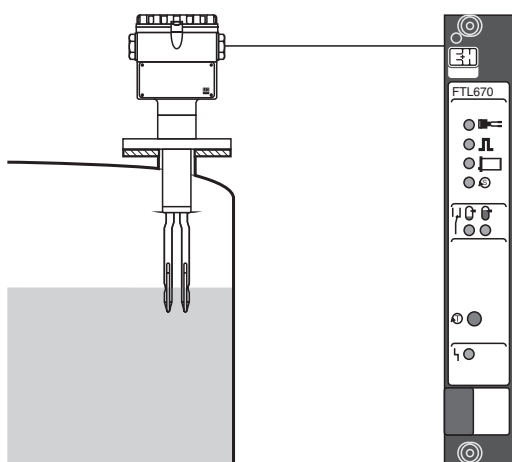




Functional Safety Manual

Liquiphant S, Nivotester FDL60/61, FTL670

Level limit measuring system



Application

Overflow protection or maximum detection of all types of liquids, to meet the particular requirements for safety-related systems as per IEC 61508.

The measuring system meets the requirements for

- Functional safety in accordance with IEC 61508
- Explosion protection by intrinsic safety
- Electromagnetic compatibility as per EN 61326 and NAMUR recommendation NE 21
- Electrical safety in accordance with IEC/EN 61010-1

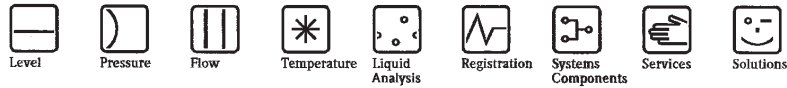
Your benefits

- For overflow protection up to SIL 3
 - independently assessed (Functional Safety Assessment) by TÜV Süd in accordance with IEC 61508
- Suitable for liquefied gases according to VdTÜV, Merkblatt 100
 - for tank categories B and C
 - no annual recurrent test required
- Permanent self-monitoring
- Error message for circuit break and short-circuit
- Functional test of follow-up devices with press of button or remote operation
- Monitoring for corrosion on the tuning fork of the sensor
- No calibration
- Insensitive to external vibration
- Easy commissioning

Table of contents

SIL Declaration of Conformity	3
General information	4
Measuring system design	4
System components	4
Description of use as a protective system	4
Permitted device types	5
Supplementary device documentation	6
Description of the safety requirements and boundary conditions	7
Safety function	7
Restrictions for use in safety-related applications	7
Functional safety figures	8
Behavior of device during operation and in case of error	9
Installation	10
Initial operation	11
Maintenance	11
Proof-test	11
Proof-test	11
Procedure for proof-testing	11
Repair	14
Repair	14
Appendix	15
Commissioning or proof-test protocol	15
Technical report	16
Certificate	20

SIL Declaration of Conformity



SIL-03013c/00/a2

SIL-Konformitätserklärung

Funktionale Sicherheit nach IEC 61508

SIL Declaration of Conformity

Functional safety according to IEC 61508

Endress+Hauser GmbH+Co. KG, Hauptstraße 1, 79689 Maulburg

erklärt als Hersteller, dass der Füllstandgrenzschalter für Flüssigkeiten
declares as manufacturer, that the level limit switch for liquids

Liquiphant S FDL60, FDL61 +Electronic insert FEL67 +Nivotester FTL670

für den Einsatz in Schutzeinrichtungen entsprechend der IEC 61508 / IEC 61511 geeignet ist, wenn
das Handbuch zur Funktionalen Sicherheit SD175F/00 und nachfolgende Kenngrößen beachtet werden:
is suitable for the use in safety-instrumented systems according to IEC 61508 / IEC 61511, if the functional
safety manual SD175F/00 and the following figures are observed:

Gerät / Product	Liquiphant S + FEL67	FTL670	Liquiphant S + FEL67 + Nivotester FTL670
Assessor / Assessor	TÜV Süd (Zertifikat / Certificate: Z10 03 11 20351 002)		
SIL	3		
Gerätetyp/Device type	B		
HFT	1		
Betriebsart / Mode of operation	Low demand mode / High demand mode		
Sicherheitsfunktion/Safety function	Level MAX		
$\lambda_{SD}^{2)}$	401,4 FIT	179,5 FIT	
$\lambda_{SU}^{2)}$	83,4 FIT	44,5 FIT	
$\lambda_{DD}^{2)}$	401,4 FIT	179,5 FIT	
$\lambda_{DU}^{2)}$	83,4 FIT	44,5 FIT	
SFF	91,4 %	90,1 %	91 %
β	5 %	5 %	-
β_D	2 %	2 %	-
PFDA _{avg} ¹⁾ (T ₁ = 15 Jahre/years)	$1,73 \times 10^{-4}$	$9,24 \times 10^{-5}$	$2,66 \times 10^{-4}$
PFH ¹⁾ (T ₁ = 15 Jahre/years)	$2,64 \times 10^{-9}$	$1,41 \times 10^{-9}$	$4,04 \times 10^{-9}$
Diagnose-Testintervall / Diagnostic test interval	30 sec.		
MTTR	8 Stunden/hours		
MTBF ³⁾	117 Jahre/years	254 Jahre/years	80 Jahre/ years
Empfohlenes Prüfintervall/ recommended Proof test interval	T ₁ = 15 Jahre/years		

¹⁾ Die Werte entsprechen SIL 3 nach ISA S84.01. / The values comply with SIL 3 according to ISA S 84.01.

²⁾ Gemäß Siemens SN29500 / according to Siemens SN29500

³⁾ Gemäß Siemens SN29500, einschließlich Fehlern, die außerhalb der Sicherheitsfunktion liegen /
according to Siemens SN29500, including faults outside the safety function

Das Gerät wurde in einem vollständigen Functional Safety Assessment unabhängig bewertet.
The device was assessed independently in a complete Functional Safety Assessment.

Maulburg, 08.10.2009

Endress+Hauser GmbH+Co. KG

i.V.

(Dr. Arno Götz)
Leitung Zertifizierung/Manager Certification

i.V.

(Volker Dreyer)
Leitung Projekt / Project Manager

Endress+Hauser 
People for Process Automation

General information



Note!

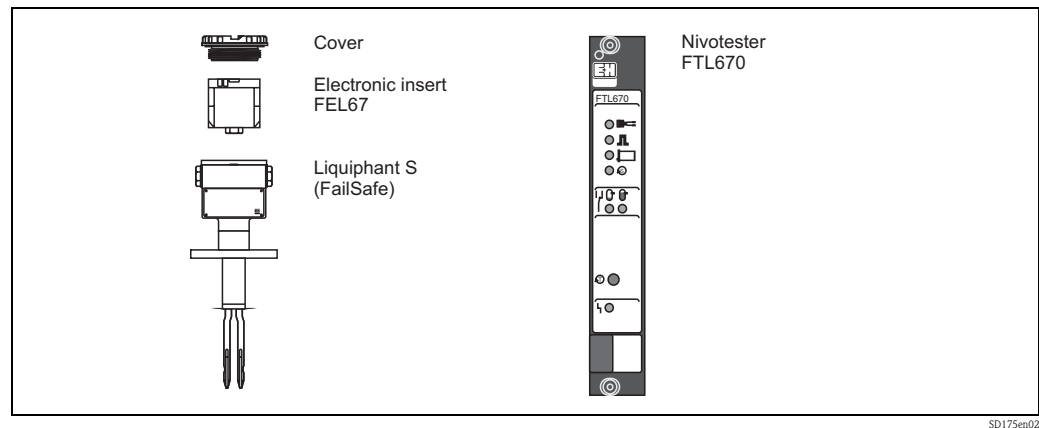
General information on functional safety (SIL) is available at:

www.de.endress.com/SIL (German) or www.endress.com/SIL (English) and in the Competence Brochure CP002Z "Functional Safety in the Process Industry - Risk Reduction with Safety Instrumented Systems".

Measuring system design

System components

The measuring system's devices are displayed in the following diagram.



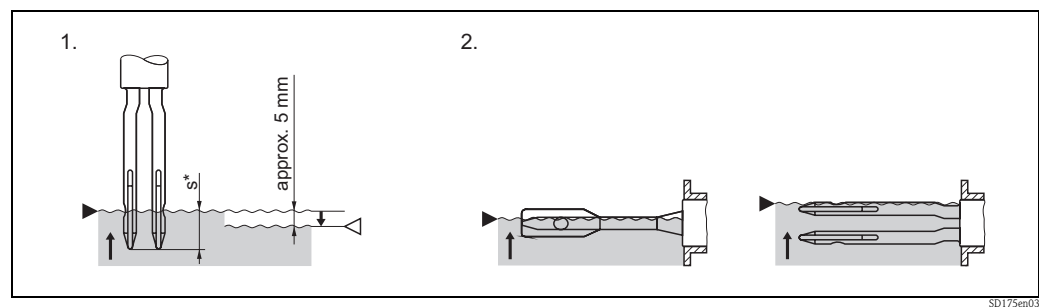
The measuring system consists of the Liquiphant S FDL60 or FDL61 sensor with the FEL67 electronic insert and Nivotester FTL670 switching unit.

A signal which is dependent on the level is generated in the sensor. This is fed to the switching unit where it is made available as a fail-safe contact.

Description of use as a protective system

The tuning fork of the sensor vibrates at its intrinsic resonance frequency. The frequency decreases if the fork is submersed in liquid. This change in frequency causes the fail-safe contact to change.

The switch point depends on installation. For information on the switch point, please refer to the Operating Instructions (→ 6, "Supplementary device documentation").



1. Installation from above
2. Installation from the side



Caution!

The measuring line only works in the overflow protection safety function (MAX safety) using the fail-safe contact!

The fail-safe contact always works in idle current safety; i.e. the contact opens when:

- The switch point is exceeded (level exceeds response height)
- A fault occurs
- The mains voltage fails

In addition to the fail-safe contact, the fault-signalling contact (alarm relay) works as a changeover contact and goes to idle condition when:

- One of the following faults occurs:
 - Fault in the sensor FDL60, FDL61 (e.g. corrosion, electronics fault)
 - Fault in data transfer
 - Fault in FTL670 limit switch
- The mains voltage fails



Note!

When the alarm relay changes to idle condition, the fail-safe contact also opens.



Note!

Correct installation is essential to the safe operation of the device.

The instructions on installation conditions in the Operating Instructions (→ 6, "Supplementary device documentation") must be followed.

Permitted device types

The functional safety assessment described in this manual applies to the device versions listed below. Unless otherwise indicated, all subsequent versions can also be used for safety functions.

In the event of device modifications, a modification process compliant with IEC 61508 is applied.

Device versions valid for use in safety-related applications:

Liquiphant S FDL60		
Options	Designation	Version
010	Approval	all
020	Process Connection	all
025	Fork Surface Finish	all
040	Electronics; Output	all
050	Housing; Cable Entry	all

Liquiphant S FDL61		
Options	Designation	Version
010	Approval	all
020	Process Connection	all
025	Fork Surface Finish	all
030	Probe Length	all
040	Electronics; Output	all
050	Housing; Cable Entry	all

Nivotester FTL670

The device version is suitable for use in safety-related applications.

Supplementary device documentation

Liquiphant S FDL60, FDL61		
Documentation	Contents	Note
Technical Information TI223F/00	<ul style="list-style-type: none"> - Technical data - Instructions on accessories 	<ul style="list-style-type: none"> - The documentation is available on the Internet. → www.endress.com.
Operating Instructions BA140F/00	<ul style="list-style-type: none"> - Introduction - Mounting the Liquiphant S - Mounting the Nivotester - Connection - Start-up - Maintenance - Trouble-Shooting - Technical Data - Liquefied Gas: Special Instructions 	<ul style="list-style-type: none"> - The documentation is available on the Internet. → www.endress.com.
Compact Instructions KA030F/00	<ul style="list-style-type: none"> - Safety and Certificates - Unpacking and Mounting - Connection 	<ul style="list-style-type: none"> - The documentation is supplied with the device. - The documentation is also available on the Internet. → www.endress.com.
Safety instructions (depending on the selected "Approval" version)	<ul style="list-style-type: none"> - Safety, mounting and operating instructions for devices suitable for use in hazardous areas or as overflow protection (German Water Resources Act). 	<p>Additional safety instructions (XA, XB, XC, ZE, ZD) are supplied with certified device versions. Please refer to the nameplate for the relevant safety instructions..</p>

Nivotester FTL670		
Documentation	Contents	Note
Technical Information TI223F/00	<ul style="list-style-type: none"> - Technical data - Instructions on accessories 	<ul style="list-style-type: none"> - The documentation is available on the Internet. → www.endress.com.
Operating Instructions BA140F/00	<ul style="list-style-type: none"> - Introduction - Mounting the Liquiphant S - Mounting the Nivotester - Connection - Start-up - Maintenance - Trouble-Shooting - Technical Data - Liquefied Gas: Special Instructions 	<ul style="list-style-type: none"> - The documentation is supplied with the device. - The documentation is also available on the Internet. → www.endress.com.
Compact Instructions KA031F/00	<ul style="list-style-type: none"> - Safety and Certificates - Connection - Signalling 	<ul style="list-style-type: none"> - The documentation is supplied with the device. - The documentation is also available on the Internet. → www.endress.com.
Safety instructions (depending on the selected "Approval" version)	<ul style="list-style-type: none"> - Safety, mounting and operating instructions for devices suitable for use in hazardous areas or as overflow protection (German Water Resources Act). 	<p>Additional safety instructions (XA, XB, XC, ZE, ZD) are supplied with certified device versions. Please refer to the nameplate for the relevant safety instructions..</p>

Description of the safety requirements and boundary conditions

Safety function

The safety function of the measuring system is maximum level limit monitoring (overflow protection).


Safety-related signal


The safety-related signal is the fail-safe contact:

- The fail-safe contact is closed in the operating state (tuning fork free).
- The fail-safe contact is opened (safe condition) on demand (tuning fork covered) or if a fault occurs.

Restrictions for use in safety-related applications

The measuring system must be used correctly for the relevant application, taking into account the medium properties and ambient conditions. The instructions for critical process situations and installation conditions, as detailed in the Operating Instructions, must be observed.

The specifications in the Operating Instructions (→  6, "Supplementary device documentation") must not be exceeded.

Depending on the Nivotester density setting (→  10, "Installation"), the density of the medium must not undershoot specific limit values:

- Setting $\rho > 0.7$ (with jumper):
 - All liquids of viscosity up to 2000 mm²/s with density greater than 0.7 g/cm³.
 - Viscosities up to 10,000 mm²/s are possible in the case of orientations as per TI223F/00.
- Setting $\rho > 0.5$ (without jumper):
 - All liquids of viscosity up to 2000 mm²/s with density greater than 0.5 g/cm³.
 - Viscosities up to 10,000 mm²/s are possible in the case of orientations as per TI223F/00.
 - Liquefied gas with density greater than 0.44 g/cm³.

Functional safety figures

The table shows the specific figures for functional safety for Liquiphant S + FEL67 + Nivotester FTL670:

Figures according to IEC 61508	Value		
	Liquiphant S + FEL67	Nivotester FTL670	Liquiphant S + FEL67 + Nivotester FTL670
Safety function	MAX Level		
SIL	3		
HFT	1		
Device type	B		
Mode of operation	Low demand mode, High demand mode		
SFF	91.4 %	90.1 %	91 %
MTTR	8 h		
Recommended proof-test interval T_1	15 years		
λ_{sd}^{*2}	401.4 FIT	179.5 FIT	
λ_{su}^{*2}	83.4 FIT	44.5 FIT	
λ_{dd}^{*2}	401.4 FIT	179.5 FIT	
λ_{du}^{*2}	83.4 FIT	44.5 FIT	
λ_{tot}^{*2}	969.5 FIT	447.9 FIT	1417.4 FIT
β	5 %	5 %	-
β_D	2 %	2 %	-
PF D_{avg} for $T_1 = 15$ years *1	1.73×10^{-4}	9.24×10^{-5}	2.66×10^{-4}
PFH for $T_1 = 15$ years *1	2.64×10^{-9}	1.41×10^{-9}	4.04×10^{-9}
MTBF *3	117 years	254 years	80 years
Diagnostic test interval *4	30 s		
Fault reaction time *5	3 s		
System reaction time *6	0.5 s with tuning fork covered 1.0 s with tuning fork uncovered		

*1 The values correspond to SIL 3 as per ISA S84.01.

*2 According to Siemens SN29500.

*3 According to Siemens SN29500, including faults outside of the safety function.

*4 During this time, all diagnostic functions are executed at least once.

*5 Time between fault detection and fault reaction.

*6 Step response time as per DIN EN 61298-2.

Dangerous undetected failures in this scenario:

A dangerous, undetected failure is defined as an incorrect output signal where the tuning fork is covered while the fail-safe contact is closed.³

Useful lifetime of electrical components:

The established failure rates of electrical components apply within the useful lifetime as per IEC 61508-2, Section 7.4.7.4. Note 3.

Behavior of device during operation and in case of error

Behavior of device during power-up

Once a device has powered up, the output signal can be regarded as safe after 10 seconds. The fail-safe contact is open during this time. After this, the device is in normal operation and shows the status of the tuning fork (free/covered).

Behavior of device on demand

Once the level limit to be monitored is reached, the fail-safe contact changes from closed to open within the system reaction time.


Behavior of device in the event of faults

Fail-safe contact

The fail-safe contact is open in the event of faults.

Alarm relay

The alarm relay changes to idle condition in the event of faults.

The type of fault is also indicated by an LED on the Nivotester; see Operating Instructions (→  6, "Supplementary device documentation").



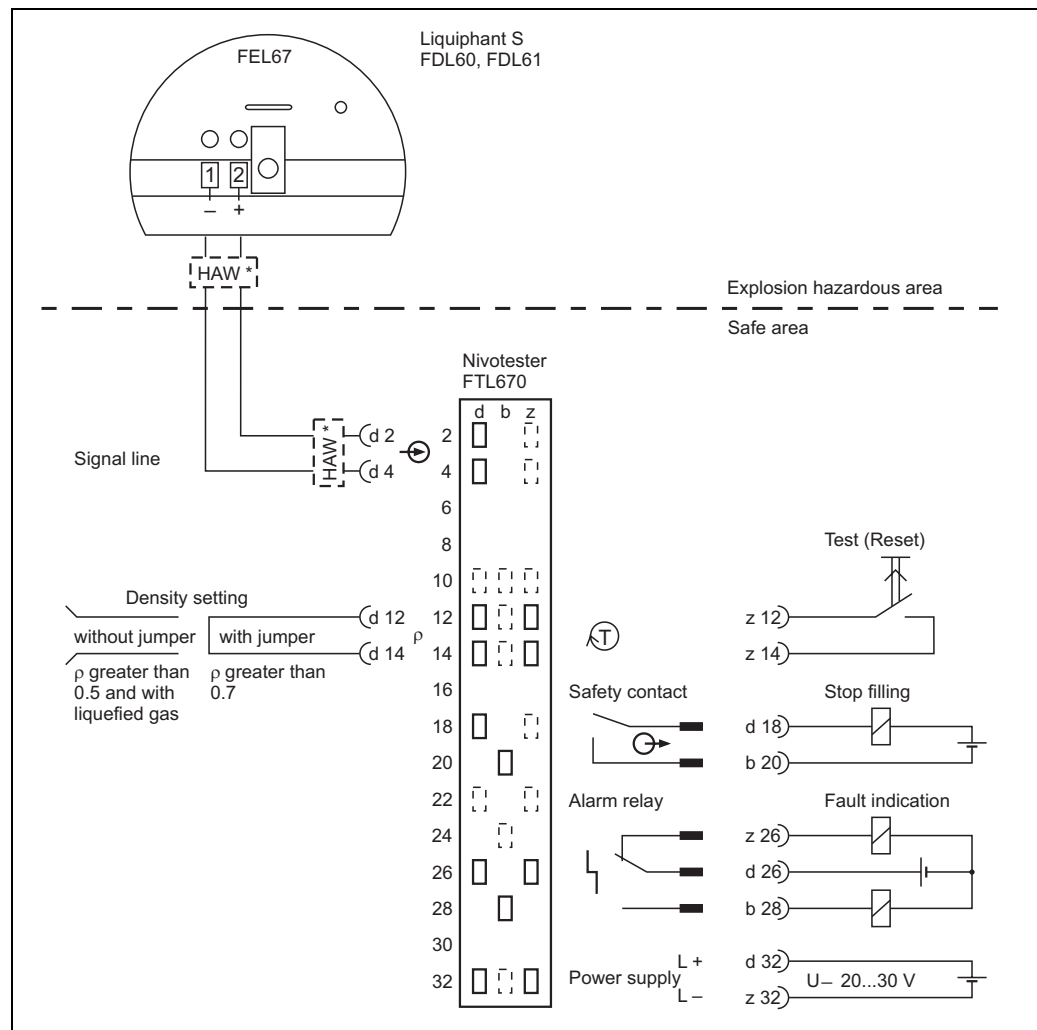
Note!

This signaling is simply an additional piece of diagnostic information and does not form part of the safety-related output signal.

Installation

Installation, wiring and commissioning

Installation, wiring and commissioning of the device is described in the Operating Instructions (→ 6, "Supplementary device documentation").



* Overvoltage protector HAW560Z and HAW562Z if required



Caution!

Note the following for Nivotester FTL670:

The operator must use suitable measures (e.g. current limiter, fuse) to ensure the following characteristics for the fail-safe contact and alarm relay are not exceeded:

- $U \leq 230 \text{ V AC}, 50/60 \text{ Hz}, I \leq 2.5 \text{ A},$
 $P \leq 600 \text{ VA at } \cos \varphi = 1.0 \text{ or } P \leq 300 \text{ VA at } \cos \varphi \geq 0.7 \text{ or}$
- $U \leq 120 \text{ V DC}, I \leq 2.5 \text{ A}, P \leq 75 \text{ W}$




Caution!

Changes to the measuring system and settings after start-up can impair the protection function!


Orientation

The permitted orientations of the device are described in the Operating Instruction (→ 6, "Supplementary device documentation").

Initial operation

When operated for the first time, the function of the entire system can be checked by raising the level in the tank to the limit value. Pressing the "test" key on Nivotester FTL670 is sufficient for the functional test of the follow-up devices (→  13, "Flow diagram").
In Germany, specific regulations must be observed for the functional test of an overflow protection system. Note the relevant information in the certificates.

Maintenance

Please refer to the relevant Operating Instructions for instructions on maintenance (→  6, "Supplementary device documentation").
Alternative monitoring measures must be taken to ensure process safety during proof-testing and maintenance work on the device.

Proof-test

Proof-test

Safety functions must be tested at appropriate intervals to ensure that they are functioning correctly and are safe. The time intervals must be defined by the operator.

Proof-testing of the device can be performed using one of the following procedures:

- Approaching the level (→ Test procedure A).
- Removing and immersing in a medium of comparable density and viscosity (→ Test procedure B).
- Simulation at the Nivotester by activating the "test" key (→ Test procedure C).


In addition, checks must be carried out to ensure that all cover seals and cable entries are sealing correctly.

Procedure for proof-testing**Preparation:**


Connect a suitable measuring device (e.g. Multimeter, downstream plant sections etc.) to display the function of the fail-safe contact.

Test procedure A

Procedure when it is possible to approach the level:


1. The tuning fork must be free. If necessary, reduce the level and wait 10 seconds.
2. Check is the LED for permanent self-monitoring flashing (→  13, "Flow diagram")?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: make a note of the initial status of the fail-safe contact (open/closed).
3. Check is the fail-safe contact closed?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: dampen the tuning fork by approaching the level.
4. Make a note of the second status of the fail-safe contact (open/closed).
5. Check is the fail-safe contact open?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: remove damping from the tuning fork; reduce the level.
6. Make a note of the third status of the fail-safe contact (open/closed).
7. Check is the fail-safe contact closed?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: the test is successful and normal operation is resumed.

**Note!**

With this type of test, the entire safety path from the tuning fork to the fail-safe contact is checked!
For troubleshooting, → Operating Instructions (→  6, "Supplementary device documentation"), Section "Troubleshooting".


Test procedure B

Procedure when it is not possible to approach the level but the device can be removed:

1. Remove the Liquiphant electrically and mechanically.
2. Connect the Liquiphant to the Nivotester electrically.
3. Wait 10 seconds. (The tuning fork must be free).
4. Check is the LED for permanent self-monitoring flashing (→  13, "Flow diagram")?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: make a note of the initial status of the fail-safe contact (open/closed).
5. Check is the fail-safe contact closed?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: dampen the tuning fork by immersing it in the medium.
6. Make a note of the second status of the fail-safe contact (open/closed).
7. Check is the fail-safe contact open?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: remove damping: the tuning fork must be free.
8. Install the Liquiphant and check electrical and mechanical installation.
9. Make a note of the third status of the fail-safe contact (open/closed).
10. Check is the fail-safe contact closed?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: the test is successful and normal operation is resumed.



Note!

With this type of test, the entire safety path from the tuning fork to the fail-safe contact is checked! For troubleshooting, → Operating Instructions (→  6, "Supplementary device documentation"), Section "Troubleshooting".




If necessary, the accuracy of the switch point can also be checked, → Operating Instructions, Section "Mounting the Liquiphant S".

Test procedure C

Note!

At the time of the test, ensure that the tuning fork is free!


Procedure when it is not possible to approach the level and the device cannot be removed:

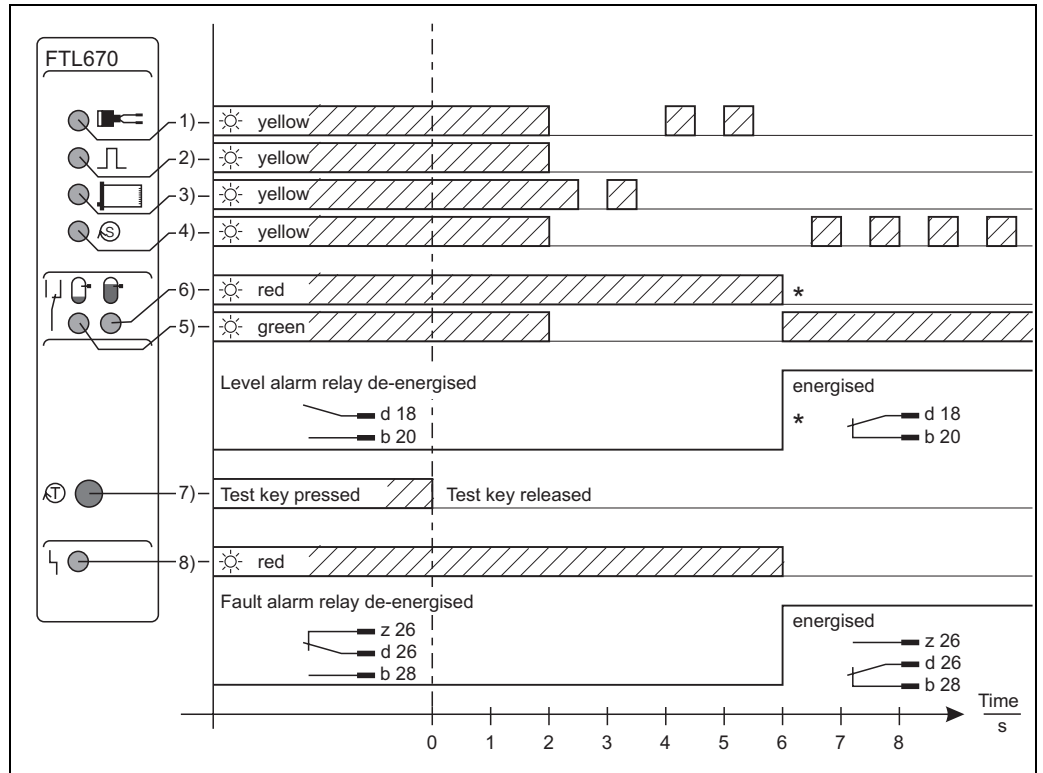
1. Make a note of the initial status of the fail-safe contact (open/closed).
2. Check is the fail-safe contact closed?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: press the "test" key (using tool) (→  13, "Flow diagram"). **Do not** release!
3. Check does the device respond to keypress?
 - No: fault in the Nivotester.
 - Yes: all LEDs lit (→  13, "Flow diagram").
4. Make a note of the second status of the fail-safe contact (open/closed).
5. Check is the fail-safe contact open?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: release the "test" key.
6. Check does the test procedure run correctly (→  13, "Flow diagram")?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: make a note of the third status of the fail-safe contact (open/closed).
7. Check is the fail-safe contact closed?
 - No: fault in the Liquiphant or Nivotester.
 - Yes: the test is successful and normal operation is resumed.



Note!

With this type of test, the entire safety path is not checked! The tuning fork is only included in test procedures A or B.

For troubleshooting, → Operating Instructions (→  6, "Supplementary device documentation"), Section "Troubleshooting".



SD175en05

Flow diagram of function test

- 1) lit: fault in sensor
- 2) lit: fault in data transfer
- 3) lit: fault in Nivotester
- 4) flashing: permanent self-monitoring
- 5) lit: level below maximum
- 6) lit: level alarm
- 7) "test" key
- 8) lit: fault; unlit: normal operation



Note!

If one of the test criteria from the test sequences described above is not fulfilled, the device may no longer be used as part of a safety instrumented system.

The purpose of proof-testing is to detect random device failures. The impact of systematic errors on the safety function is not covered by this test and must be assessed separately.

Systematic errors can be caused, for example, by process material properties, operating conditions, buildup or corrosion.

Repair

Repair

All repairs to the devices must be carried out by Endress+Hauser only.
Safety functions cannot be guaranteed if repairs are carried out by anybody else.

Exception:

The customer is permitted to replace the electronic insert if the member of staff responsible has been trained by Endress+Hauser to do so.

The replaced electronic insert must be sent to Endress+Hauser for fault analysis.

Once the electronic insert has been replaced, proof-testing must be carried out.

In the event of failure of a SIL-labeled Endress+Hauser device, which has been operated in a protection function, the "Declaration of Contamination and Cleaning" with the corresponding note "Used as SIL device in protection system" must be enclosed when the defective device is returned. Available at:
www.de.endress.com/dekontamination.

Appendix

Commissioning or proof-test protocol

System-specific data				
Company				
Measuring points / TAG no.				
System				
Medium (density and viscosity)				
Device type / Order code				
Serial number of device				
Name				
Date				
Signature				
Device-specific commissioning parameters				
Proof-test protocol				
Test procedure	A Approach level	B Remove device	C Simulation	
Please check:				
Test stage	Set point		Actual value	Result: OK / unsuccessful
1. Is the LED for permanent self-monitoring flashing?	flashing		–	
2. Initial status of the fail-safe contact?	closed		closed	
3. Second status of the fail-safe contact?	open		open	
4. Is the test procedure running correctly?	–		yes	
5. Third status of the fail-safe contact?	closed		closed	
Result: Proof test passed:	1., 2., 3., 5. = OK		2., 3., 4., 5. = OK	

SD17Sen06

Technical report



Inhaltsverzeichnis

Inhaltsverzeichnis	2
1. EINLEITUNG	3
2. PRÜFUNTERLAGEN	3
3. DEFINITIONEN	4
4. PRÜFGRUNDLAGEN	5
4.1. <u>Verwendete Variablen aus EM80670 V1.4</u>	5
4.2. <u>Berechnung der PFD_{AVG}</u>	6
5. ZUSAMMENFASSUNG	7
6. ERGEBNIS	8

Bericht: EM 82272 Rev 1.2
 Autor: Nr.: 717501905
 Bearbeiter: AchazJäckel
 16.09.2008
 Seite 2 von 9

TUV SUD Rail GmbH
 Automation, Software and Electronics-IQSE
 Ridlerstr. 57
 D-80339 München
 Tel.: +49 89 5190-1799; Fax: -2933

ManagementSummary



Technischer Bericht

zur Berechnung der Ausfallwahrscheinlichkeit
 des Systems Liquiphant Fail-Safe

Auftraggeber:

Endress + Hauser GmbH+Co. KG
 Hauptstr. 1
 79689 Maulburg

Bericht Nr.: EH 82272

Revision 1.2 vom 16. September 2008

Prüf- und Zertifizierungsstelle:
 TÜV SÜD Rail GmbH
 Automation, Software and Electronics-IQSE
 Ridlerstraße 57
 D-80339 München

Dieser Technische Bericht darf nur in vollständigem Wortlaut wiedergegeben werden. Die Verwendung zu Werbezwecken bedarf der schriftlichen Genehmigung. Er enthält das Ergebnis einer einmaligen Untersuchung an dem zur Prüfung vorgelegten Erzeugnis und stellt kein allgemein gültiges Urteil über Eigenschaften aus der laufenden Fertigung dar. Offizielle Übersetzungen dieses Technischen Berichtes sind durch die Prüf- und Zertifizierungsstelle zu autorisieren.

ManagementSummary



1. EINLEITUNG

Die Firma Endress+Hauser GmbH+Co.KG beauftragte die TÜV SÜD Rail GmbH mit der Berechnung der Ausfallwahrscheinlichkeit des Systems Liquiphant Fail-Safe für ein Proofestintervall für 10 bzw. 15 Jahre. Als Grundlage der Berechnung wurden die Annahme und Rechnungsgrundlagen aus dem Technischen Bericht EM80670_V1.4 übernommen.

Das System wird nach IEC61508 der „low demand mode“ zugeordnet, weil die Anforderungen der Sicherheitsfunktion (Füllstandsüberschreitung) nicht öfters als einmal jährlich angenommen wird. Aufgrund dieser Einstufung gilt es im folgenden den PFD_{AVG}-Wert zu berechnen.

Der PFD_{AVG}-Wert darf für SIL3-Anwendungen für ein Gesamtsystem, bestehend aus einer Eingabeeinheit, einer Verarbeitungseinheit und einer Ausgabeeinheit, den Grenzwert von 100 FIT nicht überschreiten.

Zur Durchführung der probabilistischen Berechnungen werden die folgenden Variablen bestimmt:

1. Ausfallraten
2. Anteil der Ausfälle in einen sicheren Systemzustand (SFF)
3. Common cause Faktor (β)
4. Diagnosestestintervall (t_{test})
5. Proofestintervall (T1)
6. Mittlere Reparaturzeit (MTTR)
7. DC-Wert für alle Subsysteme
8. PFH- bzw. PFD_{AVG}- Wert

Die Ermittlung der theoretischen Zuverlässigkeitskennwerte wurde anhand der unten aufgelisteten Unterlagen durchgeführt. Die Prüfung erfolgte im Juli 2008.

2. PRÜFUNTERLAGEN

Technischer Bericht zur Berechnung der Ausfallwahrscheinlichkeit des Systems Liquiphant Fail-Safe EM80670_V1.4.T vom 10.10.2003
 FEL67-Beta Berechnung IEC 61508-6.xls vom 08.08.2008

TÜV SÜD Rail GmbH
 Automation, Software and Electronics-IOSE
 Rüdigerstr. 59
 D-80339 München
 Tel.: +49 89 5190-1799; Fax: -2933
 Bericht: EM 82272 Rev.1.2
 Auflr. Nr.: 717501905
 Bearbeiter: Adriaen
 16.09.2008
 Seite 3 von 8



3. DEFINITIONEN

Abkürzung	Definition
1001	Eins-aus-Eins- System = „one out of one“
1002	Eins-aus-Zwei- System, zweikanalige Architektur, bei der mindestens ein Kanal die gewünschte Aufgabe erfüllen muss, um das System funktionsfähig zu halten.
DGL	Differentialgleichung
PFH	Wahrscheinlichkeit eines Fehlers im Anforderungsfall
PFH	Wahrscheinlichkeit eines Fehlers pro Stunde (IEC 61508-6)
PFH _{OT}	Wahrscheinlichkeit eines gefährlichen Fehlers pro Stunde des Gesamtsystems
P ₁	Wahrscheinlichkeit, dass sich das System im Zustand i befindet. "1" steht für dd, du, sd oder su.
Rate	Wahrscheinlichkeit, dass das System in einem gefährlichen Zustand ist pro Stunde, h'
dd-state	Gefährlicher, erkannter Zustand
du-state	Gefährlicher, unerkannter Zustand
sd-state	Sicherer, erkannter Zustand
su-state	Sicherer, unerkannter Zustand
Don't care	Nicht relevant
λ	Ausfallrate für Hardwarefehler
λ _{sd}	Ausfallrate in einen sicher erkannten Zustand [1/h]
λ _{su}	Ausfallrate in einen sicher unerkannten Zustand [1/h]
λ _{dd}	Ausfallrate in einen gefährlichen erkannten Zustand [1/h]
λ _{du}	Ausfallrate in einen gefährlichen unerkannten Zustand [1/h]
λ _{don't care}	Ausfallrate in einen nicht relevanten Zustand [1/h]
T	Zeit
T1	Proofestintervall
MTBF	Mittlere Zeit zwischen dem Auftreten zweier Fehler
MTTR	Mittlere Reparaturzeit [h]
SFF	Anteil der sicheren Fehler, mathematische Definition siehe IEC 61508
DC	Diagnoseerkennungsfaktor

TÜV SÜD Rail GmbH
 Automation, Software and Electronics-IOSE
 Rüdigerstr. 59
 D-80339 München
 Tel.: +49 89 5190-1799; Fax: -2933
 Bericht: EM 82272 Rev.1.2
 Auflr. Nr.: 717501905
 Bearbeiter: Adriaen
 16.09.2008
 Seite 4 von 8



β	Common cause Faktor, der einen unerkannten gefährlichen Ausfall bewirkt
β_b	Common cause Faktor, der einen erkannten gefährlichen Ausfall bewirkt
S	Anteil der sicheren Fehler
D	Anteil der gefährlichen Fehler
H	Stunde
FIT	Häufigkeit $10^{-9} h^{-1}$

Abkürzungen

4. PRÜFGRUNDLAGEN

- N1 IEC 61508, Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme, November 2002
- N2 SN 29500, Edition 1999-11, Ausfallraten Bauelemente

4.1. Verwendete Variablen aus EM80670 V1.4

Variable	Übergangsrate
λ_{su}	44,49 FIT
λ_{sd}	179,47 FIT
λ_{du}	44,49 FIT
λ_{dd}	179,47 FIT
$\mu=1 / MTTR$	0,125 h ⁻¹
$\tau=1 / t_{best}$	120 h ⁻¹

1002-System FTL670, Übergangsraten

Die gesamte Ausfallrate des Subsystems FTL670 beträgt:

$$\lambda_{(FTL670)} = 447,92 \text{ FIT.}$$

Die SFF und der DC-Wert werden in der Norm IEC61508-6 Annex C, Absatz f definiert.

$$\text{SFF (FTL670)} = 90,06\%$$

$$\text{DC (FTL670)} = 80,13\%$$

TUV SUD Rail GmbH
Automation, Software and Electronics-IQSE
Ridlerstr. 57
D-80339 München
Tel. +49 89 5190-1799; Fax: -2933
Seite 5 von 8

Bericht: EM 82272 Rev 1.2
Auftr. Nr.: 717501905
Bearbeiter: Achatz/Jäckel
16.09.2008
Seite 6 von 8

ManagementSummary

Variable	Übergangsrate
λ_{su}	83,37 FIT
λ_{sd}	401,39 FIT
λ_{du}	83,37 FIT
λ_{dd}	401,39 FIT
$\mu=1 / MTTR$	0,125 h ⁻¹
$\tau=1 / t_{best}$	120 h ⁻¹

1002-System FEL67, Übergangsraten

Die gesamte Ausfallrate des Subsystems FEL67 beträgt:

$$\lambda_{(FEL67)} = 969,52 \text{ FIT.}$$

$$\text{SFF (FEL67)} = 91,40\%$$

$$\text{DC (FEL67)} = 82,80\%$$

4.2. Berechnung der PFD_{AVG}- und PFH – Werte

	1002
PFD(T1 = 87600h)	$1,232 \cdot 10^{-4}$
PFD _{AVG}	$6,158 \cdot 10^{-5}$
PFH /h	$1,406 \cdot 10^{-9}$

	1002
PFD(T1 = 131400h)	$1,847 \cdot 10^{-4}$
PFD _{AVG}	$9,237 \cdot 10^{-5}$
PFH /h	$1,406 \cdot 10^{-9}$

1002 System FTL670, PFD- und PFH – Ergebnisse

Wichtige Gleichungen:

$$\text{PFH} = \text{PFD(T1)} / T1 [1/h]$$

$$\text{PFD}_{AVG} \approx \text{PFD(T1)} / 2$$

ManagementSummary



	1oo2
PFD(T1 = 87600h)	$2,308 \cdot 10^{-4}$
PFD _{AVG}	$1,154 \cdot 10^{-4}$
PFH /h	$2,634 \cdot 10^{-9}$

	1oo2
PFD(T1 = 131400h)	$3,462 \cdot 10^{-4}$
PFD _{AVG}	$1,731 \cdot 10^{-4}$
PFH /h	$2,635 \cdot 10^{-9}$

1oo2 System FEL67, PFD- und PFH – Ergebnisse

Wichtige Gleichungen:

$$PFH = PFD(T1) / T1 [1/h]$$

$$PFD_{AVG} \approx PFD(T1) / 2$$

5. ZUSAMMENFASSUNG

	FTL670	FEL67	Gesamt
Summe der Basis-ausfallraten / FIT	447,92	969,52	1417,44
MTBF /Jahre	254	117	80
SFF	90,06%	91,40%	90,97%
DC	80,13%	82,80%	81,95%
β	βdu=5%, βdd=2%	βdu=5%, βdd=2%	-
Diagnosetestintervall	1/120	1/120	-
t _{test} [h]	10	10	-
Proofestintervall	8	8	-
T1 / Jahre	10	10	-
MTTR /h	1,232 * 10 ⁻⁴	2,308 * 10 ⁻⁴	3,54 * 10 ⁻⁴
PFD(T1)	$6,158 \cdot 10^{-5}$	$1,154 \cdot 10^{-4}$	$1,77 \cdot 10^{-4}$
PFD _{AVG}	$1,406 \cdot 10^{-9}$	$2,634 \cdot 10^{-9}$	$4,04 \cdot 10^{-9}$
PFH /h	15	15	-
Proofestintervall	8	8	-
T1 / Jahre	10	10	-
MTTR /h	1,847 * 10 ⁻⁴	3,462 * 10 ⁻⁴	5,31 * 10 ⁻⁴
PFD(T1)	$9,237 \cdot 10^{-5}$	$1,731 \cdot 10^{-4}$	$2,66 \cdot 10^{-4}$
PFD _{AVG}	$1,406 \cdot 10^{-9}$	$2,635 \cdot 10^{-9}$	$4,04 \cdot 10^{-9}$
PFH /h			

Zusammenfassung der Analyseergebnisse

TUV SÜD Rail GmbH
Automation, Software and Electronics-IQSE
Altehring 1
D-80339 München
Tel: +49 89 5190-1799; Fax: -2933

Seite 7 von 8

Bericht: EM 82272 Rev. 1.2
Autor: N. Achatz
Bearbeiter: Achatz/Jäckel
16.09.2008
Seite 8 von 8



Verwendete Gleichungen:
 $PFD(T1)_{TOTAL} = \sum PFD(T1)(i)$
 $PFD_{AVG TOTAL} = \sum PFD_{AVG}(i)$
 $PFH_{TOTAL} = \sum PFH(i)$

6. ERGEBNIS

Ein „Low Demand Mode“ – System muß gemäß IEC 61508-1, Tabelle 2 für eine SIL3-Einstufung, der Forderung

$$PFD_{AVG} (SIL3-Limit) < 10^{-3}$$

genügen. Der PFD_{AVG}-Wert des Gesamtsystems, bestehend aus den Anteilen der zwei-kanaligen Bauteile von FTL670 und FEL67. Er berechnete sich zu:

$$PFD_{AVG} = 0,177 \cdot 10^{-3} \text{ bei einem Proofestintervall von 10 Jahren und}$$

$$PFD_{AVG} = 0,266 \cdot 10^{-3} \text{ bei einem Proofestintervall von 15 Jahren.}$$

Diese Werte sind somit kleiner als der geforderte PFD_{AVG} – Grenzwert.

Hinzu kommt die Systemeinstufung für die Hardwareintegrität, die eine Anwendung der Tabelle 3 (IEC61508-2, Kapitel 7.4.3.1.4) vorsieht. Bei einem Subsystem vom Typ B und einer Hardwarefehlertoleranz von 1 wird bei einer SFF über 90% eine Einstufung der Hardware in SIL3 möglich.

Das vorliegende System und alle seine Subsysteme erreichen eine SFF über 90%. Die zweikanalige Systemstruktur in den beiden Subsystemen FEL67 und FTL670 garantiert die Hardwarefehlertoleranz vom Wert 1. Bei einer Systemeinstufung als Typ B wurde damit der quantitative Sicherheitsnachweis für ein SIL3 – System erbracht.

TUV SÜD Rail GmbH
Automation, Software and Electronics-IQSE

Projektleiter

E. Achatz

TUV SÜD Rail GmbH
Automation, Software and Electronics-IQSE
Altehring 1
D-80339 München
Tel: +49 89 5190-1799; Fax: -2933

Bericht: EM 82272 Rev. 1.2
Autor: N. Achatz
Bearbeiter: Achatz/Jäckel
16.09.2008
Seite 8 von 8

Certificate

Certified translation from the German language



Certificate

No.: Z10 03 11 20351 002

Endress & Hauser GmbH & Co.

Hauptstr. 1

79689 Maulburg

with the manufacturing unit(s)
20351

are authorized to mark the product indicated below with the
"TÜV Mark"
in accordance with the enclosure. The notes on the back of this sheet must be followed.



Product: Overspill protection

Type: Liquiphant Fail-Safe

Characteristics:

Liquiphant FDL 60, FDL 61:	
Minimum density of a liquefied gas according to DIN 51622	0.44
Minimum density of a liquid	0.5 switchable 0.7
Type of protection:	IP 66
Nivotester FTL 670:	
Supply voltage	24 V DC
Type of protection of signal input:	EEx ia IIC

Note: Text in the test mark:
"Funktionale Sicherheit" [Functional Safety]

The report cited below is a required component of this certificate. The product meets the safety requirements only if the specifications of the current revision of this report are observed.

The product complies with the relevant safety requirements and indicated properties and was tested in accordance with:

- VdTÜV Merkblatt 100:1990
- DIN V 19250:1994, AK 1-5
- DIN V 19251:1995
- DIN V VDE 0801:1990
- DIN V VDE 0801/A1:1994
- EMV guideline 89/336/EWG
- EN 50178:1997
- EN 61508-1:1998, SIL 1-3
- EN 61508-2:2000, SIL 1-3
- EN 61508-3:1998, SIL 1-3

Report no.: EM95195C; E-(U 95 04 20351 001)

Released with the above certificate number by the
Certification agency of TÜV PRODUCT SERVICE GMBH

Department: TA-RS / Bosch

Date 2003-11-26 (Signature)



This is to certify that the above text is a true and complete translation of an original German document.
Schönau, 26 April 2004



TUEV_Z10 03 11 20351 002 en

Instruments International

Endress+Hauser
Instruments International AG
Kaegenstrasse 2
4153 Reinach
Switzerland

Tel. +41 61 715 81 00
Fax +41 61 715 25 00
www.endress.com
info@ii.endress.com

Endress+Hauser 

People for Process Automation

