FAQ for KEB Safety related devices

Content

Purpose of this document .................................................................................................................. 3

1. Generals ....................................................................................................................................... 3
   1.1. Official documents ................................................................................................................. 3
   1.2. Why don’t have the KEB devices any safe feedback contacts? ........................................... 3
   1.3. Diagnosis for the safety related mechanical brakes .............................................................. 3

2. KEB Devices with STO Function .................................................................................................. 4
   2.1. The drive runs into STO sometimes while operation .............................................................. 4
   2.2. The safety controller reports errors when testing an output ................................................. 4

3. Safety module 1 in F6-A, S6-A, H6 ......................................................................................... 5
   3.1. Functionality SBC – Description of the function of the monitoring of the brake supply current ....................................................................................................................... 5
   3.2. Function SBC – Switching of brake by intermediate relay ..................................................... 6

4. Safety module 2 and 3 in F6-A, S6-A, H6: ............................................................................. 6
   4.1. User configuration, user access, login ................................................................................... 6
   4.1.1. What happens if a wrong user or a wrong password is entered? ..................................... 6
   4.1.2. The user Login data are not known or got lost. ................................................................. 7
   4.1.3. Which data can be seen or changed without User access? .............................................. 7
   4.2. Technical characteristics ....................................................................................................... 7
   4.2.1. How does the safety module behave in the event of a power supply failure? ...... 7
   4.2.2. How sensitive is voltage monitoring? ............................................................................. 8

4.3. Connection, Wiring .................................................................................................................... 8
   4.3.1. Function SBC – Switching of brake by intermediate relay ................................................ 8
   4.3.2. How many safe inputs can be connected to the clock outputs at the same time? .... 9
   4.3.3. Using of the safety module like a safe I/O module ............................................................ 9
   4.3.4. Is it possible to switch the 2-channel safe inputs via two different ways? .............. 9
   4.3.5. Why has the Ripple-Output inverse logic to the Outputs 1 and 2? .............................. 10

4.4. Safety functions, software functions .......................................................................................... 10
   4.4.1. Interruption of a function while running (e.g. SS1) ........................................................... 10
   4.4.2. Can I delete the log files? ................................................................................................ 10
4.4.3. Does the CRC checksum change when a limit is written cyclically over FSoE? .10
4.4.4. Which safety function has triggered the failure? ...........................................11
4.4.5. With which configuration is the safety module delivered? How can you simply
turn the engine during startup of the machine? ......................................................12
4.4.6. Coupling of SBC and STO .................................................................12
4.5. The function is not like expected .................................................................13
4.5.1. The configuration of the terminals are correct, but no function is released ....13
Disclaimer...........................................................................................................14
Purpose of this document

These statements provide information and explanations on frequently asked questions about the safety-related components of KEB Automation KG. This document is not legally part of the certified device documentation. The functions described in the current KEB documentation must always be given priority. If you have any questions, please contact KEB Automation KG or your area representative.

1. Generals

1.1. Official documents
- The corresponding standards which are listed in the respective product documentation.
- In the SISTEMA Cookbook several samples are offered: http://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/sistema-kochbuecher/index.jsp

1.2. Why don`t have the KEB devices any safe feedback contacts?
The KEB devices with safety functions according to EN 61800-5-2 have no or "not safe" feedback contacts.
The feedback contacts, which are required for safe relay circuits via positively driven contacts in accordance with ISO 13849-1 Cat 3, have the task of detecting "sticky" contacts and thus achieving the required diagnostic coverage via an evaluation unit
Without this diagnostic possibility you will not know if both or only one channel is still switching. If only one channel is working the category 3 will not be respected and the risk of a complete failure of the switching is increasing strongly.
The safety functions implemented in the KEB devices have either Cat 4 (several failures do not lead to dangerous failure) and diagnostic coverage "high" (> 99%), or Cat 3, diagnostic coverage "medium" (=> 90% <99%) and an internal check if both channels are working safely. Thereby a feedback and external monitoring is not required.

1.3. Diagnosis for the safety related mechanical brakes
Mechanical safety brakes must be regularly checked for function depending on the category to be achieved.
With mechanical brakes, the braking or holding torque can be reduced due to wear. Likewise, brake torque generating components may break (e.g., the springs, lining, or torque support).
The safety function SBC-Safe Brake Control provided by KEB can only ensure that the brake voltage is switched off. With a zero current-operated brake, it is assumed that the braking torque is generated if the function is correct. The SBC function cannot check the function of the brake.
Within limits, the current monitoring at the brake output of the drive can only detect whether the brake is connected or the brake coil has a short circuit. In both cases, however, normally the safe state (vertical axis / brake closed) would be maintained. In which interval and how the brake has to be tested depends on the application. Unfortunately, there is no universally valid, defined specification. Some machine standards go into it. The use and the diagnosis of safety-oriented brakes is concerned with e.g. the IFA Report 07/2013 Chap. 6.4.3 and Appendix C

2. KEB Devices with STO Function

2.1. The drive runs into STO sometimes while operation

In many safety controls the transistor outputs must be checked regularly. That means the signal is interrupted cyclically for short time and it will be observed if the voltage drops (i.e. the switching transistors are working well) (OSSD-signals).

In the COMBIVERT F5, F6-K, S6-K and G6 the voltage at the STO connection is buffered by internal capacitors. The duration of the buffer depends on the capacitance of the capacitors, the signal voltage and whether the inverter modulates or not. Details can be found in the operating instructions.

If the signals are missing for longer than the filters are running or the voltage can be buffered, the drive briefly goes into STO state. When the signal is back, the inverter will leave STO again automatically. Depending on the setting, the inverter then behaves as after normal setting of the controller release (e.g. speed search, rotor position calibration, start of the ACC ramp at 0, etc.). For some controllers, the length of the test pulses can be set.

One solution is to put relays in between, which keep their condition due to their inertia.

2.2. The safety controller reports errors when testing an output

In many safety controls the transistor outputs must be checked regularly. That means the signal is interrupted cyclically for short time and it will be observed if the voltage drops (i.e. the switching transistors are working well) (OSSD-signals).

In the COMBIVERT F5, F6-K, S6-K and G6 the voltage at the STO connection is buffered by internal capacitors. The duration of the buffer depends on the capacitance of the capacitors, the signal voltage and whether the inverter modulates or not. Details can be found in the operating instructions.

The voltage on the signal line drops so delayed. The control detects this and concludes that the transistor cannot switch off the voltage, which would be a dangerous condition. As a solution, decoupling diodes between the control output and the STO input can be used.

For some controllers, the OSSD signals can also be adjusted.
3. Safety module 1 in F6-A, S6-A, H6

3.1. Functionality SBC – Description of the function of the monitoring of the brake supply current

The safety module monitors the current of the brake supply voltage. It is not safety related but can be used for service and protection of the brake. Monitoring is carried out only with the release of the voltage. The current monitoring can be switched off with parameter co82: “sm-cs = 0 / off” in the drive parameters. After the change, a power OFF – ON of the 24V supply of the drive must be made.

Monitoring of maximum current:
If approx. 4A current is exceeded, the safety module goes into fault and the drive shows in parameter ru01: 55 = error safety module. The fault can only be reset by power OFF - ON of the 24V supply of the drive and acknowledgment in the drive.

Monitoring of minimal current:
This can be used to monitor whether a brake is connected at all. Even a cable break can be detected.

If the current falls below a certain value (~ <100mA), however, no error is triggered. The minimal current can only be measured inaccurately because of the strong oversizing of the switching transistor. Therefore, there is no direct error message "Minimum current under-shot".

In drive parameter Sb29 (2F1Dh), bit 8 (or bit 22 in the case of a double-axis module) displays a warning message if too low current is detected (it is always "on" if the current measurement was switched off: co82 = 0).

Bit 8 can be evaluated in a PLC. The update cycle is 1ms to 80ms. In addition, the drive can be brought into error state when the minimum current is undershot via the "programmable error" function. To do this, set the condition in parameter pn30 = "256: no brake" and the error reaction in pn29 "0: fault".

The detection of whether a brake is connected (I = 0A) can only be carried out when a voltage is switched to the brake.

The minimum current monitoring does not work directly on the digital output SBC (terminal X2B, 19/20) on the safety module. The output is "on" if both SBC inputs are supplied with voltage and the brake bit 15 of the control word is set and the status "no SM errors" is present.

For further information see instructions for use Safety Module 1 No. 20109577.
3.2. Function SBC – Switching of brake by intermediate relay

If the brake current is more than 2A (or 3.3A at double axis module) or the voltage of the brake not 24V is, an intermediate relay has to be used. This relay is part of the safety chain and must be integrated as a safety component.

Please note:
If the current of the relay is lower than ca. 100mA, the brake current monitoring has to be switched off by parameter co82.

![Intermediate Relay Diagram]

The relay must never connect the "Br-" terminal to ground (e.g. electronic relay, external current monitoring or freewheeling circuit). The grounding would interrupt the internal cyclic test of the brake switching transistors and the module would go into fault state. Internal brake transistor test: in order to ensure the switching capability of the 2 (or 3 at double axis module) brake transistors, they will be switched cyclically and the switching state will be monitored (e.g. voltage drop at switching off). The test length is typically 10ms. The test cycle period is about 48min. This time will be shared to 4 different tests running one after the other every 12min. So can happen, that the drive opens the brake and after time x the safety module error occurs. That indicates that the brake test is failed.

Reason for failed test:
- Br- terminal connected to ground (Parameter Sb29 shows “Bit 11 Low-side-switch high-resistance” or “Bit 12 Low-side-switch short-cut”).

The parameter Sb29 is shown in the drive parameters and also in safety module editor state (from COMBIVIS version 6.4.0). The description can be found in the manual of the safety module.

4. Safety module 2 and 3 in F6-A, S6-A, H6:

4.1. User configuration, user access, login

4.1.1. What happens if a wrong user or a wrong password is entered?

The password or the user can be entered 3-times a wrong value. At fourth entering of wrong value the safety module goes to error state and locks for 5min. In the log file a notice will be shown. After the waiting time a new trial can be worked out.
4.1.2. The user Login data are not known or got lost.
Lost access data cannot be reconstructed by KEB! The module can be reset to the factory settings. For this, contact the KEB Service! The configuration settings will be lost at this procedure!

4.1.3. Which data can be seen or changed without User access?
Without user access the following data are shown:
- Status messages like input state or output state, error messages, current speed or position values
- Module-time of day
- Log-Files (error storage or status storage)
- Firmware version

Following values can be changed without user access:
- The time of day can be changed once after Power-On
- Blinking on/off

4.2. Technical characteristics

4.2.1. How does the safety module behave in the event of a power supply failure?
The safety module doesn’t detect a fault of the dc-link voltage. If the 24V supply is still present with external supply and if necessary UPS (and the encoder also receives voltage), all functions are executed anymore. E.G.: The function SS1 will be monitoring the encoder speed furthermore and if the drive doesn’t follow the DEC-ramp STO will be triggered.
In F6 or S6 an external 24V supply is needed. At H6 the 24V supply unit can be supplied by the DC-link rail. If the 24V supply fails, all outputs are switched off when 20.4 Vdc is exceeded and the status of the inputs is set to 0. By this STO and SBC are triggered. After a time, the processors will no longer have any voltage. How long the CC can supply the 24V bus depends on the power consumers and, if necessary, regenerative operation in the system. It must also be noted how an external safety controller behaves and possibly switches safety functions on its own.
4.2.2. How sensitive is voltage monitoring?
The safety module monitors the supply voltage. The tolerance window of the Power supply to the drive control board is 24V + -5% (see Installation Instructions). The tolerance on the safety module is 24V + -10%. Because of the polarity reversal protection circuit reduces the actual voltage at the safety module and the supply voltage for the brake also is typically - + 10%, the tolerance at the 24V input must be smaller. The limit values for the voltage check in the safety module are 24Vdc -15% + 20%, the measuring cycle is 0.5 ms, whereby the filter is 2 ms. If this value is exceeded or undershot, the module goes into the error state.

4.3. Connection, Wiring

4.3.1. Function SBC – Switching of brake by intermediate relay
If the brake current is more than 2A (or 3.3A at double axis module) or the voltage of the brake not 24V is, an intermediate relay has to be used. This relay is part of the safety chain and must be integrated as a safety component.
Please note:
If the current of the relay is lower than ca. 100mA, the brake current monitoring has to be switched off by parameter “Measurement of the brake current” in the group “SBC: brake control”.

The relay must never connect the "Br-" terminal to ground (e.g. electronic relay, external current monitoring or freewheeling circuit). The grounding would interrupt the internal cyclic test of the brake switching transistors and the module would go into fault state. Internal brake transistor test: in order to ensure the switching capability of the 2 (or 3 at double axis module) brake transistors, they will be switched cyclically and the switching state will be monitored (e.g. voltage drop at switching off). The test length is typically 10ms. The test cycle period is about 48min. This time will be shared to 4 different tests running one after the other every 12min. So can happen, that the drive opens the brake and after time x the safety module error occurs. That indicates that the brake test is failed.
Reason for failed test:
- Br- terminal connected to ground (Error message shows “Low-side-switch high-resistance” or “Low-side-switch short-cut”).
4.3.2. How many safe inputs can be connected to the clock outputs at the same time?

The clock output delivers per channel maximum 100mA. According to the specification, the safety inputs should take not more than 15mA. The real current consumption of the safe inputs of Module 2 or 3 is not more than 7mA. Thus up to 13 safe inputs can be connected to a clock output at the same time.

4.3.3. Using of the safety module like a safe I/O module

With the corresponding device description file, which contains the status of the inputs and outputs, the status of the safe inputs and outputs can be evaluated or switched directly via FSoE by the safe PLC. Often this can be used to save an additional COMBICONTROL Safe I/O module.

Compared to the safe KEB I/O modules, it should be noted that the two input channels on the safety module are not independent, but must always be switched simultaneously. The safety characteristic values also apply to this usage. For the inputs STO, SBC, F1 and F2, the clock signals can be used.

4.3.4. Is it possible to switch the 2-channel safe inputs via two different ways?

Sample: both channels of the STO input may be enabled by two different ways, one channel by door contact and the other by safe control.

In safety module 2 and 3, monitoring takes place whether both signals of the two channels switch simultaneously. A tolerance of maximal 1sec (SM2: 0.1s) can be adjusted. That means if one channel is switching the other must be switched in the tolerance time, otherwise the safety module triggers an error and will be locked in safe state. This error can only be disabled by Power-On–Reset of the drive controller.
For KEB devices that only have the STO function, such as F5, G6, S6-K or F6-K, the simultaneity is not monitored and the sample constellation could be used. Using of the KEB safety control and the safe I/O modules would be also a solution, because the signals of each channel are merged only in the SPLC.

4.3.5. **Why has the Ripple-Output inverse logic to the Outputs 1 and 2?**

An essential safety principle is that the safe state must be achieved if the cable breaks. Depending on the switched function, this can be achieved with the reverse switching logic.

Sample:
If the OUT 1 operates on the function Safe Speed Monitored, the Out 1 is on 24V when the safe low speed is detected. (Cable break principle 0V = unsafe condition).
The ripple-out would have 0V. So the ripple-out cannot be used for that.
But if, for example, the state STO is to be enabled from one module to another module or to a "normal" drive controller with STO input, the output must be 0V. At 24V on the ripple-out the 2nd drive will be in state “not STO”, means in release. (Safe Torque Off (= modulation off) is active on the terminals at 0V).

4.4. **Safety functions, software functions**

4.4.1. ** Interruption of a function while running (e.g. SS1)**
The safety functions can be interrupted at any time by supplying voltage to the input or setting of the control word. This will shut off the monitoring immediately.
Example: The SS1 function runs into the STO function after deceleration to standstill. If you interrupt SS1 in the middle of the ramp (24V returns to the input), the monitoring stops immediately and the drive can accelerate again or continue driving constantly.

4.4.2. **Can I delete the log files?**
The last 20 log files of each category are stored non-volatile in the safety module. They cannot be deleted.

4.4.3. **Does the CRC checksum change when a limit is written cyclically over FSoE?**
The CRC checksum of the configuration must be matching to the checksum stored in the Safe FSoE PLC. Thus an intermediately changed configuration in the drive can be detected by the PLC.
The CRC checksum is calculated at configuration download. Changing of limits later (e.g., SLS Upper Limit) over FSoE will not change the configuration and will not affect the CRC checksum. After power-on the module is loading the original value from the configuration.

**4.4.4. Which safety function has triggered the failure?**

If a safety function has detected that a limit value has been violated, the safety module enters the "Safety function error". How can be recognized which function triggered the error? The safety editor contains the status message "Activated safety function": The active safety functions are listed there. The order does not matter! Unfortunately, it is not easily to recognize which function triggered the error. STO can be left outside and SMS is always on. So in this example, SLS or SMS triggered the error:

```
Status | Settings | Safe parameterization | Log

Global safety state: 263330: Safety application enabled
Startup finished
Bus state: Data
Index 1: Configuration OK

Bus safety function state: Invalid address

Activated safety function: 131844: STO + Brake open + SLS + Fail safe + SMS

Error state: No Error
Last error / warning: No Error
Bus error: No Error
UO status: Input channel 1: STO.1 + SBC.1
Input channel 2: STO.2 + SBC.2
Output channel 1: Brake Out + Ripple Out1.
Output channel 2: Brake Out + Ripple Out2
Encoder speed: 0.0000 L/min
Encoder position (revolutions): 1168457
Inverter position: 76576
```

Please disable the safety function by switching on the input. The safety function, which does not leave from the status display, has triggered the error. If there is only SMS, it was SMS. Note: the error must not have been acknowledged, the module must not have been switched off.

Please do not try to supply the 24V by cable bridges or with a separate cable. That would be a manipulation of the safety function and would require at least a check of the wiring before the machine is restarted.
4.4.5. With which configuration is the safety module delivered? How can you simply turn the engine during startup of the machine?

When delivered, there is no configuration in the safety module. Means, the drive is not ready to run. At least one user must be created and one configuration must be loaded into the module. A basic function can be achieved by loading the default configuration. Thus, the digital inputs STO and SBC are active and the drive can be moved under the required safety precautions by connecting STO and (if a brake is connected) SBC. Encoder and FSoE are not evaluated.

4.4.6. Coupling of SBC and STO

If both functions STO and SBC shall be enabled simultaneously, by parameter “Coupling of SBC and STO” the SBC function can be linked to the function STO.

This means that when activating STO SBC is triggered with. Conversely, activating SBC does not include STO. For SM3, no input SBC may or must be assigned. In SM2, the fixed SBC input can be bridged with the clock output depending on the application.
4.5. The function is not like expected

4.5.1. The configuration of the terminals are correct, but no function is released

If the inputs are wired correctly and the configuration assigns the correct functions to the inputs, but no safety function releases, check whether bus operation is switched off. If the bus type is released to “FSoE” the safety module expects an enabling by safety bus control word. The terminals and the bus control word are ordered in line. Only if the bus type is set to “No bus” the module reacts on the terminals exclusively.

<table>
<thead>
<tr>
<th>Parameter group:</th>
<th>Bus general options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type:</td>
<td>Safety Module Type 3</td>
</tr>
<tr>
<td>Description:</td>
<td>Parameterversion: 3.1.0.0.</td>
</tr>
<tr>
<td>Device CRC:</td>
<td>0x3C5EFCB48B</td>
</tr>
<tr>
<td>Import date:</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus type</td>
<td>No bus</td>
</tr>
<tr>
<td>Safety address</td>
<td>10</td>
</tr>
<tr>
<td>Control and status word length</td>
<td>11</td>
</tr>
</tbody>
</table>
Disclaimer

KEB Automation KG reserves the right to change/adapt specifications and technical data without prior notification. The safety and warning reference specified in this manual is not exhaustive. Although the manual and the information contained in it is made with care, KEB does not accept responsibility for misprint or other errors or resulting damages. The marks and product names are trademarks or registered trademarks of the respective title owners.

The information contained in the technical documentation, as well as any user-specific advice in verbal or in written form is made to the best of our knowledge and information about the application. However, they are considered for information only without responsibility. This also applies to any violation of industrial property rights of a third-party.

Inspection of our units in view of their suitability for the intended use must be done generally by the user. Inspections are particular necessary, if changes are executed, which serve for the further development or adaption of our products to the applications (hardware, software or download lists). Inspections must be repeated completely, even if only parts of hardware, software or download lists are modified.

Application and use of our units in the target products is outside of our control and therefore lies exclusively in the area of responsibility of the user.

KEB Automation KG
Südstraße 38 • D-32683 Barntrup
fon: +49 5263 401-0 • fax: +49 5263 401-116
net: www.keb.de • mail: info@keb.de