ABSOLUTE POSITION ELECTRONIC SAFETY CONTROLLER

LEGEND CONTROLS CO LIMITED

Leading provider of industrial products and IoT services

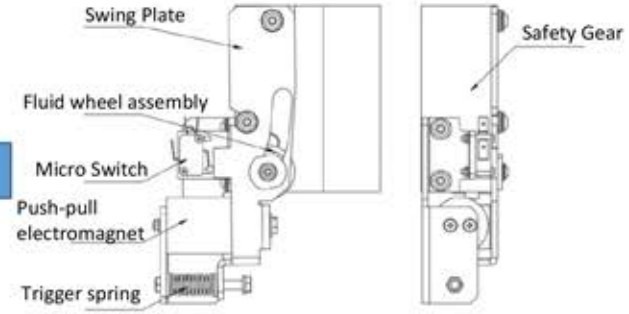
Safety Architecture

Home lift

FEMON-LF

Design sketch

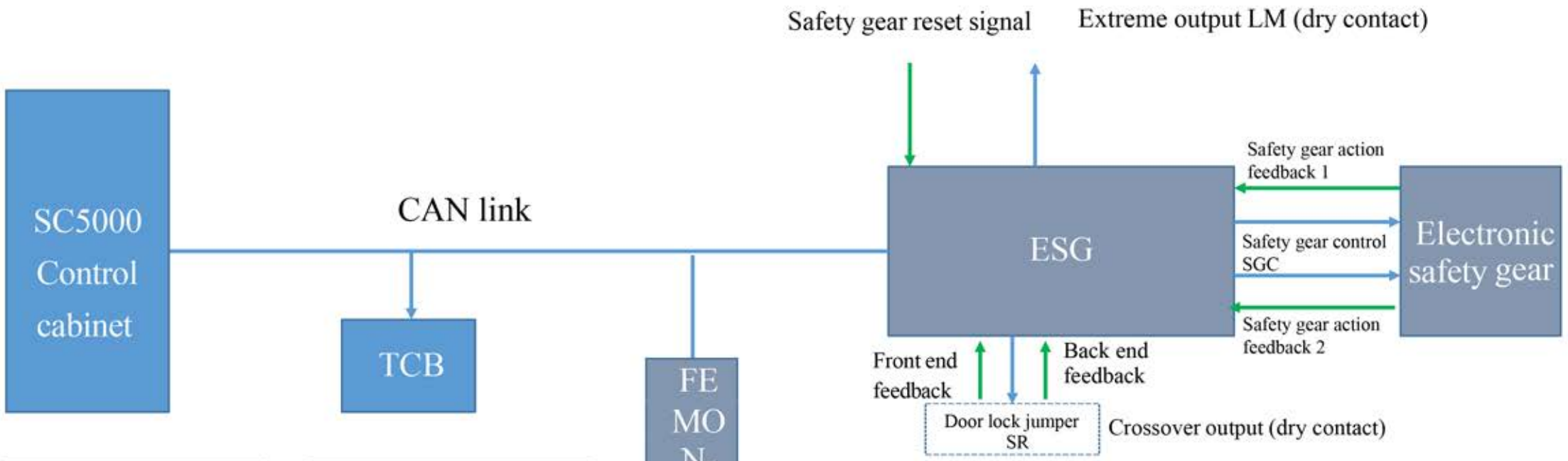
ESG: Absolute Position Safety Controller for Home Elevators



Electronic safety gear

NO.	Elevator safety function (device)	Safety Function Description (Type Specification Description)	SIL (Type Specification Requirement)	Equivalent requirements
1	Overspeed inspection	Detect if the car exceeds the set maximum speed (Not greater than the speed limiter trigger speed)	2	1
2	Check for unexpected movement of the elevator car when the door is open	Check for unexpected movement of the elevator car when the door is open	2	1
3	Check leveling, releveling, and preparatory operations	Leveling and preparatory operations when the detection door is not closed or locked	2	1
4	Limit switch	Check whether the elevator car has exceeded the limit	1	1
5	Action of electronic safety gear	--	X	1
6	Detection of electronic safety gear action	--	X	1

Electrical System Topology



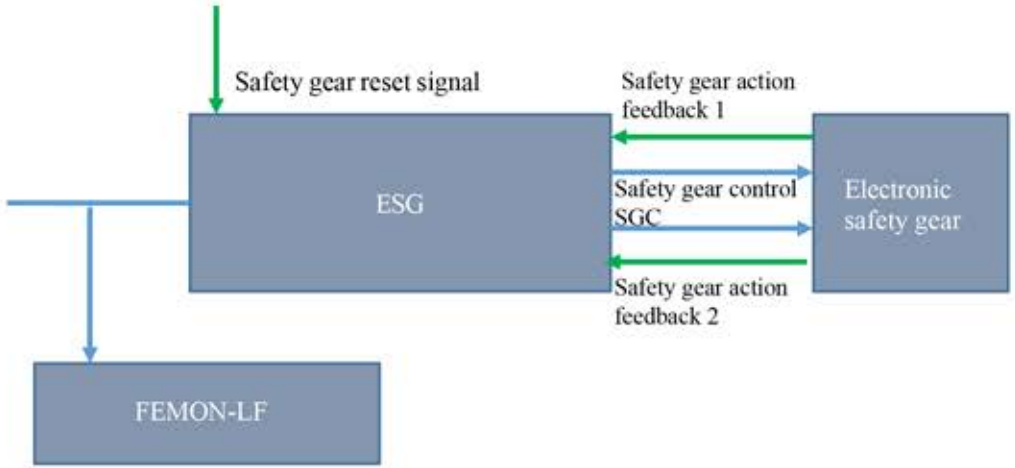
Parameter	Specifications
Interface	CAN
Baud rate	125kbps
Accuracy	1mm
Size	undetermined

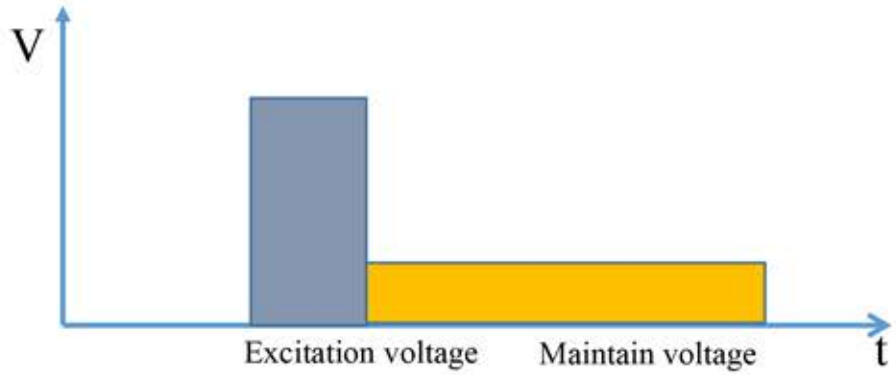
Interface	Specifications
CAN	Standard non isolated
Power input	AC220
Incentive output	DC110V
Maintain output	DC12V

Signal	Illustrate
Extreme LM	output
Safety gear control SGC	output
Door lock jumper SR	output

Signal	Illustrate
Safety reset signal	input
Safety gear action 1	input
Safety gear action 2	input
Front end feedback	input
Back end feedback	input

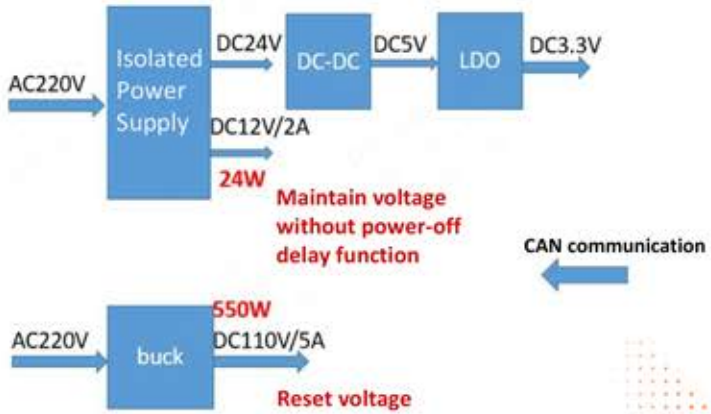
Power Design





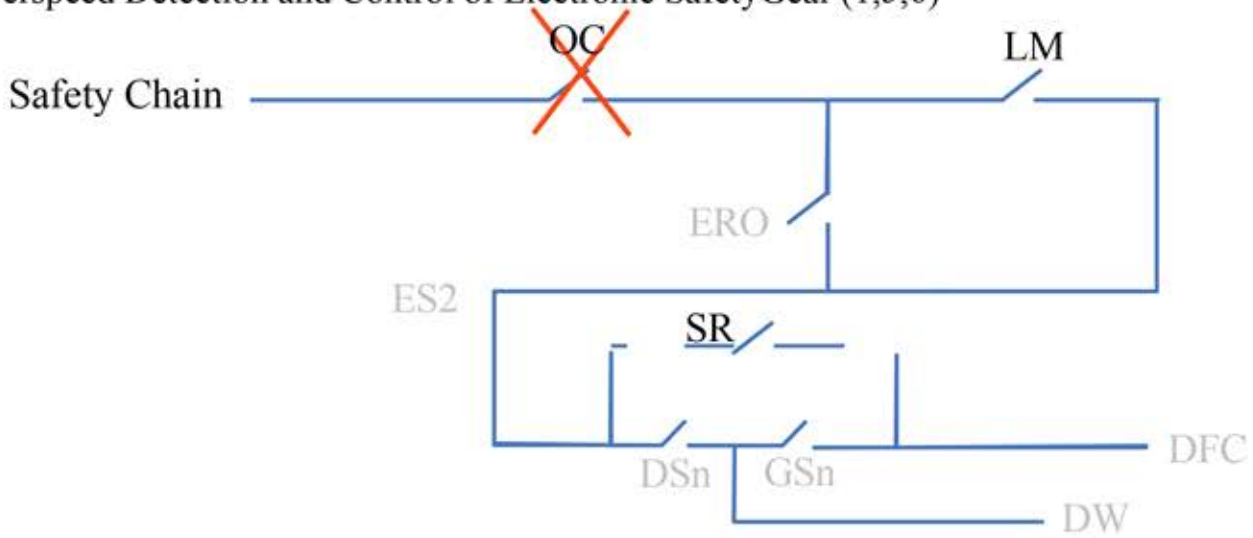
Excitation voltage:
DC110V, power 550W, using PWM modulation, holding time 300-500ms, parameters can be set

Maintaining voltage: DC12V, power 24W, using hardware BUCK circuit parameters that cannot be set



Safety Function Description

Safety Function Description 1: Overspeed Detection and Control of Electronic SafetyGear (1,5,6)



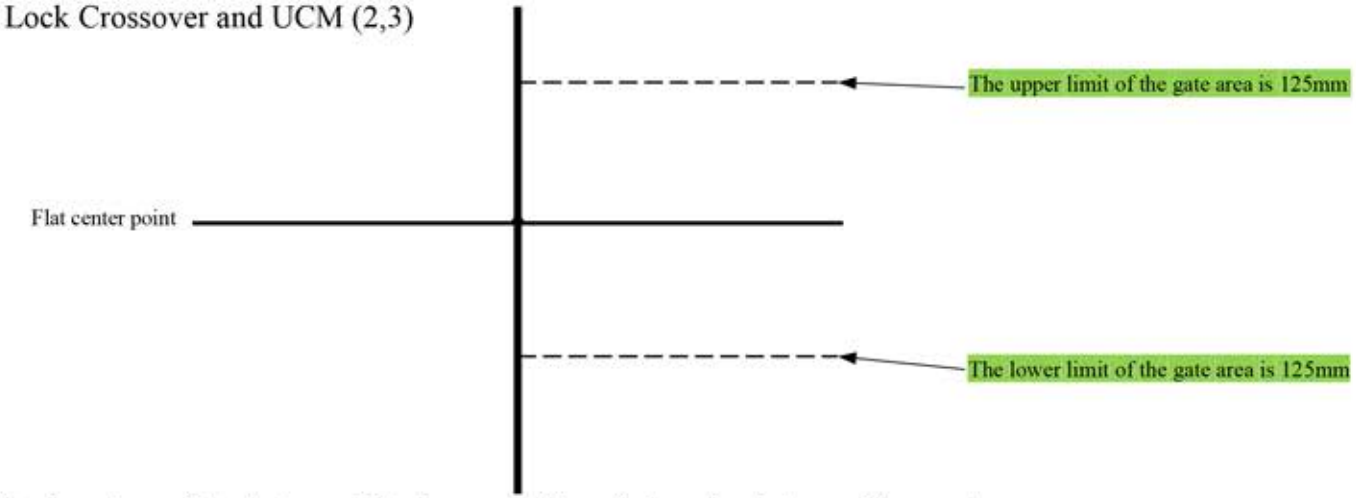
Judgment principle: The ESG absolute position safety box is installed at the top of the elevator car, and the box reads the current implementation speed of FEMON-LF. When the elevator is in operation, ESG reads the position every 10ms and compares it in real-time with the set rated speed based on the current speed. When the speed exceeds 115% of the rated speed, it is determined that the elevator car is speeding. At this time, the safety box cuts off the LM safety relay, the system enters a safe state, and at the same time, sends the information to the elevator control system. At this time, if the elevator direction is downward, the power output of the electronic safety gear will be cut off at the same time, and the electronic safety clamp will lose power and act,

Unlocking method: According to the requirements of functional safety, it will be locked after the overspeed fault is triggered. Due to the LM safety relay being connected to the safety circuit branch, the operation of ERO can bypass it. If there is an upward overspeed action, it can be directly operated by ERO;

If there is an overspeed action in the downward direction, the electronic safety power supply needs to be manually reset and turned on before the ERO can operate;

Safety Function Description

Safety Function Description 2: Door Lock Crossover and UCM (2,3)



Explanation of the intermediate layer position in the absolute position system

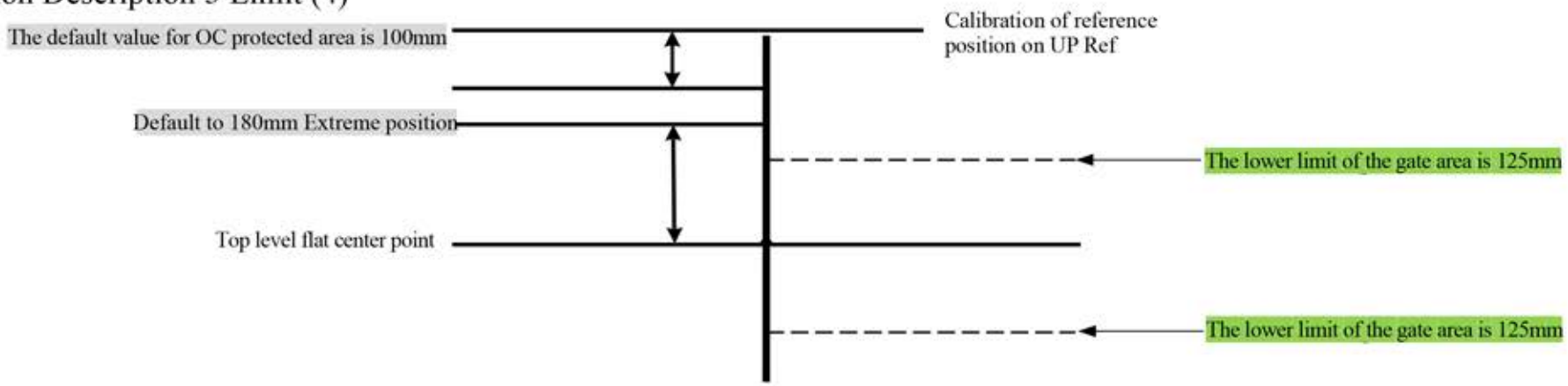
As shown in the figure, it is the installation position diagram of the level position. The door area is the openable area, and the position of the door area can be set, with a maximum distance from the center point not exceeding 200mm.

Judgment principle: The ESG safety box needs to go through a self-learning stage, calibrate the upper and lower reference positions, and the positions of each floor before it can be used normally. As the elevator needs to achieve door lock detection and early door opening function, the elevator sends a command to cross the door lock through CAN communication in the flat area, and sends the floor value and absolute position value. The safety box needs to verify whether the floor and position are consistent with the locally recorded self-learning position. If they are consistent, it will execute the SR safety relay cross connection action. During the crossover process, the safety real-time monitoring of the car displacement is carried out. When the displacement exceeds the range set by the door area, the SR and LM safety relays are immediately cut off to prevent accidental movement of the car.

Unlocking method: Due to functional safety requirements, after UCM fault is triggered and locked, it will still be locked when powered on again. After performing specific inspection steps on the entire elevator, maintenance personnel need to use a dedicated debugger or control panel to perform specific operations, and the elevator control board can restore safety to normal through CAN communication commands.

Safety Function Description

Safety Function Description 3 Limit (4)



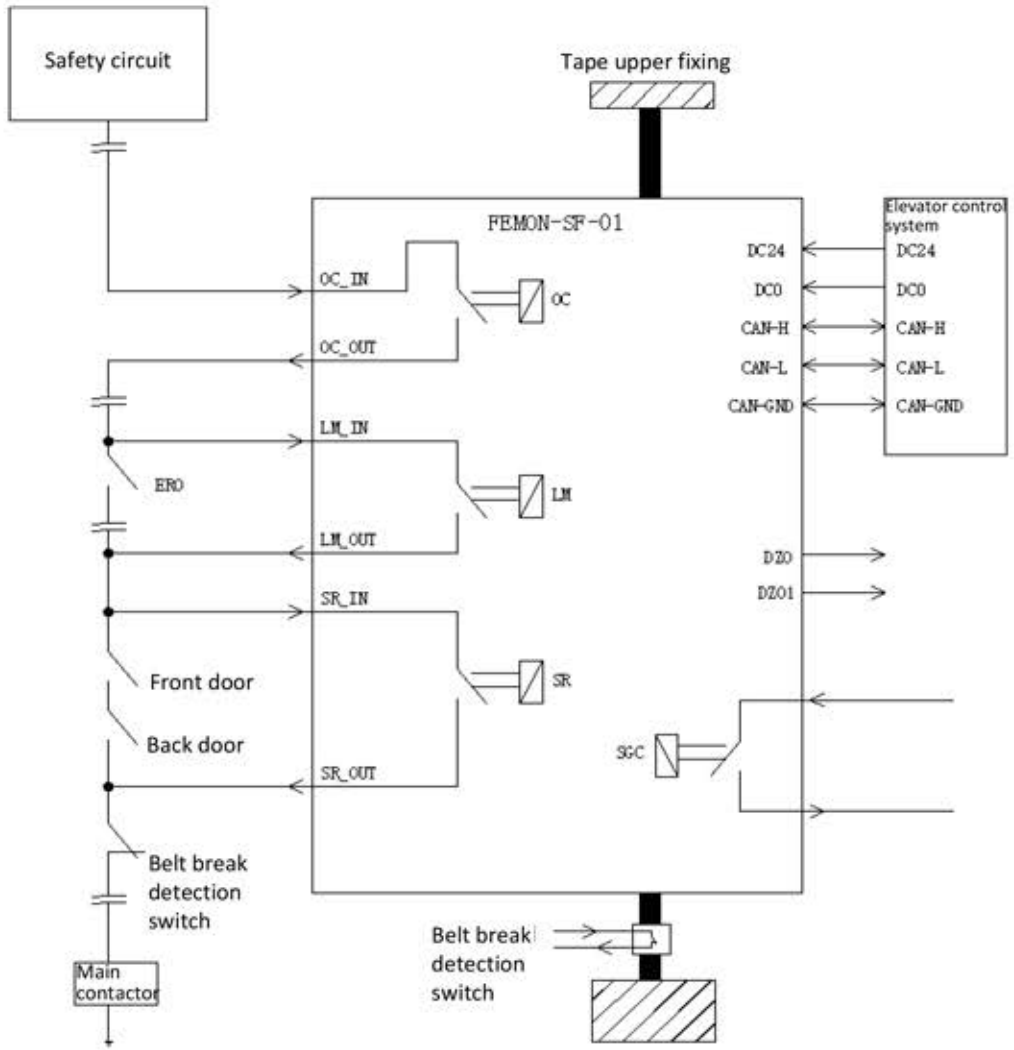
The installation positions of various switches in the elevator system are shown in the above figure, and the distance to the extreme position can be set through parameters. By default, it is upward from the center point of the end station level 50mm, further up is the limit zone.

Judgment principle: Before normal use, the ESG absolute position safety box needs to go through a self-learning stage, calibrate the upper and lower reference positions, and the positions of each floor. The safety box will store these numbers

According to the data stored in the data chip, power failure still exists. When the elevator car reaches the limit area, the LM safety relay is triggered to cut off the safety circuit, ensuring that the elevator stops.

Unlocking method: According to the requirements of functional safety, this function can be automatically unlocked after triggering, and the elevator car position can be restored to the operable area. The fault will be automatically unlocked. Due to the LM safety relay being connected to the safety circuit branch, the operation of ERO can bypass it. After performing specific inspection steps on the entire elevator, maintenance personnel restore it to the operable area through emergency electric operation.

Safety Function System Application Block Diagram



Electrical Circuit Diagram

LM: Safety relay 2, located on the safety circuit branch line, can be bypassed by ERO when it reaches the upper and lower limits and activates

SR: Bypass relay, activates when receiving bypass command SGC: Electronic safety gear output

Introduction to CAN Communication Protocol

Object	Illustrate	Brief introduction
2101H	I/O state and mode register	Output information
210FH	Device information	Device ID
2113H	Door zone size	Gate area information
2114H	Limit switches position offsets	Limit information
2118H	Deceleration control towards the shaft end	Reduced travel control
2122H	Bridging door contact	Bypass function
2124H	Reference positions	Reference upper and lower limits
2128H	Relay Test	Safety relay testing
212AH	Set Test Parameter	Set test parameters
212CH	Lift State	Elevator mode
212DH	Lift Sub State	Elevator sub mode
2140H	Floor table	Floor Schedule
2150H	Fault register	Fault
215AH	Defect log channel B	Channel B log recording
215BH	Defect log channel A	Channel A log recording

The connection between the elevator control system and ESG is achieved through CAN communication, with the main content being the object information determined in CANopen. Through this information, the control system can fully understand the status, position, speed, faults, and other information of the safety box, as well as the implementation of bypass and self-learning functions.

Design Failure Mode Analysis

No.	Project	Function	Potential Failure Modes	Potential consequences of failure	Severity	Potential Failure Causes/Mechanisms	Existing design			RPN
							Control and prevention	incidence rate	Control detection	Detectability	
1	LM safety relay	End station protection function	Abnormal disconnection	Elevator emergency stop, affecting passenger experience	5	1. Poor contact of relay contacts 2. The calibration of the upper and lower reference positions does not exceed 100mm above the top level	1. Choose the HFA2 series Hongfa safety relay used on our company's safety board; 2. The user manual requires that the upper and lower reference positions be 300mm away from the top and bottom flat layers.	3		4	60
2			Cannot be effective to break off	End station protection function fails, Elevator roof or bottom	6	1. Relay contact adhesion; 2. The limit protection parameter setting exceeds the operating range of the elevator	1. Adopting a redundant design of two sets of relays; 2. The default limit protection range of the parameter is 180mm; Software addition: When entering the upper and lower reference areas, it will also enter a protected state.	3		4	72
3		UCM function	Abnormal disconnection	Elevator emergency stop, affecting passenger experience	5	Poor contact of relay contacts	Choose the HFA2 series Hongfa safety relay used on our company's safety board;	3		4	60
4			Cannot be effective to break off	After the UCM is activated, the elevator may move in abnormal conditions such as communication loss.	6	1. Relay contact adhesion; 2. UCM action only disconnects SR relay	1. Adopting a redundant design of two sets of relays; 2. Add software design, UCM action not only disconnects SR relay, but also disconnects LM relay	3		4	72
5		Overspeed protection function	Abnormal disconnection	Elevator emergency stop, affecting passenger experience	5	1. Poor contact of relay contacts; 2. The speed of the safety box does not match the rated speed of the elevator	1. Choose the HFA2 series Hongfa safety relay used on our company's safety board; 2. The user manual requires that the safety box must match the actual elevator configuration.	3		4	60
6			Cannot be effective to break off	The overspeed protection function of the safety box has failed	6	1. Relay contact adhesion; 2. The speed of the safety box does not match the rated speed of the elevator	1. Adopting a redundant design of two sets of relays; 2. The user manual requires that the safety box must match the actual elevator configuration.	3		4	72

7		Other security integrity features	Abnormal disconnection	Elevator emergency stop or malfunction, affecting passenger experience	5	Poor contact of relay contacts	1. Choose the HFA2 series Hongfa safety relay used on our company's safety board; 2. Adopting a redundant design of two sets of relays; 3. Set up relay status monitoring in the software. When there is an abnormality, a fault will be reported and startup is not allowed.	3		4	60
8			Cannot be effective to break off	Failure of safety integrity protection function, elevator operation risk	6	Relay contact adhesion		3		4	72

ESG Certification

Product Principle Introduction-Safety Function Requirements

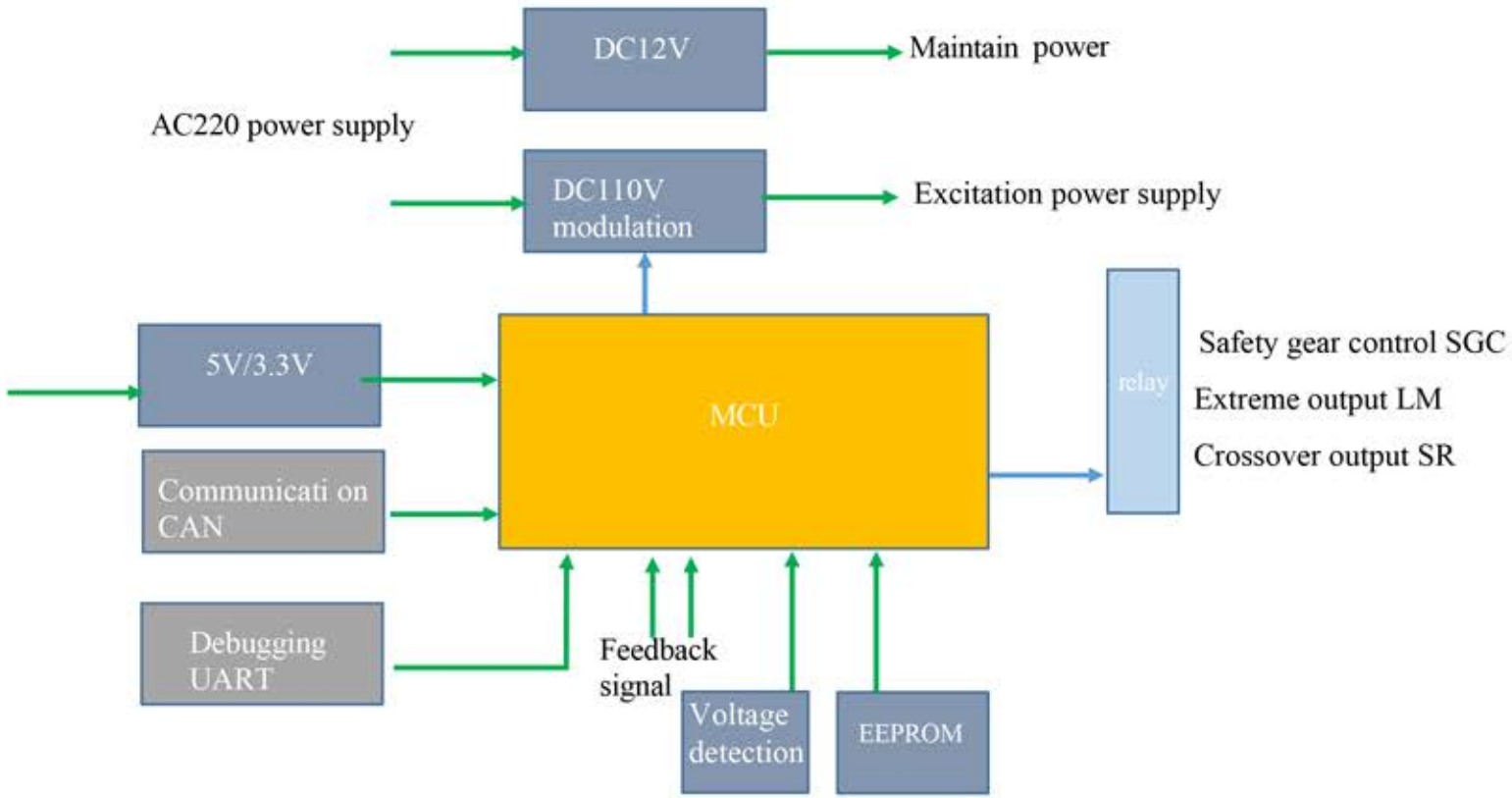
Equivalent safety certification, referring to the requirements of passenger elevators

1. GBT 20438-2017 Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
2. GB/T 35850.1-2018 Application of Programmable Electronic Systems for Safety Related Elevators, Escalators, and Moving Walks Part 1: Elevators (PESSRAL)
3. TSG T7007-2016 Elevator Type Test Rules
4. GB/T 7588.1-202X Elevator New National Standard

NO.	Elevator safety function (device)	Safety Function Description (Type Specification Description)	SIL (Type Specification Requirement)	Equivalency requirements
1	Overspeed inspection	Detect the elevator car exceeding the set maximum speed (not exceeding the speed limit triggered by the speed limiter)	2	1
2	Check for unexpected movement of the elevator car when the door is open	Check for unexpected movement of the elevator car when the door is open	2	1
3	Check leveling, re leveling, and preparatory operations	Leveling and preparatory operations when the detection door is not closed or locked	2	1
4	Limit switch	Check whether the elevator car has exceeded the limit limit	1	1
5	Action of electronic safety gear	--	X	1
6	Detection of electronic safety gear action	--	X	1

Hardware Design

ESG security hardware design diagram



MCU peripheral usage

RCC GPIO

CAN

UART TIMER

ADC

PWM

IIC

The hardware fault margin of the design is 0, with a single channel design that meets SIL1 safety integrity certification requirements

Software Design

1. MCU internal FLASH partition: APP (128K)+SRAM (20K)

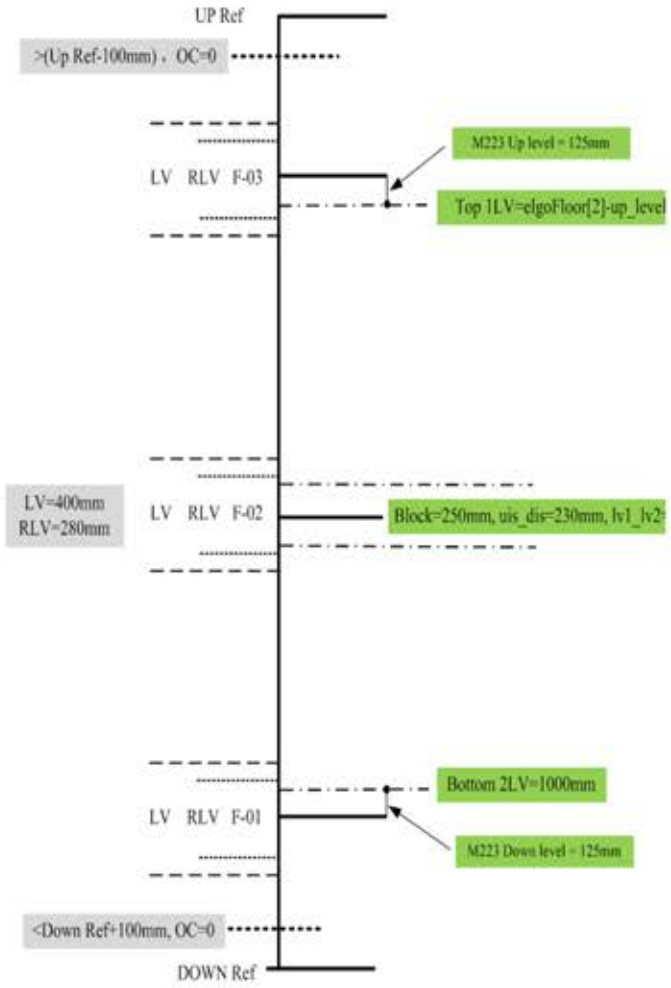
2. Software task architecture: using time slices to retrieve executed tasks

```
{5u,    CAN_COMM_MAS   &Time1msSPI      },
        TER,
{5u,    Task_input,    &Time1msInput    },
{20u,   Task_STLRun,   &Time1msCpuTes   },
                       t
{50u,   Task_WRCNST,   &Time1msOutput   },
{200u,  Task_Menu,     &Time1msMenu     },
{0u,    dummy,         &Time1msDumm     },
                       y
```

3. Key Function Description:
Position reading frequency: Accurately read the absolute position once every 10ms, and when combined with a maximum ladder speed of 1000mm/s, there will be a maximum position response delay of 5mm.

Implement security self check function, realize security function

Control cabinet matching design guidance



Well location model

Elevator controller docking method:
Docking FEMON-LF through CAN port, with a baud rate of 125k standard frames and a communication frequency of 10ms

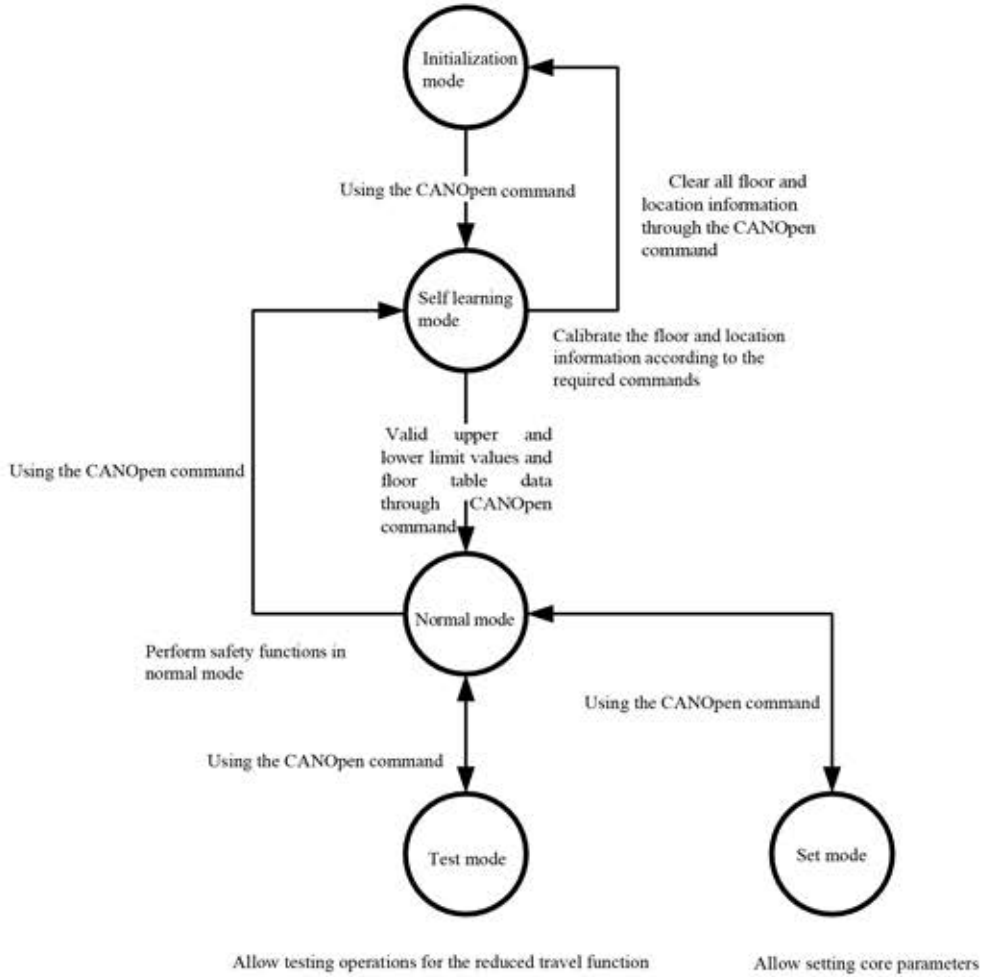
Implementation method of function
1. Acquisition of position and velocity information
According to the data refreshed every 10ms provided by FEMON-LF, it serves as feedback information and speed detection function for closed-loop position control.

2. Zero point position calibration
Due to the application of the magnetic grid ruler, a section is cut according to different configurations of the entire ladder height. Therefore, the absolute position information of the starting point of each ladder is different. When using it, it is necessary to calibrate the 0 point as the relative 0 position of this ladder.

3. Acquisition of self-learning location for floors
Before the express train runs, it is necessary to conduct self-learning of the shaft position, including the positions of each floor.

4. Position control
During operation, based on the learning values of each floor, the software generates simulated positions of each floor station in the shaft, and infers the current shaft position based on the current absolute position.

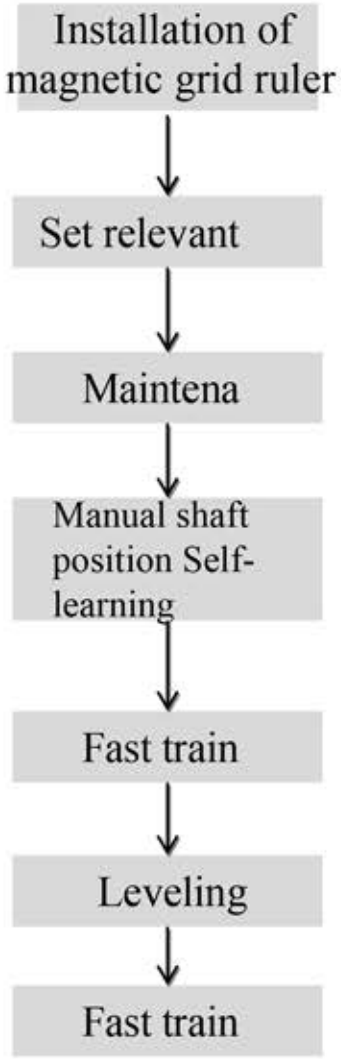
Safe Mode Design



ESG has set multiple modes internally, with varying performance in different modes. There are five modes: factory mode (initialization), self-learning mode, normal mode, testing mode, and setup mode. The relay output status in each mode is shown in the table below.

Pattern	SGC	LM	SR
Factory mode (initialization)	Connect	Connect	to break off
Self learning mode	Connect	Connect, disconnect when speeding	to break off
Normal mode	Execute according to status	Execute according to status	Execute according to status
Test mode	Execute according to status	Execute according to status	Execute according to status
Set mode	Execute according to status	Execute according to status	Execute according to status

Control cabinet matching design guidance



Server menu	Illustrate
M511	ESG status monitoring
M512	Self learning menu
M513	Fine tune the floor leveling position
M514	History of Safety Box Malfunctions
M515	Mode, reference position, floor calibration
M516	Manually write CANopen command
M517	Elevator position signal monitoring and zero point calibration
M518	Whole ladder testing mode
M519	Key parameters of safety box

Detailed debugging method reference: "FEMON-SF Debugging Guidebook. doc"

THANKS

support@legendcontrols.com
www.legendcontrols.com