第3章

安全风险评估

3.1 概述

安全风险评估是设计安全相关控制系统的根本依据。评估的主要内容包括：使用设备的安全风险点，降低风险需要的安全相关控制功能，风险降低措施及安全相关控制功能的SIL。在标准IEC 62061中，机械设计和风险评估采用ISO 12100《机械安全 设计通用原则：风险评估和风险降低》及ISO 14121《机械安全 风险评估》中规定的方法。

ISO 12100标准中规定了机械设计过程中用于实现机械安全的基本术语、原则和方法，以及风险评估与风险降低的原则，帮助设计者实现机械安全的目标。这些原则基于机械相关设计、使用、事件、事故和风险的知识和经验。标准还规定了在机械生命周期的相应阶段内识别危险、估计和评价风险的程序，消除危险或充分降低风险的程序，以及记录和验证风险评估与风险减少程序的指南。

ISO 14121是机械安全标准中的重要方法性标准，它规定了降低风险的一般原则，并统称为风险评估。风险评估考虑了机械相关设计、生产、运输、安装、使用和拆卸等产品生命周期内的各个阶段，提供了进行风险评估所需要的信息，规定了用于识别危险、评估风险和评定风险的程序。该标准对确定机械产品安全和证明产品进行过风险评估所要求的证书类型提供指导。

标准IEC 62061的附录A中，也给出了风险评估和SIL分配的定性方法示例，适用于机器的SRCF。因此，本章将结合标准ISO 12100、ISO 14121，对标准IEC 62061的附录A进行解读，并详细阐述符合标准要求的安全相关控制系统的风险评估方法。

3.2 风险评估

风险评估是以系统方法对机械相关风险进行分析和评定的一系列逻辑步骤。需要时，风险评估之后采用ISO 12100中所描述的方法降低风险。当采取保护措施尽可能消除危险和充分降低风险时，重复进行风险评估是必要的。

3.2.1 SIL 分配概述

【IEC 标准条款】

Annex A

SIL assignment

A.1 General

This informative Annex provides one example of a qualitative approach for risk estimation and SIL assignment that can be applied to SRCFs for machines. Examples of other techniques that may be used for SIL assignment are given in IEC 61508-5 and will be outlined in a proposed future IEC TC 44 Technical Specification.

NOTE 1 The methodology described in this Annex uses qualitative estimation of risk and is intended to be generally applied for the assignment of a SIL(s) to SRCF(s) of machines. The risk parameters used whilst applying this methodology to particular machines and their specific hazards should be subject to agreement with those involved to ensure that the SRECS can provide adequate risk reduction.

NOTE 2 In a large number of machine specific standards ("C" type standards in CEN) risk estimation has been carried out to select a required Category in accordance with ISO 13849-1:1999 for safety-related parts of machine control systems. It is noted that, for simplification, the following relationships are commonly used: required Category 1 to required SIL 1, required Category 2 to required SIL 1, required Category 3 to required SIL 2 and required Category 4 to required SIL 3. More comprehensive methods of mapping between required Categories of ISO 13849-1:1999 and required SILs used in this international standard are under consideration.

For each specific hazard, the safety integrity requirements should be determined separately for the safety-related control function(s) to be performed by the SRECS (see 5.2.4.2).

Figure A.1 is an example of a practical way of carrying out a risk assessment at a specific hazard leading to estimation of a SIL requirement for a SRECS function. This methodology should be performed for each risk that is to be reduced by a safety-related control function that is to be implemented by a SRECS. Figure A.1 should be used in conjunction with the guidance information in this Annex.

Risk estimation is an iterative process, this means that the process will need to be carried out more than once.

Figure A.1 shows a feedback arrow to risk estimation. This is required because the provision of a particular protective measure to implement an SRCF may have an affect on the risk parameters (e.g. the use of a protective light curtain may result in a greater frequency of access). A failure of the light curtain will then expose the operator to a greater risk than originally envisaged. This requires that the process should be repeated following the same method but using the amended risk parameter(s).

At the end of the process shown in Figure A.1 , the SIL estimated is the SIL requirement for the safety-related control function.

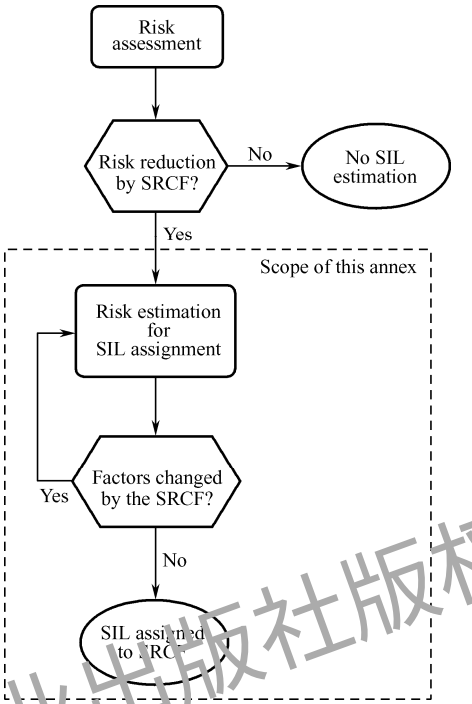

Figure A.1– Workflow of SIL assignment process

【非标准条款】

附　录　A
SIL 分配

A.1 概述

本附录提供了风险评估和 SIL 分配的定性方法的示例，适用于机器的 SRCF。在 GB/T 20438.5 中有用于 SIL 分配的其他技术的例子，并且将会在即将提出的 IEC TC44 技术规范中略述。

注 1：本附录所描述的方法论使用风险的定性评估，通常适用于对机器的 SRCF 的 SIL 分配。对特定的机器应用这种方法时所使用的风险参数和其具体的危险应与相关人员协议，以确保 SRECS 能够将风险降至足够低。

注 2：大量的机器特定标准（CEN 中的“C”类标准）中执行了风险评估，按照 GB/T 16855.1 中机器控制系统有关安全部件选择要求的类别，为了简化，要注意下列常用的关系：要求的类别 1——要求的 SIL1；要求的类别 2——要求的 SIL1；要求的类别 3——要求的 SIL2；要求的类别 4——要求的 SIL3。GB/T 16855.1 所要求的类别和本标准所要求的 SIL 之间更多映射的综合方法在考虑中。

对于每一个特定危险，其安全完整性要求由 SRECS 执行的安全相关控制功能分别决定（见 5.2.4.2）。

图 A.1 是一个在特定危险处进行风险评估的实用方法示例，该方法可用于评估 SRECS 功能的 SIL 要求。对于每个风险应执行这种评估方法，这些风险会通过 SRECS 执行的安全相关控制功能而降低。图 A.1 应与本附录的指导信息结合使用。

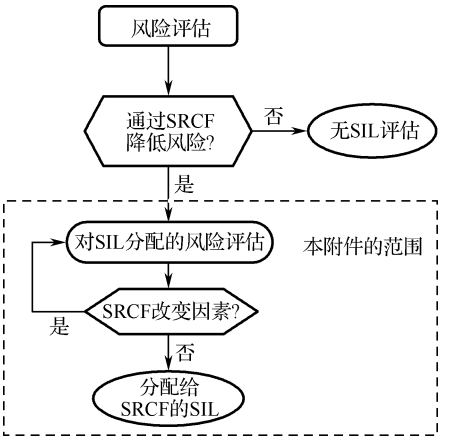

图 A.1 SIL 分配过程的工作流程

风险评估是一个迭代过程，这是指该过程需要不止一次地执行。

图 A.1 显示了风险评估的反馈箭头，这是必要的，因为提供特殊保护措施来执行 SRCF 可能对风险参数有影响（例如，使用保护光幕可能会导致更大的访问频率）。光幕失效将操作者暴露到比最初设想的更大的风险中。这要求遵循相同的方法重复该过程，但使用的是修改过的风险参数。

在图 A.1 所示的过程结束时，经过评估的 SIL 就是安全相关控制功能要求的 SIL。

安全完整性（Safety Integrity）是指在所有规定情况下，安全控制系统或其子系统圆满执行所要求的安全相关控制功能的概率，由硬件安全完整性和软件安全完整性组成。安全完整性等级越高，其未能执行所要求的安全相关控制功能的概率就越低。

安全完整性等级（Safety Integrity Level，SIL），是一种离散的等级，用于规定分配给 SRECS 的安全相关控制功能的安全完整性要求。在这里，安全完整性等级 3（SIL3）是最高的，安全完整性等级 1（SIL1）是最低的。IEC 62061 标准不考虑 SIL4，因为一般情况下 SIL4 不适合用于对机械相关风险的评估。IEC 62061 标准提供了一种 SIL 分配方法，该方法能对安全风险进行评估并给出量化的 SIL 值。

3.2.2 风险评估和 SIL 分配

如果风险评估判定控制器失灵，或者保护装置的故障可能带来超过容许程度的严重风险，则必须将该风险的概率降低至剩余风险可以被接受的程度，也就是说该控制系统必须达到“安全等级”。

IEC 62061 附录 A 中提供了一个计算公式，采用一种对风险进行分级的方法，进行概率、量化分析，形成相关安全功能的安全完整性等级（SIL）。

1．危险识别/指示

【IEC 标准条款】

A.2 Risk estimation and SIL assignment

A.2.1 Hazard identification/indication

Indicate the hazards, including those from reasonable foreseeable misuse, whose risks are to be reduced by implementing an SRCF. List them in the hazard column in Table A.5.

【GB 标准条款】

A.2 风险评估和 SIL 分配

A.2.1 危险识别/指示

指示危险，包括可预见的误用所引起的危险，通过执行 SRCF 降低风险。将它们在表 A.5 的“危险”列（栏）中列出。

1）危险因素

安全工作的核心是危险的识别。危险源是指可能导致伤害或疾病、财产损失、工作环境破坏或这些情况的组合发生的根源或状态。它的特性包括以下方面。

- 客观现实性：存在于客观现实中，不以人的主观认识为转移。
- 潜在性：不易被意识到或发觉到；虽然显暴露，但没有转变为现实的危害。
- 复杂多变性：受制于作业情况，并随作业情况的变化而变化。
- 可知可防性：危险源可以辨别并能采取一定的手段去预防。

危险的分类有多种维度。例如，GB/T 6441—1986《企业职工伤亡事故分类》中，综合考虑起因物、引起事故先发的诱导性原因、致害物、伤害方式等后，将危险因素分为 20 类。

2）危险识别

危险识别应遵循科学性、系统性、全面性和预测性原则，危险识别的方法可分为对照法和安全分析法两类。

对照法是一种基于经验的方法，即与相关技术安全规范、标准、操作规程及以往类似工作经验进行对照从而识别危险源的方法，具体包括询问交谈法、检查表法、现场观察法、查阅外部信息法、查阅相关记录法等。对照法的优点是操作简单、易行；缺点是重点不突出且容易遗漏，尤其是无先例的新活动应用该方法较为困难。

IEC 62061 标准选择的是另外一种识别方法——安全分析法。安全分析法是通过揭示导致故障或事故的各种因素及相互关联来辨识系统中的危险源的方法，具体包括危险与可操作性（HAZOP）研究、工作任务分析、事件树分析（ETA）、故障树分析（FTA）等。安全分析法的优点是系统、全面；缺点是对人员素质的要求高。

2．风险评估

【IEC 标准条款】

A.2.2 Risk estimation

Risk estimation should be carried out for each hazard by determining the risk parameters that

as shown in Figure A.2 should be derived from the following:

– severity of harm, Se; and

– probability of occurrence of that harm, which is a function of:

- frequency and duration of the exposure of persons to the hazard, Fr;
- probability of occurrence of a hazardous event, Pr; and
- probability to avoid or limit the harm, Av.

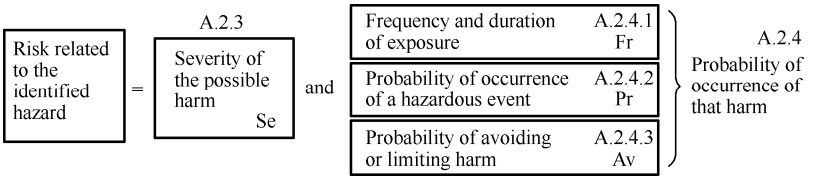

Figure A.2–Parameters used in risk estimation

The estimates entered into Table A.5 should normally be based on worst-case considerations for the SRCF. However, in a situation where, for example, an irreversible injury is possible but at a significantly lower probability than a reversible one, then each severity level should have a separate line on the table. It may be the case that a different SRCF is implemented for each line. If one SRCF is implemented to cover both lines, then the highest target SIL requirement should be used.

【GB 标准条款】

A.2.2 风险评估

应通过确定风险参数对每个危险进行风险评估。如图 A.2 所示，风险参数来源于下列要素：

——伤害严重程度，Se；

——伤害发生概率，它是下列因素的函数：

- 人暴露在危险中的频率和持续时间，Fr；
- 危险事件发生概率，Pr；
- 避免或者限制伤害发生的概率，Av。

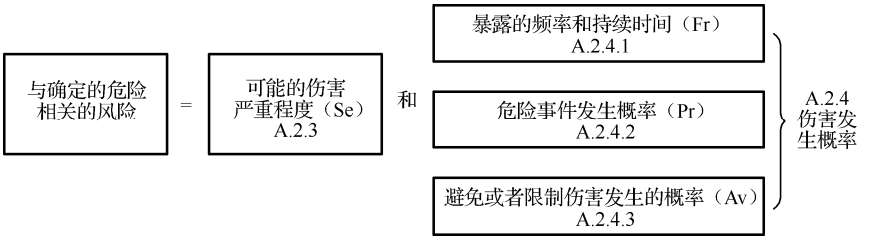

图 A.2 用于风险评估的参数

进行表 A.5 的评估通常是以对 SRCF 最坏情况的考虑为基础的。然而，在一种情况下，如有一个不能挽回的伤害可能发生，但是比可以挽回的伤害的发生概率要低得多，那么每一个严重程度等级应在表格中占单独一行。可能每一行都执行不同的 SRCF。如果两

行执行同一个 SRCF，那么应使用最高目标 SIL 要求。

风险评估可通过以下 4 种风险因素进行判定，包括：

（1）伤害严重程度（Se）；

（2）暴露的频率和持续时间（Fr）；

（3）危险事件发生概率（Pr）；

（4）避免或限制伤害发生的概率（Av）。

这些风险因素构成了实现安全相关控制功能的输入参数，采用这些输入参数，可以将风险分摊给安全相关控制功能。

3．伤害严重程度

【IEC 标准条款】

A.2.3 Severity (Se)

Severity of injuries or damage to health can be estimated by taking into account reversible injuries, irreversible injuries and death. Choose the appropriate value of severity from Table A.1 based on the consequences of an injury, where:

4 means a fatal or a significant irreversible injury such that it will be very difficult to continue the same work after healing, if at all.

3 means a major or irreversible injury in such a way that it can be possible to continue the same work after healing. It can also include a severe major but reversible injury such as broken limbs;

2 means a reversible injury, including severe lacerations, stabbing, and severe bruises that requires attention from a medical practitioner;

1 means a minor injury including scratches and minor bruises that require attention by first aid.

Select the appropriate row for consequences (Se) of Table A.1. Insert the appropriate number under the Se column in Table A.5.

Table A.1–Severity (Se) classification

Consequences	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

【GB 标准条款】

A.2.3 严重程度（Se）

伤害或者损坏健康的严重程度能够通过可以挽回的伤害、不可挽回的伤害和死亡来进

行评估。根据伤害的后果从表 A.1 中选择严重程度的适当值，其中：

4 代表致命的或者严重且不能挽回的伤害，在康复后难以进行相同的工作，即使有也极少；

3 代表严重或者不能挽回的伤害，但在康复后存在可以继续从事相同工作的可能性，同时它还包括重大的但可以挽回的伤害，比如断肢；

2 代表可以挽回但需要专业医疗护理的伤害，包括严重的破口、刺伤及严重的撞伤；

1 代表需要急救护理的较小伤害，包括擦伤和较轻的撞伤。

根据伤害的后果在表 A.1 中选择适当的行。在表 A.5 的“Se”列中填入适当的数字。

表 A.1 严重程度（Se）等级

后 果	严重程度（Se）
不可挽回：死亡、失去眼睛或者胳膊	4
不可挽回：断肢、断指	3
可挽回：要求医疗	2
可挽回：要求急救	1

标准条款 A.2.3 定义了伤害的严重程度量化值，使用时可通过评估确定量化值。具体的例子详见第 8 章。

4．伤害发生概率

【IEC 标准条款】

A.2.4 Probability of occurrence of harm

Each of the three parameters of probability of occurrence of harm (i.e. Fr, Pr and Av) should be estimated independently of each other. A worst-case assumption needs to be used for each parameter to ensure that SRCF(s) are not incorrectly assigned a lower SIL than is necessary. Generally, the use of a form of task-based analysis is strongly recommended to ensure that proper consideration is given to estimation of the probability of occurrence of harm.

A.2.4.1 Frequency and duration of exposure

Consider the following aspects to determine the level of exposure:

• need for access to the danger zone based on all modes of use, for example normal operation, maintenance; and

• nature of access, for example manual feed of material, setting.

It should then be possible to estimate the average interval between exposures and therefore the average frequency of access.

It should also be possible to foresee the duration, for example if it will be longer than 10 min. Where the duration is shorter than 10 min, the value may be decreased to the number in the row below in Table A.2. This does not apply to frequency of exposure≤1h, which should not be decreased at any time.

NOTE The duration is related to the performance of activities that are carried out under the