保密等级
公开

Q/DX

青岛鼎信通讯股份有限公司技术文档

Q／DX D121.096-2022

设备安全方案配置规范

V1.0

2022-09-30 发布　　2022-12-15

青岛鼎信通讯股份有限公司　　发布

目　　次

前　　言

针对公司线体、单机类设备的安全防护配置方案的设计及安全等级系数的计算。在编制过程中参考了IEC 61508电气/电子/可编程电子安全相关系统的功能安全、ISO12100 机械安全 基本概念与设计通则等相关要求。

此规范作为机电工程师设计中安全方案配置规范和评审依据。

本规范由青岛鼎信通讯股份有限公司自动化工程部负责制定和解释。

本标准由青岛鼎信通讯股份有限公司标准化小组起草。

本标准主要起草人： 刘文龙

设备安全方案配置规范

1 范围

本规范适用于青岛鼎信通讯有限公司线体、单机等设备安全防护方案的设计、评审。

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。

IEC 61508 电气/电子/可编程电子安全相关系统的功能安全

ISO 12100-1/2 机械安全 基本概念与设计通则 第1部分和第2部分

ISO 14121 风险评价原则

3 定义

3.1风险

发生危害的概率与危害严重程度的组合（风险=危害的严重性X危害发生的概率）。

3.2安全

免于难以承受的风险。

3.3风险评价

为了确保工作人员和其他人员的安全，并将危害发生可能性降到最低的安全确认方法。包含：明确机器的预期用途和使用条件并评估不正确的使用方法；识别机器存在的危险；对风险程度以及存在风险状态的频率进行评估；判断风险程度是否以降低到可接受的水平。

3.4防护措施

旨在实现风险降低的措施，可分为由设计者实施的防护措施和由用户实施的防护措施。

3.5性能等级（PL）

定义控制系统的安全相关部分的能力，以使其在可预见条件下执行安全功能。

3.6所要求的性能等级（PLr）

用于实现每项安全功能所需要的风险降低。

4 设计方案说明

4.1 机械设计流程

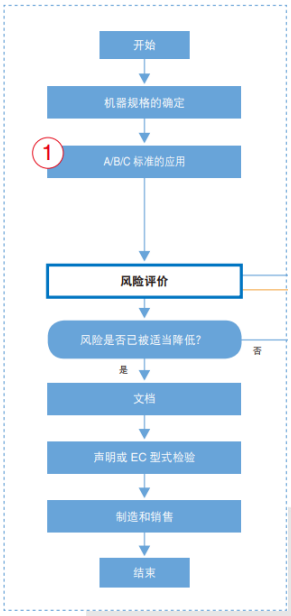

图4.1 机械设计流程

A/B/C标准类型：

A类标准：基本安全标准包括适用于各种产品和系统的一般安全相关的基本概念、原则和要求。

B类标准：成组安全标准包括适用于集中产品或系统或者类似系列产品或系统，且尽可能参照基本安全标准的安全要求。

C类标准：产品安全标准包括使用与特定产品或系统或者系列产品和系统，且尽可能参照基本安全标准的安全要求。

4.2 风险评价流程

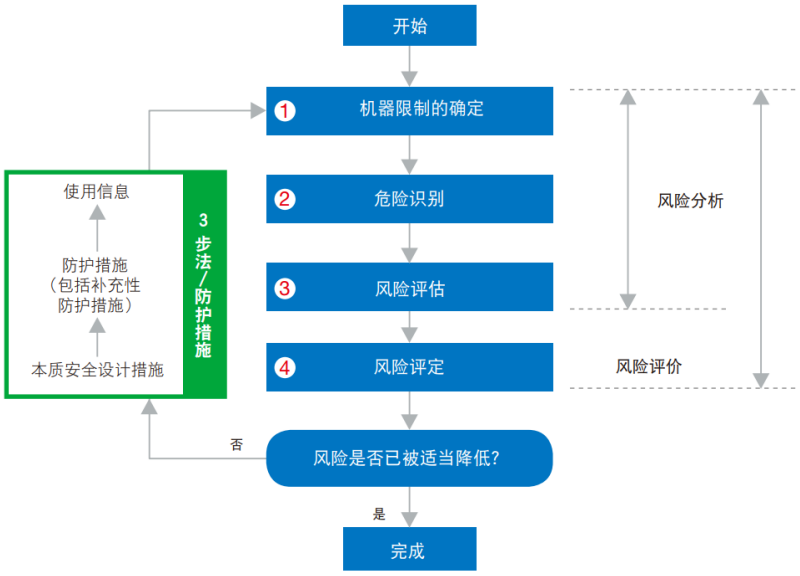

图4.2 风险评价流程

4.2.1机器限制：

使用限制：包括预期应用和合理可预见的误用。

空间限制：包括运动范围或人机交互（如操作员与机器界面）范围。

时间限制：包括机械和/或某些零件的寿命极限。

4.2.2机械危险：

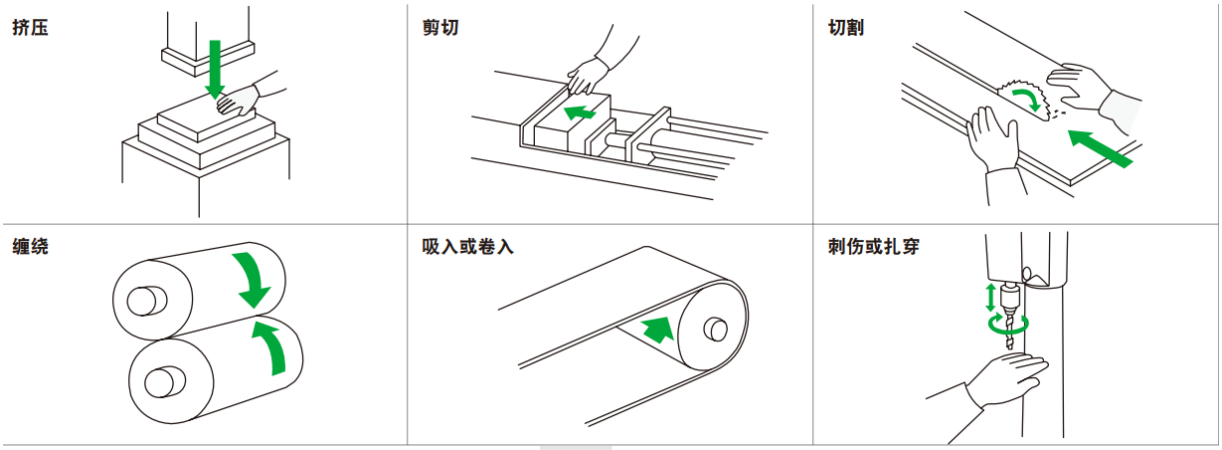

图4.2.2 机械危险

其他危险：

电气危险、热危险、噪声引起的危险、振动引起的危险、辐射引起的危险、材料和物质引起的危险以及因忽略人体工学原理而引起的危险等。

4.2.3风险评估（风险评估矩阵：危害的严重性X危害发生的概率）：

		伤害或疾病的严重性			
		致命	严重	中等	轻微
伤害或致病的可能性	极高	5	5	4	3
	较高	5	4	3	2
	可能	4	3	2	1
	低	4	3	1	1

表4.2.3 风险评估矩阵

4.2.4风险评定

风险	优先事项	
4至5	高	必须立即采取降低风险的措施。在采取措施前必须停止操作。必须投入充足的管理资源。
2至3	中等	必须及时采取降低风险的措施。在采取措施前最好避免使用机器。必须优先投入管理资源。
1	低	如有必要，应采取降低风险的措施。

表4.2.4 风险评定

4.3 3步法及防护措施

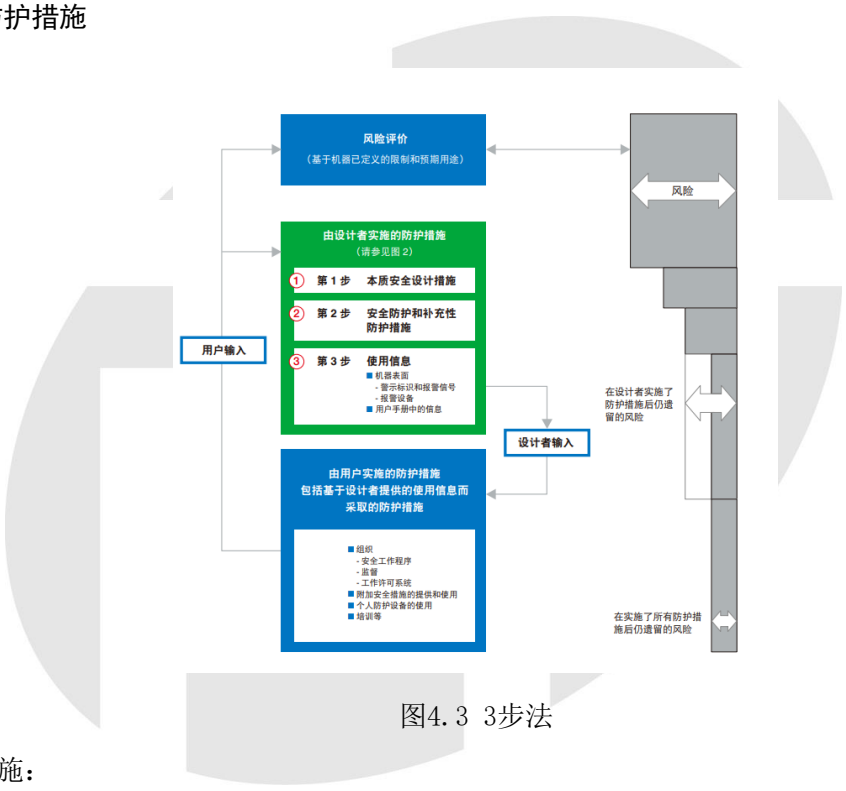

图4.3 3步法

本质安全设计措施：

通过改变机器设计或操作特性而无需采取防护措施或采用保护装置消除危险或降低与危险相关风险。

安全防护：

使用安全装置保护人员免除无法合理消除的危险或安全设计措施不足以降低的风险。

补充防护措施：

非本质安全设计措施、也非安全防护（防护装置和/或保护装置的落实）或使用信息，应按机器预期用途和合理可预见的误用要求来实施。

使用信息：

包括单独或组合使用的通讯链路（如文本、文字、标志、信号、符号、图表等），以便向用户传递信息。

5 性能等级确定

5.1 所需性能等级 PLr 计算

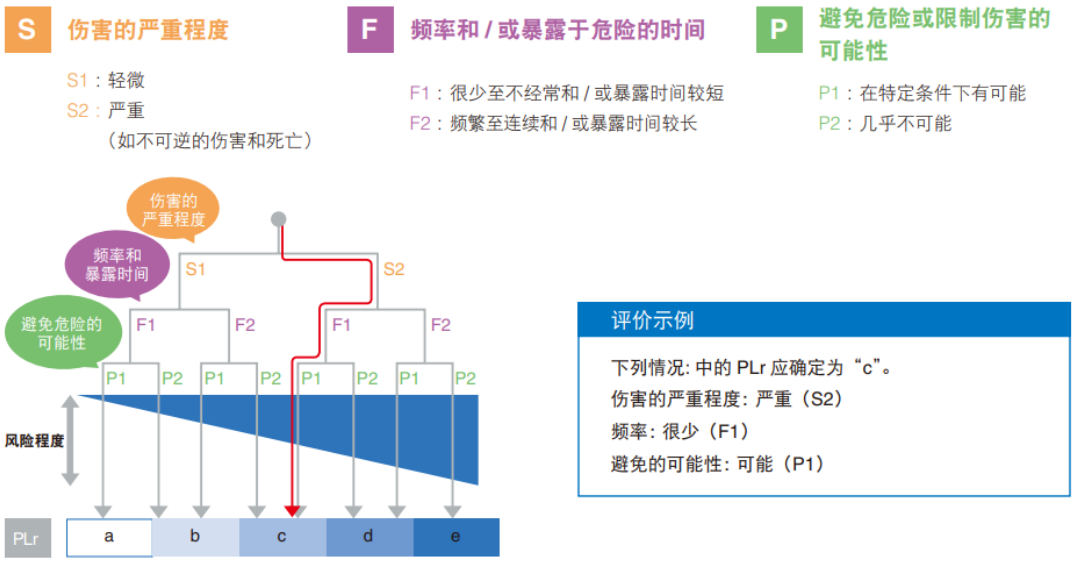

图5.1 性能等级PLr

5.2 性能等级 PLr 计算

PL

参数	详细情况	等级
类别	类别是用于实现特定性能等级的基本参数。它表述了控制系统的安全相关部分在出现故障的情况下所需的行为。（请参见第 21 页的其他详细信息）	B 1 2 3 4
DC	它是指对安全相关控制系统的诊断覆盖。DC 值分为四个等级。（请参见第 22 页的其他详细信息）	高（≥ 99%） 中等（90% 至 99%） 低（60% 至 90%） 无（< 60%）
MTTFd	它是指安全相关系统的全部或部分危险失效平均时间。每个通道的 MTTFd 值分为三个等级。（请参见第 22 页的其他详细信息）	高（30 至 100 年） 中等（10 至 30 年） 低（3 至 10 年）
CCF	它是指整个安全相关控制系统在可预见共因失效方面的可靠性。 它可分为两个类型：≥ 65 点和 < 65 点。（请参见第 22 页的其他详细信息）	≥ 65 点 < 65 点

表5.2 性能等级PLr计算

图5.2 性能等级PLr计算

版本记录

版本编号/修改状态	拟制人/修改人	审核人	批准人	备注
V1.0	刘文龙	沙冲	沙冲	