

Table 2-1: Valid MPC4 card processing modes for safety-related systems

Processing mode	Reference in VM600 MPS hardware manual
(BBAB) Broad-band absolute bearing vibration	Section 7.2
(RS) Shaft relative vibration with gap monitoring	Section 7.4
(AS) Shaft absolute vibration	Section 7.5
(PS) Position measurement	Section 7.6
(DMF) Dual mathematical function	Section 7.17

Refer to the *VM600 machinery protection system (standard version) hardware manual* for a complete list of all processing modes supported by the MPC4 (see 1.5 Related documentation).

2.3 Safety inputs and outputs

Table 2-2: Overview of valid safety inputs and outputs

Signal	Comments	Reference in VM600 MPS hardware manual
MPC4 channel 1 to channel 4 (inputs)	Ensure cabling follows the guidelines	Table 9-1 (part 1 of 3)
MPC4 relay contacts (outputs)		Table 9-1 (part 2 of 3)
RLC16 relay contacts (outputs)		Figure 11-1

NOTE: Speed/phase reference (tachometer) processing can be performed but the processing results must not be used for any safety-relevant functionality, as the speed/phase reference inputs are not safety inputs.

NOTE: The speed/phase reference (tachometer) buffered (TTL) outputs from the MPC4 card and the VM600 rack's Tacho Bus must not be used to feed safety-relevant signals to other safety-relevant equipment, including other VM600 cards, as these are not safety outputs.

NOTE: The buffered (raw) outputs from the MPC4 card and the IOC4T card must not be used to feed safety-relevant signals to other safety-relevant equipment, including other VM600 cards, as these are not safety outputs.

2.4 Safety function

With reference to IEC 61508, the safety function for a VM600-rack based system is defined in Table 2-3.

Table 2-3: Definition of the safety function for a VM600 MPS

SF number	Description	Safe state	Required safety parameters
SF1	If an input value (or values) exceed(s) a predefined limit, then a trip activation signal is made.	De-energise to trip (open relay contact). That is, the EUC and the VM600 interpret a de-energised state as a safe state.	See Table 2-4

For the required safety function SF1, the safety parameters (SP) listed in Table 2-4 are required in accordance with IEC 61508.

Table 2-4: Safety parameters

SP number	Safety parameter	Requirement	Comment					
SP1	Safety integrity level	SIL 1						
SP2	Operational mode	Low demand mode						
SP3a	Component type sensor	Type B						
	Component type logic (measuring logic)	Type B						
	Component type actuator (relay)	Type A						
SP4	Hardware fault tolerance (HFT)	0	Single channel architecture of an already existing proven-in-use system should be used for SIL 1 application without any changes					
SP5	Average probability of failure on demand (PFDavg)	$\geq 10^{-2}$ to 10^{-1}	PFDavg by proof test years FMEDA					
			<table border="1"> <tr> <td>PT=0.5a</td> <td>PT=1a</td> <td>PT=2a</td> <td>PT=5a</td> </tr> <tr> <td>2.81e-3</td> <td>5.60e-3</td> <td>1.12e-2</td> <td>2.79e-2</td> </tr> </table>	PT=0.5a	PT=1a	PT=2a	PT=5a	2.81e-3
PT=0.5a	PT=1a	PT=2a	PT=5a					
2.81e-3	5.60e-3	1.12e-2	2.79e-2					
SP6	Safe failure fraction (SFF) for Type A subsystem	< 60% for SIL 1 and HFT 0						
	Safe failure fraction (SFF) for Type B subsystem	60% to < 90% for SIL 1 and HFT 0						

In practice, the output relay or relays are normally an 'input' to a safety-related PLC that takes this input together with other safety-related signals.

2.5 ISO 13849-1 performance level

Table 2-5 shows the breakdown of performance level (PL) by diagnostic coverage and mean time to dangerous failure (MTTFd).

Table 2-5: Determination of the performance level according to DIN EN ISO 13849-1

DC / MTTFd	Without	Without	Low	Medium	Low	Medium	High
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

Table 2-6 shows the calculated results for the VM600 MPS.

Table 2-6: ISO 13849 performance level achieved

Component	MTTFd (years)	MTTFd Category	Postulated DC for PL c	DC according to FMEDA	PL
VM600 MPS	118	High	< 60 %	35.64 %	c

2.6 Safety time

After the defined safety level threshold has been exceeded, a VM600-rack based system will open the associated safety relay within 100 ms.

2.7 Protection of relay contacts



IN A SAFETY-RELATED SYSTEM IT IS IMPORTANT TO PROTECT AGAINST A RELAY CONTACT BECOMING WELDED DUE TO EXCESSIVE CURRENT BEING INADVERTENTLY PASSED. THEREFORE, THE OUTPUTS MUST BE PROTECTED BY A 5A (T) FUSE.

NOTE: A type T fuse is a "timed" or slow-blow fuse, designed to allow a current which is above the rated value of the fuse to flow for a short period of time without the fuse blowing.

2.8 Installation

A VM600-rack based system must be installed following the procedures described in the *VM600 machinery protection system (standard version) hardware manual* (see 1.5 Related documentation).

Environmental restrictions are described in Appendix A of the hardware manual.

2.9 Configuring the system



IT IS IMPORTANT THAT THE LEVELS (VIBRATION AND SO ON) ARE ADJUSTED TO SUIT THE SYSTEM UNDER PROTECTION AND THAT A MANUAL VERIFICATION IS MADE OF THE PARAMETERS THAT ARE UPLOADED TO A VM600-RACK BASED SYSTEM (MPC4 CARD).

NOTE: The procedures described should only be performed by competent and authorised personnel following the plant specific guidelines in force at the installation site.

2.9.1 Define the levels

The choice of alarm levels must be made in consultation with the site manager. It is the end user's responsibility to ensure that the alarm levels are appropriate for the particular system being protected.

The levels are defined using either the VM600 MPS1 software (supplied) or the VM600 MPS2 software (optional). Refer to the appropriate documentation for complete information.

NOTE: Refer to a *VM600 MPSx configuration software for machinery protection systems software manual* for further information (see 1.5 Related documentation).

2.9.2 Define the alarm outputs

Any relay on the MPC4 or RLC16 cards can be configured to provide the safety function. As previously noted in 2.1 VM600 in a safety-related system, for a safety relay corresponding to an alarm, the alarms and relays must be configured depending on the role of the VM600 in the safety loop.

- If a safety function is performed by a VM600-rack based system only, any safety relay corresponding to an alarm must be configured as latching and normally energised (de-energised to trip).
- If a safety function is performed by an external system using an alarm detected by a VM600-rack based system as an input, the relay corresponding to this alarm may not be configured as latching.

However, an analysis must be carried out at the safety-related system level to ensure that no alarm can be missed or to identify all possible impacts and acceptability of residual risks in case of a missed alarm.

- If a safety function uses a VM600-rack based system alarm that is configured as latching, the use of an alarm delay time is not allowed. That is, the alarm delay time (**Delay**) for the alarm must be configured as zero (**0.0**).

2.9.3 Upload the levels and configuration

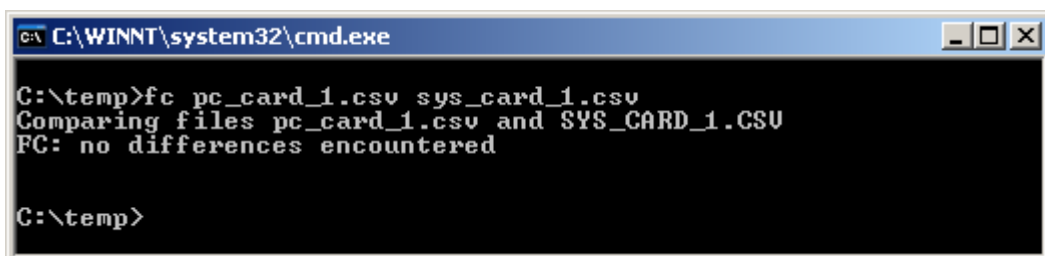
Once the system parameters have been correctly defined using the VM600 MPSx software, the configuration for each MPC4 card must be uploaded to the card. This procedure is described in the *VM600 MPS1 configuration software for machinery protection systems software manual* (see 1.5 Related documentation).

2.9.4 Configuration verification

Whilst the actual upload of data is controlled by CRC verification and other techniques, a manual verification of this upload is required in order to fulfill the IEC 61508 requirements. The verification is made by downloading the configuration from the MPC4 card to the computer and comparing the data received with the original data uploaded to the card.

To verify an upload:

- 1- Select the appropriate MPC4 card with the VM600 MPSx software (as used in 2.9.3 Upload the levels and configuration).
- 2- Use the **Dump to File** option to save the configuration as *pc_card_1.csv*.
- 3- Define a dummy rack using a Tag name *from_sys_1*.
- 4- Select this rack, connect to the MPC4 card concerned and read its configuration back to the computer.
- 5- Dump this file as *sys_card_1.csv*.
- 6- Use the MS-DOS `fc` (file compare) command to compare the two files, as shown in Figure 2-1.



```
C:\WINNT\system32\cmd.exe
C:\temp>fc pc_card_1.csv sys_card_1.csv
Comparing files pc_card_1.csv and SYS_CARD_1.CSV
FC: no differences encountered
C:\temp>
```

Figure 2-1 : MS-DOS `fc` command screen shot

NOTE: If any differences exist, then the upload must be repeated and the comparison repeated.
