OPW Fluid Transfer Group Europe BV

RACK safety manual

For the 88XX RACK series

Engineering Department
5-8-2022

Table of Contents

1. Introduction

1.1. General

The Rack has various models. They are listed in Table 1.1. Throughout this document the descriptor "the rack" will be used for all models. All models have the format 88YX-XXXX where Y is 2, 5 o 7 and X is any value.

Rack model	Sil rating	Description
88xxx-xxxxx	1	Rack monitor
88xxx-xxSxx	2	Rack monitor wth secondary rack

Table 1.1 Rack model overview

1.2. Purpose of this document

This document contains information and safety instructions that you will require when using the Rack in safety-instrumented systems.
It is aimed at system planners, constructors, service and maintenance engineers and personnel who will commission the device.

1.3. Additional documentation

This documentation is exclusively for the safety function of the Rack. Table 1.2 shows which other documents are important with respect to the Rack.

Document	Purpose
H72611_X0	Installation manual
EN13922:2020	Working principle and signal compatibility

Table 1.2 Additional documents

1.4. Change history

Table 1.3 shows all released versions of this document

Edition	Document name	Notes	Date
A.0	H72858_A0	First edition	13-September-2022

Table 1.3 document change history

1.5. Further information

The instructions in this document won't add to or modify any existing agreement, commitment or legal relationship. Any statements contained in this document do not create new warranties.

2. General Safety instructions

2.1. Safety instrumented system

2.1.1. Safety instrumented system

A safety instrumented system is responsible for executing the safety functions that are required to achieve a safe status in a system. A safety instrumented system consist of a sensor, logic unit or control system and a final controlling element.

A typical example for the Rack:
A system made up of multiple overfill detection probes connected to a Rack monitor (sensor), a PLC to read the Rack status (control system) and a control valve (final controlling element).

2.1.2. Safety function

A defined function executed by a safety instrumented system with the objective of achieving or maintaining a safe state. The safe state takes a defined dangerous occurrence into account.

2.1.3. Dangerous undetected failure

Failure with the potential of causing a dangerous state in the safety instrumented system.
This document exclusively describes the RACK as part of a safety function.

2.1.4. Function with 2-wire overfill probes

For 2-wire systems, the RACK measures 8 input channels that all must be connected to a EN13922:2020 compliant 2-wire overfill probe, thermistor probes are **not** supported. When any of the 2-wire probes stop oscillating, or if the signal is out of spec, the RACK switches the permit relay (K1) and relay AUX1 (K2) to open. It's the responsibility of the plant manager to setup the relays K1 and K2 in a 1oo2 configuration.

2.1.5. Function with 5-wire overfill probes

For 5-wire systems, the RACK sends out a pulse and requires a return pulse from the 5-wire overfill probes according to the EN13922:2020. When the return pulse is missing, or the return pulse is out of spec, the RACK switches the permit relay (K1) and relay AUX1 (K2) to open. It's the responsibility of the plant manager to setup the relays K1 and K2 in a 1oo2 configuration.

2.2. Safety Integrity Level (SIL)

Four discrete Safety Integrity Levels (SIL) are defined in the IEC 61508:2010. The rating is given over the entire safety instrumented system. A higher SIL rating of the safety instrumented system means a higher probability the required safety function will be executed correctly.
The achievable SIL rating is determined by the following characteristics:

- Average probability of dangerous failure of a safety function in case of demand (PFD_{AVG})
- Hardware fault tolerance (HFT)
- Safe failure fraction (SFF)

Table 2.1 shows the relation between PFD_{AVG} and the SIL rating.

SIL	PFD_{AVG}
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Table 2.1 Safety Integrity levels

Table 2.2 shows the achievable SIL for the entire safety instrumented system for type B systems depending on the safe failure fraction (SFF) and the hardware fault tolerance (HFT). Type B systems contain complex components. For example a microcontroller. See IEC61508:2010 section 2.

SFF	HFT		
	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60% … 90%	SIL 1	SIL 2	SIL 3
90% … 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Table 2.2 Relation SFF and HFT for type B systems

3. Device specific safety instructions

3.1. Applications

The RACK specifies the requirements in terms of functional safety up to SIL 2 in accordance with IEC 61508:2010 and IEC 61511-1:2017. Please refer to Table 1.1 for the SIL rating of the specific device.

3.2. Safety function

The RACK is designed to detect a non-permissive state in optic 2- and 5-wire sensors as defined in the EN13922:2020. Permit relay (K1) and relay AUX1 (K2) and the Rack inputs are part of the safety functions. A dangerous undetected failure occurs when both K1 and K2 are closed while there is a non-permissive signal on the RACK input.

3.3. Installations

The RACK must be installed according to the H72611_X0 installation manual by qualified personnel. The permit relay (K1) and relay AUX1 (K2) must be wired in a 1oo2 fashion. For SIL 1 variants (refer to Table 1.1) it is allowed to wire K1 and K2 in series see Figure 3.1. However wiring both relays individually is recommended as in Figure 3.2. For SIL 2 variants K1 and K2 must be individually wired up to the safety PLC see Figure 3.2. The individual wiring of Figure 3.2 allows the safety PLC to see if either K1 or K2 is stuck in the closed or open position.
Both relays are normally open. They both close when loading of the truck is allowed. The safety PLC must be programmed to go to a safe situation when 1oo2 of the relays is open.

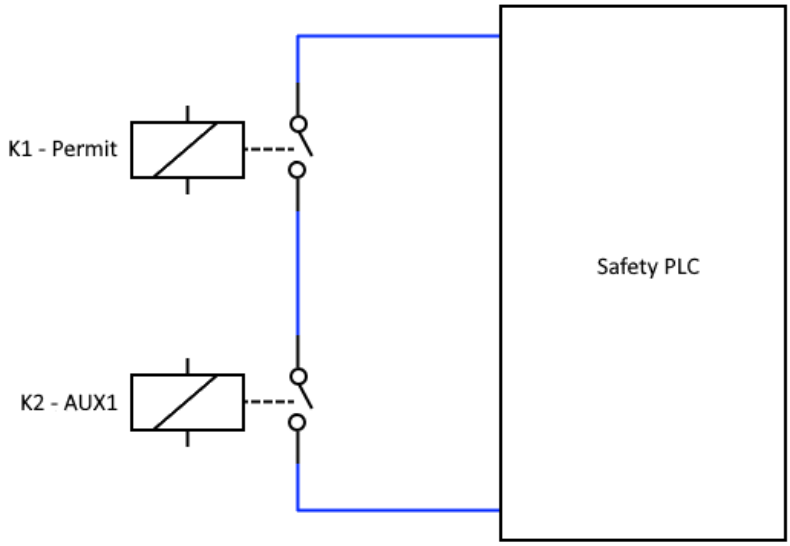

Figure 3.1 Relays K1 and K2 in series

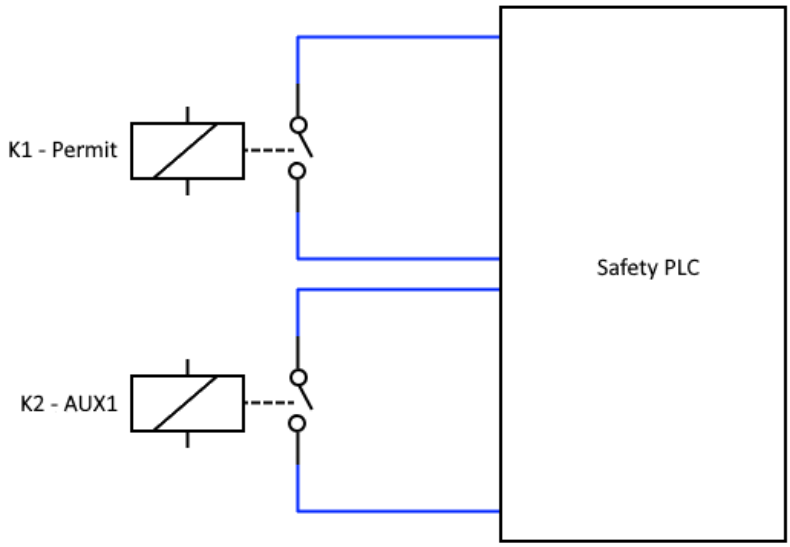

Figure 3.2 Relays K1 and K2 wired individually, required for SIL 2 systems recommended for SIL 1 systems

3.4. Behavior in case of faults

In case of a dangerous undetected failure the permit relay (K1) and relay AUX1 (K2) stay closed even though a non-permissive signal is present on the input. For all other failures at least one of the relays K1 and K2 is open when it should be closed or closed when it should be open.
In the case of power loss the fuses FH1 and FH2 should be checked and replaced if necessary.
In case a relay is always open FH3, FH4 and FH5 should be checked and replaced if necessary.
For other faults a new device or replacement kit is needed. Please contact OPW and mention the RACK model as engraved on the side.

3.5. Maintenance

Whenever the RACK is not connected to any sensors both relays, permit relay (K1) and relay AUX1 (K2), must be open. It's recommended to check this before and after every load. In addition to that It's recommended to check the safety function of the probe detection once every four years with testing equipment. The testing equipment must simulate a valid EN13922:2020 signal and go to non-permissive after a given interval. Permit relay (K1) and relay AUX1 (K2) must both open within 450 mS after the loss of the permissive signal. The useful lifetime of the device is 20 years.

3.6. Safety characteristics

The safety characteristics necessary for use of the system are listed in the SIL declaration of conformity (see Appendix A). These values apply under the following conditions:

- Both the permit relay (K1) and the AUX1 relay (K2) must be wired up. For SIL 2 the wiring given in Figure 3.2 must be used. For SIL 1 the wiring of Figure 3.1 is allowed.
- The safety PLC must be able to detect that the relays are stuck in the "closed" position.
- Overfill detection probes must comply to the EN13922:2020.
- For SIL 2, check Table 1.1 to validate if the RACK model is allowed to be used in SIL 2 systems.
- Temperature range: -40 °C … +70 °C (-40 °F … 158 °F)
- Installation of the RACK monitor must be done according to the H72611_X0 installation manual by qualified personnel.
- Voltage and current at relay contacts should not exceed 3 A @ 250 VAC or 5 A @ 30 VDC.

I. Certificate of compliance

Certificate of compliance

Rack Monitor

OPW Fluid Transfer Group Europe BV

Product identification	- 88xxx-xxxxx
Certification basis	- IEC 61508:2010, parts 1, 2 and 3 - IEC 61511:2017, part 1 - EN 13922:2020
Assessment basis	- FMEA studies - Feedback from the installed base and performed tests - Audit which confirms OPW's implemented management system
Condition	The output signal of sensors is pulsed (according EN 13922). The pulsed signal disappears if the sensor is wetted. Sensor failure leads as well to loss of the pulsed signal. The rack monitor detects disappearance of the pulsed signal and immediately switches over to non-permissive status by de-energizing relays.
Safety integrity	Type 88xxx-xxxxx **SIL 1** Type 88xxx-xxSxx **SIL 2** *The S means: with secondary rack*
Reference documents	doc. 21040-2 SIL assessment report doc. H72790 Rack Safety Manual for 88XX rack series
Certificate number	21040B
Issue date	7 September 2022
Expire date	7 September 2027

Herman Jansen
TÜV certified FS expert

Page 1 of 2

www.consiltant.com