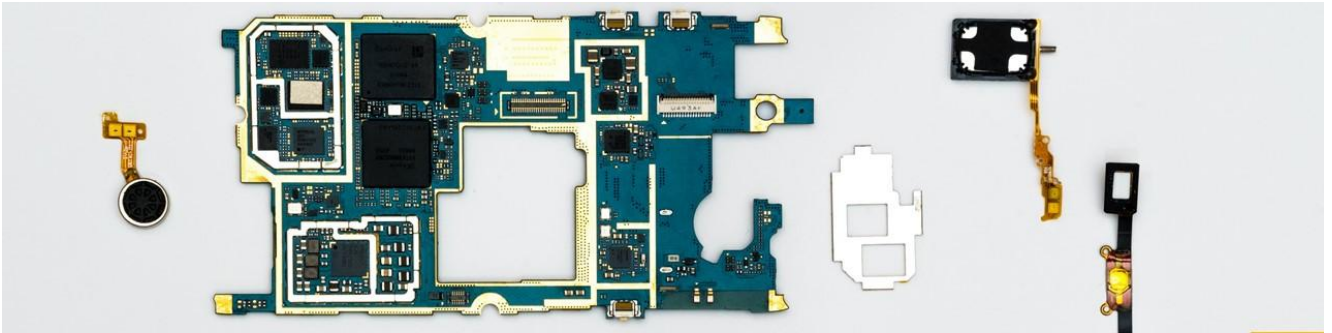


<SPC200>

<示例工程>



## SAFETY DESIGNER ENGINEERING TOOL 2023.11

2024 PRAJNASAFE



### 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	2025/10/29	Scholar Su	David Chu	初版
V1.0.1	2026/1/20	Ray Lin	David Chu	修改雷达切区方式

Table of Contents

示例工程说明 ..... 1

**1. 基本信息 ..... 4**

    1.1. 目的 ..... 4

    1.2. 适用范围 ..... 4

    1.3. 参考文件 ..... 4

    1.4. 名词解释 ..... 4

**2. 安全功能 ..... 5**

    2.1. SF01 急停 ..... 7

    2.2. SF02 雷达切区 ..... 7

    2.3. SF03 雷达警告区减速检测 ..... 9

    2.4. SF04 雷达保护区速度保护 ..... 10

    2.5. SF05 最大速度保护 ..... 10

    2.6. SF06 载货检测 ..... 11

    2.7. SF07 高度保护 ..... 11

    2.8. SF09 倒车限速 ..... 12

    2.9. SF10 模式切换 ..... 12

    2.10. SF11 接触器黏连检测 EDM ..... 13

## 1. 基本信息

### 1.1. 目的

对安全功能示例工程进行解读，让用户对使用 SPC200 搭建安全功能有一个参考模板。

### 1.2. 适用范围

适用于工业 AGV、无人叉车等自主运行的机器车。

### 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

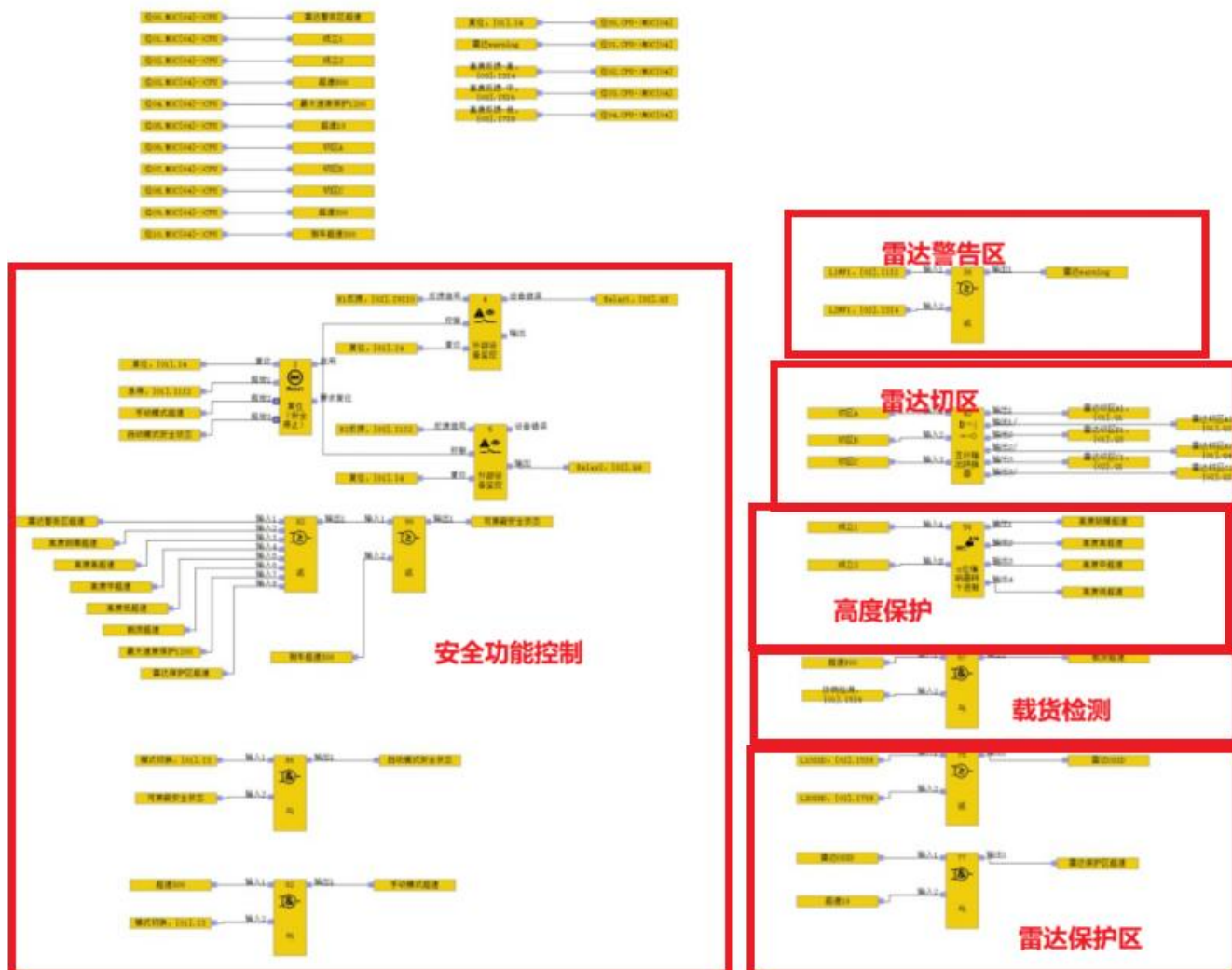
### 1.4. 名词解释

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. 安全功能

安全功能示例工程概览图:



## 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，进入安全状态
SF02	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）
SF03	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）
SF04	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
SF05	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
SF06	载货检测	Cat.III	PLr. D	Cat.1	当机器载货，对机器进行限速
SF07	高度保护	Cat.III	PLr. D	Cat.1	当机器叉子举高，根据高度不同限制不同运行速度
SF08	倒车限速	Cat.III	PLr. D	Cat.0	倒车场景下机器速度不得超过 0.3m/s
SF09	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运动
SF10	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

## 输入信号列表：

零部件/零部件信号	零部件类型	对应安全控制器资源	有关安全功能
急停按钮	双 NC	IO[01].I1I2	急停
模式切换按钮	单 NO	IO[01].I3	模式切换
复位按钮	单 NO	IO[01].I4	安全功能控制
货物检测开关	双 NC	IO[01].I5I6	载货检测
雷达 1 警告区信号 (L1WF1)	单 NC	IO[02].I1I2	雷达警告区_减速检测
雷达 2 警告区信号 (L1WF1)	单 NC	IO[02].I3I4	雷达警告区_减速检测
雷达 1 保护区信号 (L1OSSD)	双 NC	IO[02].I5I6	雷达保护区_速度保护
雷达 2 保护区信号 (L2OSSD)	双 NC	IO[02].I7I8	雷达保护区_速度保护
Relay1 反馈触点信号	双 NC	IO[02].I9I10	接触器黏连检测 EDM
Relay2 反馈触点信号	双 NC	IO[03].I1I2	接触器黏连检测 EDM
高度检测开关(高)	双 NC	IO[03].I3I4	高度保护
高度检测开关(中)	双 NC	IO[03].I5I6	高度保护
高度检测开关(低)	双 NC	IO[03].I7I8	高度保护
正余弦编码器	安全编码器	MOC[04].E1	雷达警告区_减速检测 雷达保护区_速度保护 高度保护 最大速度保护 倒车限速 载货检测 雷达切区 模式切换(手动模式)
正余弦编码器	安全编码器	MOC[04].E1	雷达警告区_减速检测



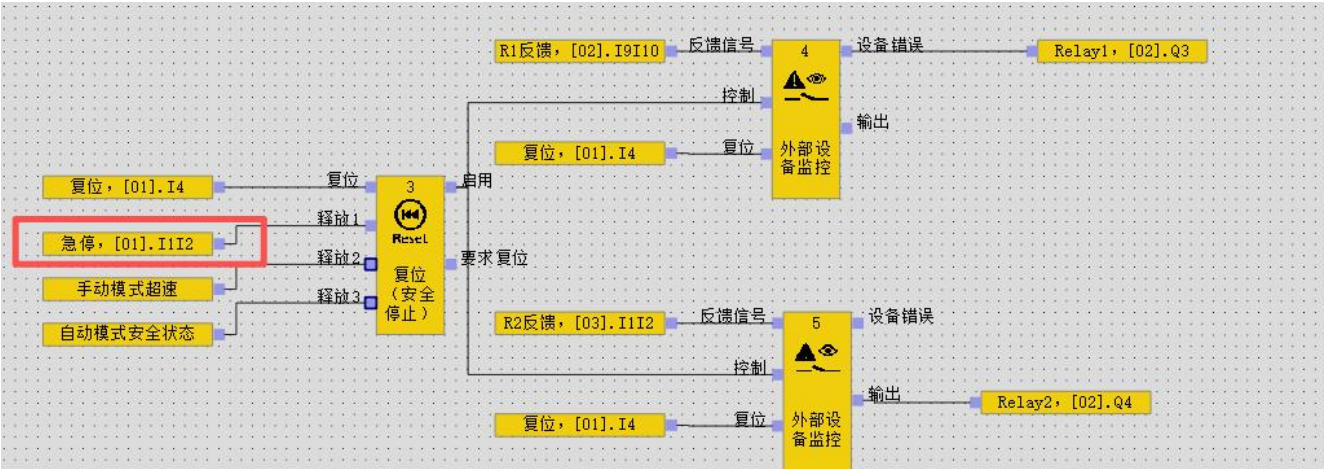
			雷达保护区_速度保护 高度保护 最大速度保护 倒车限速 载货检测 雷达切区 模式切换(手动模式)
--	--	--	--

输出信号列表:

信号名称	对应安全控制器资源	描述
雷达切区 A1	IO[01].Q1	雷达切区信号, A1-A2 为一对互补信号
雷达切区 A2	IO[01].Q2	
雷达切区 B1	IO[01].Q3	雷达切区信号, B1-B2 为一对互补信号
雷达切区 B2	IO[01].Q4	
雷达切区 C1	IO[02].Q1	雷达切区信号, C1-C2 为一对互补信号
雷达切区 C2	IO[01].Q2	
Relay1	IO[02].Q3	继电器 1 控制
Relay2	IO[02].Q4	继电器 2 控制

2.1. SF01 急停

急停功能在【安全功能控制】实现:



机器当前工作在自动模式还是手动模式下急停功能都会生效, 急停按钮为双 NC 类型:

- 当急停按钮按下后, 安全控制器关断 Relay1 和 Relay2。
- 当急停按钮松开后, 按下复位按钮(NO 类型)后松开, 安全控制器接通 Relay1 和 Relay2。

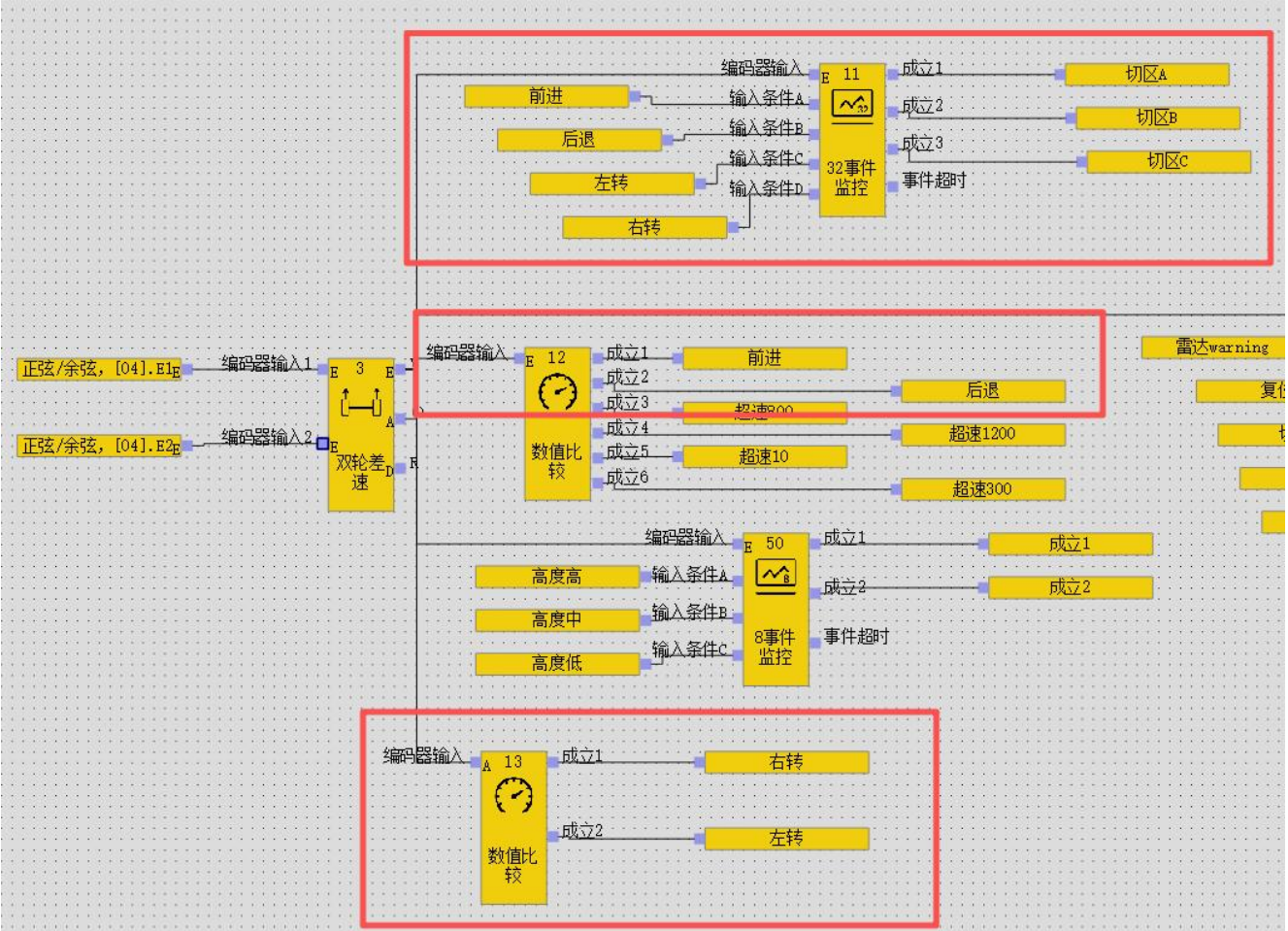
2.2. SF02 雷达切区

本示例根据速度、速度方向和转向信息划分了 32 个雷达区(field set), 本示例使用两个安全雷达, 但共享雷达切区信号, 用户可以在不同雷达的相同 field set 内设定不同大小的保护区和警告区以适用不同应用场景:

机器运行状态	雷达区
倒车	1
停车	2
前进速度 1-200mm/s	3
前进速度大于 200mm/s	4

左转速度 0-200mm/s	5
左转速度大于 200mm/s	6
右转速度 0-200mm/s	7
右转速度大于 200mm/s	8

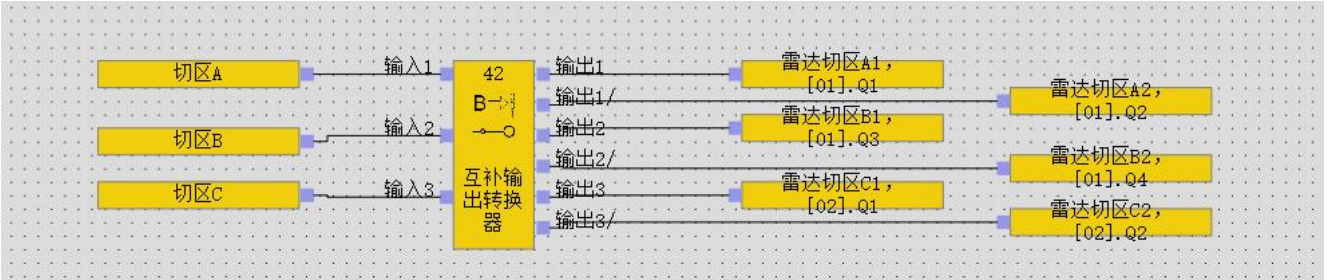
**MOC 逻辑:**



雷达切区基于运动模型【双轮差速】和【数值比较】逻辑块来判断前进、后退、左转和右转。再通过【32 事件监控】结合速度情况即可实现 32 雷达切区

**CPU 逻辑:**

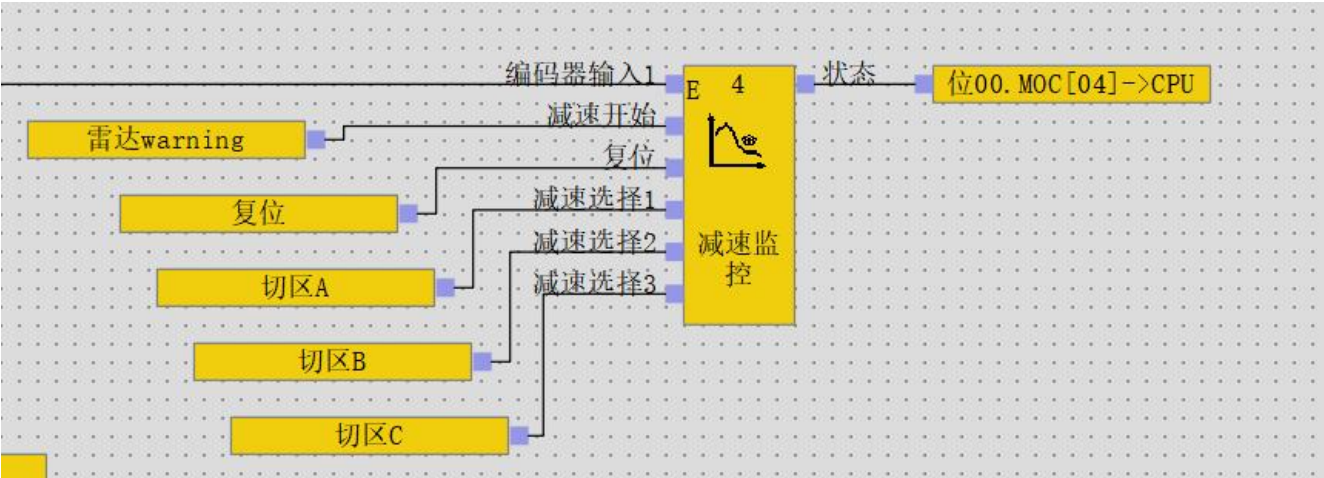
再将对应事件成立输出传递到 CPU 页面，由于雷达切区使用的是互补信号，所以还需要将单个位信号转换为一对对互补信号：





2.3. SF03 雷达警告区减速检测

MOC 模块内的实现：



【减速监控】逻辑块配置

减速检测1	减速检测5
每秒速度下降 200 mm/s	每秒速度下降 200 mm/s
减速起始速度 500 mm/s	减速起始速度 500 mm/s
减速结束速度 100 mm/s	减速结束速度 100 mm/s

减速检测2	减速检测6
每秒速度下降 200 mm/s	每秒速度下降 200 mm/s
减速起始速度 500 mm/s	减速起始速度 500 mm/s
减速结束速度 100 mm/s	减速结束速度 100 mm/s

减速检测3	减速检测7
每秒速度下降 200 mm/s	每秒速度下降 200 mm/s
减速起始速度 500 mm/s	减速起始速度 500 mm/s
减速结束速度 100 mm/s	减速结束速度 100 mm/s

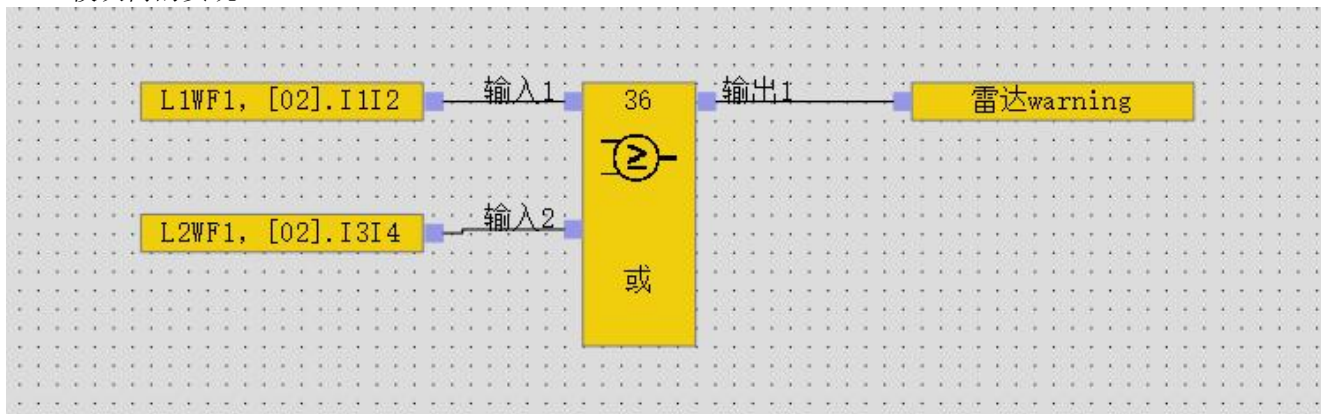
减速检测4	减速检测8
每秒速度下降 200 mm/s	每秒速度下降 200 mm/s
减速起始速度 500 mm/s	减速起始速度 500 mm/s
减速结束速度 100 mm/s	减速结束速度 100 mm/s

减速检测数: 7

减速检测区: 0-7

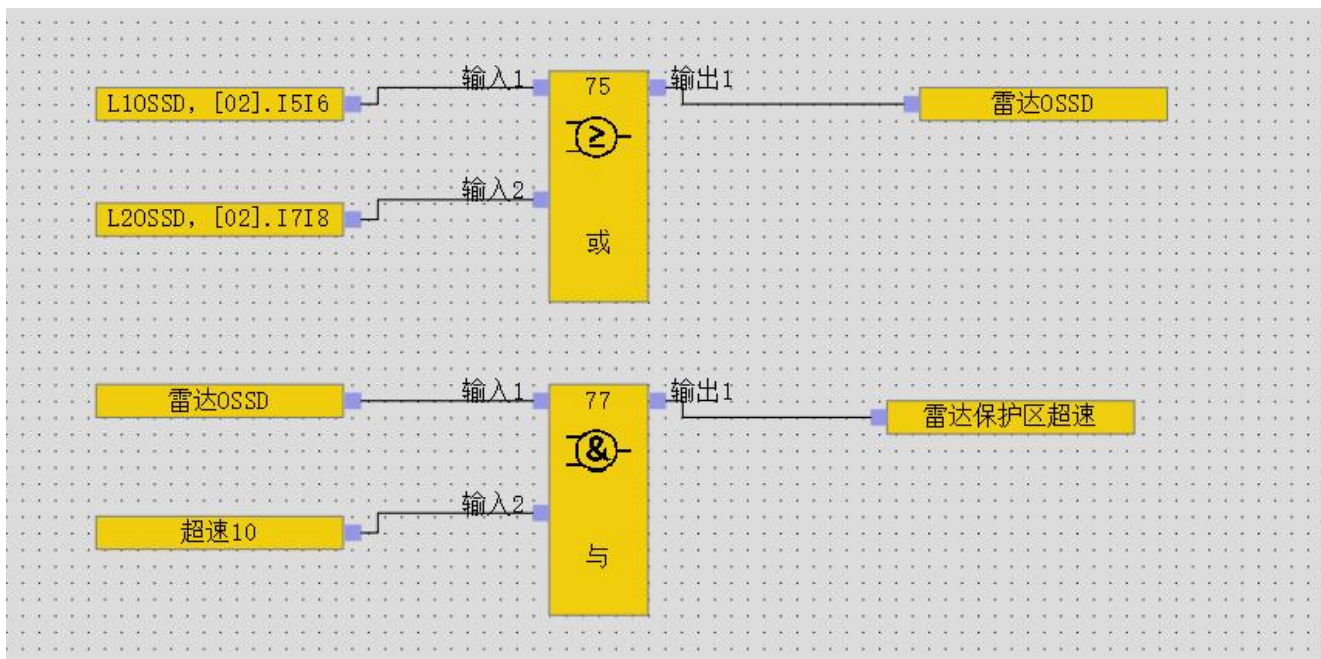
减速开始延时时间 300 ms

【减速检测】逻辑块内可设置减速参数，如 8 个雷达区可设置对应 8 个雷达区的减速参数  
CPU 模块内的实现：



当两个雷达任一雷达警告区触发时，MOC 模块会检查机器是否按照预设减速参数进行减速，如果不符合则安全控制器进入安全状态，关断 Relay1 和 Relay2

## 2.4. SF04 雷达保护区速度保护



当两个雷达任一雷达保护区触发时(OSSD)，MOC 模块会检测机器速度是否超过 10mm/s，如果超速，安全控制器进入安全状态，关断 Relay1 和 Relay2

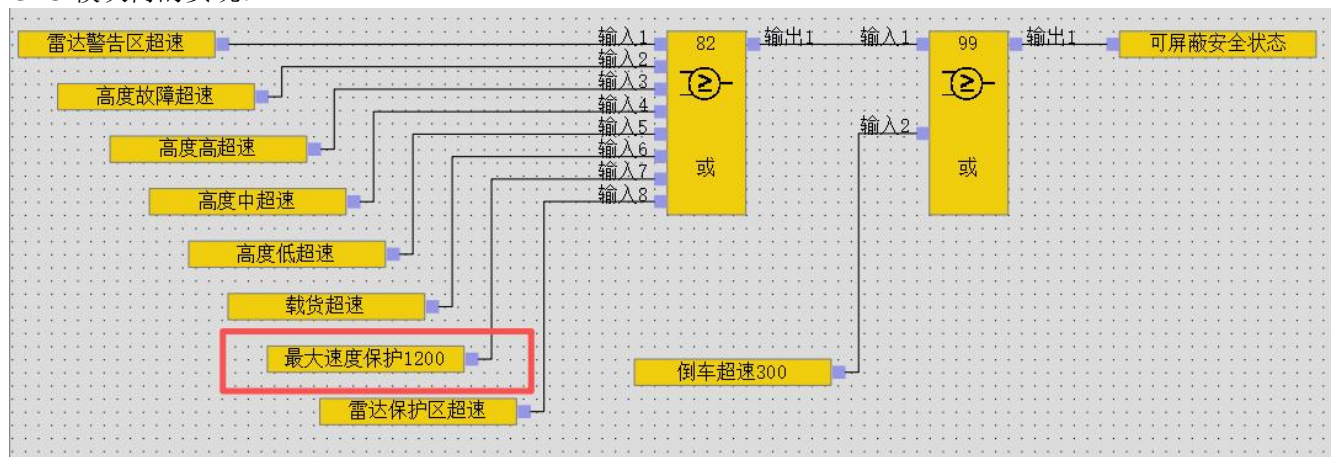
## 2.5. SF05 最大速度保护

MOC 模块内的实现：



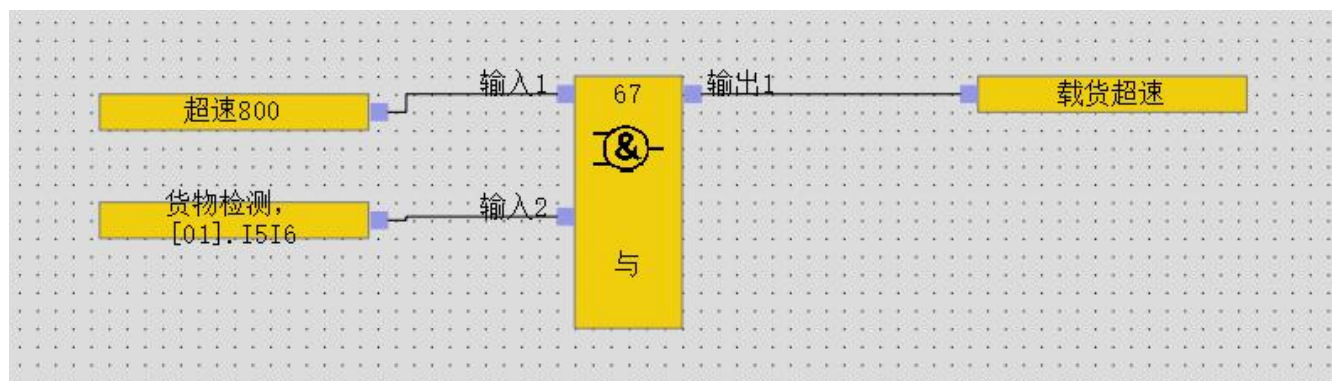


CPU 模块内的实现:



当机器速度超过 1200mm/s 时，安全控制器进入安全状态，关断 Relay1 和 Relay2

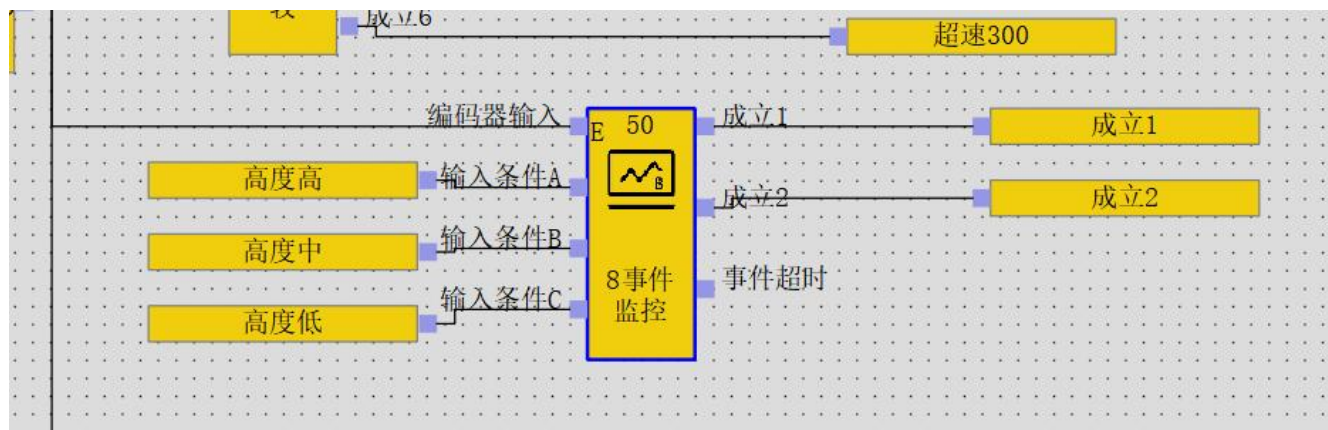
## 2.6. SF06 载货检测



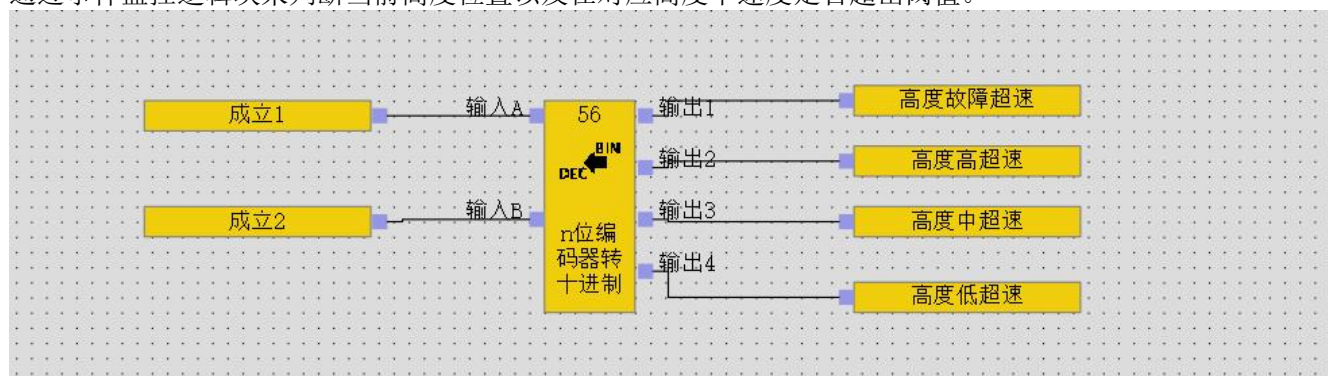
当机器在载货时，速度不得超过 800mm/s，否则安全控制器进入安全状态，关断 Relay1 和 Relay2

## 2.7. SF07 高度保护

叉车举升货物的高度使用三个安全机械开关，分别对应高/中/低三种高度，所以先将高度检测开关的状态，如果三个高度的开关都没触发(无法判断举升高度)，则认为高度开关故障，按照举升高度为高的情况进行处理:



通过事件监控逻辑块来判断当前高度位置以及在对应高度下速度是否超出阈值。



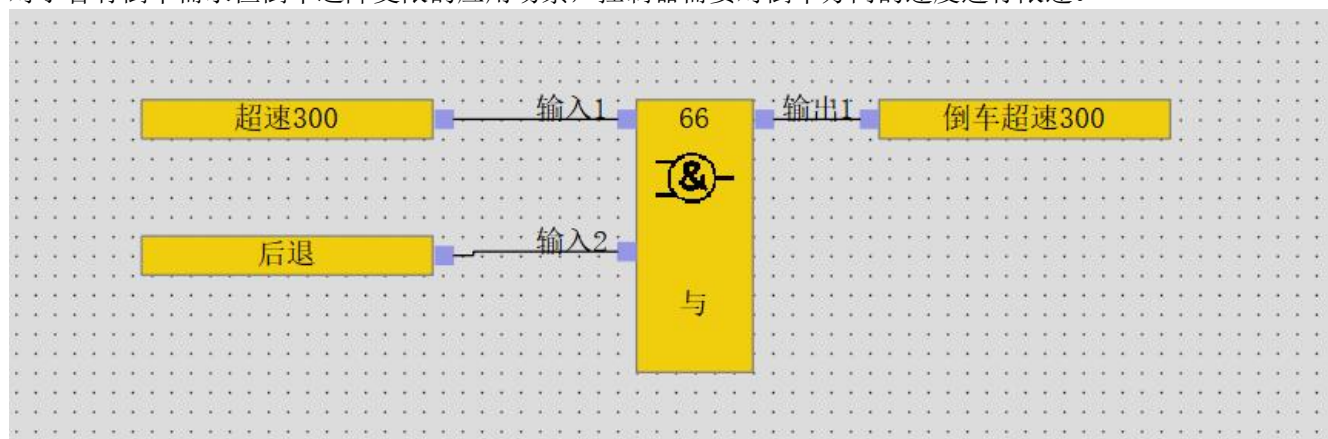
当举升高度为高或高度开关故障时，机器速度不得超过 300mm/s，否则安全控制器进入安全状态，关断 Relay1 和 Relay2。

当举升高度为中时，机器速度不得超过 500mm/s，否则安全控制器进入安全状态，关断 Relay1 和 Relay2。

当举升高度为低时，机器速度不得超过 800mm/s，否则安全控制器进入安全状态，关断 Relay1 和 Relay2。

## 2.8. SF08 倒车限速

对于含有倒车需求但倒车避障受限的应用场景，控制器需要对倒车方向的速度进行限速。



当倒车速度超过 300mm/s，安全控制器进入安全状态，关断 Relay1 和 Relay2。

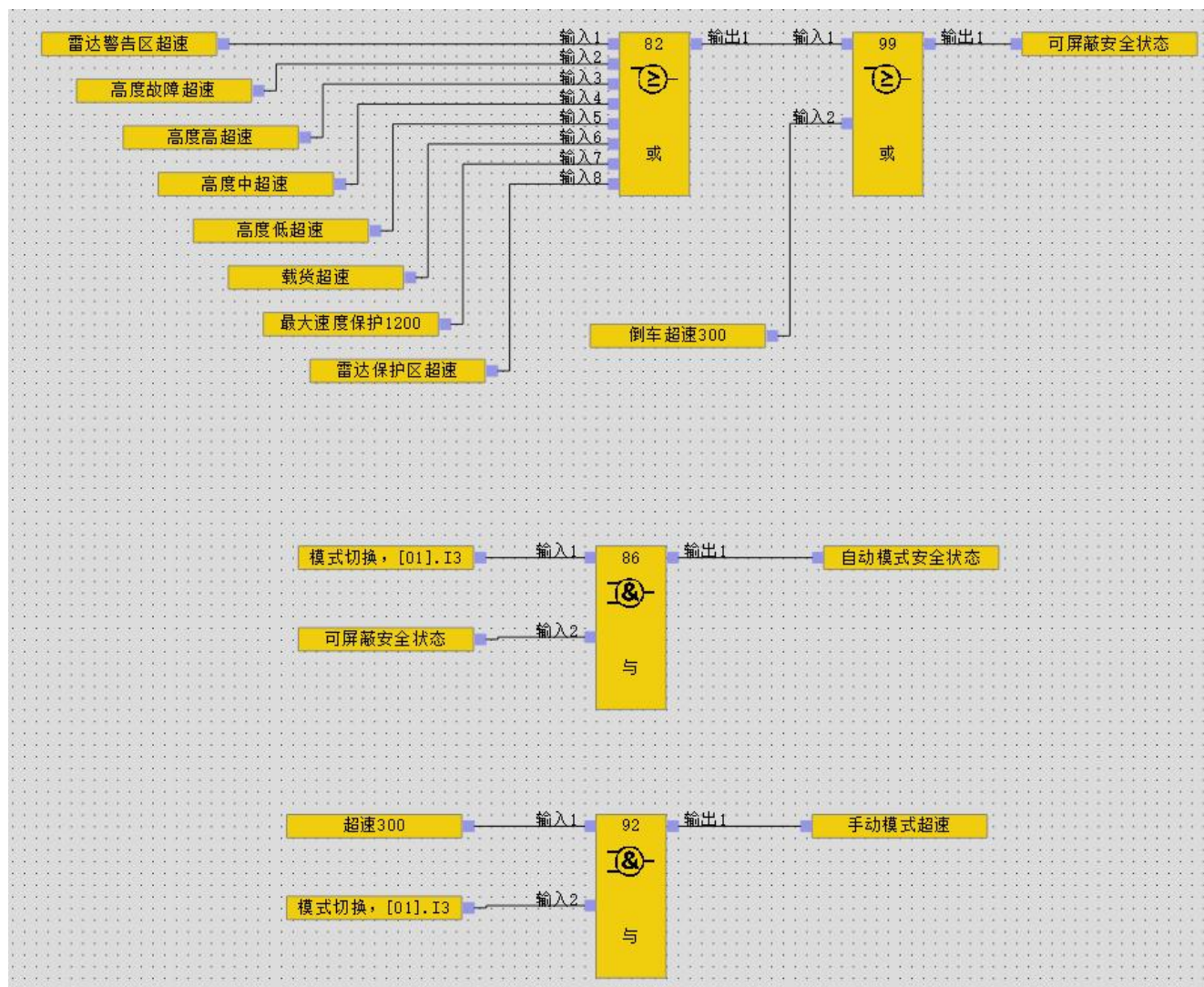
## 2.9. SF09 模式切换

机器一般拥有自动模式/手动模式(维护模式)

在手动模式下，需要由经过培训的工作人员手动持续控制，且速度不得超过 300mm/s。

在手动模式下会屏蔽除急停以外的安全功能





## 2.10. SF10 接触器黏连检测 EDMw

本示例使用两个外部继电器来控制电机的动力电源，要求继电器有双 NC 反馈触点，能够监控继电器是否有黏连：

