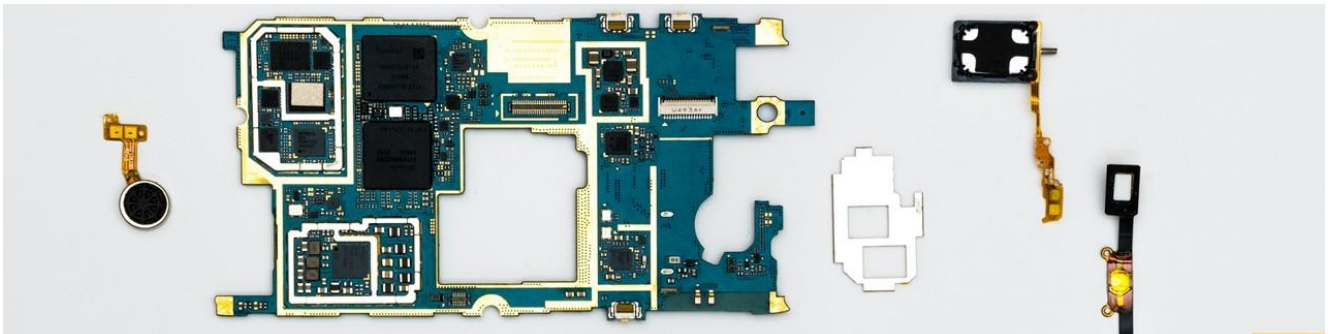


SAFETY FUNCTION LIST EXAMPLE

<SPC200>

<SAFETY FUNCTION LIST>



SAFETY DESIGNER ENGINEERING TOOL 2023.11

2024 PRAJNASAFE



若彗电子科技

安全解决方案先行者

文档声明

<为求准确，本手册已经过验证和复审。后续手册可能变动，恕不另行通知。对直接或间接地由于产品与手册之间的错误、遗漏或差异而引起的损害，若彗电子科技（上海）有限公司不承担任何责任。>

本文为若彗电子科技(上海)有限公司财产，包含该公司的商业秘密。
对本文任何未经授权的使用和传播都是严格禁止的。

历史记录

版本号	编写日期	拟稿	审核	描述
V1.0.0	2025/8/13	Scholar Su	David Chu	初版
V1.0.1	2025/9/1	Scholar Su	David Chu	补充安全功能列表
V1.0.2	2025/9/3	Scholar Su	David Chu	补充安全功能描述
V1.0.3	2025/9/5	Scholar Su	David Chu	修改零部件清单

Table of Contents

SAFETY FUNCTION LIST EXAMPLE 1

1. 基本信息 3

 1.1. 目的 3

 1.2. 适用范围 3

 1.3. 参考文件 4

 1.4. 名词解释 4

2. 安全架构介绍 5

 2.1. 零部件清单 5

3. 安全功能 5

 3.1. SF01 急停 6

 3.2. SF02 雷达警告区减速检测 6

 3.3. SF03 雷达保护区速度保护 7

 3.4. SF04 最大速度保护 7

 3.5. SF05 载货检测 8

 3.6. SF06 高度保护 8

 3.7. SF07 雷达切区 9

 3.8. SF08 模式切换 9

 3.9. SF09 接触器黏连检测 EDM 9

4. 参数 10

 4.1. 速度转换相关参数 10

 4.2. 减速检测相关参数 10

 4.3. 雷达保护区相关参数 10

 4.4. 最大速度保护参数 10

 4.5. 维护模式相关参数 11

1. 基本信息

1.1. 目的

定义项目的安全功能及其实现原理

1.2. 适用范围

无人叉车安全相关功能

1.3. 参考文件

No.	Reference Description
[R1]	IEC 61508: 2010 Functional safety of E/E/PE safety-related systems, Part 1: General requirements
[R2]	IEC 61508: 2010 Functional safety of E/E/PE safety-related systems, Part 2: Requirements for E/E/PE safety-related systems
[R3]	IEC 61508-3: 2010 Functional safety of E/E/PE safety-related systems, Part 3: Software requirements
[R4]	EN 62061: 2015 Safety of machinery - Functional safety of safety-related E/E/PE control systems
[R5]	ISO 13849-1: 2015 Safety of machinery - Safety-related parts of control systems, Part 1: General principles for design
[R6]	ENISO 3691-4: 2023 Industrial trucks-Safety requirements and verificationPart 4:Driverless industrial trucks and their systems

1.4. 名词解释

Terms	Definition
FSR	功能安全需求 定义产品应具备的功能，含安全和非安全相关功能 有时功能安全需求可独立形成 FSR，本文档整合了 FSR 以及 TSR
TSR	技术安全需求 定义实现 FSR 的技术需求和安全措施，如安全架构，诊断机制等
SIL	安全完整性等级 确定了为将残余软件故障降低到一个适当水平所必须采用的技术和措施，安全完整性等级数值越高，安全性水平也越高，分 SIL1-4
PL	性能等级 确定了为将残余软件故障降低到一个适当水平所必须采用的技术和措施，性能等级含 Plae, Ple 代表最高安全等级
RBD	可靠性结构框图 从可靠性角度定义的系统与部件之间的逻辑图，是系统单元及其可靠性意义下的连接关系的图形表达，它只反映各个部件之间的串并联关系(冗余形式)
HFT	硬件故障冗余 HFT=N 代表 N+1 个故障将导致系统发生危险失效，如单通道架构 HFT=0 表示 1 个故障将会引起系统发生危险失效 HFT 与 Category 之间的关系:Cat.B~Cat.2 对应 HFT=0;Cat.3/4 对应 HFT=1 HFT 与 MooN 之间的关系:HFT=N-M, 如 2o03 对应 HFT=1
Cat.3	电路架构类别 ISO13849-1 将安全控制系统电路架构分为 5 类，Cat.B,Cat.1~Cat.4
DC	诊断覆盖率 通过自动在线诊断检测到的危险失效分数，诊断覆盖率由可检测到的危险失效除以总的危险失效(含可检测危险失效与不可检测危险失效)
SFF	安全失效分数 安全组件属性，定义如下： $SFF = (\sum \lambda_s + \sum \lambda_{Dd}) / (\sum \lambda_s + \sum \lambda_{Dd} + \sum \lambda_{Du})$
PFHd	平均每小时危险失效率

	E/E/PE 安全系统在一个给定的时间周期内执行规定安全功能时的危险失效概率
MTTFd	平均危险失效时间

2. 安全架构介绍

2.1. 零部件清单

No.	安全零部件	厂家	型号	数量	认证	说明
1	安全控制器	若彗电子科技	SPC200	1	PL D	安全控制器, EN61508 和 ISO13849 认证。SIL II/ PL D
2	急停按钮	欧姆龙	A22RE-M-02-C	1	PL D	急停按钮, 双 NC 回路, EN 60947-5-5 标准
4	安全雷达	欧镭	GS1-5	1	PL D	安全雷达, EN61508 和 ISO13849 认证。SIL II/ PL D
5	安全编码器	Sick	DFS60S-BAO L01024	1	PL D	安全编码器, 正余弦, 增量式, SIL II/ PL D
6	安全接近开关	Sick	IME2S12-04B 4DC0	2	PL D	非接触式安全开关, SIL II/ PL D
7	安全机械开关	EUCHNER	NZ1PS-538-M	1	PL D	小型安全限位开关, 2NC, EN60947-5-1
8	接触器	/	/	2	/	通用接触器, 采用两个接触器串联的方式实现 Cat.III

3. 安全功能

安全功能列表:

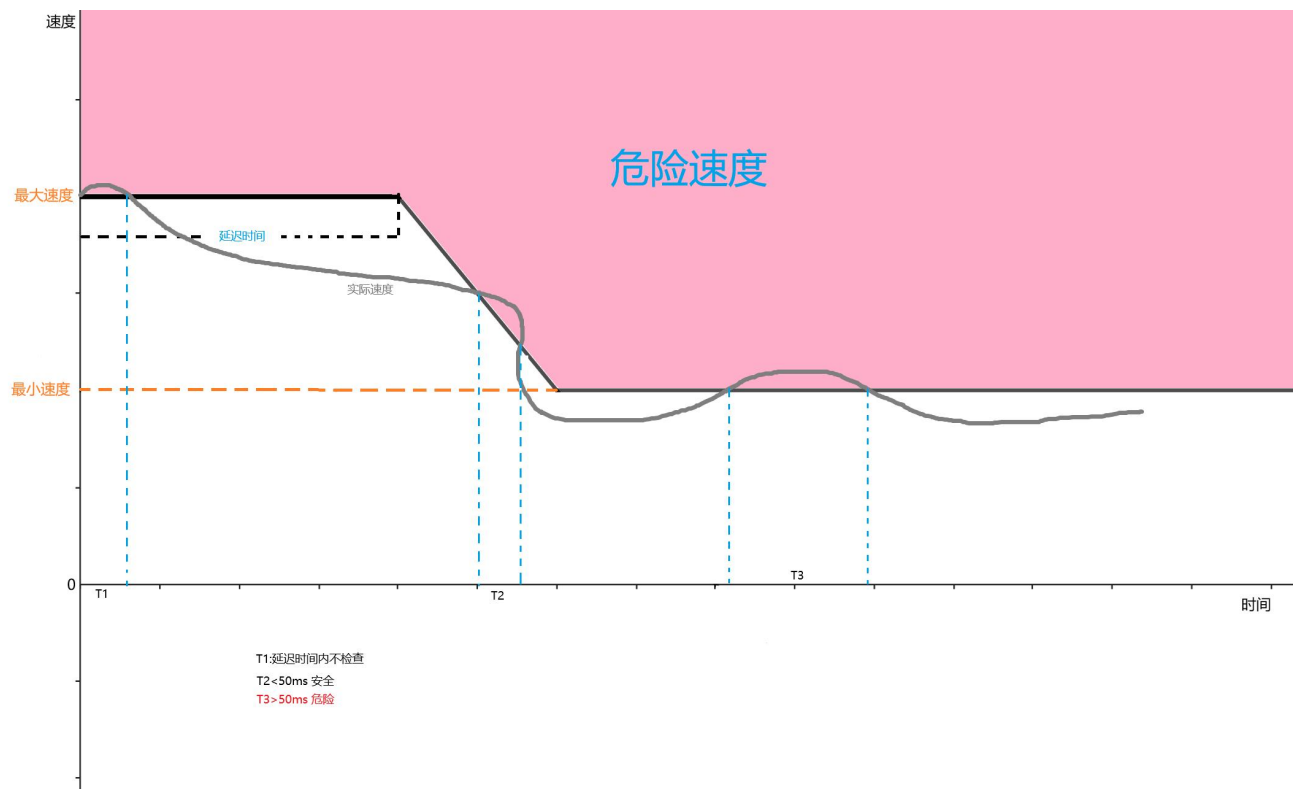
No.	安全功能名称	架构	安全等级	停止类别	安全功能说明
SF01	急停	Cat.III	PLr. D	Cat.0	当急停拍下, 触发安全功能, 切断动力电
SF02	雷达警告区_减速检测	Cat.II	PLr. C	Cat.1	当雷达警告区内存在障碍物, 开始减速检测。如果违反减速规则, 就会触发安全功能, 切断动力电。(安全等级取决于雷达的警告信号)
SF03	雷达保护区_速度保护	Cat.III	PLr. D	Cat.0	当雷达保护区内存在障碍物, 如果机器继续运动, 就会触发安全功能, 切断动力电
SF04	最大速度保护	Cat.III	PLr. D	Cat.0	任意状态下, 机器朝向叉子运动速度大于 0.3m/s 或者是背向叉子运动速度大于 1.0m/s, 就会触发安全功能, 切断动力电
SF05	载货检测	Cat.III	PLr. D	Cat.1	当机器载货, SF04 的最大速度会变小
SF06	高度保护	Cat.III	PLr. D	Cat.1	当机器叉子举高, SF04 的最大速度会变小
SF07	雷达切区	Cat.III	PLr. D	Cat.0	采用动态切区(安全控制器根据机器运行速度和当前状态来动态切换雷达区), 暂定 8 个雷达分区
SF08	模式切换	Cat.II	PLr. C	Cat.0	手动模式下, 机器运行速度大于 0.3m/s 时切断动力电, 且操作员需要持续手操时才可运动
SF09	接触器黏连检测 EDM	Cat.III	PLr. D	Cat.0	继电器的辅助触点状态与控制不符时, 切断动力电
SF10	手动模式	Cat.III	PLr. D	Cat.0	在手动模式下, 速度不得超过 0.3m/s

3.1. SF01 急停

安全功能	SF01 急停
安全功能描述	当急停按钮被按下时，安全控制器进入安全状态
安全完整性等级	PLd
触发事件	安全控制器收到按钮按下信号，进入安全状态
安全状态	切断动力电(0 类停止)
安全响应时间	80ms
工作模式	高需求模式
安全功能电路架构	Cat.3
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10^{-6} ; 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

3.2. SF02 雷达警告区减速检测

安全功能	SF02 雷达警告区减速检测
安全功能描述	当雷达警告区内存在障碍物，延迟预设时间后安全控制器开始检查机器是否按预设参数进行减速到安全速度以下，若不符合减速曲线，则进入安全状态。
安全完整性等级	PLc
触发事件	雷达警告区触发(warning1)且机器超速
安全状态	切断动力电(1 类停止)
安全响应时间	雷达响应时间(Ams)+安全控制器响应时间(80ms)+ 减速逻辑时间(Bms)+接触器执行时间(Cms)
工作模式	高需求模式
安全功能电路架构	Cat.2
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10^{-6} ; 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].



3.3. SF03 雷达保护区速度保护

安全功能	SF03 雷达保护区速度保护
安全功能描述	当雷达保护区内存在障碍物，机器应停车，否则进入安全状态
安全完整性等级	PLd
触发事件	雷达保护区触发(OSSD)且机器超速
安全状态	切断动力电(0类停止)
安全响应时间	雷达响应时间(Ams)+安全控制器响应时间(80ms)+接触器执行时间(Bms)
工作模式	高需求模式
安全功能电路架构	Cat.3
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10 ⁻⁶ ; 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

3.4. SF04 最大速度保护

安全功能	SF04 最大速度保护
安全功能描述	机器在任何场景下都不允许超过最大速度阈值，否则进入安全状态，在朝叉子方向运动时，机器速度不得大于 0.3m/s
安全完整性等级	PLd
触发事件	机器超速
安全状态	切断动力电(0类停止)

安全响应时间	安全控制器响应时间(80ms)+接触器执行时间(Bms)
工作模式	高需求模式
安全功能电路架构	Cat.3
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10-6: 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

3.5. SF05 载货检测

安全功能	SF05 载货检测
安全功能描述	机器在载货时，最大运行速度应降低，如果机器超速，则进入安全状态(当存在举升高度检查时，应考虑举升高度)
安全完整性等级	PLd
触发事件	机器超速
安全状态	切断动力电(1 类停止)
安全响应时间	安全控制器响应时间(80ms)+接触器执行时间(Bms)
工作模式	高需求模式
安全功能电路架构	Cat.3
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10-6: 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

3.6. SF06 高度保护

安全功能	SF06 高度保护
安全功能描述	机器在载货时，货物举升高度不同时(低/中/高),最大运行速度阈值应有所区别，机器超速时安全控制器进入安全状态
安全完整性等级	PLd
触发事件	机器超速
安全状态	切断动力电(1 类停止)
安全响应时间	安全控制器响应时间(80ms)+接触器执行时间(Bms)
工作模式	高需求模式
安全功能电路架构	Cat.3
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10-6: 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

3.7. SF07 雷达切区

安全功能	SF07 雷达切区
安全功能描述	安全控制器根据机器运行状态来动态切换雷达区，安全控制器通过 DO 输出互补信号给到安全雷达，安全控制器提供 6 个 DO 对应雷达的 IN1-IN6，每两个 IN 为一组，作为 1 个 bit，最大可支持 8 个雷达区
安全完整性等级	PLd
触发事件	机器运行状态切换
安全状态	切到默认区
安全响应时间	安全控制器响应时间(80ms)+雷达(Bms)
工作模式	高需求模式
安全功能电路架构	Cat.3
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10 ⁻⁶ : 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

3.8. SF08 模式切换

安全功能	模式切换
安全功能描述	允许机器进行模式切换，维护模式下，仅急停功能生效，自动模式下所有功能生效，且维护模式下，机器速度不得超过 0.3m/s
安全完整性等级	PLc
触发事件	模式切换按钮状态改变
安全状态	切断动力电(0 类停止)
安全响应时间	安全控制器响应时间(80ms)+雷达(Bms)
工作模式	高需求模式
安全功能电路架构	Cat.2
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10 ⁻⁶ : 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

3.9. SF09 接触器黏连检测 EDM

安全功能	EDM
安全功能描述	安全控制器通过控制接触器断开或接通动力电，在运行过程中也要检查接触器是否按照安全控制器的输出状态来正常执行，所以需要对接触器的辅助触点进行检查，当触电反馈的状态不符合安全控制器的输出状态时，进入安全状态。
安全完整性等级	PLc
触发事件	触电反馈与控制电平一致
安全状态	切断动力电(0 类停止)
安全响应时间	安全控制器响应时间(80ms)+雷达(Bms)

工作模式	高需求模式
安全功能电路架构	Cat.2
诊断覆盖率	任一安全回路(平均)诊断覆盖率应不低于 60%;
目标失效率	安全回路 PFHD 值应不高于 10^{-6} ; 安全回路 MTTFD 值应不低于 30 年。
共因失效	共因失效分数应不低于 65 [ISO13849-1].

4. 参数

4.1. 速度转换相关参数

功能相关	参数名称	参数描述	参数值	参数单位	备注
编码器换算参数	每圈脉冲数	机器轮毂运动一周编码器输出多少脉冲	27500	个	用于将收到的编码器脉冲换算成速度值
	每圈运动距离	机器轮毂运动一周机器运动多少距离	565.5	mm	

4.2. 减速检测相关参数

参数名称	参数描述	默认值	参数单位
减速开始延迟	安全 PLC 在收到雷达警告区信号后延迟多久才开始进行减速检测	300	ms
减速检测最大值	在减速检测时, 速度不得超过此阈值	500	mm/s
减速检测最小值	当机器速度小于此速度后, 不再检测机器的减速斜率, 但之后机器不得超过此速度	100	mm/s
减速斜率	速度每秒下降幅度	200	mm/s

4.3. 雷达保护区相关参数

参数名称	参数描述	默认值	参数单位
保护区速度阈值	在雷达保护区触发时, 机器速度不得大于此速度	10	mm/s

注意: 对于保护区而言, 不管雷达处于那个分区, 只要保护区触发, 速度就不得大于此速度阈值

4.4. 最大速度保护参数

参数名称	参数描述	默认值	参数单位
最大速度阈值	机器运行速度任何情况下不得大于此速度	1200	mm/s

4.5. 维护模式相关参数

参数名称	参数描述	默认值	参数单位
速度阈值	速度不得大于此速度	300	mm/s