AN1118

Safety Manual for Sendyne SIM100MOD Isolation Monitor

This document describes how to use the Sendyne SIM100MOD isolation monitor in a safety related system.

Contents

List of figures

Introduction

The system and equipment manufacturer or designer intending to use this product is responsible to ensure that their system incorporating Sendyne's SIM100MOD meet all applicable safety, regulatory and system level performance requirements. All information presented in this document is for reference only. Users understand and agree that their use of SIM100MOD in safety-critical applications is entirely at their risk, and that user (as buyer) agrees to defend, indemnify, and hold harmless Sendyne from any and all damages, claims, suits, or expense resulting from such use.

This safety manual provides information to assist system developers in creating safety-related systems incorporating the Sendyne SIM100MOD isolation monitoring device. This document contains:

- Overview of the SIM100MOD architecture
- Overview of the safety architecture for management of hardware failures
- Assumptions of Use

Sendyne assumes that the user of this document has a general familiarity of the SIM100MOD. This document is intended to be used in conjunction with the relevant datasheet and application notes.

Sendyne SIM100MOD overview

The SIM100MOD is an electrically isolated device that when connected properly to an idle or active high voltage IT power system (floating ground) can estimate the resistive and capacitive paths between each power rail of the IT system and a third reference point. The SIM100MOD can communicate through CAN bus (250 or 500 kbits/s) and when interrogated by a host it can provide estimates on the values of each resistive and capacitive path.

The SIM100MOD, based on information programmed by the host for the designed maximum voltage of the IT power system, will calculate a value for the minimum resistance path between the two IT power system rails and the third voltage reference point, expressed in Ohms/Volt (max designed voltage). In addition, it will estimate the total energy that can be potentially stored in the IT power system capacitances. If the CAN bus host fails to provide information on the maximum IT power system voltage, the SIM100MOD will calculate these values based on the maximum voltage observed during its operation.

The SIM100MOD power input accepts any supply voltage between 4.8 V and 53 V. The input voltage is pre-regulated and then stepped down through a DC/DC converter feeding through galvanically isolated inputs the +5 V IC supply and the 12.5 V excitation voltage source supply.

The SIM100MOD safety architecture includes a watchdog timer, CRC check on internal non-volatile program memory, diagnostics for proper connections of chassis and IT power system terminals, monitoring of the unregulated power supply voltage level for the main IC before local voltage regulator (LDO), environment temperature monitoring and excitation pulse voltage monitoring. In addition, the

SIM100MOD safety architecture monitors the voltage divider values for chassis, positive and negative voltage connections and provides a visual heartbeat signal indicating proper IC operation.

All estimates of isolation resistances and capacitances are submitted along with an uncertainty percentage value. This value defines the interval within which the actual value lies with a probability of 95%.

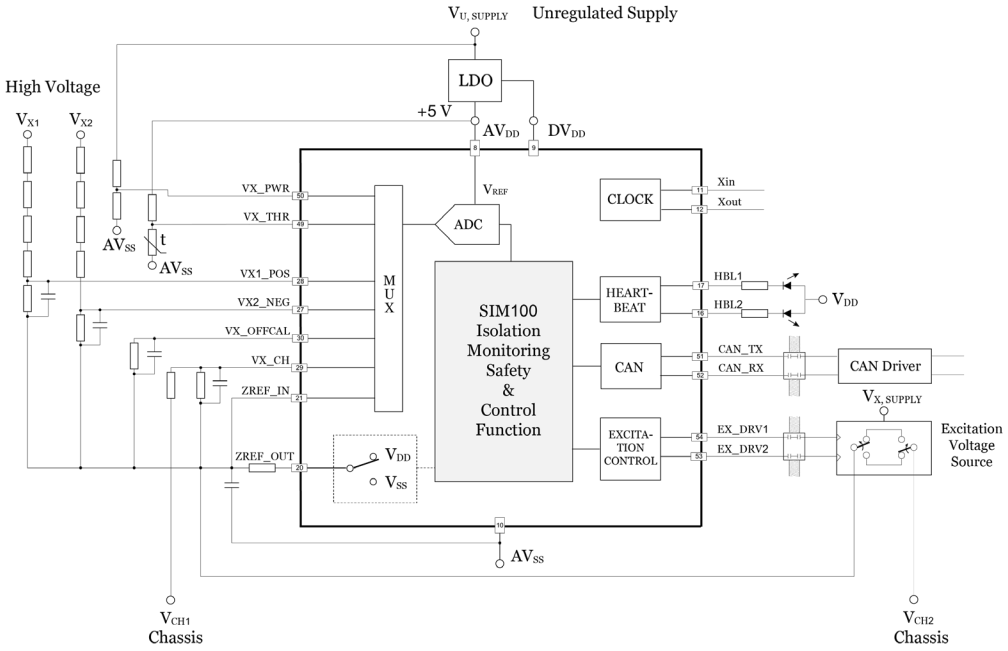

Figure 1: SIM100MOD functional diagram

Safety functions and diagnostics overview

The SIM100MOD is intended for use in automotive and industrial safety-relevant applications. All components used are automotive rated.

Hardware

The following list of monitoring functions are implemented in the SIM100MOD.

- $V_{U, SUPPLY}$ monitor
- $V_{X, SUPPLY}$ monitor
- V_{X1} connection monitor
- V_{X2} connection monitor
- V_{X1} voltage divider ratio monitor
- V_{X2} voltage divider ratio monitor
- V_{CH1} and V_{CH2} connections monitor

- V_{X_CH} voltage divider ratio monitor
- V_{X_CH} Excitation Voltage Source voltage value monitor
- V_{X_THR} environment temperature monitor

Upon diagnosing a hardware error, the SIM100MOD will set the appropriate flags and enter a SAFE state.

Software

On the RESET state the SIM100MOD performs CRC check on the non-volatile memory. During active operation a watchdog timer ensures proper program flow. In addition, every estimate on the isolation state of the monitored IT power system is accompanied by the uncertainty value of this estimate.

Target applications

The Sendyne SIM100MOD has been designed to be used as an element for the isolation safety system in applications such as:

- Automotive
- Charging stations
- Industrial high voltage ungrounded systems

Fig. 2 and Fig. 3 show the boundary diagram for the SIM100MOD as a SEooC (Safety Element out of Context) in two different applications.

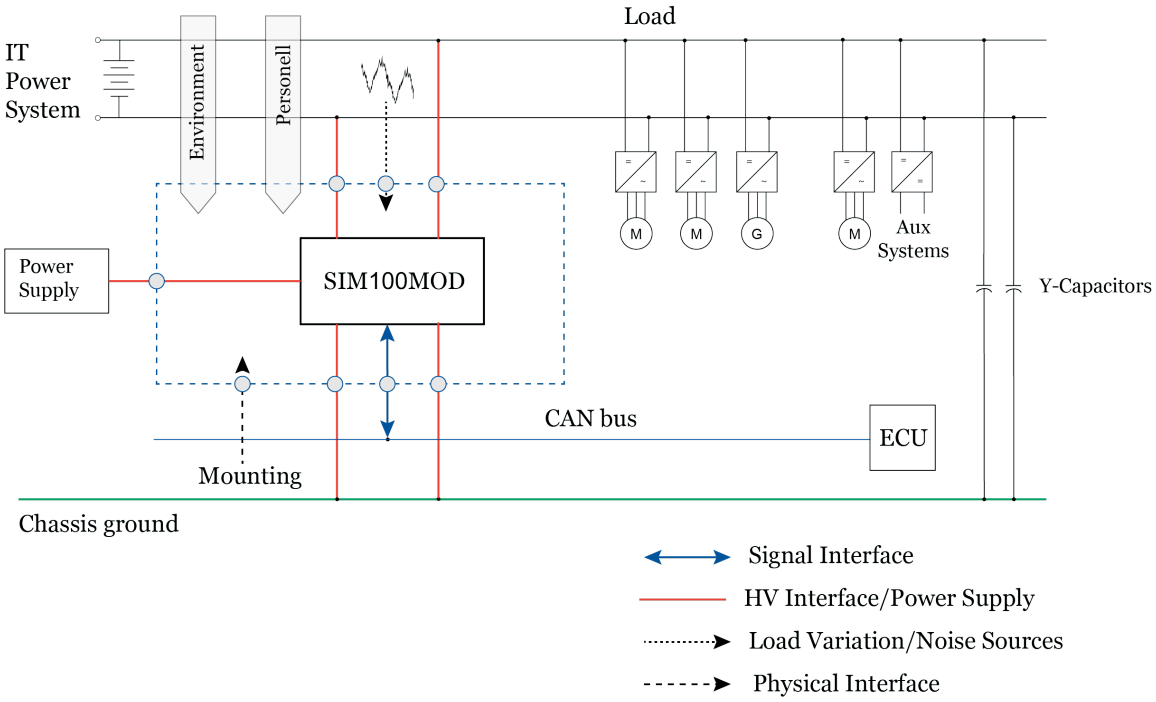

Figure 2: The boundary diagram of SIM100MOD as SEooC in EV implementations

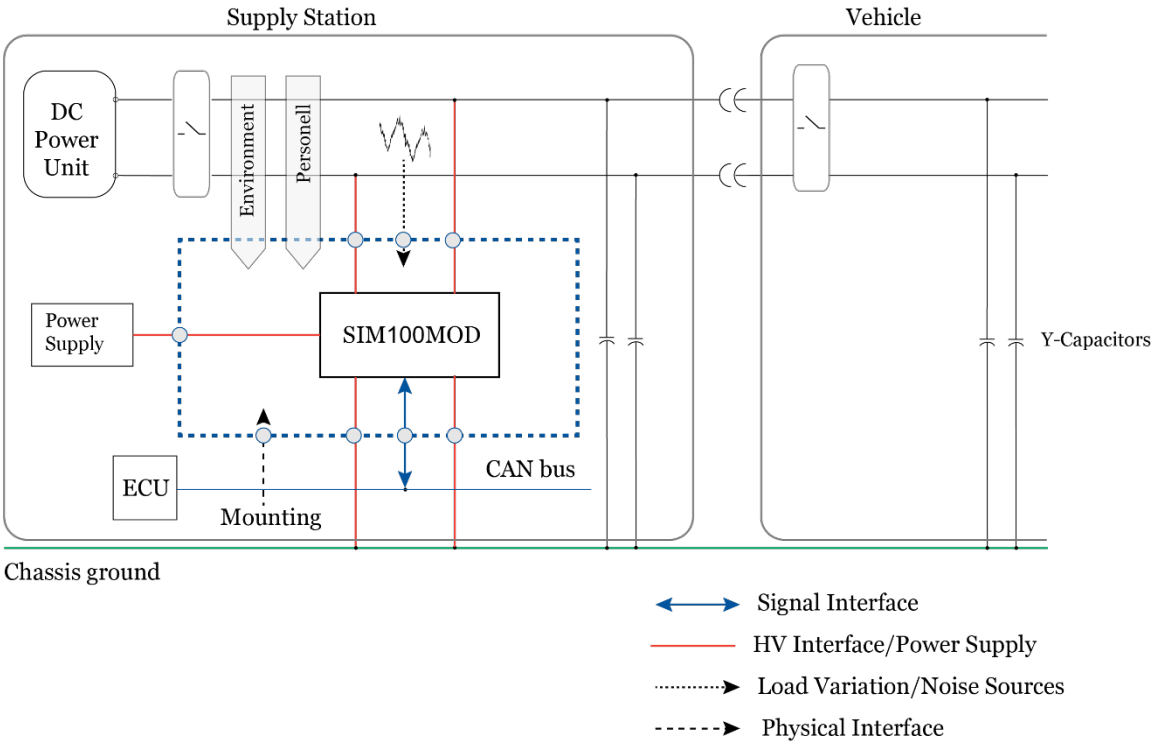

Figure 3: The boundary diagram of SIM100MOD as SEooC in EV implementations

Assumptions

The following table lists the assumptions made for safe employment of the SIM100MOD is a safety critical system.

ID	Type	Assumed Requirement
AR01	Assumed Requirement	The SEooC is defined as the SIM100MOD playing a role as an isolation monitoring element as shown in *Fig. 2 and Fig. 3*
AR02	Assumed Requirement	Thermal environment is between -40 °C and +105 °C (Temperature range is limited by connector thermal specifications. For SIM100MODAZ1, operating range is -40 °C to +125 °C)
AR03	Assumed Requirement	The IT Power System voltage monitored by the SIM100MOD will vary between 15 V and 962 V
AR04	Assumed Requirement	The IT Power System is connected to chassis through Y-Capacitors of at least 100 nF on each side of the power supply
AR05	Assumed Requirement	The SIM100MOD-xxx is supplied with proper power according to the specifications of the *SIM100MOD datasheet*
AR06	Assumed Requirement	Safety Integrity Level is ASIL B
AR07	Assumed Requirement	No other isolation monitoring device is active in the monitored system

Table 1: Assumed Requirements for SIM100MOD as a SEooC

Custom development

The SIM100MOD has been developed as a safety element out of context and it is offered as a commercial off-the-shelf product. Safety requirements used were based on Sendyne's understanding of the safety requirements of potential applications. Sendyne can customize the product in order to meet specific customer safety requirements through a development interface agreement (DIA). To request customization contact info@sendyne.com

Safety documentation

Verification and validation of the SIM100MOD safety features was performed through testing and computer simulation. Results of SIM100MOD testing following guidelines of different standards as well as the model used for SIM100MOD safety function testing can be made available at Sendyne's discretion under an NDA (non-disclosure agreement)

Audits and certification

Sendyne has no plans to perform an external audit of the SIM100MOD to ISO 26262 or other standards. Documentation, including this manual can be made available to support customer system audit and certification. Forward any request for an independent audit to your sales contact or info@sendyne.com.

Device operating states

Fig. 3 shows an overview of the operating states of SIM100MOD. Refer to the product datasheet and other documentation for details.

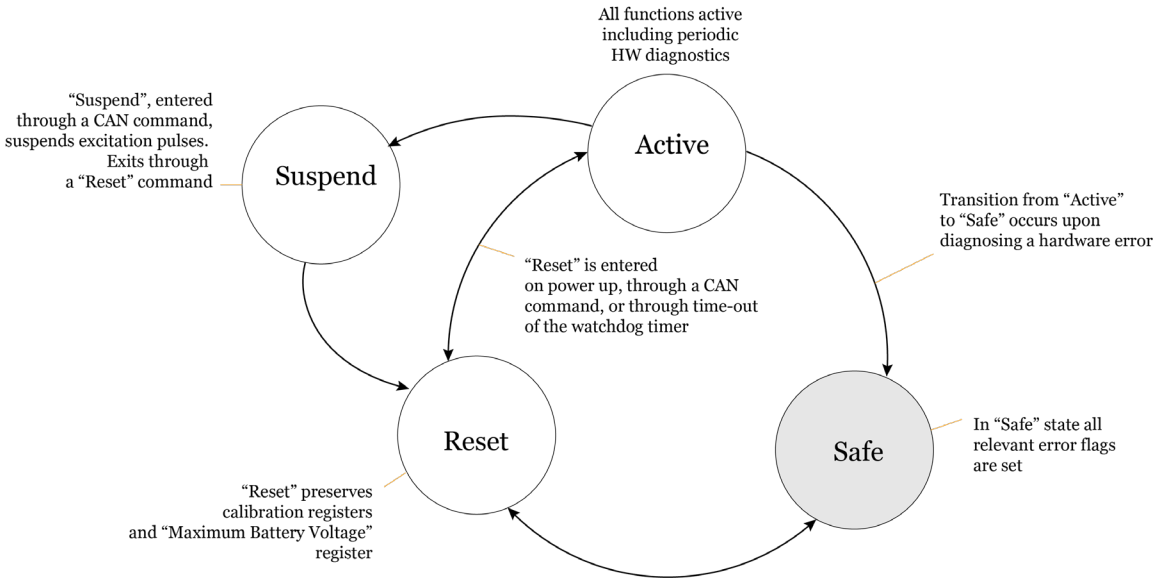

Figure 4: Operating states of the SIM100MOD

Product lifecycle support

The SIM100MOD contains a safe bootloader capable of field upgrades through the CAN bus interface.

Appendix

Proper connection to the target system

Connection to the IT power system

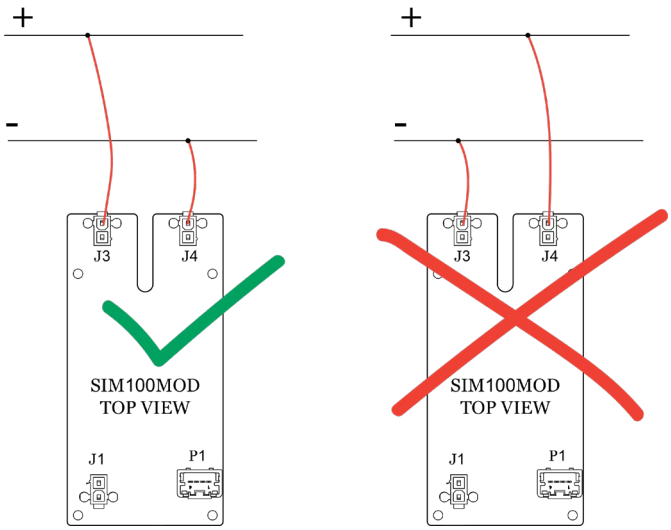

Figure 5: Proper connection to IT power system terminals

Connection to chassis

The SIM100MOD should connect through J1 at two separate chassis points. The SIM100MOD relies on this type of connection to detect proper connection to the chassis. If both leads from J1 are connected to the same point there is a possibility of an undetected disconnection. Such an event will jeopardize the SIM100MOD safety function.

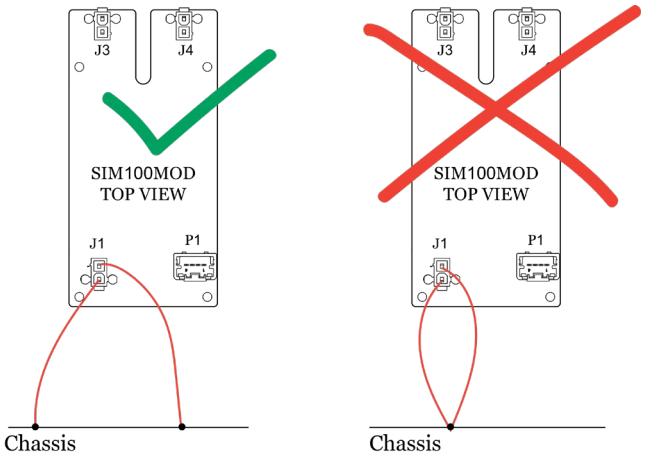

Figure 6: Proper connection at two distinct point to the chassis

Presence of Y-capacitors

The SIM100MOD relies on the presence of the ubiquitous Y-capacitors to perform its safety function. Absence of Y-capacitors with a minimum value of 100 nF will flag a connection error and lead the SIM100MOD into the SAFE state.

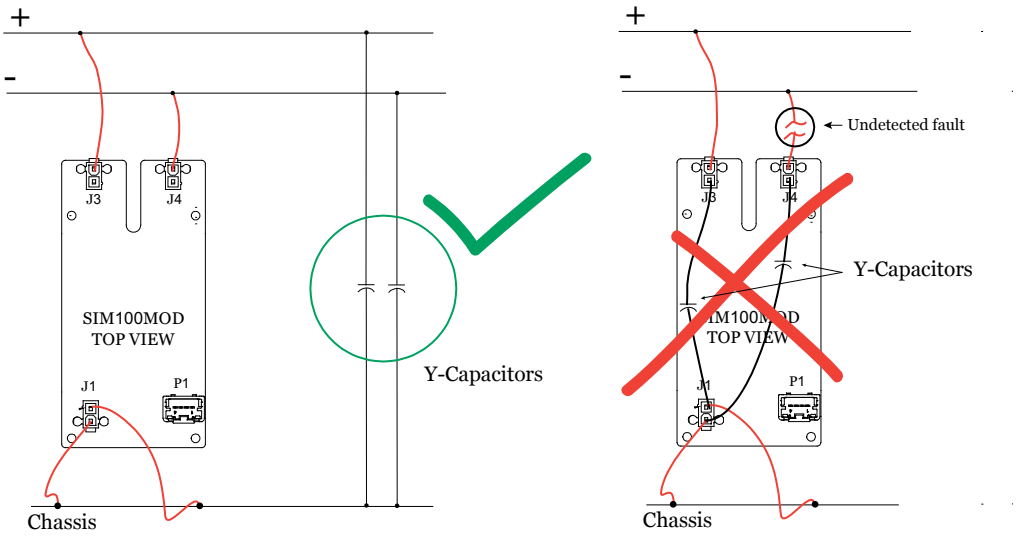

Figure 7: Presence of Y-capacitors is a requirement for proper function of the SIM100MOD. The capacitors should be connected directly to the power lines. Connecting them on the SIM100MOD board instead would impair the ability of the monitor to detect disconnection from the monitored IT power lines.

Revision history

Date	Revision	Changes
11/15/2018	0.1	Initial release
1/17/2019	0.2	Added image for proper connection of Y capacitors
2/11/2019	0.2a	Added image for isolation monitoring in charging stations. Added assumed requirement for no other active isolation monitoring device in the IT power system

Table 2: Document revision history