

HYDAC

ELECTRONIC

Functional Safety
PL d
SIL 2

Electronic Inclinometers

HIT 1000 Safety
HIT 1500 Safety

Safety Manual

Safety Manual

(Translation of original
instructions)



Table of Contents

Table of Contents	2
Preface.....	4
1. General Information.....	5
1.1. Scope of application.....	5
1.2. Customised models.....	6
1.3. Other applicable documents.....	6
1.3.1. Instruction manual.....	6
1.3.2. Protocol description.....	6
1.3.3. Data sheets	7
1.4. Exclusion of liability	7
1.5. Copyrights	7
1.6. Symbols	8
1.7. Abbreviations used and definitions.....	8
1.7.1. General abbreviations and terms	8
1.7.2. Terms from DIN EN ISO 13849	10
1.7.3. Terms from DIN EN 61508.....	10
2. Sicherheitsconcept.....	12
2.1. Relevante standards and key figures	12
2.1.1. Performance Level - CAT2 Version	12
2.1.2. Performance Level - CAT3 Version	13
2.1.3. Safety integrity level – Cat 2 Version (HFT 0).....	13
2.1.4. Safety integrity level – Cat 3 Version (HFT 1).....	14
2.2. Safety functions.....	14
2.2.1. Safety Functions "System diagnosis"	15
2.2.2. Safety function "Status safe process values"	15
2.2.3. Safety Function "safe inclination"	15
2.2.4. Limit values for the "safe inclination".....	16
2.2.5. Safety Function "safe acceleration"	17
2.2.6. Limit values for the safety function of "safe acceleration"	17
2.2.7. Safety Function "safe gyro"	17
2.2.8. Limit values for the "safe gyro"	17
2.3. Operating conditions of the measurement system	18
2.3.1. Normal operation.....	18
2.3.2. Operation outside of the data sheet specifications	18
2.3.3. Safe state	19
2.4. Response and availability times	20

2.5. Functions in addition to the safety functions20

3. Safety measures 21

3.1. Notes on proper use.....21

3.2. Life expectancy21

4. Contact data 22



Preface

This safety manual provides the user with information and specifications for the functional safe application of products by HYDAC ELECTRONIC GMBH.

It will help you to familiarise yourself with the requirements for a functionally safe use of the product and assist you in obtaining maximum benefit in the possible applications for which it is designed.

All information in this safety manual represent the state of the art of the product at the moment of its preparation and relate to the operating conditions and applications described in the related operation instructions. Due to further product developments, it is possible that there can occur modifications to technical data, illustrations and dimensions.

For applications or operating conditions not described, or if you have any suggestions for changes or additions to this product documentation, please contact the relevant technical HYDAC department.

If you have any questions or suggestions or encounter any problems of a technical nature, please contact your HYDAC representative.

For any suggestions relating changes or additions, please contact the technical documentation department. We look forward to receiving your input.

“Putting experience into practice”

HYDAC ELECTRONIC GMBH

Technical documentation
Hauptstrasse 27
66128 Saarbruecken
-Germany-


Phone: +49(0)6897 / 509-01

Fax: +49 (0) 6897 / 509-1726


Email: electronic@hydac.com

1. General Information

Before commissioning the product, please read this safety manual, the related operating instructions as well as the corresponding protocol description. Ensure that the unit described, hereinafter referred to as the measuring system, is suitable for your application.



Before each startup, installation or replacement, the measuring system including related accessories has to undergo a visual check for damage.



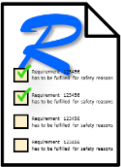
If the instrument is not handled correctly, or if the operating instructions and specifications are not adhered to, damage to property and/or personal injury can result.

1.1. Scope of application

This safety manual exclusively applies to the following measuring system types for inclination measurement related to the horizontal plane with increased demands upon functional safety:


CANopen Safety HIT 1xxx-F13-x-xxx-x-xx-x-S2PD-x-000

The products are components of a system or machine, labelled with affixed nameplates.

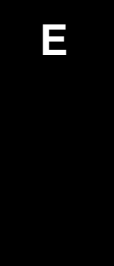


Scope of application669998-01-01

Prior to commissioning, the user should check the validity for the application of this safety manual, comparing it with the model code indicated on the measurement system.



If the used measurement system shows a deviation from the modification of
HIT 1xxx-F13-x-xxx-x-xx-x-S2PD-x-000
, please check the data sheet which has been specifically made for this modification.
The data sheet indicates if this safety manual is also valid for the used modification.



1.2. Customised models

Customised models of this measuring system (modification code deviating from "-000") may vary with respect to technical details including the connection types as described herein or in the protocol description.



Information regarding existing deviations from the standard described herein can be found in the corresponding data sheet.

In case of doubt, the manufacturer should be consulted, specifying the part number.

1.3. Other applicable documents

This safety manual is not valid on its own, further documents have to be consulted for the intended use of the measurement system. The contents of the various applicable documents are described below, making it easier to look up the corresponding information.

1.3.1. Instruction manual

The operating instructions is the core document of the measurement system, containing all information from technical data and type codes, the intended use, mounting and orientation within the coordinate system, commissioning, disposal, description of the signal characteristics through to the device dimensions.

The EU declaration of conformity is part of the operating instructions.



Instruction manual

669998-15-01

To ensure functionally safe use of the measurement system, the requirements in the operating instructions have to be met.

Basic requirements to safety are marked by hazard symbols in the operation instructions, see chapter *1.6 Symbols*.

1.3.2. Protocol description

The protocol description is a subordinate category to the safety manual. If the measurement system provides different communication protocols, there will be separate descriptions to each protocol. The description will be named after the relevant measurement system and the described protocol.

The signal transmission in the form of process data is described in the protocol description. The value and the structure of the binary data is also described herein. The meaning of the identifiers in bit fields, as status signals for example, is also described in the protocol description.

1.3.3. Data sheets

Data sheets are an extract of the technical data from the measurement systems' operating instructions. The data sheets are therefore superordinate to the operating instructions.



For sensors with a customised modification it is indicated, which further general or specific documents are applicable for the used measurement system.

See chapter 1.2 *Customised models*.

1.4. Exclusion of liability

This safety manual was made to the best of our knowledge. Nevertheless and despite the greatest care, it is possible that it may contain errors. Therefore please understand that in the absence of any provisions to the contrary hereinafter our warranty and liability – for any legal reasons whatsoever – are excluded in respect of the information in this safety manual.

In particular, HYDAC ELECTRONIC GMBH - hereinafter referred to as the *manufacturer* - shall not be liable for lost profit or other financial loss. This exclusion of liability does not apply in cases of intent or gross negligence.

Moreover, it does not apply to defects which have been deceitfully concealed or whose absence has been guaranteed, nor in cases of culpable harm to life, physical injury and damage to health. If any material contractual obligation is negligently breached, liability shall be limited to foreseeable damage. Claims due to the product liability shall remain unaffected.



In the event of translation, only the original German version of the safety manual is legally valid.

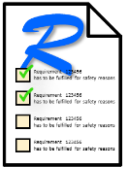
1.5. Copyrights

This safety manual, including the illustrations contained therein, is subject to copyright protection. Use of this safety manual by third parties in contravention of copyright regulations is forbidden.

Reproduction, translation as well as electronic and photographic archiving and modification require the written permission of the manufacturer. Offenders will be liable for damages.

1.6. Symbols

The following symbols serve as an indication of requirements, as a warning and/or information relating functions, settings or measures which require particular attention.



<Req-designation>

<Req-ID>

This symbol indicates a safety requirement, i.e. a requirement which has to be met by the user for a safe application of the measurement system.



The symbol means that the circumstances described here are forbidden (according to ISO 7010).



The symbol means that death, serious injury or major personal damage or severe damage to property could occur if the precautions stated here have not been adhered to or have not been taken (according to ISO 7010).



The symbol indicates important information or features and application suggestions for the product used.



The symbol means that appropriate ESD-protective measures must be observed according to DIN EN 100 015-1.

(Cause of a potential equalisation between body and device-mass as well as the housing-mass about a high-impedance resistance (approx. 1 MOhm) e.g. with a commercial ESD wrist strap).

1.7. Abbreviations used and definitions

The following tables provide an overview of the used abbreviations and terms used in this safety manual.

1.7.1. General abbreviations and terms

Below, please find a list of the general abbreviations and terms.

Abbrevia- tion	Meaning
ACC	Accelerometer
CAN	Controler Area Network
CANopen	CAN based communication protocol for automation tasks

CiA	CAN IN AUTOMATION international users' and manufacturers' group e. V CiA (EU trademark 00 710 98 46)
DIN	Deutsches Institut für Normung e.V. (DIN - German Institute for Standardisation)
EDS	Electronic data sheet; electronically legible description of the CANopen "object dictionary"
EC	European Community
EMC	Electro Magnetic Compatibility
EN	European standard
ESD	Electro static discharge
g	Gravity; gravitational acceleration
GYRO	Gyroscope
HIT	Absolute measuring inclination sensor by HYDAC ELECTRONIC GMBH
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
J1939	CAN based communication protocol for vehicle manufacturing (SAE J1939)
MEMS	Micro-Electro-Mechanical System
NEC	National Electrical Code
RMS	Root Mean Square
SAE	Society of Automotive Engineers
SRDO	Safety relevant data object Object for the safe transmission of values for CANopen Safety
UL	Underwriters Laboratories
VDC	Direct current
VDE	Registered Association of the Electrical, Electronic and Information Technology

1.7.2. Terms from DIN EN ISO 13849

Below, please find a list of the most important abbreviations and terms used in the machinery regulations ISO 13849.

Abbrevia- tion	Meaning
MTTF _D	Mean time to dangerous failure
DC _{avg}	Average Diagnostic Coverage
CCF	Common Cause Failure
PL	Performance Level

1.7.3. Terms from DIN EN 61508

Below, please find a list of the most important abbreviations and terms used in the DIN EN 61508.

Abbrevia- tion	Meaning
SIL	Safety Integrity Level
HFT	Hardware Failure Tolerance
SFF	Safe failure fraction
MooN	M out of N architecture
PFH	Probability of a Dangerous Failure per Hour
PFD	Probability of a Dangerous Failure on Demand
FMEDA	Failure Mode, Effects and Diagnosis Analysis
λ_{sd}	Rate for safe detected failures
λ_{su}	Rate for safe undetected failures
λ_{dd}	Rate for safe dangerous detected failures
λ_{du}	Rate for safe dangerous undetected failures

DCs	Diagnostic coverage of safe failures
DCd	Diagnostic coverage of dangerous failures
FIT	Failure per time unit (1 FIT = 1 failure within 10 ⁹ hours)
MTBF	Mean time between failure
MTTF	Mean time to failure
MTTR	Mean time to repair

2. Sicherheitsconcept

This chapter summarises all important information related with the safety concept implemented in the measurement system.

2.1. Relevante standards and key figures

The measurement system has been developed in accordance with the following standards.

- **Performance Level** DIN EN ISO 13849-1:2015
Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
- **Safety Integrity Level** DIN EN 61508:2010
Functional safety of safety-related electrical, electronic and programmable electronic control systems



Standards

669998-02-01

To ensure a functionally safe application of the measuring system, the user has to determine the required safety level of the entire signal chain in which the measuring system is integrated and check that it is fulfilled.

2.1.1. Performance Level - CAT2 Version

The safety-related data for a measurement system set-up in compliance with Category 2 (Cat 2) of ISO 13849 are as follows:

Device	HIT 1508–F13–x–xxx–x–xx–x–S2PD– 2 –xxx
TÜV Nord certificate	44 207 13709209
Based on	EN ISO 13849-1:2015
PL	d
Architecture	Category 2
MTTFd [years]	High 100 (168)
PFH [1/h]	$2.29 \cdot 10^{-7}$
DC _{avg} [%]	Medium 93.51

2.1.2. Performance Level - CAT3 Version

The safety-related data for a measurement system set-up in compliance with Category 3 (Cat 3) of ISO 13849 are as follows:

Device	HIT 1508-F13-x-xxx-x-xxx-x-S2PD-3-xxx
TÜV Nord certificate	44 207 13709209
Based on	EN ISO 13849-1:2015
PL	d
Architecture	Category 3
MTTFd [years]	High 100 (168)
PFH [1/h]	$4.29 \cdot 10^{-8}$
DC _{avg} [%]	Medium 98.65

2.1.3. Safety integrity level – Cat 2 Version (HFT 0)

The safety-related data for a measurement system set-up in compliance with HFT 0 of the EN 61508 are as follows:

Device	HIT 1508-F13-x-xxx-x-xx-x-S2PD-2-xxx
TÜV Nord certificate	44 207 13709209
Based on	EN 61508:2010
SIL	2
Classification	Type B System
Architecture	1oo1D
Demand mode	Continuously
PFH [1/h]	4.16×10^{-8}
SFF [%]	93.06
HFT	0

2.1.4. Safety integrity level – Cat 3 Version (HFT 1)

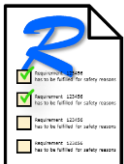
The safety-related data for a measurement system set-up in compliance with HFT 1 of the EN 61508 are as follows:

Device	HIT 1508–F13–x–xxx–x–xx–x–S2PD–3–xxx
TÜV Nord certificate	44 207 13709209
Based on	EN 61508:2010
SIL	2
Classification	Type B System
Architecture	1oo2D
Demand mode	Continuously
PFH [1/h]	3.44×10^{-10}
SFF [%]	99.0
HFT	1

2.2. Safety functions


Safety functions serve to check the signals provided by the measurement system in a functionally safe way. Depending on the result of each safety function, the measurement system can take on a variety of operating conditions, see chapter 2.3 *Operating conditions of the measurement system*.

The signals corresponding to these functions are transmitted to a higher-level control system via functionally safe process data.

	Safety functions	669998-03-01
	Only signals that are provided via a functionally safe process data transmission may be used in the application for functionally safe tasks.	

All safety functions described below are based on the fact that the measurement system, regardless of its safety architecture, has redundant sensor technology.

Safety functions plausibilise the result of their specific function by comparing the two sensor groups. In this case the below described specific signal limits apply. Depending on whether one of these limits is exceeded, the corresponding indicator is set in the signal "Status safe process values".

	A detailed description for the transmission of functional safe process data can be found in the related protocol description of the measurement system.
---	---

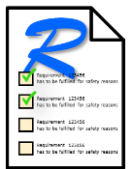
2.2.1. Safety Functions "System diagnosis"

The safety function "system diagnosis" monitors all the important hardware components of the measurement system. For this purpose, different areas are monitored in different cycles, see also chapter 2.4 *Response and availability times*.

If the safety function recognises that the measurement system is in a hazardous state, it will be switched to its "safe state", see chapter 2.3.3 *Safe state*.

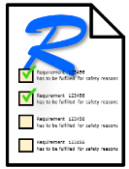
2.2.2. Safety function "Status safe process values"

In general, all functionally safe signals of the measurement system are protected via this status signal. The status safe process values is recalculated and provided constantly and in parallel to the output of functionally safe signals.



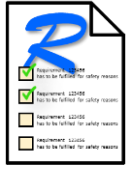
Status safe process values669998-04-01

For the functionally safe application of a signal monitored by the safety functions described below, this may only be done in conjunction with the evaluation of the status described here.




Status safe process values669998-04-02

The status of the safe process values and the functionally safe signals have to be recorded and evaluated simultaneously.



Status safe process values669998-04-03

The status must not be recorded and temporarily stored in a temporally larger interval.

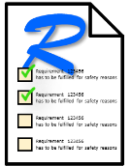


The meaning of the individual indicators of the status safe process values is described in detail in the associated measurement system's protocol description.

2.2.3. Safety Function "safe inclination"

The safety function "safe inclination" monitors the functionally safe output of the signal "safe statical inclination". Monitoring is carried out synchronously with each recalculated signal value.

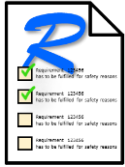
The monitoring result is signalled by setting one or more indicators in the status described above, see chapter 2.2.2 *Safety function "Status safe process values"*.



Safe inclination

669998-05-01

The signal "safe static inclination" secured by the safety function "safe inclination", may only be carried out together with the evaluation of the indicators of the signal "status safe process values".



Safe inclination

669998-05-02

The signal "safe static inclination" is only valid at rest. The state "device in motion" is part of the "status safe process values" and has to be checked for the functionally safe application.

Please observe chapter 2.3.2 *Operation outside of the data sheet specifications*.



The signal "safe inclination" is output via a filter. The temporal behaviour of the signal and its further properties are described in the operation instructions of the measurement system.

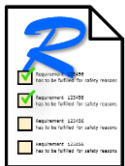


The output and the structure of the signal as a process value as well as the associated state are described in the related protocol description of the measurement system.

2.2.4. Limit values for the "safe inclination"

The limit values for the monitoring of the signal "safe inclination".

Designation	Unit	Value
Maximum diverse deviation of the safe longitudinal axis.	°	2
Maximum diverse deviation of the safe lateral axis.	°	2



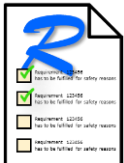
Safe inclination

669998-06-01

For the safety approach of the whole machine system, the limit value for the "safe inclination" has to be considered in addition to the accuracies listed in the operation instructions.

2.2.5. Safety Function "safe acceleration"

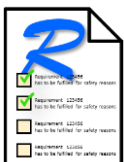
The safety function "safe acceleration" monitors the provision of the signal "acceleration". The monitoring result is provided via the signal "status safe process values".

	Safe acceleration	669998-07-01
The signal "safe acceleration" secured by the safety function "acceleration", may only be carried out together with the evaluation of the indicators of the signal "status safe process values".		

2.2.6. Limit values for the safety function of "safe acceleration"

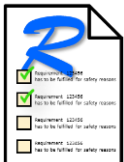
The limit values for the monitoring of the signal "acceleration".

Designation	Unit	Value
Maximum diverse vectorial deviation of the acceleration.	m/s ²	0.35

	Safe acceleration	669998-08-01
For the safety approach of the whole machine system, the limit value for the "safe acceleration" has to be considered in addition to the accuracies listed in the operation instructions.		

2.2.7. Safety Function "safe gyro"

The safety function "safe gyro" monitors the provision of the signal "gyro". The monitoring result is provided via the signal "status safe process values".

	Safe gyro	669998-09-01
The signal "safe gyro" secured by the safety function "gyro", may only be carried out together with the evaluation of the indicators of the signal "status safe process values".		

2.2.8. Limit values for the "safe gyro"

The limit values for the monitoring of the signal "gyro".

Designation	Unit	Value
Maximum diverse vectorial deviation of the angle speed.	rad/s	0.1



Safe gyro

669998-10-01

For the safety approach of the whole machine system, the limit value for the "safe gyro" has to be considered in addition to the accuracies listed in the operation instructions.

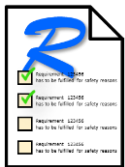
2.3. Operating conditions of the measurement system

From the point of view of functional safety, the measurement system can take on various operation conditions, controlled via the mechanisms described in chapter 2.2 *Safety functions*. Depending on the operation conditions, the use of the measurement system should be considered as safe - otherwise there are special measures to be taken in order to avoid personal injury or damage to the environment.

2.3.1. Normal operation

At "safe operation" the measurement is to be considered as functionally safe. The values of the individual signals can be used without limitations for functionally safe control and monitoring tasks in a machine.

In this state, all functionally safe signals are provided at any time via functionally safe process data.



Normal operation

669998-11-01

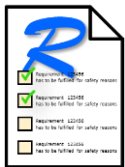
The application has to check whether normal operation is ensured. In this state only, signals may be used for functionally safe applications without limitations.

Under "normal operation" the signal "status safe process values" is available at all times as a process value and has the content 0.

2.3.2. Operation outside of the data sheet specifications

The operating status "outside of data sheet specifications" marks a special state of the measurement system. Signals continue to be provided at any time via safe process data, however, in this state, the specifications from the data sheet can no longer be guaranteed.

This state can be abandoned by the measurement system itself if there is a change of the external influences, i.e. change of the movement situation of the measurement system.




Operation outside of the data sheet specifications

669998-12-01

During operating conditions "outside of the data sheet specifications" signals provided by the measurement system may no longer be used without additional external plausibility measures for functional safe tasks.

The operating status "outside of data sheet specifications" is marked by the signal "status safe process values" which has a value unequal to 0.



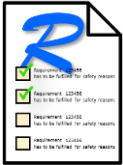
The "status safe process values" unequal to 0 generally marks that the measurement system ranges "outside of the data sheet specifications". If just one single signal of the measurement system is used, this signal may be excluded from this status.

The protocol description provides a detailed description of the indicators of the "status safe process values". These indicators can be used to assess whether a signal is affected or not.


2.3.3. Safe state

The "safe state" of the measurement system is automatically activated by one of the above described safety functions after detection of a serious error, see chapter 2.2 *Safety functions*. In this state, no more signals will be provided by the measurement system.

The measurement system remains in this state, but will continue diagnosing its own functions internally. If the absence of the triggering error is detected, the measurement system attempts to resume operation by a restart (reset).



Safe state	669998-13-01
<p>The "safe state" of the measurement system is marked by the absence of functional safe signals in the form of the process data.</p> <p>Having detected an absence of the signals, the higher-level control ("E/E/PES") has to ensure that immediate action is taken in order to avoid personal injury or damage to the environment.</p>	



In dependence of the used type of communication, the measurement system can mark the reset via a special signal. For further information, please see the related protocol description.

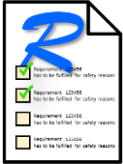
2.4. Response and availability times


In order to achieve the safety values listed in chapter 2.1 *Relevante standards and key figures*, various regular checks are carried out by the measurement system. The cycle times of the individual checks are listed below.

Diagnostic time	Value
"ready" relay	< 2500 ms
System safety time	< 1000 ms
Diagnosis interval	100 ms Parameter monitoring Voltage monitoring Reference voltage monitoring Stack monitoring Stack pointer monitoring Supply voltage monitoring
Diagnosis interval of the diversity deviation	< 20 ms
Refreshing interval for signal calculation	5 ms
External watchdog with its individual time base	< 310 ms
Program process monitoring	< 800 ms

2.5. Functions in addition to the safety functions

The measurement provides further signals in addition to the signals listed in chapter 2.2 *Safety functions*.

	Functions outside of the safety function	669998-14-01
	Signals which are transmitted via non-functionally safe signal channels - provision via non-functionally safe process data channels - must not be used for functionally safe tasks.	

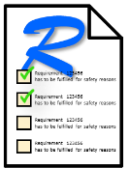
	<p>Example for CANopen / CANopen Safety</p> <p>Signals, i.e. process data, being provided via a PDO and not via a functionally safe SRDO, may not be used for functionally safe tasks.</p> <p>Further information on general and functionally safe process data channels are listed in the associated protocol description.</p>
---	---

3. Safety measures

Below, please find further measures to take for a functionally safe use of the measurement system.


3.1. Notes on proper use


For functionally safe handling of the measurement system, the associated operating instructions are mandatory, see chapter 1.3.1 *Instruction manual*.

	<p>Proper use 669998-16-01</p>
	<p>The signals provided by the measurement system may only be evaluated by a functionally safe "Electrical, Electronic, Programmable Electronic System" (E/E/PES).</p> <p>If the "E/E/PES" does not have a level of functional safety suitable for the overall application, the signal processing is to be considered unsafe.</p>

3.2. Life expectancy

The operating life of the inclination sensor is defined as 20 years. The reliability of the electrical, electronic and mechanical components is such that no repeat testing is required during the unit's operating life.

	<p>Service life 669998-17-01</p>
	<p>The measurement system has to be replaced by the user/machine operator after its service life of 20 years has expired.</p>

	<p>Using the measurement system beyond the aforementioned period is to be considered uncertain and the responsibility then is transferred completely to the user/machine operator.</p>
---	--

4. Contact data

HYDAC ELECTRONIC GMBH

Hauptstrasse 27
D-66128 Saarbruecken

Germany

Web: www.hydac.com
Email: electronic@hydac.com
Phone: +49 (0)6897 509-01
Fax.: +49 (0)6897 509-1726

HYDAC Service

If you have any questions concerning repair work, please do not hesitate to contact HYDAC SYSTEMS & SERVICES:

HYDAC SYSTEMS & SERVICES GMBH

Sonnenallee 1
D-66287 Quierschied-Göttelborn

Germany