IMAC SIL EMERGENCY STOP QUALIFICATION

Integrated Monitoring and Control System

Introduction

The primary safety function of the iMAC Controller is that its Control Relay (CR) will de-energise on loss of communications with the iMAC EOL module. This allows an emergency stop system to be simply implemented by installing emergency stop switch contacts in series with the signal line that connects the iMAC Controller to EOL module. When an emergency stop switch contact operates, the connection between the iMAC Controller and EOL module is open circuited causing a loss in communication between the Controller and EOL module which the Controller detects and forces its CR to open (de-energise).

There are four standard iMAC E/Stop system configurations which are shown pictorially in Figures 1-4:

- 2-wire fieldbus with iMAC Controller and EOL Module (1oo1)
- 2-wire fieldbus with iMAC Controller, CRM Module, and EOL Module (1oo2)
- 3-wire fieldbus with iMAC Controller, MEOL Module and EOL Module (1oo1)
- 3-wire fieldbus with iMAC Controller, CRM Module, MEOL Module and EOL Module (1oo2)

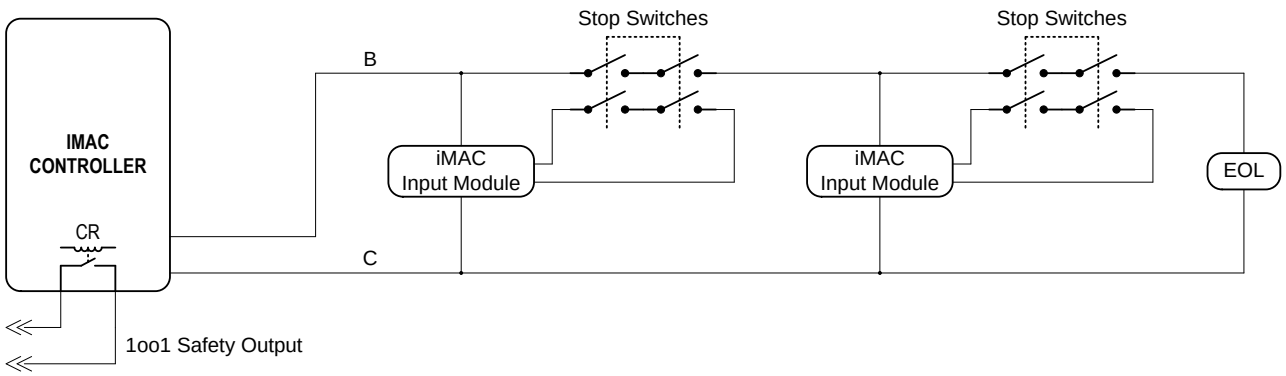

Figure 1: iMAC 2-wire configuration

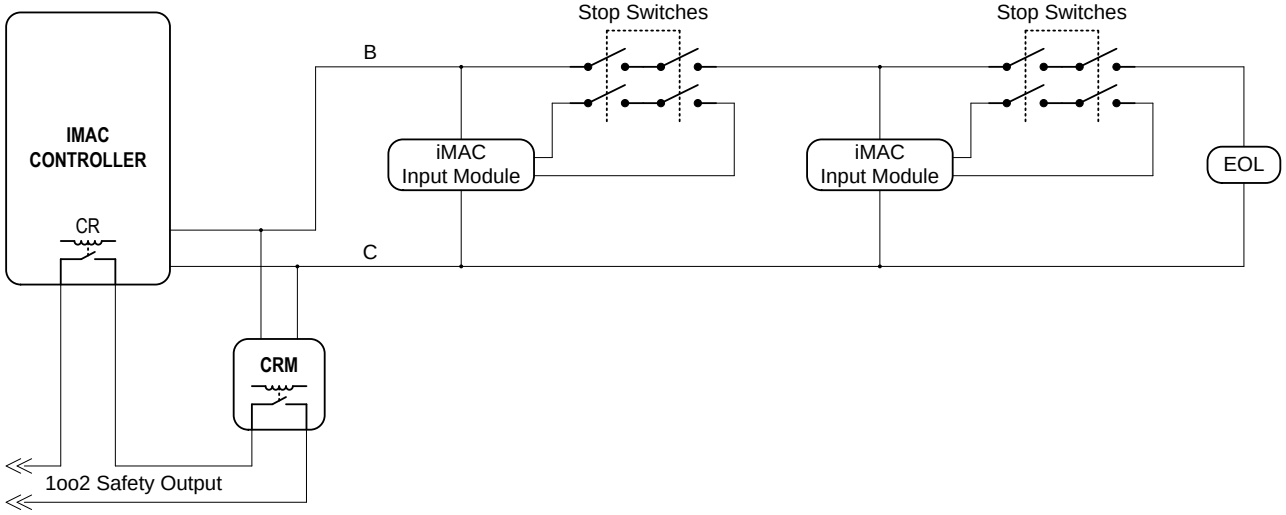

Figure 2: iMAC 2-wire configuration with CRM

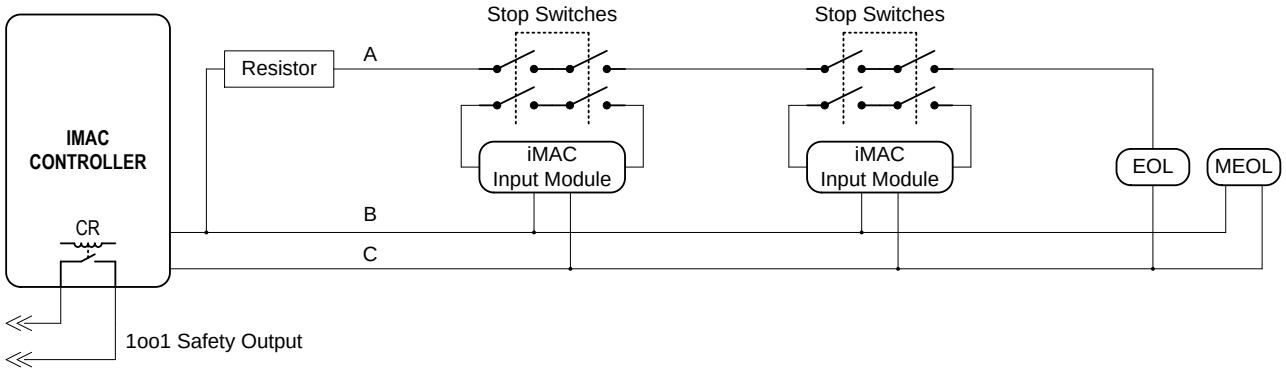

Figure 3: iMAC 3-wire configuration

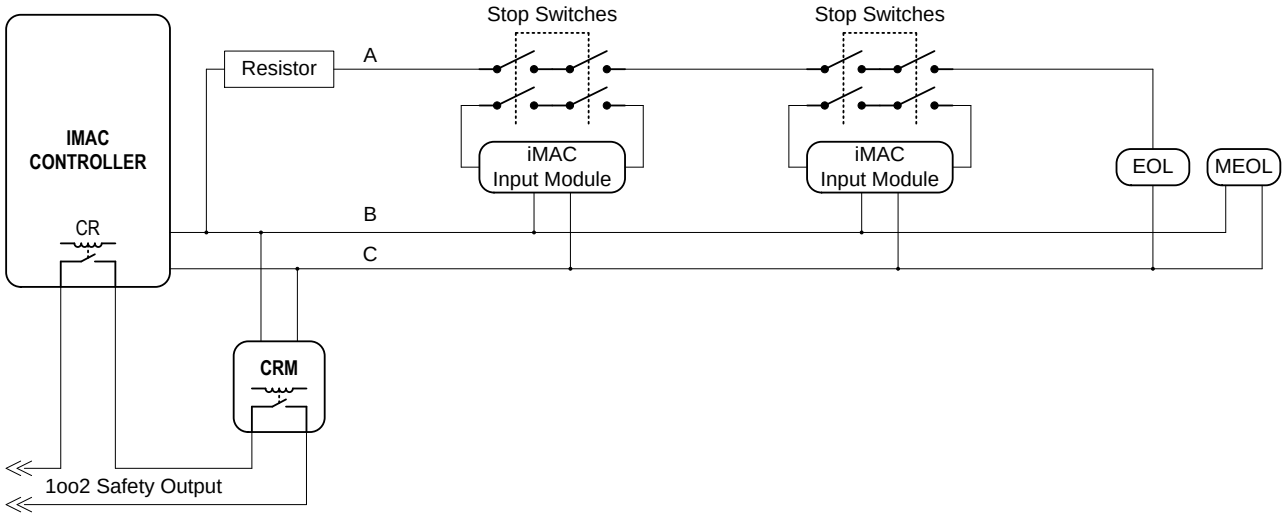

Figure 4: iMAC 3-wire configuration with CRM

This document summarizes the overall SIL qualifications obtainable for each of the four iMAC E/Stop system configurations.

These SIL qualifications do not include consideration of the customer's equipment which may be controlled by the relay outputs of the iMAC/iMAC2 Controller CR and CRM module. Since this customer equipment varies, it is highly recommended that system integrators and/or end users perform safety integrity verifications on the complete scope of their safety related systems, including site-specific equipment and configurations that may be controlled by the relay outputs of the iMAC/iMAC2 Controller CR and CRM module.

Terms and Definitions

DD	Dangerous Detected failure
DU	Dangerous Undetected failure
FIT	Failure in Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects and Diagnostic Analysis
PFD	Probability of Failure on Demand
PFH	Probably of dangerous Failure per hour
PIU	Proven In Use
SD	Safe Detected failure
SFF	Safe Failure Fraction – a determination of the fraction of failures which result in a safe state and the fraction of failures which are detected leading to a safe action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SU	Safe Undetected failure

iMAC Emergency Stop SIL Qualifications

The iMAC system has undergone both hardware FMEDA assessments (exida[1,2]) and PIU assessments (Marcus Punch Pty Ltd[3,4]) according to IEC 61508.

The tables below summarise the results of the latest editions of these assessments for each of the four standard iMAC E/Stop system configurations using either an iMAC Controller or iMAC2 Controller.

Table 1 Standard 2-wire and 3-wire system configurations with iMAC Controller

Name/Description of the Safety Function	PFD[5]	PFH	SIL Range of PFD/PFH	Architectural SIL Claim Limit	Overall SIL "Capability"
"2-Wire" system used for lanyard stop or emergency stop.	$1.1x10^{-3}$	$2.6x10^{-7}$	Low Range SIL2[6] (Low Demand) Low Range SIL2 (High Demand)	SIL2	SIL2
"2-Wire with CRM" system used for lanyard stop or emergency stop.	$8.3x10^{-5}$	$1.9x10^{-8}$	High Range SIL4 (Low Demand) Low Range SIL3 (High Demand)	SIL3	SIL3
"3-Wire" system used for lanyard stop or emergency stop.	$1.2x10^{-3}$	$2.6x10^{-7}$	Low Range SIL2 (Low Demand) Low Range SIL2 (High Demand)	SIL2	SIL2
"3-Wire with CRM" system used for lanyard stop or emergency stop.	$8.5x10^{-5}$	$1.9x10^{-8}$	High Range SIL4 (Low Demand) Low Range SIL3 (High Demand)	SIL3	SIL3

Table 2 Standard 2-wire and 3-wire system configurations with iMAC2 Controller

Name/Description of the Safety Function	PFD[5]	PFH	SIL Range of PFD/PFH	Architectural SIL Claim Limit	Overall SIL "Capability"
"2-Wire" system used for lanyard stop or emergency stop.	$1.2x10^{-3}$	$2.8x10^{-7}$	Low Range SIL2[6] (Low Demand) Low Range SIL2 (High Demand)	SIL2	SIL2
"2-Wire with CRM" system used for lanyard stop or emergency stop.	$9.0x10^{-5}$	$2.0x10^{-8}$	High Range SIL4 (Low Demand) Low Range SIL3 (High Demand)	SIL3	SIL3
"3-Wire" system used for lanyard stop or emergency stop.	$1.3x10^{-3}$	$2.9x10^{-7}$	Low Range SIL2 (Low Demand) Low Range SIL2 (High Demand)	SIL2	SIL2
"3-Wire with CRM" system used for lanyard stop or emergency stop.	$9.1x10^{-5}$	$2.1x10^{-8}$	High Range SIL4 (Low Demand) Low Range SIL3 (High Demand)	SIL3	SIL3

References and Disclaimer

- *[1]AMP 06-05-01 R001 V2 R4 FMEDA iMAC.pdf*
- *[2]AMP 08-03-46 R002 V2 R4 Application Example iMAC.pdf*
- *[3]AMP-11-05-A iMAC 2-wire & 3-wire - SIL Verification Oct20 Rev6.pdf*
- *[4]AMP-15-01-A iMAC2 2-wire & 3-wire - SIL Verification Oct20 Rev7.pdf*
- *[5]These PFD values are provided on the basis of a one (1) year proof-test interval. It is suggested that these intervals or more frequent proof-testing be applied.*
- *[6]Interpretation: "Low Range" means the better end of the scale and "High Range" means the worst end of the scale.*