# Handbuch zur Funktionalen Sicherheit

Dieses Handbuch gilt für Druckmessumformer, Einschraub- und Tauchsonden der Reihen

DMK, DMP, LMK und LMP mit SIL 2-Konformität

**Wichtige Hinweise:**

- ☞ Bitte lesen Sie dieses Handbuch vor Montage und Inbetriebnahme Ihres Gerätes in sicherheitsrelevanten Anwendungen genau durch.
- ☞ Dieses Handbuch ist zur weiteren Verwendung an einem zugänglichen Ort aufzubewahren.
- ⚠ Das Gerät darf nur von Personen installiert, benutzt und gewartet werden, die mit diesem Handbuch sowie den geltenden Vorschriften über Arbeitssicherheit und Unfallverhütung vertraut sind.
- ⚠ Dieses Handbuch ist nur in Verbindung mit der produktspezifischen Bedienungsanleitung und ggf. der Zusatzanleitung für die Installation in Ex-Bereichen gültig!

BD SENSORS GmbH
BD-Sensors-Straße 1
D - 95199 Thierstein
Telefon +49 (0) 92 35 / 98 11- 0
Telefax +49 (0) 92 35 / 98 11- 11
www.bdsensors.de
info@bdsensors.de

# Anwendungen mit Funktionaler Sicherheit

## 1. Allgemeines

### 1.1 Informationen zur bestimmungsgemäßen Verwendung

Dieses Handbuch stellt eine Ergänzung zur produktspezifischen Bedienungsanleitung dar. Deshalb ist sie nur in Verbindung mit dieser gültig. Generell gilt dieses Handbuch nur für Geräte mit SIL 2-Konformität.

### 1.2 Zielgruppe

Dieses Handbuch richtet sich an qualifiziertes Fachpersonal.

### 1.3 Verwendete Symbole

⚠ : Achtung! ☞ : Hinweis

### 1.4 Sicherheitshinweise

Um Gefahren für den Bediener und sein Umfeld auszuschließen, sind folgende Hinweise zu beachten:

⚠ Beachten Sie für Installation, Wartung und Reinigung des Gerätes unbedingt, die Funktionale Sicherheit behandelnden Verordnungen und Bestimmungen (IEC 61508, IEC 61511, etc.) sowie die Unfallverhütungsvorschriften (UVV).

⚠ Lassen Sie Installation, Wartung und Reinigung der Geräte ausschließlich von hierfür ausgebildeten und berechtigten Personen durchführen, soweit diese mit dem Gerät vertraut sind!

⚠ Veränderungen am Gerät und den Anschlüssen führen zum Erlöschen der Funktionalen Sicherheit und der Garantie!

⚠ Es obliegt dem Anwender zu überprüfen, ob die gewählte Geräteausführung für den vorgesehenen Einsatz und die gegebenen Umfeldbedingungen geeignet ist. Für eine fehlerhafte Auswahl und deren Folgen übernimmt BD SENSORS keine Haftung!

⚠ Die technischen Daten zur Funktionalen Sicherheit entnehmen Sie bitte dem beiliegendem Sicherheitsdatenblatt (Functional Safety Data Sheet®).

## 2. Produktidentifikation

Vergewissern Sie sich, dass Ihr Gerät SIL2-konform bestellt und entsprechend geliefert wurde.

Am einfachsten können Sie dies feststellen, indem Sie das Typenschildes überprüfen. Besteht der dritte Segmentblock bzw. bei einem Gerät der Reihe LMP der fünfte Segmentblock des Bestellcode aus "1S" oder "ES", existiert SIL-Konformität für das Gerät.

## 3. Voraussetzungen

- Die Geräte erzeugen ein analoges Ausgangssignal von 4 ... 20 mA, das proportional dem anliegenden Druck entspricht. Dieses ist durch eine nachgeschaltete Logikeinheit (z.B. SPS) zu überwachen. Zur Störungsüberwachung muss die Logikeinheit dabei zwischen 4 ... 20 mA-Signalen und dem Fehlerstrom < 3,6 mA bzw. > 21 mA unterscheiden.

- Beachten Sie bei der Konzeption Ihrer Anlage, dass die technischen Daten des produktspezifischen Datenblatts sowie des entsprechenden Datenblattes zur Funktionalen Sicherheit nicht überschritten werden. Speziell die zulässigen Betriebsbedingungen (Temperatureinsatzbereich, etc.) sind sicherzustellen.
- Vergewissern Sie sich, dass die gesamte Zusammenschaltung aus unterschiedlichen Komponenten die Anforderungen der Anwendung erfüllt. Für die korrekte Auslegung des Gesamtsystems ist der Betreiber verantwortlich.
- Bei der Inbetriebnahme des Gerätes wird empfohlen die gesamte Sicherheitsfunktion zu überprüfen.
- Die Funktionsfähigkeit des Messgerätes sollte durch Wiederholungsprüfungen in regelmäßigen Zeitabständen geprüft werden. Für die Festlegung des Prüfungsumfangs und der -intervalle ist der Betreiber verantwortlich.

## 4. Ermittlung des erreichbaren Sicherheits-Integritätslevels

Ein E/E/PE sicherheitsbezogenes System besteht in der Regel aus Eingangs-, Logik, und Ausgangsteilsystem. In der folgenden Abbildung ist eine mögliche Aufteilung der mittleren Wahrscheinlichkeit eines Ausfalles im Anforderungsfall dargestellt.

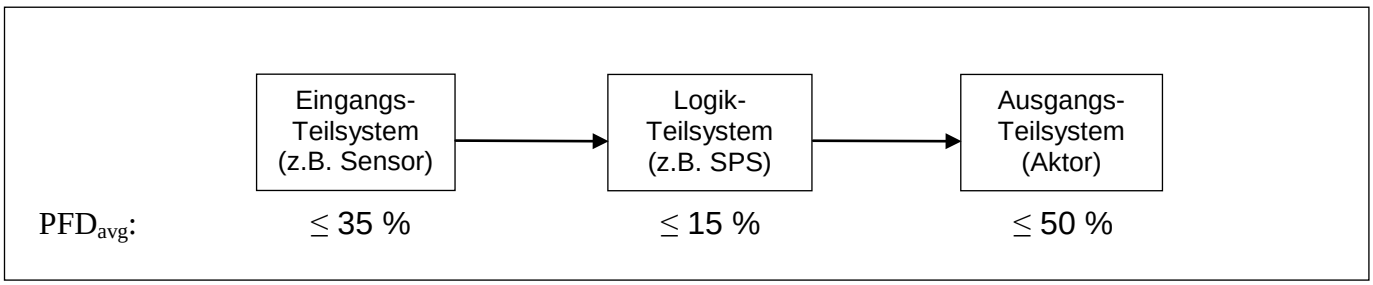


*Abb. 2 übliche Aufteilung der $PFD_{avg}$ auf die Teilsysteme*

Aufgrund der höchstzulässigen mittleren Ausfallwahrscheinlichkeiten der entworfenen Sicherheitsfunktion bei Anforderung kann, anhand von Tabelle 1 der erforderliche Sicherheits-Integritätslevel des Teilsystems bestimmt werden. Hierbei darf die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr betragen und nicht größer als die doppelte Frequenz der Wiederholungsprüfung sein.

| **Sicherheits-Integritätslevel** | **mittlere Ausfallwahrscheinlichkeit der entworfenen Funktion bei Anforderung ($PFD_a$)** für Betriebsart mit niedriger Anforderungsrate |
|---|---|
| SIL 4 | $\geq 10^{-5}$ bis $<10^{-4}$ |
| SIL 3 | $\geq 10^{-4}$ bis $<10^{-3}$ |
| SIL 2 | $\geq 10^{-3}$ bis $<10^{-2}$ |
| SIL 1 | $\geq 10^{-2}$ bis $<10^{-1}$ |

*Tab. 1 Sicherheits-Integritätslevels bezogen auf $PFD_a$*

Um den Sicherheits-Integritätslevel eines Gerätes zu bestimmen sind zwei weitere Parameter erforderlich. Zum einen die SFF (Safe Failure Fraction), die den Anteil der ungefährlichen Fehler zu den insgesamt möglichen Fehlern definiert und zum anderen die HFT (Hardware Failure Tolerance), die die Fehlertoleranz der Hardware angibt. In Abhängigkeit dieser beiden Parameter kann anhand Tabelle 2 der Sicherheits-Integritätslevel ermittelt werden.

| Anteil ungefährlicher Ausfälle (SFF) | Fehlertoleranz der Hardware (HFT) für Betriebsart mit niedriger Anforderungsrate | | |
|---|---|---|---|
| | **0** | **1** | **2** |
| < 60 % | SIL 1 | SIL 2 | SIL 3 |
| 60 % ... < 90 % | SIL 2 | SIL 3 | SIL 4 |
| 90 % ... < 99 % | SIL 3 | SIL 4 | SIL 4 |
| ≥ 99 % | SIL 3 | SIL 4 | SIL 4 |

*Tab. 2 Sicherheits-Integritätslevels bezogen auf HFF*

Alle Druckmessgeräte von BD SENSORS mit SIL-Konformität sind für sicherheitsrelevante Anwendungen mit niedriger Anforderungsrate bis einschließlich SIL 2 geeignet. Zulässige Sicherheits-Integritätslevels sind in den Tabellen grau hinterlegt.

## 5. Prüfbericht

### 5.1 Erklärung / Definitionen zum Prüfbericht

Nachfolgend sind die wichtigsten Begriffe erklärt. (Auszug der Norm EN 61508-4:2001)

| Deutsch | Englisch | Erklärung |
|---|---|---|
| Funktionale Sicherheit | functional safety | Teil der Gesamtsicherheit, bezogen auf das EUC und das EUC-Leit- oder Steuerungssystem, die von der korrekten Funktion der E/E/PE-sicherheitsbezogenen Systeme, anderer Technologien und externer Einrichtungen zur Risikominderung abhängt |
| Sicherheits-funktion | safety function | festgelegte Funktion, die von einem sicherheitsbezogenen System zur Risikominderung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die Anlage zu erreichen oder aufrechtzuerhalten |
| Sicherheits-integrität | safety integrity | Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt |
| SIL (Sicherheits-Integritäts-level) | SIL (safety integrity level) | eine, von vier diskreten Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sichereheitsbezogenen System zugeordnet wird, wobei der Sicherheits-Intigritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste Stufe darstellt |
| Betriebsart | mode of operation | Verwendung, für die ein sicherheitsbezogenes System bestimmungsmäßig vorgesehen ist, hinsichtlich seiner Anforderungsrate, die folgende Ausprägungen annehmen kann:<br>- Betriebsart mit niedriger Anforderungsrate (low demand mode), wobei die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelt Frequenz der Wiederholungsprüfung ist<br>- Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung (high demand or continuous mode), wobei die Anforderungsrate an das sicherheitsbezogene System mehr als einmal pro Jahr beträgt oder größer als die doppelte Frequenz der Wiederholungsprüfung ist |

| Deutsch | Englisch | Erklärung |
|---|---|---|
| Fehler-toleranz | fault tolerance | Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen |
| gefahr-bringender Ausfall | dangerous failure | Ausfall mit dem Potential, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu versetzten |
| unge-fährlicher Ausfall, Versagen | safe failure | Ausfall ohne das Potential, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu setzen |

Nachfolgend weitere Abkürzungen und Erläuterungen die im Datenblatt zur Funktionalen Sicherheit (Functional Safety Data Sheet®) verwendet werden:

| Englisch | Erklärung |
|---|---|
| type | entspricht der Betriebsart (mode of operation) gemäß EN 61508-4:2001 |
| hardware fault tolerance (HFT) | Hardware-Fehlertoleranz, die die Anzahl an Fehlern anzeigt, die ein Gerät oder Subsystem verkraftet, ohne seine Sicherheitsfunktion zu verlieren. |
| safe failure fraction (SFF) | Anteil von Ausfällen ohne das Potential, das sicherheitsbezogene System in einem gefährlichen oder funktionsunfähigen Zustand zu setzen |
| mean time to failure, dangerous (MTTFd) | mittlere Zeit bis zum ersten Ausfall mit dem Potential, das sicherheits-bezogene System in einem gefährlichen oder funktionsunfähigen Zu-stand zu setzen |
| mean time to failure, safe (MTTFs) | mittlere Zeit bis zum ersten Ausfall ohne das Potential, das sicherheits-bezogene System in einem gefährlichen oder funktionsunfähigen Zu-stand zu setzen |
| probability of failure on demand (PFD) | Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion bei Anforde-rung |
| average probability of failure on demand ($PFD_{avg}$) | gemittelte Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion bei Anforderung |
| PFS | Wahrscheinlichkeit, dass die Sicherheitsfunktion eine Fehlauslösung des Prozesses verursacht |
| AV | Wahrscheinlichkeit, dass die Funktionsfähigkeit des Gerätes gewährleis-tet ist |
| OK | Wahrscheinlichkeit, dass das Gerät ohne internen Fehler funktioniert |
| failure mode and effects analysis (FMEA) | Fehler-Möglichkeits- und Einfluss-Analyse |

RISKNOWLOGY®

## Summary

BD Sensors has requested Risknowlogy to support a reliability study on pressure transmitters. Risknowlogy has carried out an FMEA and a Markov study to determine the most important reliability properties of the product. These studies have been carried out following the rules of IEC 61508 and IEC 61511.

To fully understand the calculation results it is necessary to read the complete report. Table 1 gives and overview of the different product names and groups them for further analysis. Table 2 summarizes the functional safety results per group. Table 3 summarize the results for sample calculations that have been carried out on the following reliability properties:

- PFD: The probability that the safety function has failed upon demand
- PFDavg: The average probability that the function has failed upon demand
- PFS: The probability that the safety function causes a spurious trip of the process
- AV: The probability that the function of the product is available
- OK: The probability that the product is running without any internal failures

**Table 1 – Product overview per group**

| Group | Product Names |
|---|---|
| Group 1 | DMP 331, DMP 457, DMP 331P, LMP 331, LMP 307, LMP 308, LMP 808, DMP333 |
| Group 2 | DMK 331, DMK 457, DMK 331P, LMK 331, LMK 307, LMK 807 |
| Group 3 | DMP 331 Ex, DMP 457 Ex, DMP 331P Ex, LMP 331 Ex, LMP 307 Ex, LMP 308 Ex, DMP 333 Ex |
| Group 4 | DMK 331 Ex, DMK 457 Ex, DMK 331P Ex, LMK 331 Ex, LMK 307 Ex |

**Table 2 – Functional safety summary results per group – 55 °C**

| Properties | Group 1 | Group 2 | Group 3 | Group 4 |
|---|---|---|---|---|
| Type | A | A | A | A |
| Hardware fault tolerance | 0 | 0 | 0 | 0 |
| Safe failure fraction | 61,0% | 61,0% | 61,1% | 61,5% |
| Safe detected failure rate [1/h] | 0,00E+00 | 0,00E+00 | 0,00E+00 | 0,00E+00 |
| Safe undetected failure rate [1/h] | 6,13E-08 | 6,13E-08 | 6,13E-08 | 5,95E-08 |
| Dangerous detected failure rate [1/h] | 3,66E-08 | 3,66E-08 | 3,74E-08 | 3,79E-08 |
| Dangerous undetected failure rate [1/h] | 6,28E-08 | 6,28E-08 | 6,28E-08 | 6,10E-08 |
| Dangerous diagnostic coverage | 37% | 37% | 37% | 38% |
| MTTFd [y] | 1138 | 1138 | 1139 | 1154 |
| MTTFs [y] | 1863 | 1863 | 1863 | 1920 |
| Fit for use in Safety Integrity Level | 2 | 2 | 2 | 2 |
| Fit for use in Spurious Trip Level™ | 5 | 5 | 5 | 5 |





RISKNOWLOGY®

**Table 3 – Sample probability calculations per group – 55 °C**

| Property | Group 1 | Group 2 | Group 3 | Group 4 |
|---|---|---|---|---|
| Mission time | 10 years | 10 years | 10 years | 10 years |
| Periodic testing | None | None | None | None |
| PFD | 5.49E-03 | 5.49E-03 | 5,49E-03 | 5.33E-03 |
| PFDavg | 2,75E-03 | 2,75E-03 | 2,75E-03 | 2,67E-03 |
| PFS | 1,46E-06 | 1,46E-06 | 1,46E-06 | 1,42E-06 |
| AV | 9,95E-01 | 9,95E-01 | 9,95E-01 | 9,95E-01 |
| OK | 9,95E-01 | 9,95E-01 | 9,95E-01 | 9,95E-01 |



BD|SENSORS pressure measurement

# Anwendungen mit Funktionaler Sicherheit

## 5.2 Auszug aus dem Prüfbericht

Die Zuordnung der einzelnen Geräte erfolgt über die Gruppen 1 bis 4, die Sie aus Tabelle 1 des Prüfberichtes entnehmen können.

**BD SENSORS GmbH**

**BD-Sensors-Str. 1**

**95199 Thierstein**

**Telefon +49 (0) 92 35 / 98 11- 0**
**Telefax +49 (0) 92 35 / 98 11- 11**

Die Adressen unserer Auslandsvertretungen finden Sie unter **www.bdsensors.de.** Außerdem werden Ihnen auf unserer Homepage Datenblätter, Bedienungsanleitungen, Bestellschlüssel und Zertifikate zum Download angeboten.

***unsere Vertretungen finden Sie in***

**EUROPA**

- Belgien
- Dänemark
- England
- Finnland
- Frankreich
- Griechenland
- Italien
- Litauen
- Luxemburg
- Niederlande
- Norwegen
- Polen
- Portugal
- Rumänien
- Schweden
- Schweiz
- Slowakei
- Spanien
- Türkei
- Ukraine

**ASIEN**

- Indien
- Iran
- Israel
- Japan
- Kasachstan
- Korea
- Malaysia
- Singapur
- Thailand
- Vietnam

**AFRIKA**

- Ägypten
- Südafrika

**AUSTRALIEN**

Dieses Handbuch ist inhaltlich auf dem Stand, der zum Druckzeitpunkt vorlag. Sie wurde nach bestem Wissen und Gewissen erstellt. Für fehlerhafte Angaben und deren Folgen können wir leider keine Haftung übernehmen.

– Technische Änderungen vorbehalten –