What safety level can be reached when combining a contactor with a circuit-breaker for fail-safe switching?

SIRIUS Safety Integrated

What safety level can be reached when combining a contactor with a circuit-breaker for fail-safe switching?

Entry-ID: 40349715, V3.1, 06/2018
1 Explanation

Question
What safety level can be reached when combining a contactor with a circuit-breaker for fail-safe switching?

Answer
Since circuit-breakers do not offer any diagnostic functions, i.e. mirror contacts, they cannot be used as a second functional channel in a safety function. Additionally it would be impractical to trip the circuit-breaker with every fail-safe switching, since it needs to reset manually.

However, it is possible to use a circuit-breaker as an "output of the test equipment". In combination with a power contactor this conforms to Cat. 2 according to ISO 13849-1 und thus the safety function can reach up to PL d. According to IEC 62061 a hardware fault tolerance (HFT) of 0 can be assumed und thus the safety function can reach up to SILCL 2.

Cat. 2 is fulfilled by monitoring the power contactor by a safety evaluation unit and executing a fault reaction within sufficient time in case the power contactors fails (welding of the contacts). In case of a hardware failure, the circuit-breaker is tripped by the means of an undervoltage release.

The architecture is thus a single-channel architecture with a specified fault reaction. In addition, the power contactor and the circuit-breaker are well-tryed components in accordance with ISO 13849-2.

The diagnostic coverage (DC) can be assumed to be 90 %-99 %.

Reason
Due to the mirror contacts of the power contactor, its diagnostics capability can be assumed to be 99 %.

Now it has to be considered that this diagnostics capability alone can trigger or even prevent the fault reaction.

It is absolutely necessary that this fact be taken into account.

An additional worst case consideration should thus be made by reducing the diagnostic coverage from originally 99 % to 90 % and increasing the associated dangerous failure rate accordingly.

Table E.1 of ISO 13849-1 lists additional measures that recommend the use of a 90 % diagnostic coverage.

The failure rate of the power contactor is calculated based on the operating cycles. As an example, it is assumed that the safety function is demanded once per week (or 52 times per year). In a worst case consideration, the same demand mode is assumed for the circuit-breaker.
What safety level can be reached when combining a contactor with a circuit-breaker for fail-safe switching?

1 Explanation

NOTE

In some cases a circuit breaker can have a specific diagnosis level. Necessary for a diagnosis is a dynamic monitoring of the circuit breaker during safety and normal switching. This is possible with an F-PLC and a remote control unit to switch on the circuit breaker remotely.

Details are described in this FAQ: https://support.industry.siemens.com/cs/de/de/view/109483115/en

In that case a higher safety level can be reached.

DANGER

To avoid an undetected accumulation of faults, the circuit-breaker must be tested after 6-12 months at the latest.

This test set-up has to be documented in the description of the safety function and in the operating instructions (of the machine).

The tests performed must also be verifiably documented by the user during the phase of use.

The set time delay influences the maximum reaction time. It must be ensured that, based on the risk assessment, this reaction time is sufficiently short in the event of a fault.

Why can Category 2 according to ISO 13849-1 be used?

In accordance with the simplified procedure of ISO 13849-1, Category 2 is a single-channel tested system: If a dangerous fault occurs, the fault detection is only effective if the test detecting the fault takes place before the next demand of the safety function. Against this background, a test rate is required that is 100 times greater than the demand mode of the safety function.

An alternative realization of effective fault detection is not explicitly specified in ISO 13849-1, but also possible.

The following relevant information is provided in IEC 62061, 6.3.2:

"Where a diagnostic function(s) is necessary to achieve the required probability of dangerous random hardware failure and the subsystem has a hardware fault tolerance of zero, then the fault detection and specified fault reaction shall be performed before the hazardous situation addressed by the SRCF can occur."

This means: If, after a dangerous fault has occurred, the fault detection and the specified fault reaction can initiate a safe state before a hazardous situation can occur, the requirement of Category 2 is basically met.
Why is an evaluation with Category 3 according to ISO 13849-1 inadvisable?

Category 3 is characterized by a two-channel architecture. Both channels have to be considered independently of one another. In this case, this independence is not given.
2 Hardware components

As an example, the following industrial switchgear and switchgear and protective gear for power distribution can be used:

The safety values in the table are just example values.
The actual valid safety data for each product can be found in the data sheet of the product, or additional for SIRIUS products on the web page:

https://support.industry.siemens.com/cs/de/en/view/109739348

The conditions for used for each product must be followed.

Table 2-1

<table>
<thead>
<tr>
<th>Designation – Type</th>
<th>B10 value</th>
<th>Lifetime T1</th>
<th>Dangerous failure ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIRIUS Power contactors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3RT10/ 3RT20/ 3RT50/ 3RT60</td>
<td>1,000,000</td>
<td>20 Years</td>
<td>73 %</td>
</tr>
<tr>
<td>3TF6</td>
<td>1,000,000</td>
<td>20 Years</td>
<td>73 %</td>
</tr>
<tr>
<td>3TF2</td>
<td>400,000</td>
<td>20 Years</td>
<td>73 %</td>
</tr>
<tr>
<td>SIRIUS Circuit-breakers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3RV ( up to 100A)</td>
<td>5,000</td>
<td>10 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>With undervoltage release</td>
<td>3RV1902-1A, 3RV2902-1A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SENTRON 3VL Circuit-breaker</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3VL1... - 3VL4</td>
<td>10,000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>3VL5...</td>
<td>5,000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>3VL6...</td>
<td>3,000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>3VL7... - 3VL8...</td>
<td>1,500</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>With undervoltage release</td>
<td>3VL9400-1U.00, 3VL9800-1U.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SENTRON 3VA Circuit-breaker</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3VA10/11/12 up to 250 A</td>
<td>8,000</td>
<td>20 Years</td>
<td>100%</td>
</tr>
<tr>
<td>3VA20/21 up to 160 A</td>
<td>12,000</td>
<td>20 Years</td>
<td>100%</td>
</tr>
<tr>
<td>3VA22 up to 250 A</td>
<td>10,000</td>
<td>20 Years</td>
<td>100%</td>
</tr>
<tr>
<td>3VA23 up to 400 A</td>
<td>6,000</td>
<td>20 Years</td>
<td>100%</td>
</tr>
<tr>
<td>3VA24 up to 630 A</td>
<td>4,000</td>
<td>20 Years</td>
<td>100%</td>
</tr>
<tr>
<td>With undervoltage release</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2 Hardware components

<table>
<thead>
<tr>
<th>Designation – Type</th>
<th>B10 value</th>
<th>Lifetime T1</th>
<th>Dangerous failure ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>SENTRON 3WL Air-Circuit-breaker</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3WL Size I</td>
<td>20.000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>3WL Size II up to 2500 A</td>
<td>15.000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>3WL Size II up to 3200 A</td>
<td>15.000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>3WL Size II up to 4000 A</td>
<td>10.000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
<tr>
<td>3WL Size III up to 6300 A</td>
<td>10.000</td>
<td>20 Years</td>
<td>50 %</td>
</tr>
</tbody>
</table>

NOTE
The SIRIUS contactor with size S6-S12 (3RT1...-S...) with failsafe PLC input can also be used. With this contactor a SILCL2 or PLc can be reached without the use of a circuit breaker. The contactor is certified up to this safety level. If a circuit breaker is used as output of the test equipment, as mentioned in this FAQ, a SILCL 2 or PLd can be reached. This is also a categorie 2 system.
3 Calculation

3.1 ISO 13849-1

For architectures of Cat. 2, the calculations of the MTTF\(_d\) and DC\(_{avg}\) only include the functional channel and not the testing channel. Thus the circuit-breaker has no influence on the evaluation of the safety function.

However, it is evaluated if the circuit-breaker can withstand the expected operating conditions, i.e. the switching capacity or the operating cycles.

3RT2 power contactor

The MTTF\(_d\) of each channel is calculated as follows:

\[
B10_d = \frac{B10}{\text{dangerous failure ratio}} = 1,369,863 \text{ [Switching cycles]}
\]

\(n_{op} = 52\) [Operations/year]

B10 = 1,000,000 (manufacturer information, SN 31920)

Dangerous failure ratio = 73% (manufacturer information, SN 31920)

\[
\text{MTTF}_{d} = \frac{B10_d}{0.1 \cdot n_{op}} = 2.63 \times 10^{5} \text{ [years]}
\]

3RV2.1 circuit-breaker, as an output of the test equipment (TE)

The MTTF\(_d\) of each channel is calculated as follows:

\[
B10_d = \frac{B10}{\text{dangerous failure ratio}} = 10,000 \text{ [Switching cycles]}
\]

\(n_{op} = 52\) [Operations/year]

B10 = 5,000 (manufacturer information, SN 31920)

Dangerous failure ratio = 50% (manufacturer information, SN 31920)

\[
\text{MTTF}_{d,TE} = \frac{B10_d}{0.1 \cdot n_{op}} = 1.92 \times 10^{3} \text{ [Years]}
\]

ISO 13849-1 suggests that for Cat. 2 the MTTF\(_{d,TE}\) should be higher than half of the MTTF\(_{d,L}\). Since the MTTF\(_d\) is limited to 100 years, this suggestion is fulfilled.
3 Calculation

According to Table 7 of ISO 13849-1 the subsystem “Reacting” reaches PL d.
- Cat. 2
- $\text{DC}_{\text{avg}}$ medium (DC = 90 %)
- MTTF$_d$ of each channel is high (>30 Years) (Power contactor)

According to Annex K this results in PFH$_D$ of $2.29 \times 10^{-7}$.
- Cat. 2
- $\text{DC}_{\text{avg}}$ medium (DC = 90 %)
- MTTF$_d$ of max. 100 years (Power contactor)
3.2 IEC 62061

Since the circuit-breaker is not part of the safety function but instead a diagnostic function, it is not included in the evaluation of the safety function.

The probability of dangerous failures $\lambda_D$ of the power contactor is calculated as follows:

$$ C = \frac{\text{Operations per week}}{7 \times 24 \text{ hours}} = 5.95 \times 10^{-3} \text{ [Operations per hour]} $$

$B_{10} = 1,000,000$ (manufacturer information, SN 31920)

Dangerous failure ratio = 73 % (manufacturer information, SN 31920)

$$ \lambda_D = (\text{dangerous failure ratio}) \cdot \frac{0.1 \cdot C}{B_{10}} = 4.33 \times 10^{-10} $$

According to Table 5 of IEC 62061 the subsystem “Reacting” reaches SILCL 2.

- DC = 90 %
- SFF = 90 %
- HFT = 0

According to Subsystem C (zero fault tolerance with a diagnostic function) this results in a $PFH_D$ of $4.33 \times 10^{-11}$.

- $T_1 = 175,200 \text{ [hours]}$ (20 years, 8,760 hours/year)
- DC = 90 %

**NOTICE**

Even if DC = 99 % was selected, max. SIL CL 2 can be achieved.

When determining the SFF, the exception in section 6.7.7.2 of IEC 62061 must be additionally considered:

For a subsystem with a hardware fault tolerance of zero and where fault exclusions have been applied to faults that could lead to a dangerous failure, then the SILCL due to architectural constraints of that subsystem is constrained to a maximum of SIL 2.

Fault exclusions in this case are:

- Non-failure of the diagnostic unit by means of the mirror contacts and

- Non-failure of the fault reaction (circuit-breaker) during the 6-12 months until the next test of the circuit-breaker by means of undervoltage tripping.


4 Application examples

Table 4-1

<table>
<thead>
<tr>
<th>Title</th>
<th>Entry-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency stop up to SIL 2 or PL d with a SIRIUS 3SK1 safety relay</td>
<td>38472027</td>
</tr>
</tbody>
</table>

5 History

Table 5-1 History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>01.02.2010</td>
<td>First edition</td>
</tr>
<tr>
<td>V2.0</td>
<td>25.11.2013</td>
<td>Replacement of SIRIUS 3TK28 safety relays by SIRIUS 3SK1 safety relays</td>
</tr>
<tr>
<td>V3.0</td>
<td>12.11.2014</td>
<td>Change of structure of the FAQ. The illustrated application examples will be published separately and thus deleted from this FAQ.</td>
</tr>
<tr>
<td>V3.1</td>
<td>22.06.2018</td>
<td>Add 3WL, 3VA and additional notes regarding SIRIUS contactor S6-S12 with F-PLC Input.</td>
</tr>
</tbody>
</table>
What safety level can be reached when combining a contactor with a circuit-breaker for fail-safe switching?

Entry-ID: 40349715, V3.1, 06/2018