SUNDOOR

SYSTEM ARCHITECTURE DESCRIPTION

STPL/SUNDOOR/AD/80 Ver 1.0

6 May 2023

SUNDOOR

APPROVAL HISTORY

	Prepared By	Reviewed By	Approved By
Name	C S Suryaraj	Dr. V Ranganathan	R C Nautiyal
Signature			
Date			

REVISION HISTORY

Version (x.y)	Date of Revision	Description of Change	Reason for Change
1.0	05/04/2023	Base Line Document	

Table of Contents

List of Figures

List of Tables

1. Preface

SUNDOOR module is primarily intended for automatic operation of sliding screened doors. SUNDOOR is used for speed and position control for the open and close positions of the door. In addition, SUNDOOR detects any obstruction and manages door movement during motion and prevents accidents.

The Metro has multiple compartments, each compartment will have the doors for passenger entry and exit. The platform will also have screened doors corresponding to the compartments. The compartment doors and platform doors are synchronized for opening and closing. The SUNDOOR controls and monitors the screened door on the platform. There is one SUNDOOR to control one set of left and right doors. The SUNDOOR ensures safety by detecting any obstructions in closing or opening movement. SUNDOOR is not responsible for synchronizing with compartment doorsof the Metro which is handled by the central controller of the metro station. The central controller communicates with the multiple SUNDOORs for control and monitoring of all the PSDs(Platform Screen Door) on the platform.

Bharat Electronics Limited, Panchkula, Haryana is the nodal agency for SUNDOOR. Technical Requirement Document [Ref 6], Problem Definition Statement [Ref 5], and Requirement Breakdown Structure [Ref 7] have all been provided as requirement documents. system's functionality is to control the platform screen doors of Metro platforms based on the inputs from master and field devices(name the master and field devices). SUNDOOR shall comply with CENELEC EN 50126-1:2017[Ref 1] and part-2 [Ref 2], EN 50128: 2011[Ref 3], EN 50129:2018 [Ref 4] to achieve functional safety level of SIL 3.

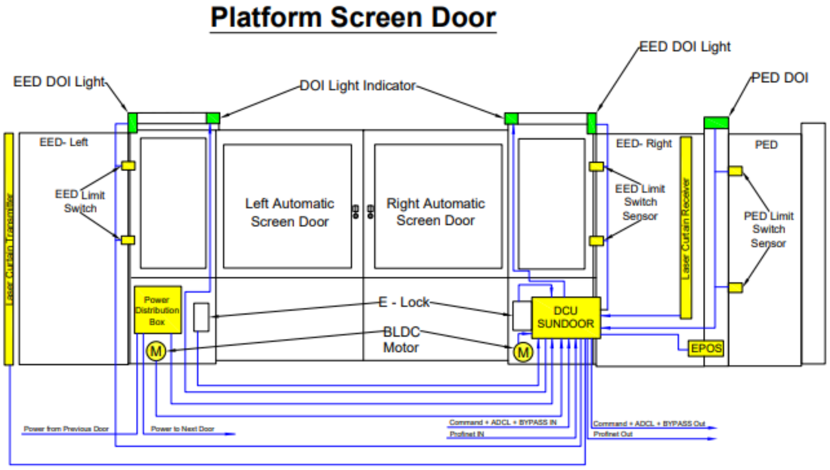

Figure 1: System Context Diagram

2. INTRODUCTION

2.1 PURPOSE

The purpose of this document is to provide a detailed description about the system architecture of SUNDOOR.

2.2 SCOPE

The Scope of architecture design document is for demonstrating how SUNDOOR architecture meets Safety Integrity Level 3 as per CENELEC standards. Customer specification for Technical Requirement Document [Ref 6], Problem Definition statement [Ref 5], and Requirement Breakdown Structure [Ref 7] have been referred as requirement documents.

2.3 SYSTEM OVERVIEW

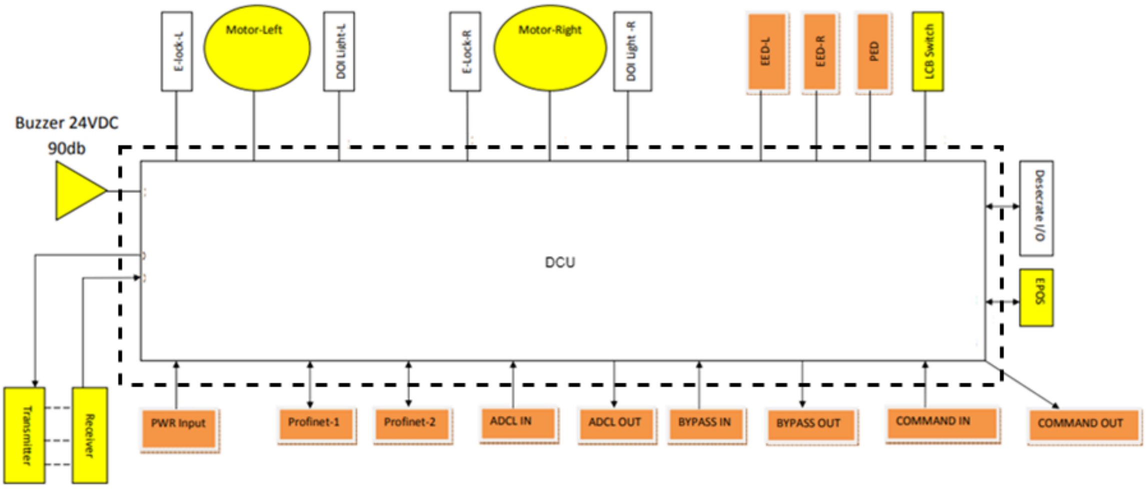

Figure 2: System Overview

SUNDOOR shall control the screened doors on the platform for metros. The half-height or full height PSD will consist of 2 sliding leaves. These leaves are called left and right doors and are driven by independent motors. SUNDOOR will be mounted on the right FDP panel as shown in figure 2. Both the motors will be connected to the SUNDOOR. The doors are mechanically locked by an electromechanical latch called E-lock. The E-Lock has two Limit switches for door open/close monitoring. The safety inputs for door open and close are generated by these limit switches when the E-lock operates with electrical actuation from the SUNDOOR. The Motor drive command is given based on the ENABLE and NOT-ENABLE inputs from E-lock. The E-Lock can be operated manually under emergency conditions with lever connected to the E-Lock. The manual operation activates the limit switches which give two Signals to SUNDOOR ERM and NOT-ERM as inputs.

The SUNDOOR provides the following statuses to the central controller,namely ADCL of right and Left PSDoors, PED, EED. For safety of the passengers there is laser switch to avoid any accidents when the PSD is closing. The EPOS (Digital Positioning system) sends a signal to SUNDOOR to stop the door from closing and provides a flashing light Indicator and Buzzer. SUNDOOR signals to the lamps and the buzzer for alerts. The SUNDOOR controls the opening and closing of the door in the set time(set time?) and also detects obstruction and takes corrective action during closing of the doors for safety. The Process to handle any obstruction while closing of PSDs is predefined in the SUNDOOR.

The opening and closing of the doors are defined with learn mode. The drive parameters for the motor speed, torque and distance for the profile(profile ??) are learnt and stored in non-volatile memory for use during normal operation. So, the Learn mode becomes safety operation. The learn mode is activated by a pushbutton switch mounted inside the SUNDOOR enclosure. It is manually activated by pressing it for 20 seconds to avoid any accidental activation. The learn mode parameters and the events will be logged in the non-volatile memory and these cannot be modified or erased without authorisation. There is an application SUNCOFIG which will run on laptops to program the door profile. This application will also have facility to down load the set parameters and events with authorisation.

SUNDOOR Communicates with Central controller on PROFINET Protocol on ethernet physical media. There are other interfaces like USB, CAN bus and RS485 interfaces on the SUNDOOR for external connection(External Connection is required in what situations?). There is data logger with on board flash memory for storage –(On SUNDOOR? Data is stored for how long and then backed up?). How does this data of door opening and closing timestamps help with the safety measures? The events with time stamps will be logged in the Data Logger and also the same information is transferred to central controller on PROFINET for monitoring,

2.4 SUNDOOR OPERATION

Learn mode (One Time after Installation of Door): A learn run serves to determine and store the characteristics of the door. The learned door parameters are stored in the SUNDOOR retentively. The parameters must be adapted in accordance with the friction of the door system, so that the learn run can be completed error free and these parameters for the door are stored in non-volatile memory for operation.

Learn mode is used while testing the SUNDOOR system. Based on the door weight and size the door movement in normal operation the parameters to be learnt are

- Movement of the door distance
- Time for opening and closing
- Force value for normal operation
- Speed of the movement as per the profile to be finalized. – profile has to be explained
- Control value parameters as per algorithm.--- State the control parameters
- Operation sequence timings
- Obstruction detection parameters.
- Motor Voltage
- Motor Currents.
- The learn mode is safety mode as it generates parameters for the safe running of the gate. Gate ??
- Learn mode is initiated by the Pushbutton by pressing it for 20 seconds continuously. Manual, so it is done while testing?

The SUNConfig Application running on the laptop (remotely? Or at each station? Because there are many SUNDOOR units on each platform) is connected to the SUNDOOR. The Media configuration is RS-485 (Media Config? Or serial communication between each SUNDOOR and the app?). The communication happens with one MCU but the parameters are collected by both the controllers(drivers and controllers?) and vetted for safety. The configuration interface and the software follow the same guide lines as per EN 50128: 2011[Ref 3].

SUNConfig has programmable parameters for the doors including door width and door movement profile. This will be detailed in design documents. SUNDOOR has a data logger which saves the data for up to 2 hours, this data is accessible by using SUNConfig application.

With learn mode parameters as reference the SUNDOOR operated in following modes for Door opening and closing with obstruction detection features.--- statement not clear.

Normal mode: In normal mode, SUNDOOR controls the doors on learned parameters.

LCB mode: Based on command from central controller and LCB mode selection switch, the SUNDOOR performs door opening and closing operation.

LCB mode selection is divided into the following three parts: --LCB full form

Auto Mode: In auto mode, SUNDOOR will receive hardwire switch commands from signalling through central controller and perform the door opening and closing action.

During door opening, the SUNDOOR controls the electromagnetic lock to unlock and drives the motor to open the sliding door.

After closing the doors as operation, the door is locked with electromagnetic lock

Isolation mode: Disconnect the central controller hardwire command and release the motor to the drive the door.--- When will this mode be used?

Bypass Mode: Include local closing and local opening, cuts off the central controller hardwire Command, provides power to the local switch control, bypass the safety circuit, and provide the local bypass signal to the central controller. --- when will this mode be used?

Restart after power failure: At recovery from power failure SUNDOOR shall first determine the status of the door (closed end position) and close the door. After achieving a safe state of door closure SUNDOOR should initialize in normal run mode and shall be able to execute normal commands. ---- Door positions should be explained, what is door end position and close door position?

Maximum response time for the motor drive 80 m Sec.--- This should be in the problem statement.

2.5 Key Safety Functions for SUNDOOR

There are SIL 3 functions identified for the screened door operation which are as listed below. These are taken care by the SUNDOOR.

- Safe force output
- Safe speed observance
- Safe monitoring of the rotor position
- Safe reading in of digital control signals
- SUNDOOR validation - self-tests
- Safe stopping process
- Obstruction detection during opening or closing.
    - If there is any obstruction during opening conditions the SUNDOOR will check for this and wait for 1 second and retry for three times and if the obstruction persists it will alert and open the doors fully.
    - If there is obstruction during closing the SUNDOOR will stop and open the doors for 25 cm and try to close again and will try this for three attempts and if the obstruction persists it will alert and open the gate.

2.6 DEFINITIONS

Terms	Definitions
PROFINET	An open industrial ethernet solution built on global standards. It is a protocol for communicating between controllers and devices in an automation environment.

Terms	Definitions
Modules	Each hardware block is considered as module.

Table 1: Definitions

2.7 ACRONYMS AND ABBREVIATIONS

Abbreviations	Description
ADCL	All Door Closed Locked signal
ADC	Analog to Digital Converter
ASD	Automatic Screen Door
PED	Platform End Door
PG	Platform Gate
EED	Emergency Exit Door
CAN	Controller Area Network
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DCU	Door Control Unit
E-LOCK	Electromagnetic Lock
EOF	End of Frame
ERM	Emergency Release Manual
GUI	Graphical User Interface

Abbreviations	**Description**
ID	Identification Data
IC	Integrated Circuit
LED	Light Emitting Diode
RS-485	RS485 is a common communications standard for serial communication with multidrop facility with 2 or 4 wire media.
RTC	Real Time Clock
SIL	Safety Integrity Level
SUNDOOR	Sunlux Name for Door Control Unit.
PFC	Potential Free Contact.
MCU	Microcontroller unit
RTC	Real Time Clock
UART	Universal Asynchronous Receiver and Transmitter.
USB	Universal Serial Bus
TVS	Transient Voltage Suppressor
CRC	Cyclic Redundancy Check

EPOS full form not provided, GPIO full form not provided, SPI full form not providedTable 2: Abbreviations

2.8 REFERENCES

The following are the reference documents referred during the preparation of System Requirement Specifications for SUNDOOR:

Ref. No.	**Document Title**	**Version**	**Document Description**
1.	EN 50126-1:2017	-	The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
2.	EN 50126-2:2017	-	The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
3.	EN 50128: 2011	-	Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems
4.	EN 50129: 2018	-	Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signaling.
5.	PDS-DCU	1.1	Problem definition statement provided by BEL; Panchkula dated: 27/02/23 Ver 1.1
6.	Technical Requirement Document	-	Technical Requirement provided by BEL, Panchkula
7.	Requirement Breakdown Structure	-	Requirement Breakdown Structure provided by BEL Panchkula.
8.	EN 50159:2010	-	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Table 3: References

3. Architecture Description

SUNDOOR is designed as 2oo2 architecture with two micro controllers. The basic philosophy of SUNDOOR architecture is validation of the safety inputs by both the controllers. The digital outputs and motor drive are also activated once the two controllers agree with voting. The two controllers communicate with each other on

UART for validating the inputs and outputs. The communication protocol will adhere to EN 50159 :2010 [Ref 8] recommendations.

3.1 Power Supply of SUNDOOR

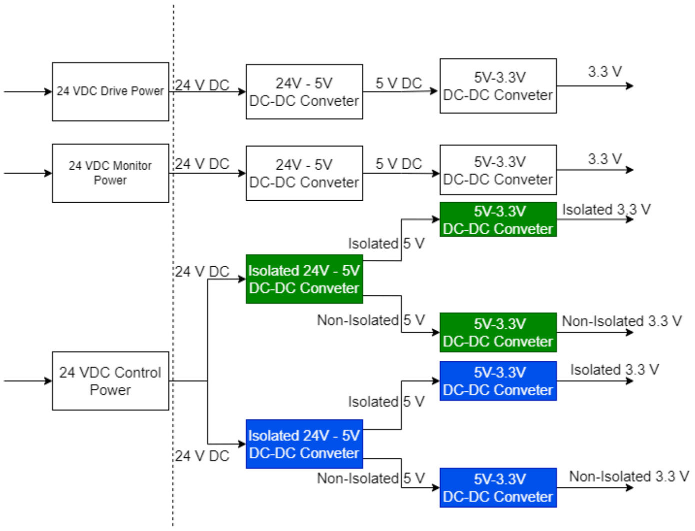

Figure 3: Power Supplies of SUNDOOR

SUNDOOR has 3 different power supplies, they are Drive Power, Monitor Power and Control Power. All power supplies have input voltage 24 V DC. Drive Power is for driving motor and E-LOCK. 24 V DC Monitor power is used for monitoring signals, these signals are listed out in table 5. Control power supply is for controller section. Drive power supply, monitor power supply and control power supply are isolated with each other. Controller Section will be isolated from field side. Application of various power supply voltages will be described in Hardware Design Document. Power supply interface details are illustrated in figure 3. Power supply voltages are monitored against the required tolerances. Power supply voltages generated by one DC-DC converter are checked by devices which are powered by other power supplies.

3.2 Inputs of SUNDOOR

SUNDOOR has two types of inputs, vital and non-vital inputs.

3.2.1. Vital Inputs

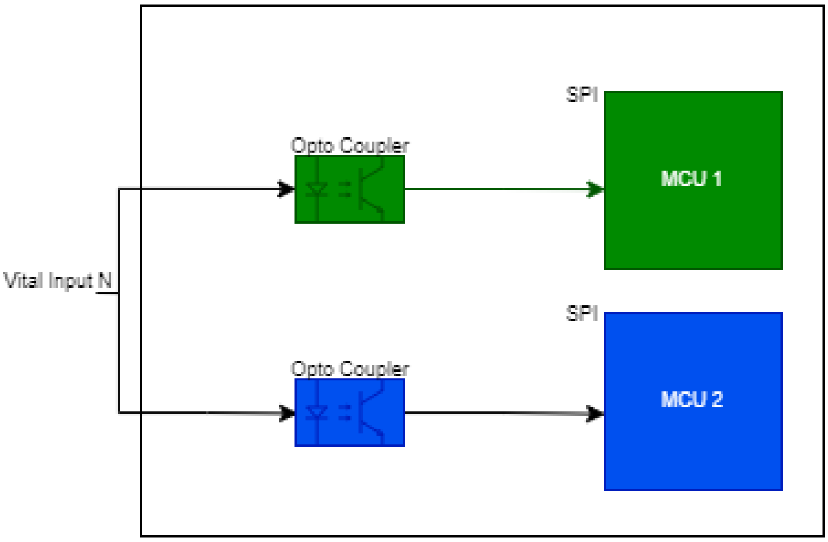

Figure 4: Vital Inputs

Vital inputs are isolated and connected to GPIO as digital inputs. The vital inputs are connected to both MCUs for validation with inter processor communication. Vital inputs shall be connected to MCU1 and MCU2 after isolation.

Vital inputs shall have protection for over voltage and surge and filtering, this shall be described in design document.

Vital input channels will have provision for diagnostics. The diagnostics of Vital inputs will be done by using simulated signals. Simulated signals will be generated by SUNDOOR. Interfacing of vital inputs are as described in figure 4. Health status of vital inputs circuits will be detected by using the diagnostics.

3.2.2. Non-Vital Inputs

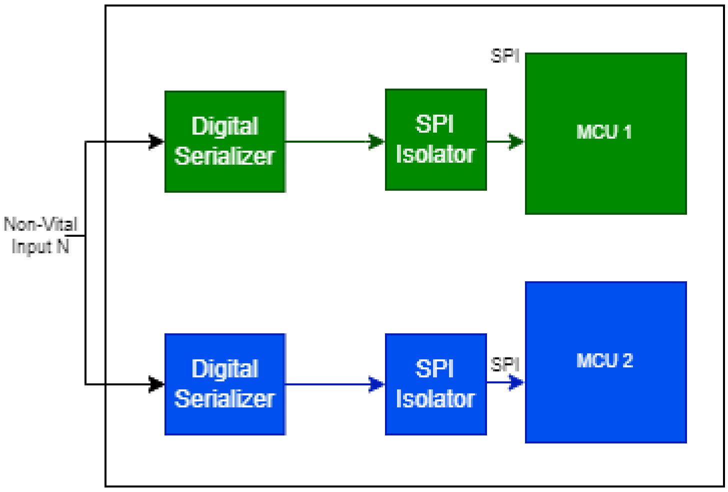

Figure 5: Non-Vital Inputs

Non- vital inputs are connected using digital serializer IC. Digital serializer IC have SPI interface with MCU. Non-Vital Inputs of SUNDOOR will also be connected to both the MCU's for validation. Non-vital inputs shall be isolated from MCU. NON-Vital Inputs will have protection for over voltage and surge and filtering, this shall be described in design document. Interfacing of non-vital inputs are as described in figure 5. Non-vital input channels will have provision for diagnostics.

3.3 Outputs of SUNDOOR

SUNDOOR has two types of outputs, vital output and non-vital output.

3.3.1. Vital Outputs

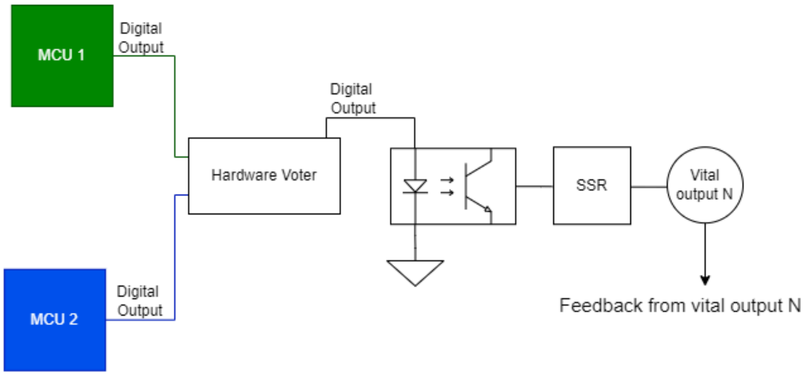

Figure 7: Vital Outputs

Vital outputs are activated when both controllers are in agreement. Vital outputs have feedback to ensure output is driven correct. Handling of this feedback is described in section 3.6. Figure 7 gives illustration of vital outputs.

This vital output will be used to drive the ELOCK coil, the status of ELOCK will be read through Enable and Not-Enable signals. Based on the status of these signals motor will be driven.

3.3.2. Non-Vital Outputs

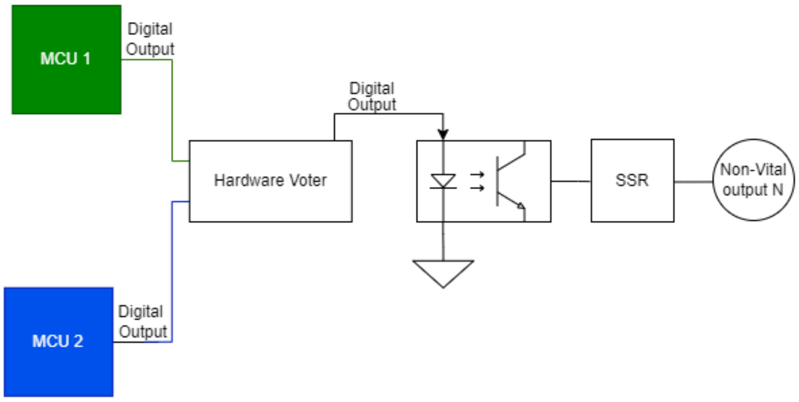

Figure 8: Non-Vital Outputs

Non-Vital outputs are activated when both controllers are in agreement. Figure 8 gives illustration of non-vital outputs.

If any fault occurs a two-character seven segment display will indicate the fault. The error codes will be detailed in design document.

3.4 SUNDOOR Motor Interface

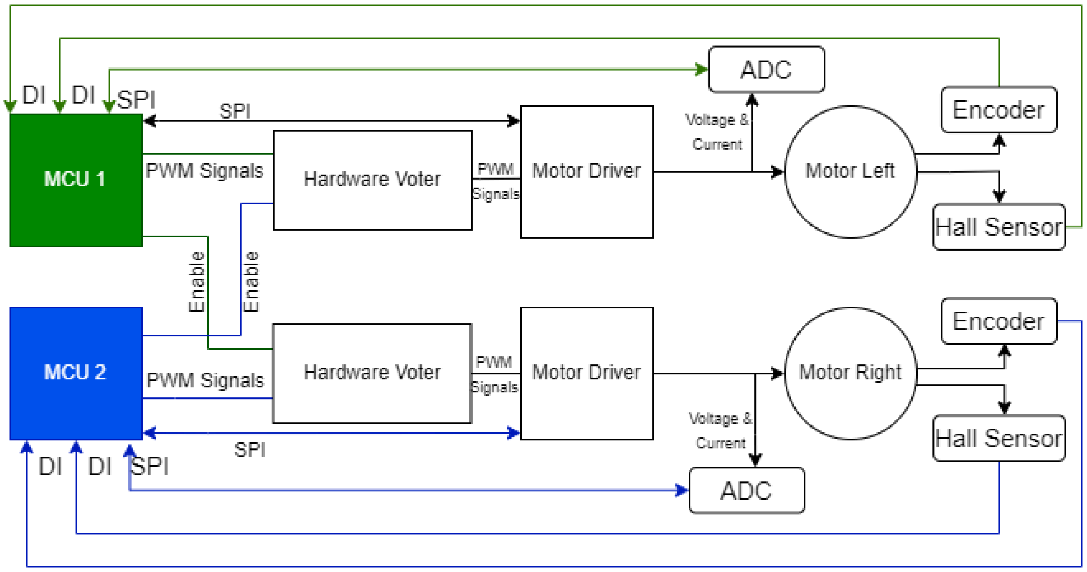

Figure 9: Motor Interface

SUNDOOR controllers shall have Motor interfaces connecting to Motor 1 and Motor 2. MCU 1 will control motor 1 and MCU 2 will control motor 2. The motor drive will be initiated with Enable and Not-Enable inputs being validated by both the controllers.

SUNDOOR motor driver consist of BLDC(full form) motor driver IC and H bridge Inverter. Motor drive IC will have PWM (full form)signals as input from MCU. Required parameters are configured with the SPI interface to MCU. Configured parameters and health status of motor driver IC will be monitored with help of health diagnostics. If any fault occurs, it will stop driving the motor and put the system in to safe state as mentioned in section 4.8.

The doors movement is achieved by the belt drive driven by the motor. The motor drive for the door movement and torque control is done in closed loop operation. This interface is illustrated in figure 9. The PWM signals will be generated based on the feedback from the encoder for door position control. Hall sensor feedback is using for rotor position and current feedback is using to get the torque/force.

The motor speed, door position and door speed are controlled based on the parameters acquired during the learn mode. These parameters are stored in non-volatile memory. The normal operation reference for motor current will be generated in learn mode.

The vital parameters such as each phase voltage and phase current will be monitored from the motor in real time to ensure the correct operation. The phase current is also monitored for the required torque levels. High precision ADCs are used for the measurement of voltage and current. The ADC has a SPI interface to the MCU. The current feedback of each motor is connected to the respective MCU. The obstruction is detected by measuring the motor current. During obstruction detection, the current profile will not match with normal operation reference profile, this mismatch in profiles is used for detecting the obstruction.

SUNDOOR will take encoder feedback. Encoder will be interfaced with MCU as Digital Inputs. Encoder feedback from motor 1 will be given to MCU 1 and encoder feedback from motor 2 will be given to MCU 2. SUNDOOR identifies the door position based on the encoder feedback. The encoder feedback is used in closed loop for position control. The belt drive is also monitored with the help of encoder feedback to detect any break in the belt, looseness of the belt and taughtness of the belt. The control algorithm will be detailed in design document.

The motor has hall effect sensors. Hall effect sensor will be interfaced with MCU as Digital Inputs. Hall effect sensor feedback from motor 1 will be given to MCU 1 and hall effect sensor feedback from motor 2. The hall effect sensor feedback will be used for rotor potion which will also be used for position control.

The motor drive IC has protection features like temperature sense which will be used to detect the raise in temperature.

3.5 SUNDOOR Communication Interface

SUNDOOR will have PROFINET, USB, RS485, and CAN interface for communication with external device. These interfaces will be connected to either of the two MCU. Data communicated in these interfaces will be available in both the MCUs.

Sl No.	Interface	Interface details
1	PROFINET	Communication with central controller for updating monitoring signal status

SI No.	Interface	Interface details
2	RS-485/USB	Interfaced with laptop for configuration.
3	CAN	Spare interface for future expansion

Table 4: Communication Interface

3.6 SUNDOOR Functional Flow

Open command status should be yes or no in the flow diagram

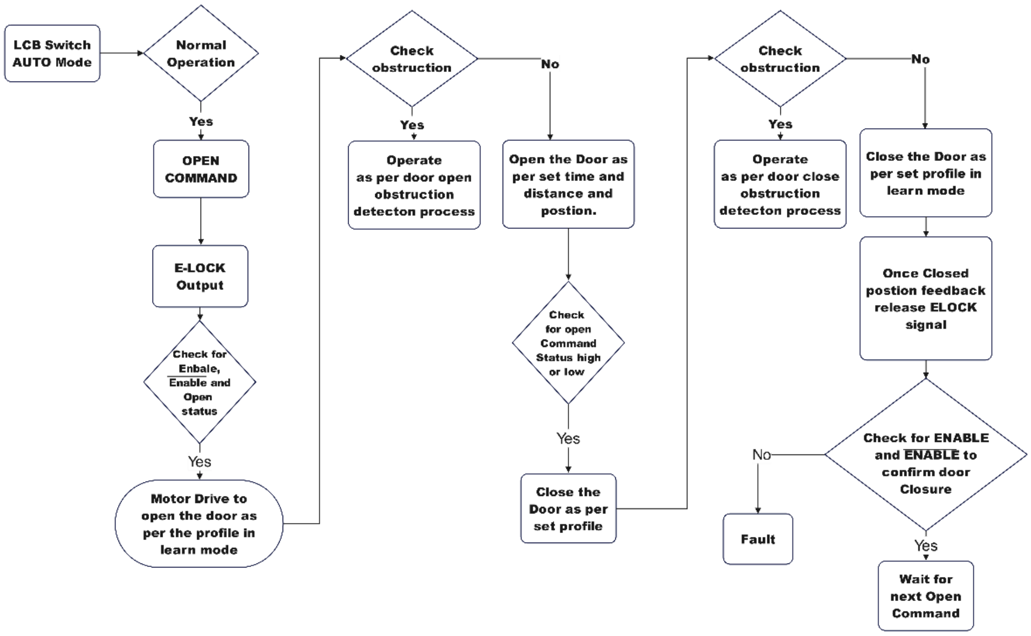
LCB Switch AUTO Mode
Normal Operation
Yes
OPEN COMMAND
E-LOCK Output
Check for Enbale, Enable and Open status
Yes
Motor Drive to open the door as per the profile in learn mode
Check obstruction
Yes
No
Operate as per door open obstruction detecton process
Open the Door as per set time and distance and postion.
Check for open Command Status high or low
Yes
Close the Door as per set profile
Check obstruction
Yes
No
Operate as per door close obstruction detecton process
Close the Door as per set profile in learn mode
Once Closed postion feedback release ELOCK signal
Check for ENABLE and ENABLE to confirm door Closure
No
Fault
Yes
Wait for next Open Command

Figure 10: Functional Flow of SUNDOOR

If the LCB is in AUTO mode the door control operation happens as per normal operation. SUNDOOR will have two different types of procedure to follow if obstruction is detected. First procedure is followed during opening operation of door and second procedure is followed during closing operation of door

While SUNDOOR is in auto mode, if an open command is received from central controller, SUNDOOR will activate vital outputs to unlatch ELOCK. ELOCKs will generate a enable and not-enable signal. Once ELOCK is unlatched SUNDOOR will open the door based on this signal. If obstruction is detected during opening, SUNDOOR shall follow procedure configured for obstruction detection in opening direction. When SUNDOOR receives door close command, SUNDOOR will close the door. If obstruction is detected during closing, SUNDOOR shall follow procedure configured for obstruction detection in closing direction. This functional flow of SUNDOOR is illustrated in figure 10. The logic for opening and closing signal is mentioned in table 5.

ENABLE Signal	**Signal**.	**DOOR Open Signal**..	**PG Operation**
1	0	1	Valid OPEN Signal
1	0	0	Valid CLOSE Signal
0	1	1	Not Enable Invalid Signal
0	1	0	Not Enable Invalid Signal
1	1	1	Enable Fault, Invalid signal
1	1	0	Enable Fault, Invalid signal
0	0	1	Enable Fault, Invalid signal

Table 5: Truth table for opening and closing of door

3.7 SUNDOOR Architecture and Boundary

The Scope of SUNDOOR is inside the dotted line marked area in the figure 2. The external field devices are not included in the scope of the SUNDOOR SIL 3 certification. Reliable control and motor power supply must be provided by the user to SUNDOOR.

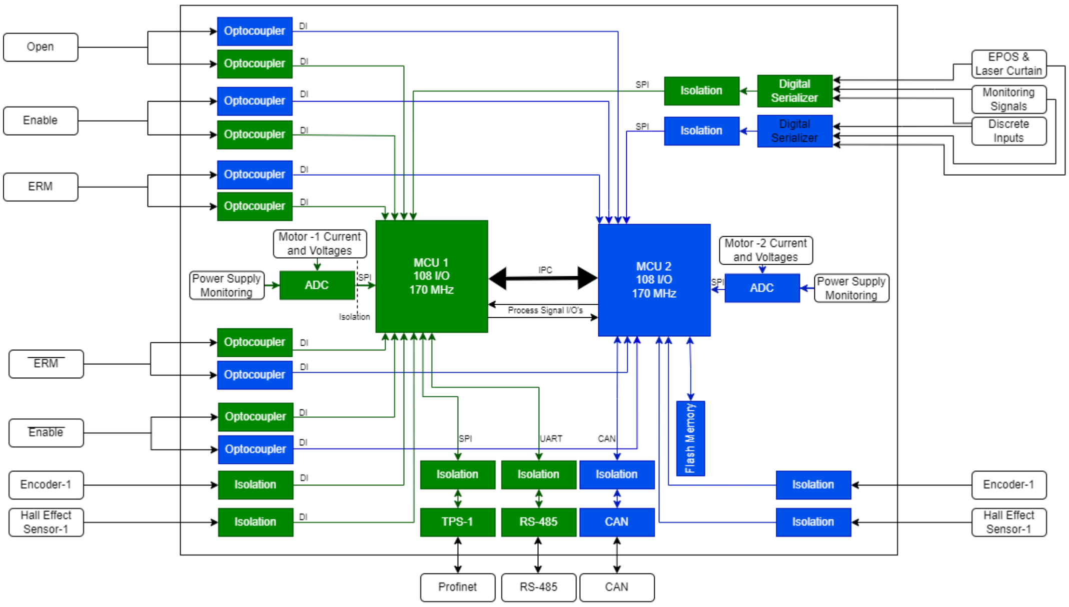

Figure 11: SUNDOOR Architecture (Inputs, Communications)

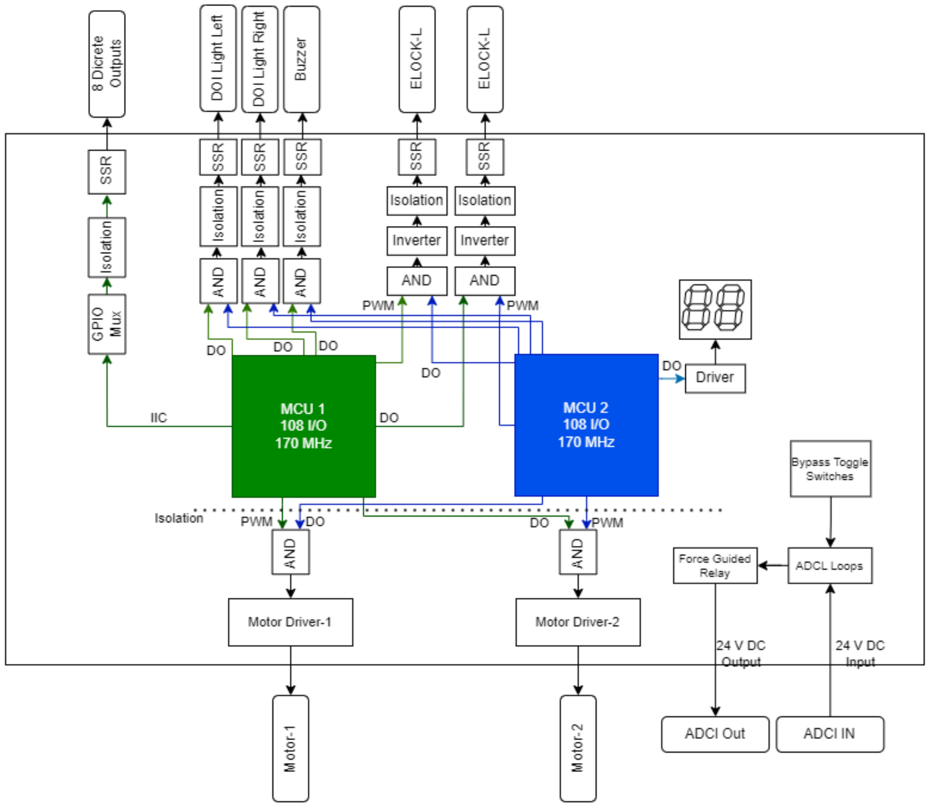

Figure 12: SUNDOOR Architecture (Output, ADCL)

As per figure 9 and figure 10 following are the signals for SUNDOOR as shown in table 4.

Sl No.	Signal	Description
1	ERM	24 V DC Signal for Emergency Release Manual, this will be generated as when ERM level is manually operated.
2	ERM-NOT	24 V DC complimentary Signal for Emergency Release Manual, this will be generated as when ERM level is manually operated.
3	Enable	24 V DC feedback final generated by left E-lock when E-lock is activated.
4	Enable Not	24 V DC complimentary feedback Signal left generated by E-lock when E-lock is activated.
5	Open	24 V DC open command signal from central controller.
6	Left Door Monitoring -1	24 V DC signal generated by limit switch for monitoring left ASD
7	Left Door Monitoring -2	24 V DC signal generated by limit switch for monitoring left ASD
8	Right Door Monitoring -1	24 V DC signal generated by limit switch for monitoring right ASD
9	Right Door Monitoring -2	24 V DC signal generated by limit switch for monitoring right ASD
10	EED Right Bypass Monitoring	24 V DC signal generated by bypass toggle switch of right EED for monitoring right EED bypassing

SI No .	Signal	Description
11	EED Left Bypass Monitoring	24 V DC signal generated by bypass toggle switch of left EED for monitoring left EED bypassing
12	EED Monitoring-1 Left	24 V DC signal generated by limit switch for monitoring left EED
13	EED Monitoring-2 Left	24 V DC signal generated by limit switch for monitoring left EED
14	EED Monitoring-1 Right	24 V DC signal generated by limit switch for monitoring right EED
15	EED Monitoring-2 Right	24 V DC signal generated by limit switch for monitoring right EED
16	PED Monitoring 1	24 V DC signal generated by limit switch for monitoring PED
17	PED Monitoring 2	24 V DC signal generated by limit switch for monitoring PED
18	PED Bypass Monitoring	24 V DC signal generated by bypass toggle switch of PED for monitoring PED bypassing
19	Auto Status Monitoring	24 V DC signal generated by LCB switch for auto mode status monitoring
20	Bypass Status Monitoring	24 V DC signal generated by LCB switch for bypass mode status monitoring
21	Isolate Status Monitoring	24 V DC signal generated by LCB switch for isolate mode status monitoring
22	EPOS Relay-1	24 VDC signal generated by Relay -1 of EPOS
23	EPOS Relay-2	24 VDC signal generated by Relay -2 of EPOS

Sl No.	Signal	Description
24	EPOS Test Pulse In	24 VDC signal given out for health monitoring of EPOS
25	EPOS ON/OFF Monitoring	24 VDC signal generated by EPOS if EPOS is ON
26	Laser Curtain ON/OFF Monitoring	24 VDC signal generated by EPOS if laser curtain is ON
27	Laser Curtain K1	24 V DC signal output of laser curtain
28	Laser Curtain K2	24 V DC signal output of laser curtain
29	Discrete Input -1	24 V DC Discrete Input-1
30	Discrete Input -2	24 V DC Discrete Input-2
31	Discrete Input -3	24 V DC Discrete Input-3
32	Discrete Input -4	24 V DC Discrete Input-4
33	Discrete Input -5	24 V DC Discrete Input-5
34	Discrete Input -6	24 V DC Discrete Input-6
35	Discrete Input -7	24 V DC Discrete Input-6
36	Discrete Input -8	24 V DC Discrete Input-8
37	E-Lock-Left	24 V DC output for E-Lock left
38	E-Lock-Right	24 V DC output for E-Lock right
39	EPOS Test Pulse Out	24 VDC input signal for health monitoring of EPOS
40	Buzzer	24 V DC output for buzzer
41	DOI Light Left	24 V DC output for DOI light left
42	DOI Light Right	24 V DC output for DOI light right
43	Discrete Output-1	24 V DC Discrete Output-1
44	Discrete Output-2	24 V DC Discrete Output-2
45	Discrete Output-3	24 V DC Discrete Output-3

SI No .	Signal	Description
46	Discrete Output-4	24 V DC Discrete Output-4
47	Discrete Output-5	24 V DC Discrete Output-5
48	Discrete Output-6	24 V DC Discrete Output-6
49	Discrete Output-7	24 V DC Discrete Output-7
50	Discrete Output-8	24 V DC Discrete Output-8
51	Motor -1 A phase output	Output for motor 1 phase A
52	Motor -1 B phase output	Output for motor 1 phase B
53	Motor -1 C phase output	Output for motor 1 phase C
54	Hall Effect Sensor input phase-1 A	5 V DC input from hall effect sensor 1 phase A
55	Hall Effect Sensor input phase-1 B	5 V DC input from hall effect sensor 1 phase B
56	Hall Effect Sensor input phase-1 C	5 V DC input from hall effect sensor 1 phase C
57	Encoder A-1 Channel	5 V DC input from encoder 1 phase A
58	Encoder B-1 Channel	5 V DC input from encoder 1 phase B
59	Encoder A-1 Not Channel	5 V DC input from encoder 1 phase A not
60	Encoder B-1 Not Channel	5 V DC input from encoder 1 phase B not
61	Motor A phase output	Output for motor 2 phase A
62	Motor B phase output	Output for motor 2 phase B
63	Motor C phase output	Output for motor 2 phase C
64	Hall Effect Sensor input phase-2 A	5 V DC input from hall effect sensor 2 phase A
65	Hall Effect Sensor input phase-2 B	5 V DC input from hall effect sensor 2 phase B

Sl No.	Signal	Description
66	Hall Effect Sensor input phase-2 C	5 V DC input from hall effect sensor 2 phase C
67	Encoder-2 A Channel	5 V DC input from encoder 1 phase A
68	Encoder-2 B Channel	5 V DC input from encoder 1 phase B
69	Encoder -2 A Not Channel	5 V DC input from encoder 1 phase A not
70	Encoder -2 B Not Channel	5 V DC input from encoder 1 phase B not

Table 6: Signals of SUNDOOR

It is assumed that the field devices connected to SUNDOOR are reliable and comply with the system requirement levels. The field devices are connected to SUNDOOR. These include safety IO and non-safety IO.

- Left and right door E-lock with limit switches used for mechanical latching of the doors.
- Limit switches
- Encoder input from left and right motors
- Hall sensors from the motor.
- EPOS input
- Indication lamps
- Indication Buzzer
- EPOS output
- Laser curtain
- Left and right motor
- Left and right encoder
- Motor
- E-Lock

3.8 SUNDOOR Modules

SUNDOOR Consist of thirteen different hardware modules as shown in table 4. The safety modules are designed as per EN50129 standards.

Sl. No.	Module
1	Power Supply Module

2	Safety Input Module
3	Non-Safety Input Module
4	Safety Output Module
5	Non-Safety Output Module
6	2oo2 Configured Controller Module
7	Motor Drive Module
8	Analog Input Module
9	PROFINET Communication Module
10	USB Communication Module
11	CAN Bus Communication Module
12	RS-485 Communication Module
13	Data Logger Module

Table 7: Hardware Modules

4. Design guidelines followed as per EN 50129: 2018 for different safety modules.

4.1 As per EN50129 Table E4 serial number 6 dual electronic structure based on composite fail-safety with fail-safe comparison technique is used for the SUNDOOR.

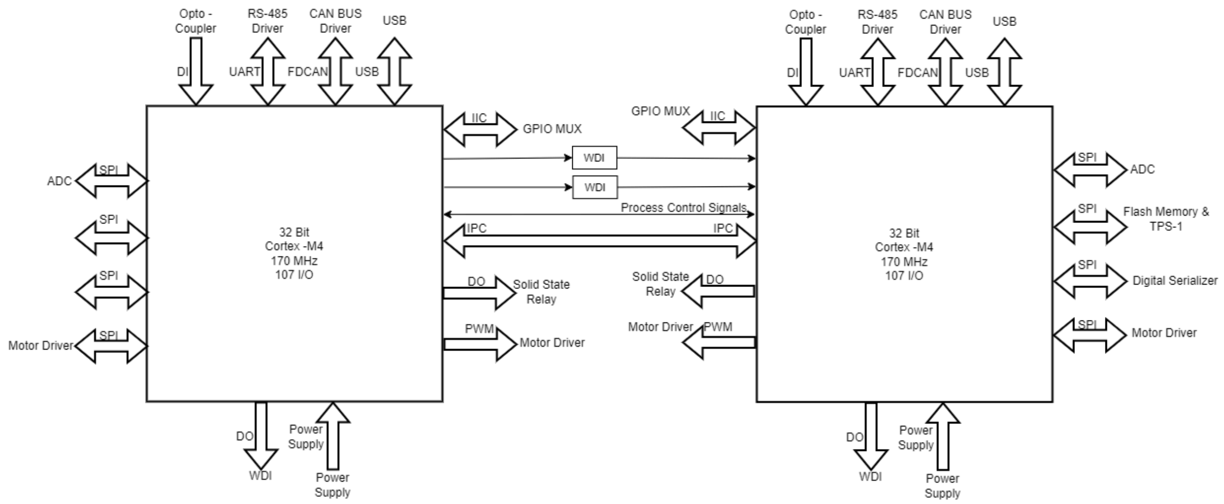

Figure 13: 2oo2 Controller Module

- The Control Module consists of two MCU as per figure 9.
- The controllers selected have high MTBF value.
- Each MCU will be powered with redundant control supply.
- Safety inputs are connected to both the controller.
- The outputs are driven only after the two controllers agree with voting.
- Hardware watchdog timer is used to detect and recover from controller malfunctions. Watchdog facilitates automatic correction of temporary hardware faults, and to prevent errant or malevolent software from disrupting system operation.
- Strict flow control is assured in software by providing predefined operational cycles and operation sequence.
- Data protection and validation is used for software.
- Obsolete data deletion.
- CRC for vital data.
- Minimum number of Interrupts are used in software.
- Time out provision where the program waits for an event.
- Periodic Self-Check routines are included in the software.
- Integrity check for the code memory and application data memory.
- Memory read, write and addressing test for RAM.
- CPU Instruction Check.
- Peripheral hardware testing.
  - UART loopback Testing.
  - Timer test using independent reference clock

- A single failure in any one processor is considered as failure for driving the doors to attain a safe situation with indication. Manual intervention may be required in case the doors are not able to be driven to a safe closed state. The motors run in closing direction.
- The faulty module is shut down and a fault message is generated by the central controller. The SUNDOOR is disabled in view of the inability to make safety decisions.
- For recovery the entire module needs to be replaced as it is single board solution.
- Independent input and read-back channels are provided for both the controllers.
- The two processor communicate on UART with communication protocol meeting EN 50159:2010 [Ref 8] table 1 guidelines. The defences are listed below in the table.

Field Name	**Field Description**	**Defence Technique as per 50159**
Start of frame (SOF)	SOF contains two bytes of data to identify start of the message.	NA
Source Address	Source address contains transmitter CPU ID.	Source address and destination address can detect the threat "insertion" of a message from invalid source. Only CPU-A and CPU-B are connected in the transmission channel.
Destination Address	Destination address contains receiver CPU ID	
Control Byte	Control byte determines the type of message	NA
Sequence Number	Sequence number contains 16-bit length. Sequence numbering consists of adding a running number to each message exchanged	Receiver check the sequence of messages provided by the transmitter.

Field Name	Field Description	Defence Technique as per 50159
	between CPU-A and CPU-B.	Message will not be processed, if the message is not received in sequence. “Repetition”, “Deletion”, “Insertion”, “Re-sequence” threats will be eliminated by using the sequence number.
Dynamic Health Signature	Health signature will be generated based on the sequence of activities performed each CPU. Sequence number will be added to health signature to make it dynamic.	NA
Data	Input or output data to be exchanged between two CPUs	NA
Data complement	Data complement to detect the bit errors	NA
CRC	16-bit CRC to detect the bit errors in the transmission channel	Corruption of the message will be detected by using correct CRC polynomial.
End of Frame (EoF)	EOF contains two bytes of data to identify end of the message	NA

Table 8: Protocol for IPC

4.2 Interfaces.

- Power supply will have reverse polarity protection to avoid hazardous situation in case of wrong connection given to SUNDOOR
- Communication to MCU by any of the interfaces like RS-485, PROFINET, and CAN will not have any write access to MCU.

- Status Monitoring with PROFINET communication by central controller.
- Message sequence numbering in serial message to check timelines of data.
- Fixed message length.
- All transfers are acknowledged.
- Ring topology.
- RS-485 connection will be protected using unique ID or password to avoid any attempt to interfere the control operation of MCU
- All the configuration settings range for the SUNDOOR for a particular gate will have setpoints predefined with input from historical data and any deviations will be alerted during configuration

4.3 Operator / maintainer friendliness to reduce the probability of human errors

Power supply connectors will be used which cannot be connected to the mating part in wrong direction, reducing the human error which may lead to any hazardous situation. All the toggle switches or push buttons shall be designed or mounted in such a way that accidently the state of switches will not change. For toggle switches a Pull to Unlock toggle switches will be used. Push buttons with hard enclosure will be used, which will be activated after continuous press. Guided GUI will be provided for maintenance to avoid human error. All the modifications for the setting will be validated by the system and alerts will be provided. Input section connectors will be used which cannot be connected to the mating part in wrong direction, reducing the human error which may lead to any hazardous situation. Output section connectors will be used which cannot be connected to the mating part in wrong direction, reducing the human error which may lead to any hazardous situation. Maintenance manual with pictures and screenshots will be provided. Board level replacement shall be recommended for maintenance at site to have very low MTTR(full form). Repair shop will have a test jig to test and validate the boards before replacement.

4.4 Protection against single faults for discrete component.

- Any of the discrete component affecting power supply leading to a fault in power supply will be identified by power supply monitoring and system will be put in to safe state. SUNDOOR will have overload and short circuit protection
- Any fault occurring in any of the discrete components related to MCU will alter the performance of MCU. As this is 2oo2 architecture and voting is done by inter processor communication the faults with one controller will be identified by the software implemented in the other MCU. Any failures will be indicated and safe state will be set.

- Any single fault occurring to the discrete components will be identified by comparing the data from two channels. If concurrence is not achieved then the system will be kept in shutdown mode.

4.5 Dynamic Fault Detection

- Monitoring of all the supply voltages by MCU will enable SUNDOOR to identify any fault in power supply.
- Variation of current drawn by motor will be measured along with phase voltages. All the power supply will be monitored. Each channel of ADC IC and Digital serializer will be stimulated and monitored for any faults.
- The comparison between data of two digital input channels enables the dynamic detection of a fault.

4.6 Multiple Faults handling as per standards

- If multiple faults occur the safe state is initiated.

4.7 Measures against voltage breakdown, voltage variations, overvoltage, low voltage.

- TVS diode will be used for surge protection, DC-DC regulators will take care of the under voltage and over voltage scenarios.

4.8 Retention of safe state

- Safe state of SUNDOOR would be stopping door operation and freewheeling of motor. In this case operator can manually move the door to closed position.
- If any fault is identified in the power supply module, system will be shut down and put in a safe state.
- If any fault is identified in a MCU by the other MCU, it will put the system in a safe state.
- If any fault is identified in an input module it will put the system to a safe state.
- MCU will have a supervisory circuit monitoring the power supply and reporting to other MCU. If a fault is identified the system will be put in safe state.
- Safe State is achieved by withdrawing drive signals from motor by DCU.
- Even If one of the MCU becomes faulty and continues to produce PWM, drive signal cannot be generated.

4.9 Control of Temperature outside specified range by monitoring critical component temperatures

- MCU, IPM, Digital Serializer and ADC have inbuilt dye temperature sensor. If value of this goes beyond the threshold, system shutdown will occur.

4.10 EMI/EMC and ESD protection are provided. EMI /EMC shall be validated at tests labs as per standards as per design documents.

4.11 Protection against sabotage (physical) IT security

- Sabotage does not happen as SUNDOOR app is not connected to the internet and no external device can connect without proper authentication.

5 SUNDOOR Hardware Specification's

Sl. No.	Feature	Specification
1	Active power input	24 VDC 2 A for Control Power 24 VDC 15 A for Motors
2	Weight	1.5 Kg ~ 2 Kg
3	Failure indications	7 segment LED provides the error code
4	Output voltage to Motor (DC)	24 V DC
5	Protections	Short CKT, Overload
6	Operating temperature	-20 °C to 70 °C
7	Storage temperature	-30 °C to 85 °C
8	Relative humidity	Min 10% and max 93% no condensation
9	Operating altitude with respect to sea level max	2000 m
10	Dimensions	Targeted for 320 mm x 60 mm x 200 mm (Lx H x W) with brackets for mounting

Table 9: Hardware Specifications