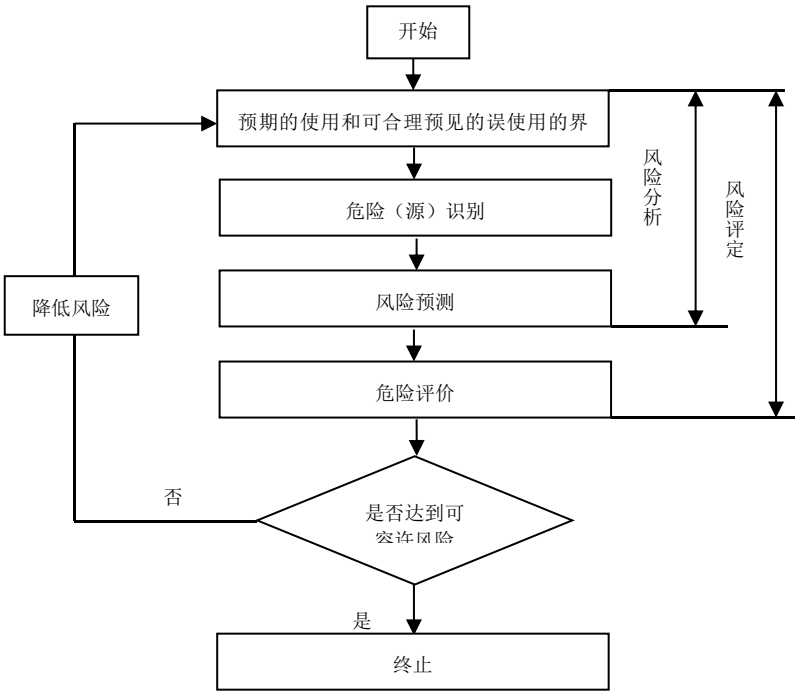


图4 风险评定和降低风险的循环过程

6.8.2 降低风险的先后顺序

降低风险宜按如下先后顺序

- a) 固有的安全设计；
- b) 防护设计；
- c) 提供给使用者的信息。

上述步骤的前提是假设使用者在风险降低措施中充当一个角色，要按设计者提供的安全信息使用产品、过程或服务（见图5）。

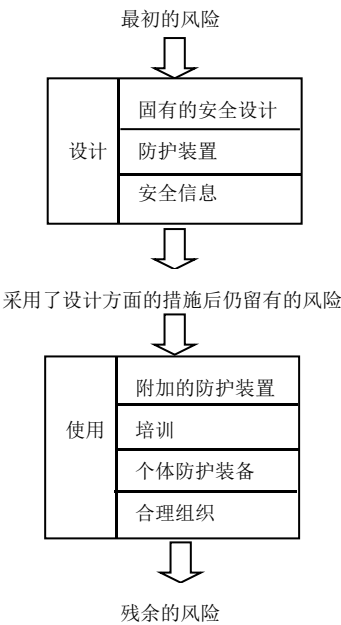


图5 降低风险的过程

设计所采取的步骤应遵循图5所示的先后顺序。使用者所采取的步骤不必遵循图5的先后顺序，而要视具体的应用情况而定。需要强调的是，不宜用附加的防护装置、个体防护设备和给使用者提供信息代替设计上的改进。

7 使用信息

7.1 起草使用信息

起草使用信息是石油钻采设备设计的组成部分。使用信息由文本、标记、信号、符号或图表等组成，以单独或联合使用的形式向使用者传递信息。使用信息预定提供给专业和/或非专业人员。

注1：使用信息的结构和表述也可见GB/T 19678.1。

7.2 预定使用信息

应向使用者提供关于石油钻采设备预定使用的信息，特别是考虑到设备的所有运行模式。该信息应包含确保安全和正确使用石油钻采设备所需的各项指南。因此，该信息应向使用者告知或警示剩余风险。

适当时，该信息应指明：

- a) 是否需要培训；

- b) 是否需要个体防护设备;
- c) 可能需要的附加防护装置或保护装置。

不应排除根据石油钻采设备名称和描述可合理预见的设备用途,也应对不按使用信息中描述的方式而按其他方式使用设备而产生的风险进行警告,尤其是考虑到可合理预见的误用。

7.3 使用信息的形式

使用信息应以单独或组合的形式涵盖石油钻采设备的运输,装配和安装、试运转、使用(设定、示教/编程或过程转换、操作、清洗、故障查找和维护)以及必要的拆卸、停用和报废。

7.4 使用信息的位置和属性

根据风险、使用者需要使用信息的时间和石油钻采设备的设计,应决定在下述位置是否需要提供使用信息或部分信息:

- a) 在设备内或设备上;
- b) 在随行文件中(特别是使用手册);
- c) 在包装上;
- d) 通过其他方式,如设备外的信号和警告。

在给出警告等重要信息时,应考虑采用标准化的语言(也可见GB/T 19678.1)。

7.5 信号和警告装置

视觉信号(如闪光灯)和听觉信号(如报警器)可能用作警告即将发生的危险事件,如石油钻采设备启动或超速。此类信号也可能在触发自动保护措施前用作警示操作者。

这些信号应满足以下基本要求:

- a) 在危险事件发生之前发出;
- b) 含义确切;
- c) 能被明显察觉到,与所用的其他所有信号相区分;
- d) 易被使用者和其他人员明确识别。

警告装置设计和位置应便于检查。使用信息应规定警告装置需要定期检查。设计者应注意由于过多的视觉和/或听觉信号引起“感官疲劳”造成的风险,这也可导致警告装置被废弃。

注2:通常有必要就此问题与使用者进行磋商。

7.6 标志、符号(象形图)和书面警告

7.6.1 石油钻采设备应加贴以下所有必要的标志:

- a) 供其明确识别用的标志,至少包括:
 - 1) 制造商的名称与地址;
 - 2) 系列或型式的说明;
 - 3) 序列号。
- b) 表明其符合强制性要求的标志,包括:
 - 1) 标志;
 - 2) 书面描述,如制造商的授权代表、设备的名称、制造年份以及预定用在潜在的爆炸环境中。
- c) 针对安全使用的标志,例如:

- 1) 旋转部件的最高转速;
- 2) 工具的最大直径;
- 3) 设备本身和/或可移除部件的质量 (kg);
- 4) 最大工作载荷;
- 5) 穿戴个体防护设备的必要性;
- 6) 防护装置的调整数据;
- 7) 检查频次。

7.6.2 直接印刷在石油钻采设备上的信息宜持久,并在预期的设备生命周期内保持清晰可见,符号或书面警告不应只写“危险”二字。标志、符号和书面警告应易于理解且含义明确,特别是那些与设备功能相关的部分。与使用书面警告相比,宜优先使用易于理解的符号(象形图)。

7.6.3 只宜采用石油钻采设备使用时所处文化氛围内能够理解的符号和象形图。设备的书面警告宜采用首次使用该设备国家的语言,如有要求,可采用操作者容易理解的语言。

注3: 某些国家对特殊语言的使用有专门的法律要求。

7.6.4 标志应符合公认的标准(如GB/T 3168、ISO 2972或ISO 7000特别是象形图符号和颜色)。

注4: 有关电气设备的标志见GB/T 5226.1。

注5: 有关液压和气动设备的标志见GB/T 3766 和GB/T 7932。

7.7 随行文件

7.7.1 内容

使用手册或其他书面说明(如包装上的说明)应包括:

- a) 关于石油钻采设备运输、搬运和贮存的信息,如:
 - 1) 设备的贮存条件;
 - 2) 尺寸、质量、重心位置;
 - 3) 搬运说明(如显示提升设备施力点的图样)。
- b) 石油钻采设备安装和试运转的有关信息,如:
 - 1) 固定/锚定以及噪声和振动抑制的要求;
 - 2) 装配和安装条件;
 - 3) 使用和维护所需的空间;
 - 4) 允许的环境条件(如温度、湿度、振动、电磁辐射);
 - 5) 设备与动力源的连接说明(尤其是关于防止电气过载的说明);
 - 6) 关于废弃物的清除/处置建议;
 - 7) 必要时,给出使用者应采取的保护措施的建议,如附加安全防护装置安全距离、安全符号和信号。
- c) 关于石油钻采设备自身的信息,如:
 - 1) 设备、设备配件、防护装置和/或保护装置的详细说明;
 - 2) 预定的设备全部应用范围,包括禁止的用途,如果可能,还应考虑样机的变化;
 - 3) 图表(尤其是安全功能的图解表示);
 - 4) 由设备产生的噪声和振动数据,由设备排放的辐射、气体、蒸汽及粉尘等数据,以及参考使用的测量方法(包括测量的不确定度);
 - 5) 电气设备的技术文件(见GB/T 5226.1);

- 6) 证明符合强制性要求的文件。
- d) 有关石油钻采设备使用的信息，如：
 - 1) 预定使用；
 - 2) 手动控制器（执行器）的信息；
 - 3) 设定和调整；
 - 4) 停机的模式和方法（尤其是急停）；
 - 5) 设计者采取的保护措施无法消除的风险；
 - 6) 由某些应用和使用某些配件后产生的特殊风险，以及关于此类应用必要的专用安全防护装置的信息；
 - 7) 可合理预见的误用和禁止的用途；
 - 8) 用于修理和干预后重新启动的故障识别和定位；
 - 9) 需要使用的个体防护设备，以及需要进行培训的信息。
- e) 维护信息，如：
 - 1) 安全功能检查的性质和频次；
 - 2) 关于使用时可能影响操作者健康与安全的备件의 详细说明；
 - 3) 关于需要一定的技术知识或特殊技能，从而只能由熟练人员（如维护人员、专家）来完成的维护工作的说明；
 - 4) 关于无需特殊技能便可由使用者（如操作者）来完成的维护工作（如更换部件等）的说明；
 - 5) 使维护人员能合理完成维护任务（尤其是故障查找任务）的图样和图表。
- f) 关于拆卸、停用和报废的信息。
- g) 关于紧急状态的信息，如：
 - 1) 发生事故或损坏时应遵循的操作方法；
 - 2) 所使用的消防设备类型；
 - 3) 关于可能排放或泄漏有害物质的警告，如有可能指明消除其影响的措施。
- h) 需要相互明显区别开的为技术熟练人员提供的维护说明和为非熟练人员提供的维护说明。

7.7.2 使用手册的编制

以下要求适用于使用手册的编制和表述。

- a) 印刷字体和大小应尽可能保证最好的清晰度。安全警告和/或注意事项宜使用颜色、符号和或大号字体加以强调。
- b) 应给出使用信息的初始版本以及采用首次使用该设备国家的语言编写的版本。如果使用一种以上的语言，则每一种语言都宜便于与其他语言区分，并尽量将译文和相关插图放在一起。

注6：某些国家对特殊语言的使用有专门的法律要求。

- c) 只要有助于理解宜为文字配插图。这些插图宜由详细的文字说明进行补充，从而能够找到手动控制器（执行器）等的位置并识别出来。插图不宜与随行的文字说明分开，并宜按操作顺序给出。
- d) 以表格形式给出信息有助于理解时宜考虑以表格形式给出，表格宜靠近相关的文字说明。
- e) 宜考虑使用颜色，尤其是对于要求快速识别的组件。
- f) 如果使用信息很长，则宜给出内容的列表和/或索引。
- g) 包含有需要立即采取的措施的安全相关说明书，宜以便于操作者可随时获取的形

式给出。

7.7.3 使用信息的起草与编辑

以下要求适用于使用手册的起草和编辑。

- a) 与样机的关系：该信息应明确的与石油钻采设备的特定样机及必要的其他合适证明（如通过序列号）相关联。
- b) 信息传递原则：准备使用信息时，为了获得最佳效果宜遵循“察看—思考—使用”的信息传递过程和顺序。宜预先提出“如何做？”、“为什么？”等问题并给出答案。
- c) 使用信息应尽量简明，术语及单位前后的表述宜保持一致，对不常用的技术术语，宜给出明确的解释。
- c) 如果预计石油钻采设备将用于非专业使用，则宜以便于非专业使用者理解的形式编写说明书。如果为安全使用设备而需要使用个体防护设备时，则宜在设备和包装等上面给出明确建议，使这类信息在销售时得以明显显示。
- d) 文件的耐久性和可获得性：给出使用说明的文件宜持久耐用（即能经受住使用者频繁拿取翻看），在文件上宜标出“留置备查”。如果采用电子形式保存使用信息，则关于需要立即采取措施的安全相关问题的信息应经常进行备份，供随时获取。

8 风险评估和风险减小的文件

风险评估和风险减小的文件应说明所遵从的程序以及得到的结果。该文件应包括下列内容：

- a) 已评估的石油钻采设备（如规格、限制、预定使用）；
- b) 已做的任何相关假设（载荷、强度、安全系数等）；
- c) 风险评估中所识别的危险、危险状态以及所考虑的危险；
- d) 风险评估所依据的信息：
 - 1) 所使用的数据及原始资料（事故历史记录适用于类似机设备的风险减小经验等）；
 - 2) 与所使用的数据有关的不确定性及其对风险评估的影响。
- e) 通过保护措施所到的风险减小目标；
- f) 用于消除识别的危险或减小风险的保护措施；
- g) 与该石油钻采设备有关的剩余风险；
- h) 风险评估的结果；
- i) 风险评估过程中完成的所有表格。

上述f)中所提到的用于选保护措施的标准或其他规范宜注明来源。

注：本文件不要求与石油钻采设备一起提交风险评估文件。有关文件的信息见 GB/T 16856-2015。

9 采用合适的产品安全标准

9.1 概述

本文件中风险评估和风险减小措施是针对石油钻采设备的基础安全提出的设计原则。如果设备存在相应的产品安全标准（石油钻采设备安全专业标准），则应优先使用。由于产品安全标准识别了通常与一种石油钻采设备相关的重大危险，并且规定了处理这些危险的保护措施/风险减小措施，因此针对一种石油钻采设备采用这些标准便于风险评估的开展。但是

采用这些产品安全标准并不能免除按照本文件进行风险评估的责任。因此，应用这类标准要求的设计者宜确保该标准与具体的设备相适应并且涵盖了所有存在的风险。如果该石油钻采设备标准存在没有涵盖的危险，则需要针对这些危险按照本文件进行完整的风险评估，并且宜采取合适的保护措施/风险减小措施处理这些危险。

9.2 遵循的步骤

- a) 查找合适的产品安全标准：这类标准最大程度的给出了特定石油钻采设备关于安全方面的指南。
- b) 检查范围：如果该石油钻采设备存在相应的产品安全标准，则设计者需要检查该标准的范围在设备限制方面是否完全涵盖实际的设备。
- c) 根据产品安全标准检查重大危险：如果b的结果表明该石油钻采设备存在相应的产品安全标准，则设计者需要细查该标准是否涵盖实际设备的用途和相关的所有重大危险。此外，设计者还需检查该标准规定的保护措施/风险减小措施是否适用于该设备。

注1：这个过程已涵盖了风险估计。因此，对于此类标准的重大危险，设计者不必再单独进行风险估计。

- d) 采用标准：
 - 1) 采用产品安全标准：如果b和c得到满足，则宜采用此产品安全标准中规定的保护措施/风险减小措施，同时可认为该石油钻采设备通过充分风险减小达到了可接受的风险。
 - 2) 采用产品安全标准，但应确定此标准范围之外的所有部件并识别相关的危险，即如果b和c其中一项或均没有满足，则设计者宜根据所选择的产品安全标准确定该石油钻采设备的哪些部件和/或重大危险、危险状态或危险事件需要考虑。对于所选择的产品安全标准没有涵盖的石油钻采设备部件和/或重大危险、危险状态或危险事件，宜根据本文件并结合通用安全标准（见图6）进行风险评估和风险减小。

注2：图6给出了可参考的通用设计安全标准，但并非所有现有的安全标准完整清单。

- 3) 如果石油钻采设备没有相应的产品安全标准，则结合通用安全标准（见图6）并根据本文件进行风险评估和风险减小，GB/T 16856-2015给出了分析评估的实施指南和方法举例。

通用安全标准					
与危险相关的标准			与危险相关的标准		
噪声	有害物质	振动与冲击	尺寸与距离标准	动力源	安全装置
工作位置发射声压级的测定, GB/T 17248	空气传播的有害物质排放的评估, GB/T 25749	全身振动, GB/T 13441	避免挤压的间隙, GB/T 12265	电气设备, GB/T 5226.1	防护装置, GB/T 8196
声功率级和声压级的测定, GB/T 6881.1~6881.2、GB/T 3767、GB/T 6882、GB/T 3768、GB/T 16538	减少有害物质对健康的风险, GB/T 18569	手臂振动, GB/T 19739	最小距离, GB/T 19876	液压设备, GB/T 7932	联锁装置, GB/T 17248
	卫生要求, GB/T 19891	手持式和手导式机械, GB/T 25631	安全距离, GB/T 23821	气动设备, GB/T 3766	双手操纵装置, GB/T 19671
声强法测定声功率级, GB/T 16404	热危险	人类工效学	进入机械的固定设施, GB/T 17888	控制系统	电敏保护装置, GB/T 19436.1~19436.2、GB 19436.3
隔声罩的隔声性能, GB/T 18669	人类接触热表面的反应, GB/T 18153	开口尺寸, GB/T 18717	警报和报警	防止意外启动, GB/T 19670	压敏保护装置, GB/T 17454
隔声间的隔声性能, GB/T 19885	火灾危险	工作台人类工效学要求, ISO 14738	安全标志设计原则, GB/T 2893.1	控制系统安全相关部件的设计, GB/T 16855.1	
	火灾防治, GB/T 23819	计算机人体模型和人体模板, GB/T 23702.1	登记的安全标记, ISO 7010	控制系统安全相关部件的确认, GB/T 16855.2	机械装配
机器和设备噪声发射值的标示和验证, GB/T 14574	电气危险	辐射危险	险情听觉信号, GB/T 1251.1	急停功能 GB/T 16754	集成制造系统 GB/T 16655
	防电击保护, GB/T 5226.1	激光术语 GB/T 15313	视觉、听觉和触觉信号, GB/T 18209.1		

图 6 根据危险种类、特征和技术分类的通用安全标准（不是全部）

参 考 文 献

- [1] GB/T 1251.1 人类工效学 公共场所和工作区域的险情信号 险情听觉信号
- [2] GB/T 2893.1 图形符号 安全色和安全标志 第1部分：安全标志和安全标记的设计原则
- [3] GB/T 3168 数字控制机床 操作指示形象化符号
- [4] GB/T 3766 液压传动 系统及其元件的通用规则和安全要求
- [5] GB/T 3767 声学 声压法测定噪声源声功率级和声能量级 反射面上方近似自由场的工程法
- [6] GB/T 3768 声学 声压法测定噪声源声功率级和声能量级 采用反射面上方包络测量面的简易法
- [7] GB/T 3836.4 爆炸性环境 第4部分：由本质安全型“i”保护的设备
- [8] GB/T 5226.1 机械电气安全 机械电气设备 第1部分：通用技术条件
- [9] GB/T 6881 声学 声压法测定噪声源声功率级和声能量级 混响室精密法
- [10] GB/T 6882 声学 声压法测定噪声源声功率级和声能量级 消声室和半消声室精密法
- [11] GB/T 7932 气动 对系统及其元件的一般规则和安全要求
- [12] GB/T 8196 机械安全 防护装置 固定式和活动式防护装置设计与制造一般要求
- [13] GB/T 12265 机械安全 防止人体部位挤压的最小间距
- [14] GB/T 13441（所有部分）机械振动与冲击 人体暴露于全身振动的评价
- [15] GB/T 14048.5 低压开关设备和控制设备 第5—1部分：控制电路电器和开关元件机电式控制电路电器
- [16] GB/T 14574 声学 机器和设备噪声发射值的标示和验证
- [17] GB/T 15241 人类工效学 与心理负荷相关的术语
- [18] GB/T 15241.2 与心理负荷相关的工效学原则 第2部分：计原则
- [19] GB/T 15313 激光术语
- [20] GB/T 15706 机械安全 设计通则 风险评估与风险减小
- [21] GB/T 16404 声学 声强法测定噪声源的声功率级 第1部分：离散点上的测量
- [22] GB/T 16538 声学 声压法测定噪声源声功率级 现场比较法
- [23] GB/T 16655 机械安全 集成制造系统 基本要求
- [24] GB/T 16754 机械安全 急停功能 设计原则
- [25] GB/T 16855.1 （所有部分）机械安全 控制系统有关安全部件
- [26] GB/T 16856 机械安全 风险评估 实施指南和方法举例
- [27] GB/T 17248 工作位置发射声压级的测定
- [28] GB/T 17454 （所有部分）机械安全 压敏保护装置
- [29] GB/T 17888 （所有部分）机械安全 接近机械的固定设施
- [30] GB/T 18153 机械安全 可接触表面温度 确定热表面温度限值的工效学数据
- [31] GB/T 18209（所有部分）机械安全 指示、标志和操作
- [32] GB/T 18569 （所有部分）机械安全 减小由机械排放的有害物质对健康的风险
- [33] GB/T 18699（所有部分）声学 隔声罩的隔声性能测定
- [34] GB/T 18717（所有部分）用于机械安全的人类工效学设计
- [35] GB/T 18831 机械安全 带防护装置的联锁装置 设计和选择原则
- [36] GB/T 19436.1 机械电气安全 电敏保护设备 第1部分：一般要求和试验

- [37] GB/T 19436.2 机械电气安全 电敏保护装置 第2部分：使用有源光电保护装置（AOPDs）设备的特殊要求
- [38] GB 19436.3 机械电气安全 电敏防护装置 第3部分：使用有源光电漫反射防护器件（AOPDDR）设备的特殊要求
- [39] GB/T 19670 机械安全防止意外启动
- [40] GB/T 19671 机械安全 双手操纵装置 设计和选择原则
- [41] GB/T 19678.1 使用说明的编制 构成、内容和表示方法 第1部分：通则和详细要求
- [42] GB/T 19739 机械振动与冲击 手臂振动 手臂系统为负载时弹性材料振动传递率的测量方法
- [43] GB/T 19876 机械安全 与人体部位接近速度相关的安全防护装置的定位
- [44] GB/T 19885 声学 隔声间的隔声性能测定 实验室和现场测量
- [45] GB/T 19886 声学 隔声望和隔声间噪声控制指南
- [46] GB/T 19891 机械安全 机械设计的卫生要求
- [47] GB/T 20000.1 标准化工作指南 第1部分：标准化和相关活动的通用术语
- [48] GB/T 20431 声学 消声器噪声控制指南
- [49] GB/T 20438（所有部分）电气 电子 可编程电子安全相关系统的功能安全
- [50] GB/T 23702.1 人类工效学 计算机人体模型和人体模板 第1部分：一般要求
- [51] GB/T 23819 机械安全 防火与消防
- [52] GB/T 23821 机械安全 防止上下肢触及危险区的安全距离
- [53] GB/T 25078.1 声学 低噪声石油钻采设备和设备设计实施建议 第1部分：规划
- [54] GB/T 25631 机械振动 手持式和手导式机械 振动评价规则
- [55] GB/T 25749（所有部分）机械安全 空气传播的有害物质排放的评估
- [56] GB/T 26118.1 机械安全 机械辐射产生的风险的评价与减小 第1部分：通则
- [57] GB/T 26118.3 机械安全 机械辐射产生的风险的评价与减小 第3部分：通过衰减或屏蔽减小辐射
- [58] ISO 2972 Numerical control of machines—Symbols
- [59] ISO 7000 Graphical symbols for use on equipment—Index and synopsis
- [60] ISO 7010 Graphical symbols—Safety colours and safety signs—Registered safety signs
- [61] ISO 14738 Safety of machinery—Anthropometric requirements for the design of workstations at machinery
- [62] IEC 61000—6（all parts）Electromagnetic compatibility（EMC）—Part 6: Generic standards
- [63] IEC 61029（all parts）Safety of transportable motor—operated electric tools
- [64] IEC 61496（all parts）Safety of machinery—Electro—sensitive protective equipment
- [65] IEC 62061 Safety of machineryFunctional safety of safety—related electrical, electronic and programmable electronic control systems

