BS EN 12830:2018

BSI Standards Publication

Temperature recorders for the transport, storage and distribution of temperature sensitive goods - Tests, performance, suitability

National foreword

This British Standard is the UK implementation of EN 12830:2018. It supersedes BS EN 12830:1999, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee RHE/19, Commercial refrigerated food cabinets (cold room and display cases).

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2018

ISBN 978 0 580 96496 1

ICS 17.200.20; 67.260

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2018.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 12830

August 2018

ICS 17.200.20; 67.260

Supersedes EN 12830:1999

English Version

Temperature recorders for the transport, storage and distribution of temperature sensitive goods - Tests, performance, suitability

Enregistreurs de température pour le transport, le stockage et la distribution des marchandises thermosensibles - Essais, performance, aptitude à l'emploi

Temperaturregistriergeräte für den Transport, die Lagerung und die Verteilung von temperaturempfindlichen Produkten - Prüfungen, Leistung, Gebrauchstauglichkeit

This European Standard was approved by CEN on 2 March 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 12830:2018 E

Contents

European foreword

This document (EN 12830:2018) has been prepared by Technical Committee CEN/TC 423 "Means of measuring and/or recording temperature in the cold chain", the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2019 and conflicting national standards shall be withdrawn at the latest by February 2019.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 12830:1999.

The standard has been completely revised and updated to the state of the art as follows:

- Scope was enlarged, i.e. location of sensors of the recorder with respect to types of usage are included now;
- Update of Clause 2 "Normative references";
- Update of Clause 3 "Terms and definitions";
- Clause 4 "Concepts" was added;
- Clause 5 "Requirements" was enlarged, i.e. subclause 5.3 "Protection of the data from manipulation" and 5.12 "Software verification levels" were added and furthermore Clause 5 has been updated, e.g. values for maximum relative timing error and response time ;
- New subclause 6.7 "Software test" and the related Annex A "Software testing" and Annex B "Manufacturer software test form" were added;
- New Annex D "Expected operation time and storage capacity" and Annex E "Required access to recorded data or functions" were added.

This European Standard is a document meeting the objectives of Directives:

- 92/1/EEC of January 13, 1992 of the Commission on the monitoring of temperatures in the means of transport, warehousing and storage of quick-frozen foodstuffs intended for human consumption;
- 93/43/EEC of June 14, 1993 of the Council of the hygiene of foodstuffs and in particular on "temperature control criteria".

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This document specifies the technical and functional characteristics of temperature recorders for the transport, storage and distribution of temperature sensitive goods between −80 °C and +85 °C.

It specifies the test methods which allow the determination of the equipment's conformity, suitability and performance requirements.

It applies to the whole temperature recording system. The temperature sensor(s) may be integrated into the recorder or be remote from it [external sensor(s)].

It gives some requirements with regards to the location of sensors of the recorder with respect to types of usage such as transport, storage and distribution.

NOTE Examples for the transport, storage and distribution of temperature sensitive goods between −80 °C and +85 °C are chilled, frozen and deep frozen/quick-frozen food, ice cream, fresh and hot food, pharmaceuticals, blood, organs, chemicals, biologicals, electronic and mechanical devices, flowers, plants, bulbs, raw materials and liquids, animals, art and furnishing.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 13486, *Temperature recorders and thermometers for the transport, storage and distribution of chilled, frozen, deep-frozen/quick-frozen food and ice cream - Periodic verification*

EN 60529, *Degrees of protection provided by enclosures (IP Code) (IEC 60529)*

EN 61000-6-2, *Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments (IEC 61000-6-2)*

EN 61000-6-3, *Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments (IEC 61000-6-3)*

EN 61010-1, *Safety requirements for electrical equipment for measurement, control and laboratory use - Part 1: General requirements (IEC 61010-1)*

ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
quantity
property of a phenomenon, body, or substance, where the property has a magnitude that can be expressed as a number and a reference

3.2
unit of measurement
particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitudes relative to that quantity

EXAMPLE The unit of temperature used in this standard is “degree Celsius”.

3.3
value of a quantity
number and reference together expressing magnitude of a quantity

EXAMPLE 15 °C.

3.4
measurement
set of operations having the object of determining a value of a quantity

3.5
measurand
particular quantity subject to a measurement

EXAMPLE Temperature.

3.6
influence quantity
quantity that, in a direct measurement, does not affect the quantity that is actually measured, but affects the relation between the indication and the measurement result

3.7
indication (of a measuring instrument)
value of a quantity provided by a measuring instrument

3.8
accuracy class
class of measuring instruments of measuring systems that meet stated metrological requirements that are intended to keep measurement errors or instrumental measurement uncertainties within specified limits under specified operating conditions

3.9
maximum permissible measurement error
maximum permissible error
extreme value of **measurement error**, with respect to a known **reference quantity value**, permitted by specifications or regulations for a given **measurement**, **measuring instrument**, or **measuring system**

3.10
measurement uncertainty
non-negative parameter characterizing the dispersion of the quantity values being attributed to a measurand, based on the information used

3.11
error of measurement
measured quantity value minus a reference quantity value

3.12
measuring instrument
device intended to be used to make measurements, alone or in conjunction with supplementary device(s)

3.13
displaying device
indicating device
part of a measuring instrument that displays an indication

3.14
recording device
part of a measuring instrument that provides a record of an indication

3.15
temperature sensor
element of a measuring instrument or measuring chain that is directly affected by the temperature

3.16
scale
scale of a measuring instrument
ordered set of marks, together with any numbering, forming part of a displaying device of a measuring instrument

3.17
adjustment
adjustment of a measuring instrument
operation of bringing a measuring instrument into a state of performance suitable for its use

3.18
span
modulus of the difference between the two limits of a nominal range

EXAMPLE For a nominal range of - 35 °C to + 25 °C, the span is 60 K.

3.19
measuring range
working range
set of values for which the error of a measuring instrument is intended to lie within specified limits

3.20
rated operating conditions
operating condition that has to be fulfilled during **measurement** in order that a **measuring instrument** or **measuring system** perform as designed

3.21
limiting conditions
extreme conditions that a measuring instrument is required to withstand without damage, and without degradation of specified metrological characteristics when it is subsequently operated under its rated operating conditions

3.22
reference conditions
operating condition prescribed for evaluating the performance of a measuring instrument or measuring system or for comparison of measurement results

3.23
resolution (of a displaying device)
smallest difference between indications of a displaying device that can be meaningfully distinguished

3.24
response time
time needed for the recorded value to reach and remain with specified limits around actual temperature to which it is measuring

3.25
storage and transport conditions
extreme conditions which a non-operational measuring instrument can withstand without damage and without degradation of specified metrological characteristics when it is subsequently operated under its rated operating conditions

3.26
chilled application
application which has been subjected to cooling (without freezing) and is intended to be maintained at low temperature

3.27
frozen food
food which has been subjected to a freezing process specially designed to preserve the wholesomeness and quality of the product

3.28
deep-frozen or quick-frozen food
food which has been subjected to a quick freezing process

3.29
recording interval
time interval that has elapsed between two successively stored measurements

3.30
recording duration
time interval between the beginning and the end of the recording

3.31
chart
tape, disk, form or other structure upon which is recorded the measurand

3.32
duration of transport
time interval between loading and unloading

3.33
subunit
distinct part or component of the temperature recorder that generates, encodes, transports, prints, indicates and/or stores relevant data

Note 1 to entry: It is housed in its own enclosure.

3.34
audit trail
chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result

Note 1 to entry: See National Information Assurance (IA) Glossary. Committee on National Security Systems. 7 August 1996. p. 4). It documents who did what and when.

3.35
service provider
organization or business which offers service to others in exchange for payment

3.36
relevant measurement data
set of temperature—time—location tuples recorded during the traceability time span

Note 1 to entry: Once data age exceeds this time span it loses its “relevant” status.

3.37
relevant parameters
parameters that affect relevant measurement data

EXAMPLE Calibration parameters, time-date settings and installation location (such as truck ID or warehouse room ID).

3.38
relevant software
software that produces, stores, process or transmits relevant data

Note 1 to entry: Relevant software can cohabit with non-relevant software.

3.39
command
any physical or logical system that enables the access to a function

3.40
relevant command
command that impacts on relevant parameters and relevant measurement data

3.41
cloud
cloud computing, also known as remote on-demand computing; it is a kind of internet-based computing, where shared resources and information are provided to computers and other devices on-demand

3.42
solution as a service (SaaS)
solution where the monitoring system hardware (sensors, recorders and base stations) is installed at the organization site, but the software, server and database are hosted by a service provider; the data are collected, stored and managed by the service provider whilst the organization owner of the recorders has access to the data through a secure web interface

Note 1 to entry: In this scenario, the service provider ensures the cloud system maintenance, correct performance and qualification.

3.43
measuring system
set of one or more measuring instruments and often other devices, including any reagent and supply, assembled and adapted to give information used to generate measured quantity values within specified intervals for quantities of specified kinds

Note 1 to entry: A measuring system can consist of one measuring instrument.

4 Concepts

4.1 General

The objective of the temperature recorder is to generate and to record at least the accurate temperature and time, and the accurate location if applicable.

An additional concept is the time span that the recorded data has to be traceable (for example, minimum one year for deep frozen food.)

The recorder can be a fully mechanical recorder, a mechanical and electronic recorder or a fully electronic recorder. This is why “relevant software” is not always present. Relevant measurement data can be exported for its exploitation by other systems, for example a fleet or warehouse management system. If the exporting mechanism cannot guarantee the traceability of the data, the exported data loses its “relevant” status.

The instrument will normally include a set of parameters that affect relevant characteristics of the temperature recorder. For example, calibration parameters, time-date settings and installation location (such as truck ID or warehouse room ID). We will call these parameters “relevant parameters”.

The combination of the relevant measurement data plus the relevant parameters forms the “relevant data”.

The software that produces, stores, process or transmits relevant data are called reporting software. Relevant software can cohabit with non-relevant software.

4.2 Temperature recorder elements

Figure 1 shows the main elements of a temperature recorder.

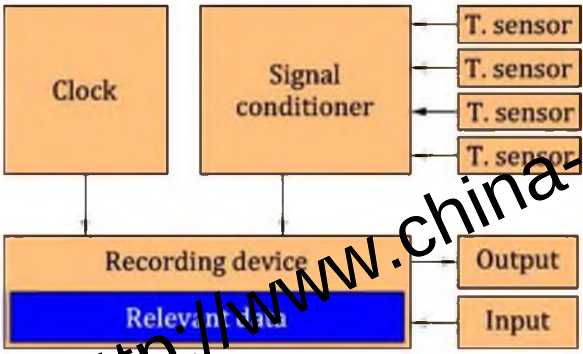

Figure 1 — Abstract view of the temperature recorder showing its main elements

Temperature sensor type can be PT100, PT1000, NTC, Thermocouple, etc. Sensor can be internal, when they are located within the unit enclosure, or external, when not. External sensors can be changeable or fixed to the unit. Sensor intended to measure the temperature of air or the core temperature of the product (insertion sensor).

External sensors can be packaged as digital probes when they include electronics to convert the temperature to a numeric value and to communicate with the recorder through a digital channel.

Power supply can be external or internal. Internal supply types can be rechargeable and non-rechargeable.

An output mechanism will provide output data. Common alternatives are display, printer, and communication port. Communication port can be wire connected or wireless, and can follow an approved standard or be of proprietary design.

An input mechanism is used to give commands to the temperature recorder. Common alternatives are keyboard, touchscreen and communication port.

The clock for electronic recorder is commonly based on a crystal oscillator that produces a very precise frequency. In order to maintain the correct time on power off, a backup power source is required to keep the clock running.

Temperature recorder memory can be volatile or non-volatile. The non-volatile memory can be erasable or permanent. When the temperature recorder program is stored in permanent memory the unit is non-reprogrammable. When the measurements are stored in volatile memory a backup power source is required to ensure that relevant data are not lost on power off.

4.3 Temperature recorder architecture (or configuration)

4.3.1 General

The temperature recorder can be built in a variety of architectures ranging from a monolithic instrument to a very complex distributed system. All the subunits of a distributed system that generates, encodes, transports, or stores relevant data will form part of the temperature recorder.

In order to clarify the boundaries of the temperature recorders, a description of the possible alternatives and major design challenges will be given in 4.3.2 to 4.3.5.

4.3.2 Monolithic instrument

A monolithic temperature recorder includes all of its components in a single package, excluding the temperature sensors that can be internal or external, as shown in Figure 2.

It has to be noted that in this solution all the relevant data are always maintained within the temperature recorder. This data could be exported to other devices but is nevertheless kept in the temperature recorder during the full duration of the traceability time span. Exported data loses its relevant status since traceability is not guaranteed.

Main challenges are:

— Instrument design to achieve the proposed accuracy within the measurement range and operational range.

— Memory design to allow for the storage of all the relevant data during the complete traceability span.

— Unit enclosure and sealing design to prevent electronic, memory and sensor tampering.

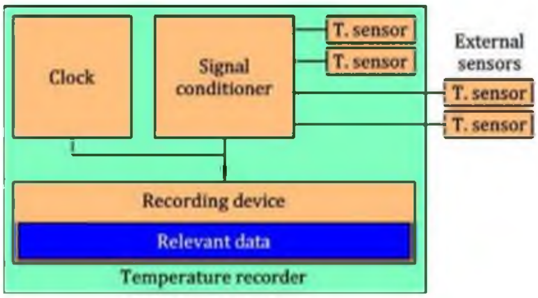

Figure 2 — Monolithic temperature recorder

4.3.3 Monolithic instrument with external relevant data

As shown in Figure 3, in this alternative the relevant data can be kept in an external medium. Relevant data are exported to an external device and can be erased from the temperature recorder. In many cases the external device will be a computer that will store in its disk the exported relevant data.

The exported relevant data are packaged in such a way as to prevent and/or detect its manipulation.

The packaging could be performed internally by the instrument or externally by a computer. In the first case, the downloading to the external storage can be done by an off the shelf application. In the second case, the data leaves the instrument in clear (that is without packaging) and is externally packaged. Therefore, the downloading and packaging application is instrumental to the traceability of the data, and is considered a subunit of the temperature recorder.

The connection between the instrument and the external storage can be by wired or wireless.

Note that the user of the temperature recorder has the responsibility of maintaining the exported relevant data, for example, implementing a sound backup policy.

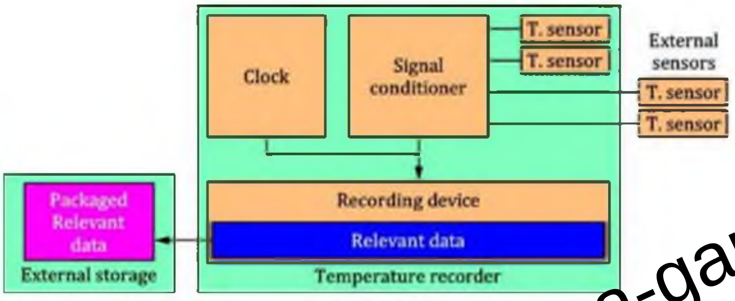

Figure 3 — Monolithic instrument with external storage of relevant data

In addition to the challenges defined for monolithic instruments, this architecture presents the following challenges:

- Design a data packaging that prevents and/or detects its manipulation;
- Design a packaging mechanism that guaranties authenticity;
- Design a communication mechanism that avoids data loss.

4.3.4 Temperature recorder with digital probes

A digital probe includes a temperature sensor as well as a signal conditioner which produces a numerical temperature value. As is depicted in Figure 4, the digital probes are connected to a base unit. The temperature recorder is a measurement system composed of the base station and the digital probes.

Digital probes can be simple, responding with the current temperature to a base command.

Alternatively, the digital probe could also include a clock and a memory to store relevant data, implementing a protocol to transmit the relevant data when appropriate.

In this architecture the temperature recorder is a measurement system composed of two subunits: the base station and the digital probe.

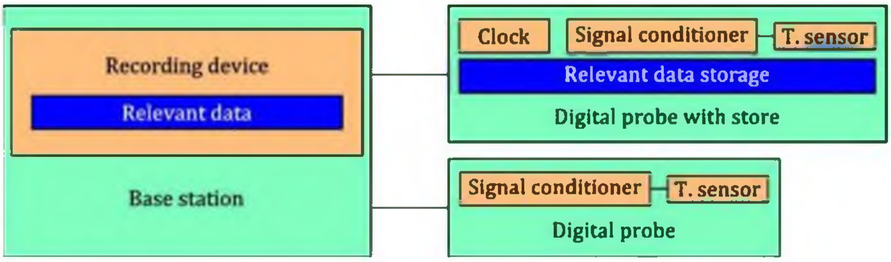

Figure 4 — Temperature recorder with digital probes

The connection of the digital probes with the base station can be made via a cable or via a wireless digital link. Wireless digital probes normally will include some storage capacity to avoid loss of data in case of link temporal failure.

Physical probe sealing is limited to wire connected probes, whereas virtual or software seals will support both wire and wireless connections.

Figure 5 shows that auxiliary communication components, such as routers, repeaters or switches, can be included to extend the range of the base stations both in distance and in number of probes.

Base stations, digital probes and communications components are subject to the challenges defined for monolithic instruments. Additionally, this architecture presents the following Probe—base station connection and protocol designed to prevent data manipulation, data loss, phishing and identity impersonation.

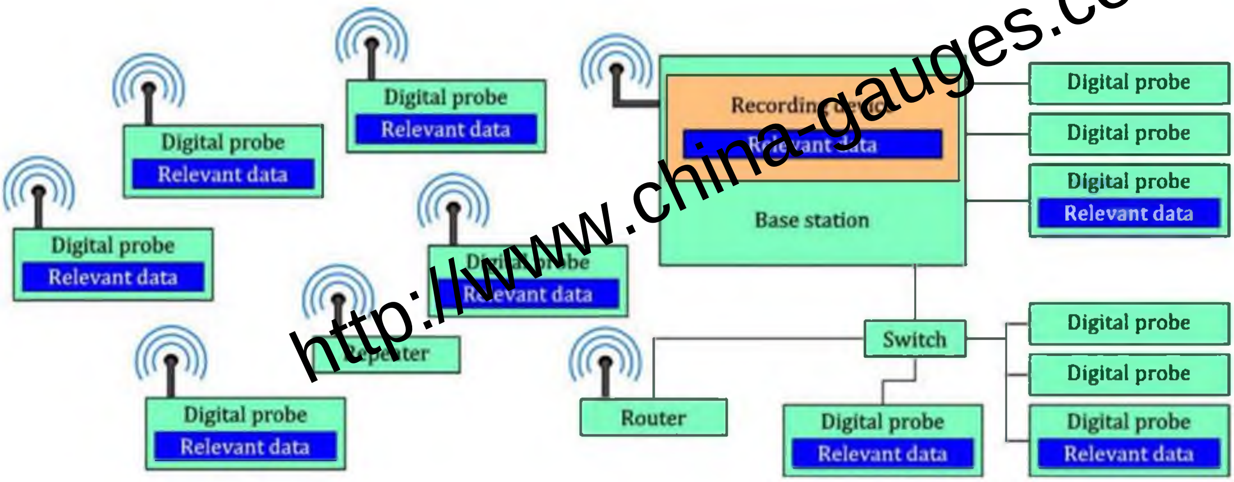

Figure 5 — Temperature recording system with wire and wireless connections

4.3.5 Temperature recorder on the cloud

An extension of 4.3.2 consists of using the cloud as the external storage medium. In that case, as Figure 6 shows, the temperature recorder system includes the transmission, processing and storage of the relevant data in the cloud.

If the data are packaged before it is sent to the cloud, transmission and storage of the encoded relevant data can be done with off the shelf applications. If that is not the case, the transmission and packaging application is instrumental to the traceability of the data, and is considered a subunit of the temperature recorder system.

There are two fundamentally different design options for the cloud server. The first is an owner hosted system and the second is the Solution as a Service (SaaS) approach.

a) *Owner hosted system*:

The cloud server and database are stored, managed and maintained by the organization owner of the temperature recorders, which is also responsible for maintaining the cloud system and ensuring its correct performance.

b) *Solution as a Service (SaaS):*

The monitoring system hardware (sensors, recorders and base stations) is installed at the organization site, but the software, server and database are hosted by a service provider. The data are collected, stored and managed by the service provider whilst the organization owner of the recorders has access to the data through a secure web interface or other remote procedure. In this scenario, the service provider ensures the cloud system maintenance, correct performance and qualification.

This solution includes all the challenges described on the previous sections. Additionally, this architecture presents the following challenge: Dimensioning, maintenance and operation of the cloud system.

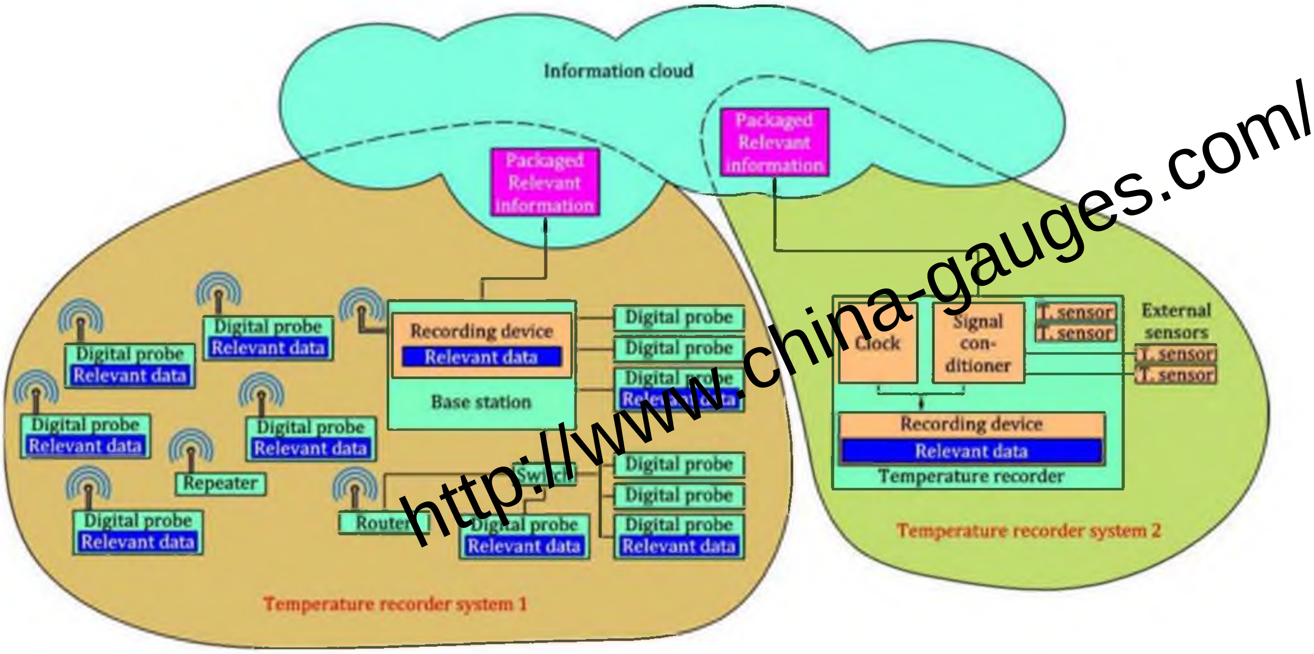

Figure 6 — Two temperature recorders with relevant data in the cloud

5 Requirements

5.1 General

The means of temperature measurement used by the recorder shall be independent of any temperature measurement which is used to control the refrigerating system.

Manufacturers shall make recommendations on the specification of ancillary equipment in order to meet the performance requirements of this European Standard.

The manufacturer shall define the use of the transport, storage and operational conditions. Examples are given in the informative Annexes C and D.

NOTE Further information is included in EN 60721-3-3 and EN 60721-2-3.

The manufacturer shall verify the defined requirements of his applications.

The system shall have the possibilities to prevent and/or detect manipulation and to prove the validity of the data;

The system shall have the possibility to log changes in the parameters that influence the relevant data for example:

a) measurement value;

b) time stamp;

c) correlation between measurement value and time stamp;

d) settings:

   1) measurement interval;

   2) measurement limits;

3) measurement mode (e.g. start/stop);

4) location.

Manipulation of the log has to be prevented and/or at least detected; the logs have to be kept at least as long as the data itself .

5.2 Measuring range

- The temperature recorder shall be able to measure in the measuring range that it is defined by the manufacturer.
- For climate classes see the relevant legislation and quality specifications.

5.3 Protection of the data from manipulation

5.3.1 General

The software shall prevent and/or at least detect both intended and not intended manipulation of the relevant data. This is true for all relevant data as long as they are managed by the measurement system, including during storage and transmission.

5.3.2 Audit trail

The software of the measurement can have an audit trail.

5.3.3 Clearly readable data copies

The software shall be able to present the relevant data in a way that is directly readable by persons or authorities in an easy way.

5.3.4 Safekeeping of accessibility of the data

The software shall have a possibility to make sure the user can access the relevant data any time, provided he/she has the rights to do so (see access restrictions 5.3.7).

- the data readability at the temperature logger shall be provided as a minimum requirement over an interface (USB, wireless, etc.), for example as pdf-file or in another digital format;

  or

- an access shall be provided directly at the display of the device at any time to display the actual recorded temperature by an (PIN) entry code in case of it's not directly accessible;

  or

- a printout of the data on an internal printer shall be provided for devices without an internal display i.e. at devices like telematic systems;

  or

- an access shall be provided by a software application for smart phone or tablets.

The informative Annex E (Table E.1) shows some examples of possible access to data and functions.

5.3.5 Safekeeping of readability of the data

The software shall have a possibility to ensure that the relevant data are directly readable by persons.

5.3.6 Safekeeping of correctness of the data

The software shall have a possibility to ensure that the data are inviolate.

5.3.7 Access restrictions

The software shall make sure that critical parts of the software can't be accessed without user verification. This means it has to have a user management system with user names and passwords to identify the users, and options to declare user rights to define various user roles (e.g. administrator vs. regular user).

5.3.8 Detailed documentation of the software

The documentation of the software shall be compiled in a way that the software mechanics are comprehensible for qualified personnel, e.g. computer scientists.

5.4 Locking of settings

The date and time of the beginning of recording shall be readable from the recorded data or it shall be possible to make them readable.

The possibility for adjusting settings which configure the recording shall:

— either be protected against accidental or unauthorised modifications;

— or record each adjustment of any settings that remain accessible.

5.5 Recording

5.5.1 General

At least the temperature and the time shall be recorded. The record shall also indicate the date and the time zone e.g. GMT or UTC. Other information as the place of measurement (e.g. return air, back door) could be also recorded, however it shall not impact the temperature data.

5.5.2 Traceability

It shall be possible to identify and retrieve the recorded data. It shall be possible to read those data, intended for archiving for a period of at least a year.

The recorder shall allow the user to keep the data for at least one year.

After one year the responsibility for the recorded values should be managed between the contracting parties within the cold chain for the different goods after the transfer in regards to relevant regulations and quality requirements including enlarged storage periods i.e. pharmaceutical products, EU food regulations and others.

The manufacturer of the device shall define instructions in its documentation for operation and maintenance taking in account, i.e. life time of batteries, storage periods and operational limitations of the device.

5.5.3 Chart only for mechanical recorder

The scrolling speed of the chart shall be greater than or equal to:

- for transport:
  - 6 mm/h for a recording duration lower than or equal to 24 h;
  - 2 mm/h for a recording duration higher than 24 h and lower than or equal to 7 d;
  - 0,5 mm/h for a recording duration higher than 7 d.

  The choice of the recorder shall be made according to the use, including the duration of transport.

- for storage: 1 mm/h.

The speed shall be verified on the following graduations:

- −20 °C for deep-frozen applications;
- 0 °C for chilled applications.

5.6 Autonomous power supply

For devices with an autonomous power supply, this shall be indicated on the recorder or on the power supply or in the technical documentation, with the corresponding usage temperature.

The manufacturer is recommended to install an indicating device (warning light or message) warning the user that the power source needs replacing.

The battery lifetime shall be indicated by the manufacturer for relevant operation temperatures taking into account typical operation of e.g. display, transmission of data, LEDs, number and kind of sensors (see 5.9.2).

NOTE See also Annex D.

The manufacturer shall indicate, if the battery is fixed or replaceable and/or rechargeable.

5.7 Degree of protection provided by the enclosure

The minimum degree of protection provided by the enclosure shall be:

- IP 20 for recorders used in heated/air conditioned closed premises or in the cabin of transport vehicles ;
- IP 55 for recorders used inside cold enclosures (storage or transport vehicles) and for external sensor ;
- IP 65 for recorders used outside buildings or transport vehicles, with sensor inside the cold enclosure.

5.8 Electrical safety (if applicable)

The recorder shall conform to the requirements of EN 61010-1.

5.9 Operating characteristics linked to external electrical influences

5.9.1 External supply voltage (if applicable)

A recorder which requires an external electrical supply shall be suitable for connection to one of the supplies given in Table 1.

Table 1 — Limits of external supply voltage

Alternating current (AC)	U_n	+ 10 %, - 15 %	
Direct current (DC)	U_n	Rated operating conditions	Limiting conditions
	12 V	10 V to 16 V	0 V to 18 V
	24 V	20 V to 32 V	0 V to 36 V

The recorder shall indicate the possible losses of data. The manufacturer shall indicate the remaining recording period in case of interrupted power supply.

External accessories should take into account the requested power consumption of the recorder using the same power source (e.g. battery of vehicle)

5.9.2 Autonomous supply (if applicable)

The manufacturer shall specify the operating time without external power at a reference temperature. The device shall give an indication if the battery status is low.

5.9.3 Frequency (AC) (if applicable)

The manufacturer shall specify the operating frequency with a tolerance of ± 3 Hz.

5.9.4 Power cut-offs

The recorded data shall not be lost during a power cut-off. The manufacturer shall state the duration for which the data are protected when the recorder is disconnected from the primary source of power.

5.9.5 Electrical power disturbances and susceptibility to radiated electromagnetic field

The recorder shall conform with the requirements of EN 61000-6-2 and EN 61000-6-3, or any other specific standard, if applicable.

5.10 Metrological characteristics and usage profiles

5.10.1 General

The metrological characteristics of the recorders result from usage profiles which determine the operating criteria.

5.10.2 Metrological characteristics

5.10.2.1 Maximum permissible errors and resolution

The recorder, under rated operating conditions, shall conform to at least one of the classes indicated in Table 2.

Table 2 — Accuracy classes

Class	0,2	0,5	1	2
Maximum permissible errors	±0,2 °C	±0,5 °C	±1 °C	±2 °C
Resolution	< 0,1 °C	< 0,2 °C	≤ 0,5 °C	≤ 1 °C

5.10.2.2 Operational requirements

Temperature recorders for the transport, storage and distribution of chilled, frozen, deep-frozen/quick-frozen food and ice-cream should have the minimum accuracy class 0,5 within the temperature range of −25 °C to + 7 °C.

NOTE E.g. red meat at + 7 °C, frozen butter at −10°C, deep-frozen/quick-frozen food, e.g quick frozen fish at −18 °C and ice-cream at −20 °C.

For traceability a minimum storage time for frozen food application of 1 year is required. This does not refer to the storage capacity of the measurement instrument.

5.10.2.3 Recording interval and storage capacity

The manufacturer shall define the recording intervals, periods and storage capacity with its minimum and maximum limits. The maximum time window for calculated temperatures shall be measured with 5 % of the recording interval and a maximum period of 15 min.

If there is any possibility of overwriting the recorded values it shall be indicated by the manufacturer.

Information is given in informative Annex D.

The recording intervals do not apply to recorders where the record is only printed in a chart or printed as values on paper.

5.10.2.4 Maximum relative timing error

The maximum relative timing error shall be:

— 0,1 % of the recording duration when the date is reset up to 31 d ;

— 0,02 % of the recording duration including the error of the date and time when the date is reset after 31 d.

5.10.2.5 Response time

The response time shall be:

— for recorders with external air sensors maximum 5 min;

— for recorders with internal sensors maximum 20 min.

The response time is the time needed for the recorded value to reach 90 % of the actual change of applied temperature in the conditions mentioned in 6.4.

5.10.3 Usage profiles

5.10.3.1 Climatic environment

The manufacturer shall give a clear statement for the climatic environmental limits for:

— the complete temperature recorder or each individual subunit of the temperature recorder;

— specified temperature ranges for batteries including their expected operation lifetime at certain temperatures (including minimum and maximum of operating temperature) and at specific recording intervals (see 5.10.2.3).

5.10.3.2 Mechanical vibrations

Equipment for use on transport vehicles shall be able to operate in the following environment conditions:

— vibration frequency: 5 Hz to 8,6 Hz ; displacement amplitude: 10 mm;

— vibration frequency: 8,6 Hz to 150 Hz ; acceleration: 3 g.

5.10.3.3 Shock resistance

Equipment for use on transport vehicles shall be able to operate in the conditions as defined in 6.6.6.

5.10.3.4 Different versions and combinations of components

The manufacturer shall give a clear description of possible combinations and versions of devices, interfaces and sensors including e.g. connectors, length of wires and distances (maximum equipment).

5.11 Data security

The data shall be protected against alteration.

5.12 Software verification levels

Depending on the type of application and on the type of system, these systems have to comply with one of the software verification levels described in the following Tables 3 and 4.

Table 3 — Software verification levels for recorders without cloud Solution as a Service (SaaS) approach

Level	No level	I[a]	II[a]	III[a]
Type of system	Mechanical systems	Electronic systems	Electronic systems	Electronic systems
Requirements	-	According to subclauses 5.1, 5.3, 5.4, 5.5 and 6.7	According to subclauses 5.1, 5.3, 5.4, 5.5 and 6.7	According to subclauses 5.1, 5.3, 5.4, 5.5 and 6.7 and Annex A
Verification	-	Compliance with manufacturer declaration	Compliance with manufacturer's declaration and test report	Compliance with the additional requirements given in Annex A

[a] Systems without cloud Solution as a Service (SaaS).

Table 4 — Software verification levels for recorders with cloud Solution as a Service (SaaS) approach

Level	No level	I[b]	II[b]	III[b]
Type of system	Mechanical systems	Electronic systems	Electronic systems	Electronic systems
Requirements	-	According to subclauses 5.1, 5.3, 5.4, 5.5 and 6.7	According to subclauses 5.1, 5.3, 5.4, 5.5 and 6.7	According to subclauses 5.1, 5.3, 5.4, 5.5 and 6.7 and Annex A
Additional requirement for the SaaS		For example compliance with ISO/IEC 27001	For example compliance with ISO/IEC 27001	For example compliance with ISO/IEC 27001
Verification	-	Compliance with manufacturer declaration	Compliance with manufacturer's declaration and test report	Compliance with the additional requirements given in Annex A

[b] Systems with cloud Solution as a Service (SaaS).

6 Test methods

6.1 Test list

The recorder shall be subjected to the tests listed in Table 5.

Table 5 — Tests and applications

Tests	Storage	Transport	Subclause
- Determination of temperature measurement error	+	+	6.3
- Determination of response time	+	+	6.4
- Determination of time recording error	+	+	6.5
- Variation in supply, voltage [a]	+	+	6.6.2
- Dielectric strength [a]	+	+	6.6.9
- Influence of ambient temperature	+	+	6.6.3
- Temperature testing for the recorder under storage and transport conditions	+	+	6.6.4
- Shock resistance		+	6.6.5
- Mechanical vibrations		+	6.6.6
- Degrees of protection provided by enclosure	+	+	6.6.7
- Electromagnetic compatibility (EMC) [a, b]	+	+	-
- Software test [a]	+	+	6.7

[a] If applicable.

[b] The recorder shall conform with the requirements of EN 61000-6-2 and EN 61000-6-3 or any other specific standard when applicable.

6.2 General conditions for tests

6.2.1 Pre-tests adjustments

The tests shall be carried out without change to the adjustments made in the factory by the manufacturer. All elements of the recorder shall be put in place according to the manufacturer's instructions.

When possible or necessary the recorder is configured in order to conduct the following tests.

6.2.2 Normal atmospheric conditions

Unless otherwise prescribed the tests are carried out in the atmospheric conditions defined as follows:

- Temperature: 23 °C ± 3 °C measured at 10 cm from the recorder;
- relative humidity: 60 % RH ± 20 % RH;
- atmospheric pressure: To be indicated as measured.

Before testing the recorders are placed in these conditions for 24 h. The charts and ink devices are stored in these conditions.

6.2.3 Reference conditions

The reference conditions for the tests are given in Table 6.

Table 6 — Reference conditions for the tests

Influence quantity	Reference conditions	Tolerance
Supply voltage [a]	Nominal voltage	±2 %
Frequency [a]	Nominal frequency	±1 %
Position	Defined by the manufacturer	±2 %
Recorder support vibrations	< 0,5 g	
Chart	Supplied by the manufacturer	
[a] If applicable.		

6.3 Determination of temperature measurement error

6.3.1 Test method

The temperature sensor, or the recorder when the sensor is internal, is placed:

- either in an enclosure with forced air circulation at 1 m/s ± 0,3 m/s;
- or in a thermostatic bath. The manufacturer shall state whether the equipment is designed to be immersed.

To validate if the operational measuring range of the declared accuracy classes (see 5.10.2.1) can be fulfilled.

For a cycle of measurements, the temperature is successively held at 0 %, 50 %, and 100 % of the span, or at the following fixed values: – 30 °C, 0 °C and + 30 °C if the span is greater than those values.

For electronic recorders, one cycle is carried out with increasing and then decreasing values.

For mechanical recorders, three similar cycles are carried out.

The stabilization time of the recorder for each temperature value is at least 1 h, or a duration sufficient to obtain temperature stabilization of the enclosure or thermostatic bath better than the resolution of the recorder under test.

The temperature surrounding the sensor is measured with at least one standard thermometer.

6.3.2 Reading the recording

Following the test, the recorded values are read using devices provided by the manufacturer.

6.3.3 Expression of results

The errors at each temperature value shall be tabulated and all shall fall within the maximum permissible errors for the class of the recorder.

These values shall be given with the uncertainty of the measurement.

Table 7 — Maximum uncertainty of the reference equipment

Class	0,2	0,5	1	2
Maximum uncertainty of the reference equipment	±0,1 K	±0,25 K	±0,5 K	±1 K
NOTE The maximum uncertainty mentioned in this table reflects all components of uncertainty associated with the calibration and use (recording, sensor, cable, drift, calibration, resolution, ...). A coefficient k = 2 is used to indicate uncertainty.				

6.4 Determination of response time

For this test, the recording interval shall if possible be held at its minimum value. The temperature sensor of the recorder is initially placed at a temperature at 25 °C measured using a working standard thermometer.

The recorder sensor is placed as rapidly as possible in an air flow the temperature of which is stabilized at a value that is 20 K lower and/or higher than the initial temperature with regard to the specified operation temperature.

The air speed is 1 m/s ± 0,3 m/s.

The response time is the time needed for the recorded value to reach 90 % of the actual change of applied temperature.

6.5 Determination of time recording error

If applicable recording device using diagrammatic charts is started before the beginning of the measurement, for a time sufficient to take up any mechanical play.

Since time instruments are sensible to their operational temperature, the test should be performed for each of the following three reference conditions:

a) device minimum operated conditions as specified by manufacturer;

b) device maximum operated conditions as specified by manufacturer;

c) device normal or average operated conditions.

For this test the recording interval shall if possible be held at its minimum value.

The device is placed in reference conditions. The elapsed time is measured using a suitable reference clock.

The reference clock should be a suitable calibrated clock.

The beginning and the end of the time recording duration are defined by any one of the following methods:

— Method 1: A sudden variation in the temperature measured;

— Method 2: An automatic or manual data gathering event that should record both the unit time

and the reference clock time with a maximum skew of one second and a resolution of one second.

The test is carried out during a recording duration of at least three days for method 1 and at least 6 h for method 2.

If applicable, the correspondence between the real time and the time recorded is checked.

The requirements of 5.10.2.4 shall be satisfied.

The error value shall be tabulated and all shall fall within the maximum permissible error. This value shall be given with the uncertainty of the measurement

6.6 Action of influence quantities

6.6.1 General

Unless otherwise indicated, during or at the end of these tests, the determination of the temperature measurement error is carried out using the method given in 6.3 but with only one cycle.

6.6.2 Variation in voltage supply (if applicable)

The temperature measurement error is determined while supplying the recorder successively at the minimum and maximum value of the rated operating conditions.

For each value of the supply voltage, the pre-heating time is one hour at the minimum.

The measurement errors shall not exceed the maximum permissible errors in 5.10.2.1.

6.6.3 Influence of ambient temperature

6.6.3.1 General

The recorder is subjected to its limiting temperatures, and then, the measurement performance is tested at the maximum and minimum operating temperatures.

6.6.3.2 Test applicable to recorders with external sensor

The recorder in operation is placed in a case which is brought successively through the temperature phases of the Table 8.

Table 8 — Phases for recorder with external sensor

Phase	Temperature
1	Maximum limiting temperature
2	Maximum operating temperature
3	Minimum limiting temperature
4	Minimum operating temperature

Each phase shall last a minimum 4 h.

The temperature measurement error is determined during phases 2 and 4 with the enclosure maintained at the maximum and minimum operating temperatures stabilized within ± 2 °C.

6.6.3.3 Test applicable to recorders with internal sensor

The recorder in operation is placed in a case which is brought successively through the temperatures phases of the Table 9. The ambient temperature shall be stabilized within ± 2 °C.

Table 9 — Phases for recorder with internal sensor

Phase	Temperature
1	Maximum limiting temperature
2	Minimum limiting temperature

Each phase shall last a minimum of 4 h. Following the test, the temperature measurement error is determined after a resettling time of 4 h at the reference temperature. (23 °C ± 3 °C).

6.6.4 Temperature testing under storage and transport conditions for the recorder

The test shall be carried out under the following conditions:

- the recorder is not in operation;
- minimum and maximum temperatures for storage and transport conditions defined by the manufacturer;
- temperature variation speed is 1 °C/min;
- air speed is between 1m/s and 2 m/s;
- dwell time: 3 h;
- number of cycles is 5.

Following the test, the temperature measurement error is determined after a resettling time of 2 h at the reference temperature.

6.6.5 Shock resistance test (if applicable)

The test shall be carried out according to the method of EN 60068-2-27 under the following conditions:

- acceleration: 10 g;
- time duration: 10 ms;
- recorder in normal operating position;
- number of shocks: 1.

If there is more than one operating position, the test shall be repeated for each of the operating positions. The shock is applied in the upward vertical direction.

Following the test, the temperature measurement error is determined after a resettling time of 2 h at the reference temperature.

6.6.6 Mechanical vibrations (if applicable)

The test applies to the recorder and its temperature sensor.

The recorder is in operation during the entire duration of the test.

The internal or external temperature sensor is kept at a constant temperature within the span.

The equipment under test is attached to the vibration table by means of a rigid component which holds the device by its usual system of attachment.

The recorder is subjected to sinusoidal rectilinear vibrations that are applied to it in three trirectangular directions. The sweep (frequency range path) is continuous and its speed is logarithmic according to time (1 octave/min).

Twenty successive sweep cycles are carried out in each of the three directions.

During the test all resonance phenomena are observed.

After the test, the variations in the value recorded during the test are determined.

6.6.7 Degrees of protection provided by enclosures (IP Code)

The degrees of protection provided by the enclosures of the recorder (see 5.7) and any external temperature sensor are checked following the methods defined in EN 60529.

NOTE The enclosure is that of the device in working conditions, i.e. including connectors (with possible stoppers), packing box or other accessories.

6.6.8 Electrical safety (if applicable)

The manufacturer shall confirm that the recorder conforms to the requirements of EN 61010-1.

6.6.9 Dielectric strength (if applicable)

The test voltage is applied for 1 min between the two supply wires joined together and the earth terminal of the device linked to the metal envelope of an external sensor and to accessible metallic parts.

The test voltage shall be:

- As specified in EN 61010-1, for recorders supplied with external AC power source;
- 500 V, rms value, 50 Hz, for recorders supplied with external DC power source.

6.7 Software test

6.7.1 Test objective

The objective of this test is to determine the software suitability for the temperature recorder to fulfil the requirements established in Clause 5.

The test will be based on the analysis of the temperature recorder design documentation and user documentation as well as by performing tests to check the temperature recorder functionality.

The test will be performed for a specific software version. Any software modification will require a new test and a new software version. For simple modifications this test could be restricted to the software modules been modified.

6.7.2 Test procedure

6.7.2.1 Test organization

The test is organized into the following blocks:

- G: General
- T: Transmission of relevant data via Communication Networks
- S: Software Separation
- D: Download of relevant software

Block G applies to all units or subunits with relevant software.

Block T applies to units or subunits involved in the transmission of relevant data via communication networks. It has to be used only if relevant data are transmitted via communication networks to a distant device where it is further processed and/or stored maintaining its relevant status. This extension does not apply if there is no subsequent relevant status.

It applies, for example to the transmission between a digital probe and a base station or the transmission to the cloud. It does not apply, for example, when exporting data with traceability loss for fleet or warehouse management.

Block S applies when relevant software cohabits with non-relevant software.

Block D applies when the unit or subunit can download a new relevant software on-field.

6.7.2.2 Determine test objects and applicable test blocks

The test includes a series of steps described below. Depending on the temperature recorder architecture and design, some of the steps could be non-applicable.

6.7.2.3 Determine the temperature recorder and its subunits

As described in 4.3 the temperature recorder can be a single compact unit or can be composed by several different subunits. The subunits that compose the temperature recorder have to be clearly determined.

All the temperature recorder units or subunits that include software will be subjected to this software test; see also 6.7.1.

6.7.2.4 Determine the relevant software

For each unit or subunit under test determine its relevant software and define if the relevant software cohabits with non-relevant software, see 4.1. This has to be determined by the manufacturer.

6.7.2.5 Determine the applicable test blocks

For each unit or subunit under test determine the applicable testing blocks (T, S and D). Block G is always required.

6.7.2.6 Test block G: General

6.7.2.6.1 Documentation completeness

Check that the documentation provided by the manufacturer for each of the temperature recorder and the subunits including the following items:

- a software description, including main software components and its interactions, main data structures and off the shelf components;
- the user manual and any other user documentation;
- a hardware overview, including main components such as processor, memory, user interface and communication ports;
- the software documentation shall include relevant commands that impact on measure and storage when modifications are made.

6.7.2.6.2 Software identification

Check that the software includes a clear identification that is presented on command or during operation e.g. version number of the software and date of issue.

6.7.2.6.3 Influence via user interface

Verify the relevant commands for their impact over the software behaviour and relevant data to ensure that any possible impact is admissible. Verify whether the software mechanism to refuse non-conforming commands is adequate. Test all menu items. Try undocumented commands: e.g. combinations of functions and key combinations.

6.7.2.6.4 Influence via communication interface

Verify relevant commands for their impact over the software behaviour and relevant data to ensure that any possible impact is admissible. Verify whether the software mechanism to refuse non-conforming commands is adequate. Test commands: e.g. with a command emulator. Try undocumented commands, e.g. with a command emulator.

6.7.2.6.5 Protection against accidental or unintentional changes

Verify whether the documented protection mechanisms included in the software, such as watch dogs and software auto check at reset are adequate. Verify the storage procedure to ensure that overwriting of relevant data cannot occur before the end of the data storage period. Verify the relevant data error detection or correction mechanism for its suitability. Check that data are not lost on reset or power off. Check that a warning is issued to the user if he is about to delete relevant data.

6.7.2.6.6 Protection against intentional changes

Verify whether the documented means of securing against unauthorized modification of the memory that contains relevant software or relevant data are sufficient.

6.7.2.6.7 Parameter protection

Check that relevant parameters are adequately protected. For relevant parameters that the user can modify check that the modification procedure has a protection mechanism and that for each change the old value, new value and timestamp are logged as relevant data.

6.7.2.6.8 Completeness of relevant data stored

Check whether all relevant data items are contained within the stored data structures.

6.7.2.6.9 Authenticity of measurement data stored

Verify whether the documented relevant data storage and retrieval mechanisms ensures traceability.

6.7.2.6.10 Storage capacity

Verify the storage formats and the storage media size to determine that its capacity is adequate to store all the relevant data.

6.7.2.7 Test block T: Transmission of measurement data via Communication Networks

6.7.2.7.1 Completeness of transmitted data

Verify the transmission procedure to ensure that all the relevant data will be sent and received, and that not relevant data will be deleted on the sending subunit without ensuring that it is completely stored on the receiving subunit.

6.7.2.7.2 Protection against accidental or unintentional changes

Verify the documented transmitted data error detection or correction mechanism for its suitability.

6.7.2.7.3 Integrity of data

Verify the documented transmission mechanism to ensure that the relevant data are protected against intentional changes.

6.7.2.7.4 Authenticity of transmitted data

Verify the documented transmission mechanism to ensure that it prevents identity impersonation and is properly identified and authenticated.

6.7.2.7.5 Confidentiality of keys

Verify the measures taken to prevent the secret information to be compromised.

6.7.2.7.6 Handling of corrupted data

Verify the measures taken to prevent the use of corrupted data.

6.7.2.7.7 Availability of transmission services

Verify the measures taken to prevent data loss in case of unavailability of transmission services.

Check the unit performance with a broken channel.

6.7.2.8 Test block S: Software Separation

6.7.2.8.1 Realization of software separation

Verify the software design to ensure that all the code and data structures related to the relevant data are contained within the relevant software.

6.7.2.8.2 Protective software interface

Verify the description of the protective interface between the relevant and non-relevant software to ensure that the interface comprises all the interactions and data flows between relevant and non-relevant parts. Verify the description of the protective interface between the relevant and non-relevant to ensure that the non-relevant part cannot negatively affect the performance and data of the relevant part. For each command supplied by the relevant part, verify the defence mechanism against corrupted or nonconforming parameters.

6.7.2.9 Test block D: Download of relevant software

6.7.2.9.1 Download mechanism

Verify the downloading procedure to ensure that the downloading and installation are done automatically. Verify the design documentation to ensure that integrity and authenticity checks are performed by non-downloadable fixed software. Verify the downloading procedure to ensure that no relevant data are loss and that no erroneous data are generated during the downloading and installing processes. Perform a downloading process.

6.7.2.9.2 Authentication of downloaded software

Verify the authenticity method used and how a download of fraudulent software is prevented.

Perform a downloading process with fraudulent software.

6.7.2.9.3 Integrity of downloaded software

Verify the integrity check performed by the non-downloadable fixed software to ensure that the downloaded software has not been inadmissibly changed during download.

6.7.2.9.4 Traceability of relevant software download

Verify the documentation to ensure that traceability means are implemented and protected.

Perform a downloading process and check the traceability.

6.7.2.10 Solution as a Service (SaaS)

According to 5.12, "Software verification levels", the provider of a Solution as a Service (SaaS) has to comply with ISO/IEC 27001.

Communications from customer's instruments to the SaaS have to be checked according to 6.7.2.7, "Test block T: Transmission of measurement data via Communication Networks." This will be done normally while performing test of the instruments that connect to the SaaS, therefore no additional tests will be required.

For any additional means of communications to the SaaS not covered by the instruments tests there are two possibilities:

— The channel will transmit relevant data that will maintain its relevant status. In that case it has to be checked according to 6.7.2.7, "Test block T: Transmission of measurement data via Communication Networks" and 6.7.2.6.4, "Influence via communication interface";

— If the transmitted data does not maintain its relevant status, it only has to be checked according to 6.7.2.6.4, "Influence via communication interface".

Regarding the communication via a web service the additional test has to be performed:

— 6.7.2.6.3, "Influence via user interface".

7 Conditions of acceptance

7.1 Requirements

The recorder shall correspond with the characteristics set out in Clause 4.

7.2 Operating error limits

The maximum error values shall be less than or equal to maximum permissible errors as given in Table 2 for the class specified by the manufacturer.

8 Marking

Each temperature recorder shall be marked, clearly, permanently and in the indicated order on the housing of the recorder, with the following indications:

- reference of this European Standard;
- name of the manufacturer or trade mark;
- individual identification of the product;
- suitability for storage (S) or transport (T);
- accuracy class (0,2; 0,5; 1 or 2);
- software classes “no level”, I, II or III;
- measuring range in degree Celsius.

Each sensor separable from the recorder shall carry identification marks which permit, directly or indirectly, determination of its conditions for use with the recorder.

9 Initial and periodic verification

The temperature recorder and/or the subunit with the exception of single use data loggers, when in service, shall be verified periodically in accordance with EN 13486.

The verification shall be in line with the requirements of EN ISO/IEC 17025.

Annex A
(normative)

Software testing

A.1 Software test general part – Test objective

The objective of this test is to determine the software suitability for the temperature recorder to fulfil the requirements established in Clause 5.

The test will be based on the analysis of the temperature recorder design documentation and user documentation as well as by performing functional tests to check the temperature recorder behaviour.

The test will be performed for a specific software version. As defined in A.3.2.3, "Software identification" modifications of the relevant software will require a new test and a new software version. For simple modifications this test could be restricted to the software modules been modified.

This test procedure is based on the guide WELMEC 7.2, issue 5 Risk Class C (www.welmec.org).

A.2 Test procedure

A.2.1 General

The test includes a series of steps described below. Depending on the temperature recorder architecture and design, some of the steps could be non-applicable.

A.2.2 Determine the temperature recorder subunits

As described in 4.3, "Temperature recorder architecture" the temperature recorder can be a single compact unit or can be composed by several different subunits.

The subunits that compose the temperature recorder have to be clearly determined.

All the temperature recorder subunits that include software will be subjected to this software test.

A.2.3 Determine the relevant software of each unit or subunit

For each unit or subunit under test determine the relevant software and define if the relevant software cohabits with non-relevant software.

A.2.4 Define the applicable test blocks of each unit or subunit

The tests are organized into the following blocks:

- Block G: Basic requirements;
- Block L: Specific software requirements for Long-term Storage;
- Block T: Transmission of relevant information via Communication Networks;
- Block S: Software Separation;
- Block D: Download of relevant software.

Block G applies to all units or subunits with relevant software.

Block L applies to the units or subunits that store relevant data.

Block T applies to units or subunits involved in the transmission of relevant data via communication networks. It has to be used only if relevant data are transmitted via communication networks to a distant device where it is further processed and/or stored maintaining its relevant status. This extension does not apply if there is no subsequent relevant status.

It applies, for example to the transmission between a digital probe and a base station or the transmission to the cloud. It does not apply, for example, when exporting information with traceability loss for fleet or warehouse management.

Block S applies when relevant software cohabits with non-relevant software.

Block D applies when the unit or subunit can download a new relevant software on-field.

A.2.5 Determine the type of each unit or subunit

For each unit or subunit under test determine its Type.

Type P1: The relevant software is embedded in a closed hardware (see table below).

Type P2: The relevant software runs on a general purpose computer managed by the recorder user,

Type P3: The relevant software runs on an external provider of this service (solution as a service (SaaS)).

A type P1 instrument is a measuring instrument with an embedded IT system (in general it is a microprocessor or microcontroller based system). It is characterized by the following features:

- The entire application software has been constructed for the measuring purpose. This includes both functions subject to control (relevant software) and other functions (non-relevant software);
- The user interface is dedicated to the measuring purpose, i.e. it is normally in an operating mode subject to control. Switching to an operating mode not subject to control is possible;
- If there is an operating system, it has no user shell that is accessible to the user (to load or change programs, send commands to the OS (operation system), change the environment of the application etc.).

The P1 type instrument may have additional properties and features that are covered by the following requirement extensions:

- The software is designed and treated as a whole, unless software separation according to Block S has been observed;
- The software is invariable and there are no means for programming or changing the relevant software. Software download is only allowed if Block D is observed;
- Interfaces for transmission of measurement data via open or closed communication networks are allowed (Block T to be observed);
- The storage of measurement data either on an integrated storage, on a remote or on removable storage is allowed (Block L to be observed).

To declare the unit as type P1, use the Table A.1.

Table A.1 — Decision on instrument type

Decision on instrument type				
		A	Y/N	Remarks
1	Is the entire application software constructed for the measuring purpose?	(Y)	Y/N	Include reasons
2	If there is general-purpose software, is it accessible by or visible to the user?	(N)	Y/N	Include reasons
3	Is the user prevented from accessing the operating system if it is possible to switch to an operating mode not subject to control?	(Y)	Y/N	Include reasons
4	Are the implemented programs and the software environment invariable (apart from updates)?	(Y)	Y/N	Include reasons
5	Are there any means for programming?	(N)	Y/N	Include reasons

If and only if all answers to the 5 questions can be given as in the A column, then the subunit can be considered of type P1.

A.3 Software test for type P1 and type P2

A.3.1 General

Section G is always required, whereas section L, T, S and D are required if the specific extension applies to the unit or subunit.

A.3.2 Block G: Basic requirements

A.3.2.1 General

The set of requirements of this chapter applies to all the temperature recorder units or subunits. Some additional items area marked as type P2, these items are not required for type P1.

Specific software requirements

A.3.2.2 Documentation

In addition to the specific documentation required in each requirement below, the documentation shall at least include:

- A description of the relevant software;
- a description of the accuracy of the measuring algorithms;
- a description of the user interface, menus and dialogues;
- a clear software identification;

- an overview of the system hardware, e.g. topology block diagram, type of computer(s), type of network, memory, etc., if not described in the operating manual;
- an overview of the parts of the operating system used, security aspects of the operating system utilised, e.g. protection, user accounts, privileges, etc;
- the operating manual.

A.3.2.3 Software identification

The relevant software shall be clearly identified. An identification of the software shall be inextricably linked to the software itself. It shall be determined and presented on command or during operation.

a) Specifying notes:

   1) Each change to relevant software requires a new relevant software identification;

   2) The software identification has to be easily shown for verification and inspection purposes (easily means by standard user interface, without additional tools.)

   3) The software identification shall have a structure that clearly identifies versions of the relevant software;

   4) If functions of the software can be switched by type-specific parameters, each function or variant may be identified separately or, alternatively, the complete package may be identified as a whole;

   5) If the relevant functions and the account of the measuring task are protected by a specific configuration of the operating system, the relevant configuration files shall have an additional identification.

b) Required documentation:

   The documentation shall list the software identifications and describe how the software identification is created, how it is inextricably linked to the software itself, how it may be accessed for viewing and how it is structured in order to differentiate between version changes with and without requiring a software test.

c) Validation guidance:

   Checks based on documentation:

   1) Examine description of the generation and visualization of the software identification

   2) Check whether all programs performing relevant functions are clearly identified and described so that it is clear which software functions are covered by the software identification and which are not.

   3) Check whether a nominal value of the identification (version number or functional checksum) is supplied by the manufacturer. This has to be quoted in the test certificate.

Functional checks:

4) The software identification can be visualized as described in the documentation.

5) The presented identification is correct.

d) Example of an acceptable solution:

1) The identification of relevant software comprises two parts:

   i) Part (A) has to be changed, if changes to the software require a new test.

   ii) Part (B) indicates only minor changes to the software, e.g. bug fixes, which need no new test.

2) The identification is generated and displayed on command.

3) Part (A) of the identification consists of an automatically generated checksum over the fixed code. For other relevant software, part (A) is a version number or the number of the test certificate. To prevent it from being changed with simple software tools, it is stored in binary format in the executable program file.

4) An acceptable solution for performing the checksum is the CRC-16.

NOTE (Definition:) cyclic redundancy check (CRC) is used in digital network and storage devices to detect accidental changes to raw data as an error-detection code with a polynomial length at 17 bits.

A.3.2.4 Influence via user interfaces

Commands entered via the user interface shall not inadmissibly influence relevant software and relevant data.

a) Specifying notes:

1) This implies that there is an unambiguous assignment of each command to an initiated function or data change.

2) This implies that switch or key actuations that are not declared and documented as commands have no effect on the instrument's functions and relevant data.

3) Commands may be a single action or a sequence of actions carried out by the operator. The user shall be guided which commands are allowed.

4) For type P2. Functions for changing the relevant configuration of the operating system shall not be offered to the user neither locally nor remotely. The configuration shall be secured against inadmissible changes.

b) Required documentation:

The documentation shall include:

1) A complete list of all commands together with a declaration of completeness.

2) A brief description of their meaning and their effect on the functions and relevant data of the recorder.

3) For type P2. A description how a secure configuration of the operating system is achieved. Assignment of roles (accounts) in the operating system (e.g. "administrator", "user", "Measuring Task"). Assignment of permissions granted to these roles.

4) For type P2. A documentation of remote control of the functions of the operating system (e.g. started services) and means for protection (e.g. configuration of a firewall).

c) Validation guidance:

Checks based on documentation:

1) Judge that documented commands are admissible, i.e. that they have an allowed impact on the measuring functions and relevant data or none at all.

2) Check that manufacturer has supplied an explicit declaration of completeness of the command documentation.

3) For type P2. Check the measures to secure the operating system

Functional checks:

4) Carry out practical tests (spot checks) with both documented and undocumented commands. Test all menu items if any.

d) Acceptable solution:

1) A module in the relevant software filters out inadmissible commands. Only this module receives commands, and there is no circumvention of it. Any false input is blocked. The user is controlled or guided when inputting commands by a special software module. This guiding module is inextricably linked with the module that filters out the inadmissible commands.

2) For type P2: For using the measuring system, only an account with restricted permissions is set up. Access to the administrator account is blocked according to A.3.2.7, "Protection against intentional changes".

A.3.2.5 Influence via communication interface

Commands inputted via communication interfaces of the instrument shall not inadmissibly influence the relevant software and measurement data.

a) Specifying notes:

1) This implies that there is an unambiguous assignment of each command to an initiated function or data change.

2) This implies that signals or codes that are not declared and documented as commands have no effect on the instrument's functions and data.

3) Commands may be a sequence of electrical (optical, electromagnetic, etc.) signals on input channels or codes in data transmission protocols.

4) The restrictions of this requirement are suspended when a software download according to A.3.6, "Block D: Download of relevant software" is carried out.

5) This requirement applies only on interfaces that are not sealed.

6) For type P2: The respective parts of the software that interpret relevant commands shall be considered relevant software.

7) For type P2: Other software parts may use the interface provided they do not disturb or falsify the reception or transmission of relevant commands or data.

8) For type P2: If the operating system allows remote control or remote access, the requirements A.3.2.4, "Influence via user interfaces" apply to the communication interface and the connected remote terminal respectively. Additionally A.3.4, "Block T: Transmission of measurement data via Communication Networks" shall be taken into consideration for the transmission between computer and terminal.

b) Required documentation

The documentation shall include:

1) A complete list of all commands together with a declaration of completeness.

2) A brief description of their meaning and their effect on the functions and data of the measuring instrument.

3) For type P2: Description how a secure configuration of the operating system is achieved. Assignment of roles (accounts) in the operating system (e.g. "administrator" and "user"). Assignment of permissions granted to these roles.

4) For type P2: Documentation of remote control of the functions of the operating system (e.g. started services) and means for protection (e.g. configuration of a firewall).

c) Validation guidance:

1) Checks based on documentation:

i) Judge whether all documented commands are admissible, i.e. whether they have an allowed impact on the relevant software and relevant data or none at all.

ii) Check whether the manufacturer has given an explicit declaration of completeness of the command documentation.

iii) For type P2: Check the measures to secure the operating system.

2) Functional checks:

i) Carry out practical tests (spot checks), using peripheral equipment, if available.

d) Example of an acceptable solution:

1) There is a software module that receives and interprets commands from the interface. This module belongs to the relevant software. It only forwards allowed commands to the other relevant software modules. All unknown or not allowed commands are rejected and have no impact on the relevant software or measurement data.

2) For type P2: The access to the operating system via the interfaces is restricted (see A.3.2.4, "Influence via user interfaces" and A.3.2.7, "Protection against intentional changes").

A.3.2.6 Protection against accidental or unintentional changes

Relevant software and measurement data shall be protected against accidental or unintentional changes.

a) Specifying notes:

Unintentional changes could occur through:

1) Incorrect program design, e.g. incorrect loop operation, changing global variables in a function, etc.; the avoidance requires as far as possible testing.

2) Accidental overwriting or deletion of stored data and programs (refer also to A.3.3, "Block L: Specific software requirements for Long-term Storage").

3) Incorrect assignment of measurement transaction data. Measurements and data belonging to one measurement transaction have not to be mixed with those of a different transaction due to incorrect programming or storage; the avoidance requires as far as possible testing and additional requests for confirmation of actions wherever useful.

4) Physical effects (electromagnetic interference, temperature, vibration, etc.); the avoidance requires self-checks of the software.

5) For type P2: Misuse of the operating system; the avoidance requires programmers who are sufficiently familiar with the operating system used.

b) Required documentation:

The documentation should show the measures that have been taken to protect the software and data against unintentional changes.

c) Validation guidance:

Checks based on documentation:

1) Check that a checksum of the program code and the relevant parameters is generated and checked automatically.

2) Check that overwriting of data cannot occur before the end of the data storage period that is foreseen and documented by the manufacturer.

d) Example of an acceptable solution:

1) The accidental modification of programs and data files may be checked by calculating a checksum over the relevant code, comparing it with the nominal value and stopping if the code has been modified or suitably reacting, if parameters or data are concerned.

2) For type P2: The manufacturer should make full use of the protection or privacy rights provided by the operating system or programming language, to prevent overwriting or deleting of stored data and programs.

3) For type P2: Where the operating system allows it, it is recommended that all user rights for the deletion, moving or amendment of relevant software should be removed and access should be controlled via utility programs. Access control to programs and data through the use of passwords is recommended, as is the use of read-only mechanisms. The system supervisor should restore rights only when required.

A.3.2.7 Protection against intentional changes

Relevant software and measurement data shall be secured against inadmissible modification.

a) Specifying notes for type P1:

1) Manipulation of program code could be possible by manipulating the physical memory, i.e. the memory is physically removed and substituted by one containing fraudulent software or data. To prevent this happening, either the housing of the instrument should be secured or the physical memory itself is secured against unauthorised removal.

2) All functions in the interface shall be subject to examination (see A.3.2.5, "Influence via communication interface"). Where the interface is to be used for software download, A.3.6, "Block D: Download of relevant software" has to be complied with.

3) Data are considered to be sufficiently protected if only relevant software processes them. If non-relevant Software is intended to be changed after approval, requirements of A.3.5, "Block S: Software separation" have to be followed.

b) Specifying notes for type P2:

Changes with the intention of fraud could be attempted by:

1) Changing the program code including integrated data - if the program code is an executable format (.exe) then it is sufficiently protected.

2) Changing the stored measurement data – refer to A.3.3, "Block L: Specific software requirements for Long-term Storage".

3) Means that consider the capabilities of the operating system shall be taken to prevent the approved software from being replaced by non-approved software using the operating system (see also A.3.2.4, "Influence via user interfaces"). For authorized downloading software, see A.3.6, "Block D: Download of relevant software".

4) The mass storage device where relevant data, configuration files, programs and parameters are stored shall be protected against physical exchange.

5) Means shall be taken to protect relevant software from modifications by using the operating system or other simply available and manageable tools (see also A.3.2.4, "Influence via user interfaces").

6) The parts and features of the operating system that implement the protection of the measuring system shall be considered as relevant software and be protected as such.

c) Required documentation:

The documentation should provide assurance that software and stored measurement data cannot be inadmissibly modified.

d) Validation guidance for type P1:

1) Checks based on documentation:

i) Examine whether the documented means of securing against unauthorised exchange of the memory that contains the software are sufficient.

ii) If the memory can be programmed in-circuit (without dismounting), check whether the programming mode can be disabled electrically and the means for disabling can be secured/sealed. (For checking download facilities see A.3.6, "Block D: Download of relevant software")

2) Functional checks

i) Test practically the programming mode and check whether disabling works.

e) Validation guidance for type P2:

1) Case 1: Closed shell of the software.

Checks based on documentation:

i) Software modules boot automatically;

ii) User has no access to the operating system of the PC;

iii) User has no access to other software than the approved one;

iv) A written declaration is given that there are no hidden functions to circumvent the closed shell.

2) Case 2: User-accessible operating system and/or software.

Checks based on documentation:

i) Check sum over machine code of the software modules is generated;

ii) Relevant software cannot be started if code is falsified.

f) Example of an acceptable solution for type P1:

The instrument is sealed and the interfaces comply with the requirements A.3.1.3, "Influence via user interfaces" and A.3.2.5, "Influence via communication interface".

g) Example of an acceptable solution for type P2:

1) Program code and data may be protected by means of checksums. The program is calculating its own checksum and compares is with a desired value that is hidden in the executable code. If the self-check fails, the program is blocked;

2) Any signature algorithm should have a key length of at least 2 bytes; a CRC-16 checksum with a secret initial vector (hidden in the executable code) would be satisfactory. (See also A.3.3, "Block L: Specific software requirements for Long-term Storage" and A.3.4, "Block T: Transmission of measurement data via Communication Networks");

3) The unauthorized manipulation of relevant software may be controlled by the access control or privacy protection attributes of the operating system. The administration level of these systems shall be secured by sealing or equivalent means,

4) The access to the administrator account is a) blocked for everyone or b) only granted to authorized persons as regulated by the national market surveillance laws;

   i) Solution a) Random password generated automatically, known to nobody. Change of the relevant configuration only possible by performing a new operating system set up.

   ii) Solution b) Password chosen by the authorized person and hidden and sealed in an envelope or in /at the housing.

5) Circumvention of the protection means of the operating system by direct writing to mass storages or physical replacement is prohibited by sealing.

A.3.2.8 Parameter protection

Relevant parameters shall be secured against unauthorised modification.

a) Specifying notes:

   1) Type specific parameters are identical for each specimen of the type and are in general part of the program code. Therefore, requirement A.3.2.7, "Protection against intentional changes" applies to them.

   2) Device specific secured parameters may be changed using an on-board keypad or switches or via interfaces, but only before they have been secured. Because device specific parameters could be manipulated using simple tools on universal computers they shall not be stored in standard storages of a universal computer. Storing of these parameters is acceptable only in additional hardware.

   3) Settable device-specific parameters may be changed after securing. Traceability of relevant parameter changes has to be provided.

b) Required documentation:

   The documentation shall describe all of the relevant parameters, their ranges and nominal values, where they are stored, how they may be viewed, how they are secured and when.

   The documentation shall describe how the traceability of relevant parameter modifications is guaranteed.

c) Validation guidance:

   1) Checks based on documentation:

      i) Check that the method for protection of the type specific parameters is appropriate.

      ii) Check that device specific parameters are not stored on the standard storages of the universal computer but in separate hardware that can be sealed and write-disabled.

2) Functional checks:

   i) Test the adjusting (configuration) mode and check whether disabling after securing works.

   ii) Examine the classification and state of parameters (secured/settable) at the display of the instrument, if a suitable menu item is provided.

d) Example of an acceptable solution:

1) Parameters are secured by sealing the instrument or memory housing and disabling the write enable/disable input of the memory circuit by an associated jumper or switch, which is sealed.

2) Device specific parameters are stored on a plugged-in storage which is sealed against removing or directly on the sensor unit. Writing of parameters is inhibited by sealing a write-enable switch in the disabled state.

e) Audit trails:

1) An event counter registers each change of a parameter value. The current count can be displayed and can be compared with the initial value of the counter that was registered at the last official verification and is indelibly labelled on the instrument.

2) Changes of parameters are registered in an event logger. It is an information record stored in a non-volatile memory. Each entry is generated automatically by the relevant software and contains:

   i) the identification of the parameter (e.g. the name)

   ii) the parameter value (the current and/or the previous value)

3) the time stamp of the change

The event logger cannot be deleted or be changed without destroying a seal.

A.3.2.9 Software authenticity and presentation of results (only for type P2)

Means shall be employed to ensure the authenticity of the relevant software. The authenticity of the results that are presented shall be guaranteed.

a) Specifying notes:

1) It shall not be possible to fraudulently simulate (spoof) approved relevant software using the capabilities of the operating system or other simply available and manageable tools.

2) Presented results can be accepted as authentic if the presentation is issued from within the relevant software

3) Presented measurement values shall be comprehensibly and accompanied by any information necessary to avoid confusion with other (non-relevant) information.

4) Under consideration of the capabilities of the operating system, it shall be ensured by technical means that on the universal computer only the software approved for the relevant purpose can perform the relevant functions (e.g. a sensor shall only work together with the approved program).

5) It shall be ensured by technical means, that relevant software check its integrity and authenticity on a regular basis (time intervals) during its execution.

b) Required documentation:

The documentation should describe how authenticity of the software is guaranteed.

c) Validation guidance:

1) Checks based on documentation:

i) The examination needs to determine that presentations are generated by relevant software and how spoofing by non-relevant programs may be prevented.

ii) Check that the relevant tasks can only be performed by the approved relevant software.

2) Functional checks:

i) Check through visual control if the presentation of results is easily distinguishable from other information that may also be presented.

ii) Check according to the documentation if the presented information is complete.

d) Example of an acceptable solution:

1) Formal means:

The software identification part (B) (checksum, version number or test certificate number, see A.3.2.3, "Software identification") indicated by the software is compared with the desired value in the test certificate.

2) Technical means:

A measurement application window is generated by the relevant software. The technical measures required of the window are:

i) No access to measurement values shall be given to non-relevant programs until the measurement values have been indicated.

ii) The window is refreshed periodically. The associated program checks that it is on top of the stack of windows and the user shall not be enabled to close the window or shift it outside the visible area as long as the measurement is not concluded.

iii) Processing of measurement values stops whenever this window is closed or not completely visible.

The operating manual (and test certificate) should contain a copy of the window for reference purposes.

iv) The sensor unit encrypts the measuring values with a key known to the approved software running on the universal computer (e.g. its version number). Only the approved software can decrypt and use the measurement values, non-approved programs on the universal computer cannot as they don't know the key. For key treatment see A.3.4, "Block T: Transmission of measurement data via Communication Networks".

v) Before sending measurement values the sensor initiates a handshake sequence with the relevant software on the universal computer based on secret keys. Only if the program on the universal computer communicates correctly, the sensor unit sends its measurement values. For key treatment see A.3.4, "Block T: Transmission of measurement data via Communication Networks".

vi) The key used in 2a / 2b is the hash code of the program on the universal computer. Each time the software on the universal computer is changed, the new key has to be entered into the sensor unit and sealed.

A.3.3 Block L: Specific software requirements for long-term storage

A.3.3.1 General

The requirements given in this section are to apply in addition to the previous set of requirements.

— Specific software requirements

A.3.3.2 Completeness of measurement data stored

The measurement data stored has to contain all relevant data necessary to reconstruct earlier measurements within the traceability time span.

a) Specifying notes:

The stored measurement data may be needed for reference at a later date.

All relevant data shall be stored together with the measurement value.

b) Required documentation:

Description of all fields of the data sets.

c) Validation guidance:

Checks based on documentation: Check whether all relevant data are contained in the data set.

d) Example of an acceptable solution:

1) A complete data set comprises the following fields:

   i) Measurement value(s) with correct resolution;

   ii) the unit of measure;

   iii) the place (e.g. truck ID or warehouse room ID) and time of the measurement;

   iv) identification of the instrument or probe if applicable;

2) Data are stored with the same resolution, values, units etc. as indicated or printed on a delivery note.

A.3.3.3 Protection against accidental or unintentional changes

Stored data shall be protected against accidental and unintentional changes.

a) Specifying notes:

1) Accidental changes of data can be caused by physical effects.

2) Unintentional changes are caused by the user of the device. Automatic or semi-automatic means should be used to ensure that only specified data are deleted and that the accidental deletion of "live" data are avoided. This is particularly important on networked systems and remote or removable storage where users might not realize the significance of the data.

3) A checksum shall be calculated by the receiver and compared with the attached nominal value. If the values match, the data set is valid and may be used, otherwise it has to be deleted or marked invalid.

b) Required documentation:

Description of protection measures (e.g. the checksum algorithm, including the length of the generator polynomial).

c) Validation guidance:

1) Checks based on documentation:

i) Check that a checksum over data are generated.

ii) Check that relevant software, which reads the data and calculate a checksum really compares the calculated and the nominal values.

iii) Check that overwriting of data cannot occur before the end of the data storage period that is foreseen and documented by the manufacturer.

iv) Check that measurements within their traceability time span cannot be deleted.

v) Check that a warning is issued to the user if he is about to delete old measurement data files.

2) Functional checks:

i) Check by practical spot checks that, before deleting old measurement data, a warning is given, if deleting is possible at all.

d) Example of an acceptable solution:

1) To detect data changes due to physical effects, a checksum with the CRC-16 algorithm is calculated over the entire data set and inserted into the data set to be stored.

2) The algorithm is not secret and, in contrast to requirement A.3.3.4, "Integrity of data", neither is the initial vector of the CRC-register nor the generator polynomial, i.e. the devisor in the algorithm. The initial vector and generator polynomial are known to both of the programs that create and verify the checksums.

3) Measurement data files could be protected by attaching an automatic date stamp on creation. A utility program would only delete/move files if measurements were out-of-date.

4) Measurement data are not deleted without prior authorization, e.g. a dialogue statement or window asking for confirmation of deletion.

5) Automatic overwriting of measurement data can be performed if there is adequate protection of the records to be retained. The storage size has to be sufficient to avoid an interruption due to insufficient memory space.

A.3.3.4 Integrity of data

The relevant data stored has to be protected against intentional changes.

a) Specifying notes:

1) This requirement applies to all types of storages except integrated storages.

2) The protection has to apply against intentional changes carried out by simple common software tools.

3) Simple common software tools are understood as tools, which are easily available and manageable as e.g. office packages.

b) Required documentation:

The method of how the protection is realized shall be documented.

c) Validation guidance

1) Checks based on documentation:

i) If a checksum or signature is used

I) Check that the checksum or signature is generated over the entire data set.

II) Check that relevant software, which reads the data and calculate a checksum or decrypts a signature really compares calculated and the nominal values.

ii) Check that secret data (e.g. key initial value if used) are kept secret against spying out with simple tools.

2) Functional checks:

Check that a falsified data set is rejected by the retrieval program.

d) Example of an acceptable solution:

Just before the data are reused, the value of the checksum is recalculated and compared with the stored nominal value. If the values match, the data set is valid and may be used; otherwise it has to be deleted or marked invalid.

An acceptable solution is the CRC-16 algorithm.

The algorithm is not secret but in contrast to requirement A.3.3.3, “Protection against accidental or unintentional changes”, the initial vector of the CRC-register or the generator polynomial (i.e. the divisor in the algorithm) has to be secret. The initial vector and generator polynomial are known only to the programs generating and verifying the checksums. They have to be treated as keys (see A.3.3.6, “Confidentiality of keys”).

A.3.3.5 Authenticity of measurement data stored

The measurement data stored has to be capable of being authentically traced back to the measurement that generated them.

a) Specifying notes:

  1) The authenticity of measurement data may be needed for reference at a later date.

  2) Authenticity requires the correct assignment (linking) of measurement data to the measurement that has generated the data.

  3) Authenticity presupposes an identification of data sets.

  4) Ensuring authenticity does not necessarily require an encryption of the data.

b) Required documentation:

  Description of the method used for ensuring the authenticity.

c) Validation guidance:

  1) Checks based on documentation:

    i) Check that there is a correct linking between each measurement value and the corresponding measurement.

    ii) If a checksum or signature is used, check that the checksum or signature is generated over the entire data set.

    iii) Check that secret data (e.g. key initial value if used) are kept secret against spying out with simple tools.

  2) Functional checks:

    Check whether corresponding stored data and data printed on the ticket are identical.

d) Example of an acceptable solution:

  A stored data set contains the following data fields (additional to the fields defined in A.3.3.4, "Integrity of data"):

  1) A unique (current) identification number. The identification number is also copied to the delivery note.

  2) Time when the measurement has been performed (time stamp). The time stamp is also copied to the delivery note.

  3) An identification of the measuring instrument that has generated the value.

  4) A signature that is used for ensuring the integrity of data can simultaneously be used for ensuring the authenticity. The signature covers all of the fields of the data set. Refer to requirement A.3.3.3, "Protection against accidental or unintentional changes", A.3.3.4, "Integrity of data".

5) The ticket may state that the measurement values can be compared with the reference data on a means of storage. Assignment is demonstrated by comparing the identification number or time stamp printed on the delivery note with that in the stored data set. A stored data set contains the following data fields (additional to the fields defined in A.3.3.4, "Integrity of data"):

A.3.3.6 Confidentiality of keys

Keys and accompanying data have to be treated as relevant data and have to be kept secret and be protected against compromise by software tools.

a) Specifying notes:

1) This requirement only applies if a secret key is used.

2) This requirement applies to measurement data storage, which are external from the measuring instrument or realized on universal computers.

3) The protection has to apply against intentional changes carried out by common simple software tools.

4) If the access to the secret keys is prevented, e.g. by sealing the housing of a built for purpose device, no additional software protection means are necessary.

b) Required documentation:

Description of the key management and means for keeping keys and associated information secret.

c) Validation guidance:

Checks based on documentation: Check that the secret information cannot be compromised.

d) Example of an acceptable solution:

The secret key and accompanying data are stored in binary format in the executable code of the relevant software. It is then not obvious at which address these data are stored. The system software does not offer any features to view or edit these data. If the CRC algorithm is used as a signature, the initial vector or generator polynomial play the role of a key.

A.3.3.7 Retrieval of stored data

The software used for verifying measurement data sets stored shall display or print the data, check the data for changes, and warn if a change has occurred. Data that are detected as having been corrupted has not to be used.

a) Specifying notes:

1) The measurement data stored might need to be referred to at a later date. If there is a doubt on the correctness of a delivery note or ticket, it has to be possible to identify the measurement data stored to the disputed measurement without ambiguities (refer also to A.3.3.2, "Completeness of measurement data stored", A.3.3.4, "Integrity of data", A.3.3.5, "Authenticity of measurement data stored" and A.3.3.6, "Confidentiality of keys").

2) The identification number (see A.3.3.2, "Completeness of measurement data stored") has to be printed out on the delivery note/ticket for the customer along with an explanation and a reference to the storage source.

3) Verification means checking the integrity, authenticity and correct assignment of the measurement data stored.

4) The verification software used for displaying or printing the data stored shall be considered relevant.

b) Required documentation:

1) Description of the functions of the retrieval program.

2) Description of detection of corruption.

3) Operating manual for this program.

c) Validation guidance:

1) Checks based on documentation:

i) Check that retrieval software really compares the calculated and the nominal values.

ii) Check that retrieval software is part of the relevant software.

2) Functional checks:

i) Check whether the program detects corrupted data sets.

ii) Perform spot checks verifying that retrieval provides all necessary information.

d) Example of an acceptable solution:

The data set is read from the storage by the verifying program and the signature over all data fields is recalculated and compared with the stored nominal value. If both values match, the data set is correct; otherwise the data are not used and are deleted or marked invalid by the program.

A.3.3.8 Automatic storing

The measurement data has to be stored automatically when the measurement is concluded.

a) Specifying notes:

1) This requirement applies to all types of storage.

2) This requirement means that the storing function has to not depend on the decision of the operator.

3) For the case of full storage, refer to requirement A.3.3.9, "Storage capacity and continuity".

b) Required documentation:

Confirmation that storing is automatically carried out. Description of the Graphical User Interface (GUI).

c) Validation guidance:

d) Functional checks:

Examine by spot checks that the measurement values are stored automatically after measurement or acceptance of measurement is concluded. Check that there are no buttons or menu items to interrupt or disable the automatic storing.

e) Example of an acceptable solution:

There is no menu item or button in the Graphical User Interface that supports manual initiation of storing measurement results. The measurement values are wrapped in a data set along with additional information such as time stamp and signature and are stored immediately after the measurement, or the acceptance of measurement, respectively.

A.3.3.9 Storage capacity and continuity

The long-term storage has to have a capacity which is sufficient for the intended purpose.

a) Specifying notes:

1) When a storage is full or removed/disconnected from the instrument, a warning shall be given to the operator. A warning is not necessary, if it is ensured by construction that only outdated data can be overwritten.

2) The regulation concerning the minimum period for storing measurement data are beyond the scope of this requirement and is left to national regulations. It is the responsibility of the owner to have an instrument with sufficient storage capacity to fulfil the requirements applicable to his activity. The software test will check only that the data are stored and retrieved correctly and whether new transactions are inhibited when the storage is full.

3) It is also beyond the scope of this requirement to require certain inscriptions on the device as concerning the capacity of the storage the capacity or other accompanying information that allow calculating the capacity. However, the manufacturer shall make available the information on the capacity.

b) Required documentation:

Description of management of exceptional cases when storing measurement values.

c) Validation guidance:

1) Checks based on documentation:

i) Check that the capacity of storage or a formula for calculating it is given by manufacturer.

ii) Check that overwriting of data cannot occur before the end of the data storage period that is foreseen and documented by the manufacturer.

2) Functional checks:

i) Check that a warning is issued to the user if he is about to delete measurement data files (if deleting is possible at all).

ii) Check that a warning is given if the storage is full or removed.

d) Example of an acceptable solution:

Measurement data may be automatically overwritten by a utility that checks if the measurement data are out-of-date (refer to national regulations for the relevant time period).

A.3.4 Block T: Transmission of measurement data via Communication Networks

A.3.4.1 General

This extension has to be used only if relevant data are transmitted via communication networks to a distant device where they are further processed and/or used as relevant data. This extension does not apply if there is no subsequent relevant data processing. If software is downloaded to a device the requirements of A.3.6, “Block D: Download of relevant software” apply.

a) Technical description

The set of requirements of this extension applies only if the device under consideration is connected to a network and transmits or receives measurement data that is relevant. Three network configurations are identified. The simplest is an array of relevant devices. The participants are fixed. A variant to this, is a net including participants that are not relevant but that are known and do not change during operation. An open network has no limitation in identity, functionality, presence and location of the participants.

b) Closed network

Only a fixed number of participants with clear identity, functionality and location are connected. All devices are relevant. No devices exist in the network that are non-relevant.

c) Closed network, with non-relevant devices

A fixed number of participants with clear identity and location are connected to the network. Not all devices are relevant and therefore their functionality is unknown.

d) Open network

Arbitrary participants (devices with arbitrary functions) can connect to the network. The identity and functionality of a participating device and its location may be unknown to other participants.

Any network that contains devices with IR or wireless network communications interfaces shall be considered to be an open network.

e) Specific software requirements

A.3.4.2 Completeness of transmitted data

The transmitted data has to contain all relevant data necessary to present or further process the measurement result in the receiving unit.

a) Specifying notes:

The relevant part of a transmitted data set comprises one or more measurement values with correct resolution, the unit of measure, the time and the place of the measurement.

b) Required documentation:

Document all fields of the data set.

c) Validation guidance

Checks based on documentation: Check whether all information for further processing the measurement values at the receiving unit are contained in the data set.

d) Example of an acceptable solution:

The data set comprises the following fields:

1) Measurement value(s) with correct resolution;

2) the correct unit of measure;

3) the time and date of the measurement;

4) identification of the instrument or probe if applicable (data transmission);

5) the place of the measurement.

A.3.4.3 Protection against accidental or unintentional changes

Transmitted data shall be protected against accidental and unintentional changes.

a) Specifying notes:

1) Accidental changes of data can be caused by physical effects.

2) Unintentional changes are caused by the user of the device.

3) Means shall be provided to detect transmission errors.

b) Required documentation:

Description of the checksum algorithm, if used, including the length of the generator polynomial.

Description of an alternative method if used.

c) Validation guidance:

Checks based on documentation:

1) Check that a checksum over data are generated.

2) Check that relevant software that receives the data re-calculates the checksum and compares it with the nominal value contained in the data set.

d) Example of an acceptable solution:

1) To detect data changes, a checksum with the CRC-16 algorithm is calculated over all bytes of a data set and inserted into the data set to be transmitted. Just before the data are reused, the value of the checksum is recalculated by the receiver and compared with the attached nominal value. If the values match, the data set is valid and may be used, otherwise it has to be deleted or marked invalid.

NOTE The algorithm is not secret and, in contrast to requirement A.3.3.4, "Integrity of data", neither is the initial vector of the CRC-register nor the generator polynomial i.e. the devisor in the algorithm. The initial vector and generator polynomial are known to both of the programs that create and verify the checksums.

2) Use of means provided by transmission protocols e.g. TCP/IP, IFSF.

A.3.4.4 Integrity of data

The relevant transmitted data has to be protected against intentional changes with software tools.

a) Specifying notes:

1) This requirement only applies to networks that are open or closed with non-relevant devices, not to closed networks.

2) The protection has to apply against intentional changes carried out by common simple software tools.

3) Simple common software tools are understood as tools, which are easily available and manageable as e.g. office packages

b) Required documentation:

Description of the protection method

c) Validation guidance:

Checks based on documentation:

1) If a checksum or signature is used:

i) Check that the checksum or signature is generated over the entire data set.

ii) Check that relevant software that receives the data re-calculates the checksum or decrypts the signature and compares it with the nominal value contained in the data set.

2) Check that secret data (e.g. key initial value if used) are kept secret against spying out with simple tools.

d) Example of an acceptable solution:

1) A checksum is generated of the data set to be transmitted. Just before the data are reused, the value of the checksum is recalculated and compared with the nominal value that is contained in the received data set. If the values match, the data set is valid and may be used, otherwise it has to be deleted or marked invalid.

2) An acceptable solution is the CRC-16 algorithm.

   The algorithm is not secret but in contrast to requirement A.3.3.3, "Protection against accidental or unintentional changes", the initial vector of the CRC-register or the generator polynomial (i.e. the divisor in the algorithm) are secret. The initial vector and generator polynomial are known only to the programs generating and verifying the checksums. They have to be treated as keys (see A.3.3.6, "Confidentiality of keys").

A.3.4.5 Authenticity of transmitted data

For the receiving program of transmitted relevant data, it shall be possible to verify the authenticity and the assignment of measurement values to a certain measurement.

a) Specifying notes:

   1) In a network with unknown participants, it is necessary to identify the origin of measurement data transmitted without ambiguity. (The authenticity relies on the identification number of the data set and the network address).

   2) In a closed network all participants are known. No additional IT means are necessary, but the topology of the network (the number of participants) shall be fixed by sealing.

   3) Unforeseen delays are possible during transmission. For a correct assignment of a received measurement value to a certain measurement the time of measurement has to be registered.

   4) To ensure the authenticity, an encryption of measurement data are not necessarily required.

b) Required documentation:

   Network with unknown participants: Description of the IT means for correct assigning of measurement value to measurement.

   Closed network: Description of the hardware means preserving the number of participants in the network. Description of initial identification of the participants.

c) Validation guidance:

   Checks based on documentation:

   1) Check that there is a correct linking between each measurement value and the corresponding measurement.

   2) Check that data are digitally signed to ensure their proper identification and authentication.

d) Example of an acceptable solution:

   1) Each data set has a unique (current) identification number, which may contain the time when the measurement has been performed (time stamp).

   2) Each data set contains information about the origin of the measurement data, i.e. serial number or identity of the measuring instrument that generated the value.

   3) In a network with unknown participants, authenticity is guaranteed if the data set carries an unambiguous signature. The signature covers all of these fields of the data set.

4) The receiver of the data set checks all data for plausibility.

A.3.4.6 Confidentiality of keys

Keys and accompanying data have to be treated as relevant data and have to be kept secret and be protected against compromise by software tools.

a) Specifying notes:

1) This requirement only applies if a secret key exists in the system. (Normally not in Closed networks.)

2) The protection has to apply against intentional changes carried out by common simple software tools.

3) If the access to the secret keys is prevented e.g. by sealing the housing of a built for purpose device, no additional software protection means are necessary.

b) Required documentation:

Description of the key management and means for keeping keys and associated information secret.

c) Validation guidance:

Checks based on documentation*:* Check that the secret information cannot be compromised

d) Example of an acceptable solution:

The secret key and accompanying data are stored in binary format in the executable code of the relevant software. It is then not obvious at which address these data are stored. The system software does not offer any features to view or edit these data. If the CRC algorithm is used as a signature, the initial vector or generator polynomial play the role of a key.

A.3.4.7 Handling of corrupted data

Data that are detected as having been corrupted has not to be used.

a) Specifying notes:

Though communication protocols normally repeat transmission until it succeeds, it nevertheless is possible that a corrupted data set is received.

b) Required documentation:

Description of the detection of transmission faults or intentional changes.

c) Validation guidance:

Checks based on documentation and functional checks:

Check that the corrupted data will not be used according to the delivered concept

d) Example of an acceptable solution:

When the program that is receiving data sets detects a discrepancy between the data set and the nominal value of the signature, it first tries to reconstruct the original value if redundant information is available. If reconstruction fails, it generates a warning to the user, does not output the measurement value and

1) Sets a flag in a special field of the data set (status field) with the meaning "not valid"; or

2) Deletes the corrupted data set.

A.3.4.8 Transmission delay

The measurement has not to be inadmissibly influenced by a transmission delay.

a) Specifying notes:

The manufacturer shall investigate the timing of the data transmission and shall guarantee that under worst-case conditions the measurement is not inadmissibly influenced.

b) Required documentation:

Description of the concept, how measurement is protected against transmission delay.

c) Validation guidance:

Check the concept that the measurement is not influenced by transmission delay.

d) Example of an acceptable solution:

Implementation of transmission protocols for field buses.

A.3.4.9 Availability of transmission services

If network services become unavailable, no measurement data has to get lost.

a) Specifying notes:

1) The user of the measuring system has not to be able to corrupt measurement data by suppressing transmission.

2) Transmission disturbances happen accidentally and cannot be excluded. The sending device has to be able to handle this situation.

b) Required documentation:

Description of protection measures against transmission interruption or other failures.

c) Validation guidance:

1) Checks based on documentation:

i) Check by what measures are implemented to protect from data loss.

ii) Check which measures are foreseen for the case of transmission failure.

2) Functional checks:

Spot checks shall show that no relevant data get lost due to a transmission interruption.

d) Example of an acceptable solution:

The measurement may be completed even though the transmission is down.

However, the measuring instrument or the device that is transmitting the relevant data has to have a buffer that is large enough to store the current measurements.

A.3.5 Block S: Software separation

A.3.5.1 General

Software separation is an optional design methodology that allows the manufacturer to easily modify non-relevant software. If software separation is implemented, then this extension shall be considered in addition to the basic requirements.

a) Technical description

Software controlled measuring instruments or systems in general have complex functionality and contain modules that are relevant and modules that are not. It is advantageous for the manufacturer and examiner – though it is not prescribed – to separate these software modules of the measuring system.

Two variants of software separation are described. Both variants are covered by the set of requirements.

1) Software separation is realized independently from the operating system within an application domain, i.e. at the programming language level (Low level software separation).

NOTE 1 This feature is realizable in both built-for-purpose devices and universal computers.

2) The software modules to be separated are realized as independent objects in terms of the operating system (High level software separation).

NOTE 2 This type of separation is normally possible only with universal computers. Example solutions are independently executable programs, dynamically linked libraries, etc.

The protection against inadmissible changes of measurement values and parameters is only addressed indirectly as the programmer of non-relevant software parts have not to give the user of the measuring system the opportunity of corruption. But this has in any case to be considered by the programmer (with or without separation) and the appropriate requirements are given in A.3.2, “Block G: Basic requirements”.

b) Specific software requirements

A.3.5.2 Realization of software separation

There shall be a part of the software that contains all relevant software and parameters that is clearly separated from other parts of software.

a) Specifying notes:

1) Low level separation: Merging software units on the level of the programming language or merging parts of a programme (i.e. subroutines, procedures, functions, classes) to form the relevant part of the programme. The rest of the programme is the non-relevant part.

2) High level separation: Merge all parts of the software to one object that is identifiable by the operating system (a programme, a DLL etc.). The rest of the software is the non-relevant part.

i) In the case of low level separation, all program units (subroutines, procedures, functions, classes, etc.) and in case of high level separation all programs and libraries

ii) that contribute to the calculation of measurement values or have an impact on it,

iii) that contribute to auxiliary functions such as displaying data, data security, data storage, software identification, performing software download, data transmission or storing, verifying received or stored data etc.

iv) belong to the relevant software.

v) All variables, temporary files and parameters that have an impact on measurement value or on relevant functions or data belong to the relevant software.

vi) The protective software interface itself (see A.3.5.4, "Protective software interface") is part of the relevant software.

vii) Non-relevant software comprises the remaining program units, data or parameters not covered above. Modifications to this part are allowed without informing the testing organization provided the subsequent requirements of software separation are observed.

b) Required documentation:

Description of the protective interface described in the specifying notes above.

c) Validation guidance:

Checks based on documentation:

Check that all relevant parts mentioned in specifying notes 1 through 3 are included in relevant software.

A.3.5.3 Mixed indication

Additional information generated by the software, which is not relevant, may only be shown on a display or printout, if it cannot be confused with the information that originates from the relevant part.

a) Specifying notes:

As the programmer of the non-relevant software may not know about the admissibility of indications, it is the responsibility of the manufacturer to guarantee that all indicated information fulfil the requirement.

b) Required documentation:

Description of the software that realizes the indication. Description how the indication of relevant information is protected against misleading indication generated by non-relevant software.

c) Validation guidance:

Functional checks:

Judge through visual check that additional information generated by non-relevant software and presented on display or printout cannot be confused with the information originating from relevant software.

d) Example of an acceptable solution:

The information to be displayed by the non-relevant software is transferred via the protective interface (see A.3.5.4, "Protective software interface") to the relevant software. Behind the interface, it passes through a filter that detects inadmissible information. The admissible information is then inserted into the indication controlled by the relevant software.

A.3.5.4 Protective software interface

The data exchange between the relevant and non-relevant software has to be performed via a protective software interface, which comprises the interactions and data flow.

a) Specifying notes:

1) All interactions and data flows shall not inadmissibly influence the relevant software including the dynamic behaviour of a measuring process.

2) There shall be an unambiguous assignment of each command sent via the software interface to the initiated function or data change in the relevant software.

3) Codes and data that are not declared and documented as commands have not to have any effect on the relevant software.

4) The interface shall be completely documented and any other non-documented interaction or data flow (circumvention of the interface) have not to be realized neither by the programmer of the relevant software nor by the programmers of the non-relevant software.

The programmers are responsible for observing these constraints. Technical means to prevent them from circumventing the software interface are not possible. The programmer of the protective interface should be instructed about this requirement.

b) Required documentation:

1) Description of the software interface, especially which data domains realize the interface.

2) A complete list of all commands together with a declaration of completeness.

3) A brief description of their meaning and their effect on the functions and data of the measuring instrument.

c) Validation guidance:

Checks based on documentation:

1) Check that functions of the relevant software, that may be triggered via the protective software interface, are defined and described.

2) Check that the parameters that may be exchanged via the interface are defined and described.

3) Check that the description of the functions and parameters is conclusive and complete.

d) Example of an acceptable solution:

1) The data domains of the relevant software part are encapsulated by declaring only local variables in the relevant part.

2) The interface is realized as a subroutine belonging to the relevant software that is called from the non-relevant software. The data to be transferred to the relevant software are passed as parameters of the subroutine.

3) The relevant software filters out inadmissible interface commands.

A.3.6 Block D: Download of relevant software

A.3.6.1 General

This extension shall be used for the download of relevant software as long as the measurement characteristics remain unchanged and the declaration of conformity is still valid, e.g. bug-fixes. These requirements are to be considered in addition to the general requirements.

a) Technical description

Software may be downloaded only to measuring instruments that are characterized by the following properties:

1) Hardware configuration

It may be a built-for-purpose measuring instrument (type P1) or one based on a universal computer (type P2). Communications links for the download may be direct, e.g. RS 232, USB, over a closed network, e.g. Ethernet, token-ring LAN, or over an open network, e.g. Internet.

2) Software configuration

The entire software of the target device may be relevant or it may have software separation. The download of relevant software has to follow the requirements outlined below. If there is no software separation in the measuring instrument, then all of the requirements below apply to all downloads.

A.3.6.2 Download mechanism

Downloading and the subsequent installation of software shall be automatic and shall ensure that the software protection environment is at the approved level on completion.

a) Specifying notes:

1) Downloading shall be automatic to ensure that the existing level of protection is not compromised.

2) The target device has a fixed relevant software that contains all of the checking functions necessary for fulfilling requirements A.3.6.3, "Authentication of downloaded software" to A.3.6.5, "Traceability of relevant software download".

3) The instrument should be capable of detecting if the download or installation fails. A warning shall be given. If the download or installation is unsuccessful or is interrupted, the original status of the measuring instrument shall be unaffected. Alternatively, the instrument shall display a permanent error message and its functioning shall be inhibited until the cause of the error is corrected.

4) On successful completion of the installation, all protective means should be restored to their original state unless the downloaded software has authorization in the test certificate to amend them.

5) During download and the subsequent installation of downloaded software, measurement by the instrument shall be inhibited or correct measurement shall be guaranteed.

6) The number of re-installation attempts shall be limited.

7) If the requirements A.3.6.3, "Authentication of downloaded software" to A.3.6.5, "Traceability of relevant software download" cannot be fulfilled, it is still possible to download the non-relevant software part. In this case, the following requirements shall be met:

8) There is a distinct separation between the relevant and non-relevant software according to A.3.5, "Block S: Software Separation".

9) The completely relevant software part is fixed i.e. it cannot be downloaded or changed without breaking a seal.

10) It is stated in the test certificate downloading of the non-relevant part is acceptable.

11) It shall be possible to disable the software download mechanism by means of a sealable setting (switch, secured parameter) for member states where software download for instruments in use is not allowed. In this case, it has not to be possible to download relevant software without breaking the seal.

b) Required documentation:

The documentation should briefly describe the automatic nature of the download, checking, installation, how the level of protection is guaranteed on completion, what happens if a fault occurs.

c) Validation guidance:

1) Checks based on documentation:

i) Check the documentation how the download procedure is managed.

ii) Check that downloading and installation is handled automatically, that the measuring instrument is locked (if appropriate) and that software protection is not compromised following a download.

iii) Check that there exists non-downloadable fixed relevant software for authenticity and integrity checks.

iv) Check that during software download, no measurement is possible or correct measurement is guaranteed.

2) Functional checks:

Perform at least one software download to check the correct software download.

d) Example of an acceptable solution:

A utility program resident in the fixed part of the software that:

1) Handshakes with the sender and checks for consent;

2) Automatically inhibits measurement unless correct measurement can be guaranteed;

3) Automatically downloads the relevant software to a secure holding area;

4) Automatically carries out the checks required by A.3.6.3, "Authentication of downloaded software" to A.3.6.5, "Traceability of relevant software download";

5) Automatically installs the software into the correct location;

6) Takes care of housekeeping, e.g. deletes redundant files, etc.;

7) Ensures that any protection removed to facilitate downloading and installation is automatically replaced to the approved level on completion;

8) Initiates the appropriate fault handling procedures if a fault occurs.

A.3.6.3 Authentication of downloaded software

Means shall be employed to guarantee that the downloaded software is authentic, and to indicate that the downloaded software has been approved by a testing organization.

a) Specifying notes:

1) Before the downloaded software is used for the first time, the measuring instrument shall automatically check that:

i) The software is authentic (not a fraudulent simulation).

ii) The software is approved for that type of measuring instrument.

2) The means by which the software identifies its approval status shall be made secure to prevent counterfeiting of the status.

3) If downloaded software fails any of the above tests, see A.3.6.2, "Download mechanism".

4) If a manufacturer intends to change or update the relevant software he shall announce the intended changes to the responsible testing organization. The testing organization decides whether an addition to the existing test certificate is necessary or not. For software download it is indispensable that there is a software identification which is unambiguously assigned to the approved software version.

b) Required documentation:

The documentation should describe:

1) How authenticity of the software identification is guaranteed.

2) How the authenticity of approval is guaranteed.

3) How it is guaranteed that the downloaded software is approved for the type of measuring instrument to which it has been downloaded.

c) Validation guidance:

Checks based on documentation and functional checks:

1) Check the documentation, how a download of fraudulent software is prevented.

2) Check through functional tests that a download of fraudulent software is prevented.

Ensure the authentication check of software according to documentation and through functional tests.

d) Example of an acceptable solution:

1) Authenticity
For integrity reasons (see A.3.6.4, "Integrity of downloaded software") an electronic signature is generated over the software part to be downloaded. Authenticity is guaranteed if a key stored in the fixed software part of the instrument confirms that the signature originates from the manufacturer. Key matching shall be done automatically.

2) The key is stored in the fixed software part before initial verification.

3) Correct type of measuring instrument 'Checking the instrument type requires automatically matching an identification of instrument type that is stored in the fixed software part of the instrument with a compatibility list attached to the software.

4) Approval

If authenticity is guaranteed through the use of the manufacturer's key, then approval may be assumed.

A.3.6.4 Integrity of downloaded software

Means shall be employed to guarantee that the downloaded software has not been inadmissibly changed during download.

a) Specifying notes

1) Before the downloaded software is used for the first time, the measuring instrument shall automatically check that the downloaded software has not been inadmissibly changed.

2) If the downloaded software fails this test, see A.3.6.2, "Download mechanism".

b) Required documentation:

The documentation shall describe how the integrity of the software is guaranteed.

c) Validation guidance:

Ensure the integrity check of software after downloading according to documentation and through functional tests.

d) Example of an acceptable solution:

1) Integrity may be demonstrated by performing a checksum over the relevant software and comparing it against the checksum attached to the software (see also A.3.6.4, "Software identification" for example of an acceptable solution).

2) Acceptable algorithm: CRC, secret initial vector, length 32 bit. The initial vector is stored in the fixed software part.

A.3.6.5 Traceability of relevant software download

It shall be guaranteed by appropriate technical means that downloads of relevant software are adequately traceable within the instrument for subsequent controls.

a) Specifying notes:

1) This requirement enables inspection authorities, to back-trace downloads of relevant software over an adequate period of time (that depends on national legislation).

2) The traceability means and records are part of the relevant software and should be protected as such.

b) Required documentation:

The documentation shall:

1) Briefly describe how the traceability means is implemented and protected.

2) State how downloaded software may be traced.

c) Validation guidance:

1) Checks based on documentation:

Check that traceability means are implemented and protected.

2) Functional checks:

Check the functionality of the means through spot checks.

d) Example of an acceptable solution:

   1) An audit trail. The measuring instrument may be equipped with an event logger that automatically records at least the date and time of the download, identification of the downloaded relevant software, the identification of the downloading party, and an entry of the success. An entry is generated for each download attempt regardless of the success.

   2) After having reached the limit of the event logger, it shall be ensured by technical means that further downloads are impossible. Audit trails may only be erased by breaking a physical or electronic seal and may be resealed only by the inspection authorities.

e) Download consent

   It is assumed that the manufacturer of the measuring instrument keeps his customer well informed about updates of the software, especially the relevant part, and that the customer will not deny updating it. Furthermore, it is assumed that manufacturer and customer, user, or owner of the instrument will agree on an appropriate procedure of performing a download depending on the use and location of the instrument.

A.4 Software test for type P3

Software test for type P3 has to be carried out when a solution as a service (SaaS) is used.

The company providing the SaaS has to collect, store and manage the information gathered by its customer's field measuring instruments. Additionally, it has to provide a secure remote interface providing its customers with access to the information produced by its field instruments. This will usually be done via a web service, but can also be done directly via a remote connection. According to 5.12, "Software verification levels" the SaaS provider has to comply with ISO/IEC 27001.

Communications from customer's instruments to the SaaS have to be checked according to A.3.3, "Block T: Transmission of Measurement Data via Communication Networks." This will be done normally while performing test of the instruments that connect to the SaaS, therefore no additional test will be required.

For any additional means of communications to the SaaS not covered by the instruments tests there are two possibilities:

a) The channel will transmit relevant data that will maintain its relevant status. In that case it has to be checked according to A.3.3, "Block T: Transmission of measurement data via Communication Networks" and A.3.2.5, "Influence via communication interface".

b) If the transmitted data does not maintain its relevant status, it only has to be checked according to A.3.1.4, "Influence via communication interface".

Regarding the communication via a web service the additional test has to be performed: A.3.2.4, "Influence via user interfaces".

Annex B
(informative)

Manufacturer software test form

B.1 Identification

B.1.1 Manufacturer identification

For manufacturer identification you should use the form given in Table B.1:

Table B.1 — Manufacturer identification

Name	Fill
Address	Fill
Contact person(s)	Fill

B.1.2 Test object

Identify all the components or subunits of the temperature recorder that include software. All elements acquiring, transforming, transmitting or storing relevant data have to be considered.

For each component of the Temperature Recorder please fill the following information items. Duplicate this Table as required.

Table B.2 — Information of the components of the temperature recorder

Brand	Fill
Model	Fill
Software version	Fill

B.1.3 Documents list

Include a list with this document and all referenced documents.

For each document include the following information:

a) Document title (and file name for electronic documents).

b) Document code and version.

c) Document date.

d) Publisher (instrument manufacturer or third party)

The final versions of all documents have to be signed by the Client (preferably using an electronic signature.)

B.1.4 Define the applicable test blocks of each unit or subunit (L, T, S and D)

The IT configurations comprise: long term storage of relevant data (L), transmission of relevant data (T), software separation (S) and download of relevant software (D). The corresponding requirement sets, called modular extensions, are independent of each other. The sets selected depend only on the IT configuration. If an extension set is selected, then it has to be applied in full. Decide which, if any, of the modular extensions are applicable and apply them accordingly.

Checklist to decide which extensions applies for the instrument under test. Note that if the instrument is composed of different components of subunits you should **fill this checklist for each component**.

NOTE Please fill columns YES, NO, Not Applicable and Remarks. Include the Remarks column the reasons for each line answer.

Table B.3 — Decision on required extensions

Decision on required extensions					
Req. Extension		**YES**	**NO**	**Not applicable**	**Remarks**
L	Does the device have the ability to store the measurement data either on an integrated storage or on a remote or removable storage?				Include reasons
T	Does the device have interfaces for transmission of data to devices subject to control OR is the device receiving data from another device subject to control?				Include reasons
S	Are there software parts with functions not subject to control AND are these software parts desired to be changed after type approval?				Include reasons
D	Is loading of software possible or desired?				Include reasons

For each component or subunit of the Temperature Recorder you should copy and fill the G section and only the applicable extensions.

B.1.5 Selection of the type of each unit or subunit

For each subunit under test define its Type.

Type P1: The relevant software is embedded in a closed hardware (see table below).

Type P2: The relevant software runs on a general purpose computer managed by the user,

Type P3: The relevant software runs on an external provider of this service.

A type P1 instrument is a measuring instrument with an embedded IT system (in general it is a microprocessor or microcontroller based system). It is characterized by the following features:

a) The entire application software has been constructed for the measuring purpose. This includes both functions subject to control and other functions.

b) The user interface is dedicated to the measuring purpose, i.e. it is normally in an operating mode subject to control. Switching to an operating mode not subject to control is possible.

c) If there is an operating system, it has no user shell that is accessible to the user (to load or change programs, send commands to the OS, change the environment of the application etc.).

The P1 type instrument may have additional properties and features that are covered by the following requirement extensions:

d) The software is designed and treated as a whole, unless software separation according to Block S has been observed.

e) The software is invariable and there are no means for programming or changing the relevant software. Software download is only allowed if Block D is observed.

f) Interfaces for transmission of measurement data via open or closed communication networks are allowed (Block T to be observed).

g) The storage of measurement data either on an integrated storage, on a remote or on removable storage is allowed (Block L to be observed).

To declare the unit as type P1 use the following Table B.4.

Table B.4 — Type P1 - Decision on instrument type

Decision on instrument type				
		A	**Y/N**	**Remarks**
1	Is the entire application software constructed for the measuring purpose?	**(Y)**	Y/N	Include reasons
2	If there is general-purpose software, is it accessible by or visible to the user?	**(N)**	Y/N	Include reasons
3	Is the user prevented from accessing the operating system if it is possible to switch to an operating mode not subject to control?	**(Y)**	Y/N	Include reasons
4	Are the implemented programs and the software environment invariable (apart from updates)?	**(Y)**	Y/N	Include reasons
5	Are there any means for programming?	**(N)**	Y/N	Include reasons

If and only if all answers to the 5 questions can be given as in the A column, then the subunit can be considered of type P1.

B.2 Test requirement for type P1 and P2

B.2.1 General

Please use the following sections as required by the extensions of each subunit.

B.2.2 Basic requirements

B.2.2.1 General

This section is always required.

B.2.2.2 Documentation

In addition to the specific documentation required in each of the following requirements, the documentation shall basically include the following items given in in Table B.5:

Table B.5 — Items of documentation

a.	A description of the relevant software.
Include description or reference (document(s) and pages). Main software blocs. Interaction between software blocks. System start-up. Main data structures, etc. Include a list with all software source modules with date and size expressed in bytes.	
b.	A description of the accuracy of the measuring algorithms
Include description or reference (document(s) and pages)	
c.	A description of the user interface, menus and dialogues.
Include description or reference (document(s) and pages)	
d.	A clear software identification.
Include description or reference (document(s) and pages)	
e.	An overview of the system hardware, e.g. topology block diagram, type of computer(s), type of network, memory, etc., if not described in the operating manual.
Include description or reference (document(s) and pages)	
f.	An overview of the parts of the operating system used, security aspects of the operating system utilized, e.g. protection, user accounts, privileges, etc.
Include reference	
g.	The operating manual.
Include reference	

B.2.2.3 Software identification

The relevant software shall be clearly identified. An identification of the software shall be inextricably linked to the software itself. It shall be determined and presented on command or during operation.

Table B.6 — Documentation with regard to the software identification

Required documentation: The documentation shall list the software identifications and describe how the software identification is created, how it is inextricably linked to the software itself, how it may be accessed for viewing and how it is structured in order to differentiate between version changes with and without requiring a software test.
Include information or reference (document(s) and pages)

Table B.7 — Specifying notes with regard to software identification

1. Each change to relevant software requires a new software identification.
2. The software identification has to be easily shown for verification and inspection purposes (easily means by standard user interface, without additional tools.)
Include information or reference (document(s) and pages)
3. The software identification shall have a structure that clearly identifies versions of the relevant software.
Include information or reference (document(s) and pages)
4. If functions of the software can be switched by type-specific parameters, each function or variant may be identified separately or, alternatively, the complete package may be identified as a whole.
Include information or reference (document(s) and pages)
5. If the relevant functions and the account of the measuring task are protected by a specific configuration of the operating system, the relevant configuration files shall have an additional identification.
Include information or reference (document(s) and pages)

B.2.2.4 Influence via user interface

Requirement: Commands entered via the user interface shall not inadmissibly influence relevant software and measurement data.

Table B.8 — Documentation with regard to the influence via user interface

Required documentation: If the instrument has the ability to receive commands, the documentation shall include:
1. A complete list of all commands together with a declaration of completeness.
Include list of all commands or reference (document(s) and pages) Include declaration of completeness
2. A brief description of their meaning and their effect on the functions and data of the measuring instrument.
Include information or reference (document(s) and pages)
3. For type P2. A description how a secure configuration of the operating system is achieved. Assignment of roles (accounts) in the operating system (e.g. “administrator”, “user”, “Measuring Task”). Assignment of permissions granted to these roles.
Include information or reference (document(s) and pages)
4. For type P2. A documentation of remote control of the functions of the operating system (e.g. started services) and means for protection (e.g. configuration of a firewall)
Include information or reference (document(s) and pages)

Table B.9 — Specifying notes with regard to the influence via user interface

1. This implies that there is an unambiguous assignment of each command to an initiated function or data change.
Include information or reference (document(s) and pages)
2. This implies that switch or key actuations that are not declared and documented as commands have no effect on the instrument's functions and measurement data.
Describe how unknown or not allowed sequences of switch or key actuations are rejected.
3. Commands may be a single action or a sequence of actions carried out by the operator. The user shall be guided which commands are allowed.
Include information or reference (document(s) and pages).
4. For type P2. Functions for changing the relevant configuration of the operating system shall not be offered to the user neither locally nor remotely. The configuration shall be secured against inadmissible changes.
Include information or reference (document(s) and pages).

B.2.2.5 Influence via communication interface

Requirement: Commands inputted via communication interfaces of the instrument shall not inadmissibly influence the relevant software and measurement data.

Table B.10 — Documentation with regard to the influence via communication interface

Required documentation: If the instrument has an interface the documentation shall include:
A complete list of all commands together with a declaration of completeness.
For each interface include list of all commands or reference (document(s) and pages) Include declaration of completeness
A brief description of their meaning and their effect on the functions and data of the measuring instrument
Include information or reference (document(s) and pages)
For type P2: Description how a secure configuration of the operating system is achieved. Assignment of roles (accounts) in the operating system (e.g. "administrator" and "user"). Assignment of permissions granted to these roles.
Include information or reference (document(s) and pages)
For type P2: Documentation of remote control of the functions of the operating system (e.g. started services) and means for protection (e.g. configuration of a firewall).
Include information or reference (document(s) and pages)

Table B.11 — Specifying notes with regard to the influence via communication interface

1. This implies that there is an unambiguous assignment of each command to an initiated function or data change.
2. This implies that signals or codes that are not declared and documented as commands have no effect on the instrument's functions and data.
For each interface describe how unknown or not allowed sequences of inputs are rejected.
3. Commands may be a sequence of electrical (optical, electromagnetic, etc.) signals on input channels or codes in data transmission protocols.
4. The restrictions of this requirement are suspended when a software download according to Extension D is carried out.
5. This requirement applies only on interfaces which are not sealed.
Include list of sealed interfaces
6. For type P2: The respective parts of the software that interpret relevant commands shall be considered relevant software.
Include list of the software parts that interpret relevant commands
7. For type P2: Other software parts may use the interface provided they do not disturb or falsify the reception or transmission of relevant commands or data.
Include information or reference (document(s) and pages)
8. For type P2: If the operating system allows remote control or remote access, the requirements A.3.2.4, "Influence via user interface". Influence via user interface apply to the communication interface and the connected remote terminal respectively. Additionally Part T shall be taken into consideration for the transmission between computer and terminal.
Include information or reference (document(s) and pages)

B.2.2.6 Protection against accidental or unintentional changes

Requirement: Relevant software and measurement data shall be protected against accidental or unintentional changes.

Table B.12 — Documentation with regard to the protection against accidental or unintentional changes

Required documentation: The documentation should show the measures that have been taken to protect the software and data against unintentional changes.
Include information or reference (document(s) and pages)

Table B.13 — Specifying notes with regard to the protection against accidental or unintentional changes

1. Incorrect program design, e.g. incorrect loop operation, changing global variables in a function, etc.; the avoidance requires as far as possible testing.
Include information or reference (document(s) and pages)
2. Accidental overwriting or deletion of stored data and programs (refer also to Extension.
Include information or reference (document(s) and pages)
3. Incorrect assignment of measurement transaction data. Measurements and data belonging to one measurement transaction have not to be mixed with those of a different transaction due to incorrect programming or storage; the avoidance requires as far as possible testing and additional requests for confirmation of actions wherever useful.
Include information or reference (document(s) and pages)
4. Physical effects (electromagnetic interference, temperature, vibration, etc.); the avoidance requires self-checks of the software.
Include information or reference (document(s) and pages)
5. For type P2: Misuse of the operating system; the avoidance requires programmers who are sufficiently familiar with the operating system used
Include information or reference (document(s) and pages)

B.2.2.7 Protection against intentional changes

Requirement: Relevant software and measurement data shall be secured against inadmissible modification.

Table B.14 — Documentation with regard the protection against intentional changes

Required documentation: The documentation should provide assurance that software and stored measurement data cannot be inadmissibly modified.
Include information or reference (document(s) and pages)

Table B.15— Specifying notes for type P1

1 Manipulation of program code could be possible by manipulating the physical memory, i.e. the memory is physically removed and substituted by one containing fraudulent software or data. To prevent this happening, either the housing of the instrument should be secured or the physical memory itself is secured against unauthorised removal.
Include information or reference (document(s) and pages)
2 All functions in the interface shall be subject to examination (see A.3.2.5, "Influence via communication interface"). Where the interface is to be used for software download, extension D has to be complied with.
Include information or reference (document(s) and pages)
3 Data are considered to be sufficiently protected if only relevant software processes them. If non-relevant Software is intended to be changed after approval, requirements of extension S have to be followed.
Include information or reference (document(s) and pages)

Table B.16 — Specifying notes with regard to the protection against intentional changes

1. Changes with the intention of fraud could be attempted by: a. Changing the program code including integrated data - if the program code is an executable format (.exe) then it is sufficiently protected. b. Changing the stored measurement data – refer to Extension L
Include information or reference (document(s) and pages)
2a. Means that consider the capabilities of the operating system shall be taken to prevent the approved software from being replaced by non-approved software using the operating system (see also A.3.2.4, "Influence via user interface"). For authorized downloading software see Extension D.
Include information or reference (document(s) and pages)
2b. The mass storage device where relevant data, configuration files, programs and parameters are stored shall be protected against physical exchange.
Include information or reference (document(s) and pages)
3. Means shall be taken to protect relevant software from modifications by using the operating system or other simply available and manageable tools (see also A.3.2.4, "Influence via user interface").
Include information or reference (document(s) and pages)
4. The parts and features of the operating system that implement the protection of the measuring system shall be considered as relevant software and be protected as such.
Include information or reference (document(s) and pages)

B.2.2.8 Parameter protection

Requirement: Relevant parameters shall be secured against unauthorised modification.

Table B.17 — Documentation with regard parameter protection

Required documentation: The documentation shall describe all of the relevant parameters, their ranges and nominal values, where they are stored, how they may be viewed, how they are secured and when. The documentation shall describe how the traceability of relevant parameter modifications is guaranteed.
Include information off all the relevant parameters or reference (document(s) and pages) If relevant parameters can be modified describe audit trail

Table B.18 — Specifying notes with regard parameter protection

1. Type specific parameters are identical for each specimen of the type and are in general part of the program code. Therefore requirement A.3.2.7, "Protection against intentional changes" applies to them.
List type specific parameters
2. Device specific secured parameters may be changed using an on-board keypad or switches or via interfaces, but only before they have been secured. Because device specific parameters could be manipulated using simple tools on universal computers they shall not be stored in standard storages of a universal computer. Storing of these parameters is acceptable only in additional hardware.
List device specific parameters
3. Settable device-specific parameters may be changed after securing. Traceability of relevant parameter changes has to be provided.
List settable specific parameters

B.2.2.9 Software authenticity and presentation of results (only for type P2)

Requirement: Means shall be employed to ensure the authenticity of the relevant software. The authenticity of the results that are presented shall be guaranteed.

Table B.19 — Documentation with regard to software authenticity

Required documentation: The documentation should describe how authenticity of the software is guaranteed
Include information or reference (document(s) and pages)

Table B.20 — Specifying notes with regard to software authenticity

1. It shall not be possible to fraudulently simulate (spoof) approved relevant software using the capabilities of the operating system or other simply available and manageable tools.
Include information or reference (document(s) and pages)
2. Device specific secured parameters may be changed using an on-board keypad or switches or via interfaces, but only before they have been secured. Because device specific parameters could be manipulated using simple tools on universal computers they shall not be stored in standard storages of a universal computer. Storing of these parameters is acceptable only in additional hardware.
Include information or reference (document(s) and pages)
3. Presented measurement values shall be comprehensibly and accompanied by any information necessary to avoid confusion with other (non-relevant) information.
Include information or reference (document(s) and pages)
4. Under consideration of the capabilities of the operating system, it shall be ensured by technical means that on the universal computer only the software approved for the relevant purpose can perform the relevant functions (e.g. a sensor shall only work together with the approved program).
Include information or reference (document(s) and pages)
5. It shall be ensured by technical means, that relevant software check its integrity and authenticity on a regular basis (time intervals) during its execution.
Include information or reference (document(s) and pages)

B.2.3 Extension L: Specific software requirements for long term storage

B.2.3.1 Completeness of measurement data stored

Requirement: The requirements given in this section are to apply in addition to previous set of requirements.

Table B.21 — Documentation with regard to completeness of measurement data stored

Required documentation: Description of all fields of the data sets.
Include information or reference (document(s) and pages)

Table B.22 — Specifying notes with regard to completeness of measurement data stored

1. The stored measurement data may be needed for reference at a later date. All relevant data shall be stored together with the measurement value.
Include information or reference (document(s) and pages)

B.2.3.2 Protection against accidental or unintentional changes

Requirement: Stored data shall be protected against accidental and unintentional changes.

Table B.23 — Documentation with regard to the protection against accidental or unintentional changes

Required documentation: Description of protection measures (e.g. the checksum algorithm, including the length of the generator polynomial).
Include information or reference (document(s) and pages)

Table B.24 — Specifying notes with regard to the protection against accidental or unintentional changes

1. Accidental changes of data can be caused by physical effects.
2. Unintentional changes are caused by the user of the device. Automatic or semi- automatic means should be used to ensure that only specified data are deleted and that the accidental deletion of "live" data are avoided. This is particularly important on networked systems and remote or removable storage where users might not realize the significance of the data.
Include information or reference (document(s) and pages)
3. A checksum shall be calculated by the receiver and compared with the attached nominal value. If the values match, the data set is valid and may be used; otherwise it has to be deleted or marked invalid.
Include information or reference (document(s) and pages)

B.2.3.3 Integrity of data

Requirement: The measurement data stored has to be protected against intentional changes.

Table B.25 — Documentation with regard to the integrity of data

Required documentation: The method of how the protection is realized shall be documented.
Include information or reference (document(s) and pages)

Table B.26— Specifying notes with regard to the integrity of data.

1. This requirement applies to all types of storages except integrated storages.
List all non-integrated storages.
2. The protection has to apply against intentional changes carried out by simple common software tools.
3. Simple common software tools are understood as tools, which are easily available and manageable as e.g. office packages.

B.2.3.4 Authenticity of measurement data stored

Requirement: The measurement data stored has to be capable of being authentically traced back to the measurement that generated them.

Table B.27 — Documentation with regard to the authenticity of measurement data stored

Required documentation: Description of the method used for ensuring the authenticity.
Include information or reference (document(s) and pages)

Table B.28 — Specifying notes with regard to the authenticity of measurement data stored

1. The authenticity of measurement data may be needed for reference at a later date.
2. Authenticity requires the correct assignment (linking) of measurement data to the measurement that has generated the data.
Include information or reference (document(s) and pages)
3. Authenticity presupposes an identification of data sets.
Include information or reference (document(s) and pages)
4. Ensuring authenticity does not necessarily require an encryption of the data.

B.2.3.5 Confidentiality of keys

Requirement: Keys and accompanying data have to be treated as relevant data and have to be kept secret and be protected against compromise by software tools.

Table B.29 — Documentation with regard to the confidentiality of keys

Required documentation: Description of the key management and means for keeping keys and associated information secret.
If secret key is used, include information or reference (document(s) and pages)

Table B.30 — Specifying notes with regard to the confidelity of keys

1. This requirement only applies if a secret key is used.
2. This requirement applies to measurement data storage, which are external from the measuring instrument or realized on universal computers.
3. The protection has to apply against intentional changes carried out by common simple software tools.
4. If the access to the secret keys is prevented, e.g. by sealing the housing of a built for purpose device, no additional software protection means are necessary.

B.2.3.6 Retrieval of stored data

Requirement: The software used for verifying measurement data sets stored shall display or print the data, check the data for changes, and warn if a change has occurred. Data that are detected as having been corrupted has not to be used.

Table B.31 — Documentation with regard to the retrieval of stored data

Description of the functions of the retrieval program.
Include information or reference (document(s) and pages)
Description of detection of corruption.
Include information or reference (document(s) and pages)
Operating manual for this program.
Include information or reference (document(s) and pages)

Table B.32 — Specifying notes with regard to the retrieval of stored data

1. The measurement data stored might need to be referred to at a later date. If there is a doubt on the correctness of a delivery note or ticket, it has to be possible to identify the measurement data stored to the disputed measurement without ambiguity refer also A.3.3.2 "Completeness of measurement data stored", A.3.3.4 "Integrity of data", A.3.3.5 "Authenticity of measurement data stored" and A.3.3.6 "Confidentiality of keys").
Include information or reference (document(s) and pages)
2. The identification number (see A.3.3.2 "Completeness of measurement data stored") has to be printed out on the delivery note/ticket for the customer along with an explanation and a reference to the storage source.
Include information or reference (document(s) and pages)
3. Verification means checking the integrity, authenticity and correct assignment of the measurement data stored.
Include information or reference (document(s) and pages)
4. The verification software used for displaying or printing the data stored shall be considered relevant.
Include information or reference (document(s) and pages)

B.2.3.7 Automatic storing

Requirement: The measurement data has to be stored automatically when the measurement is concluded.

Table B.33— Documentation with regard to automatic storing

Required documentation: Confirmation that storing is automatically carried out. Description of the Graphical User Interface.
Include information or reference (document(s) and pages)

Table B.34 — Specifying notes with regard to automatic storing

1. This requirement applies to all types of storage.
2. This requirement means that the storing function has to not depend on the decision of the operator.
Include information or reference (document(s) and pages)
3. For the case of full storage, refer to requirement A.3.3.9 "Storage capacity and continuity"

B.2.3.8 Storage capacity and continuity

Requirement: The long-term storage has to have a capacity which is sufficient for the intended purpose.

Table B.35 — Documentation with regard to storage capacity and continuity

Required documentation: Description of management of exceptional cases when storing measurement values.
Include information or reference (document(s) and pages).

Table B.36 — Specifying notes with regard to storage capacity and continuity

1. When a storage is full or removed/disconnected from the instrument, a warning shall be given to the operator. A warning is not necessary, if it is ensured by construction that only outdated data can be overwritten.
2. The regulation concerning the minimum period for storing measurement data are beyond the scope of this requirement and is left to national regulations. It is the responsibility of the owner to have an instrument with sufficient storage capacity to fulfil the requirements applicable to his activity. The software test will check only that the data are stored and retrieved correctly and whether new transactions are inhibited when the storage is full.
3. It is also beyond the scope of this requirement to require certain inscriptions on the device as concerning the capacity of the storage the capacity or other accompanying information that allow calculating the capacity. However, the manufacturer shall make available the information on the capacity.

B.2.4 Extension T: Specific software requirements for data transmission

B.2.4.1 Completeness of transmitted data

Requirement: The transmitted data has to contain all relevant information necessary to present or further process the measurement result in the receiving unit.

Table B.37 — Documentation with regard to the completeness of transmitted data

Required documentation: Document all fields of the data set.
Include information or reference (document(s) and pages)

Table B.38 — Specifying notes with regard to the completeness of data

1. The relevant part of a transmitted data set comprises one or more measurement values with correct resolution, the unit of measure, the time and the place of the measurement.

B.2.4.2 Protection against accidental or unintentional changes

Requirement: Transmitted data shall be protected against accidental and unintentional changes.

Table B.39 — Documentation with regard to the protection against accidental or unintentional changes

Required documentation: Description of the checksum algorithm, if used, including the length of the generator polynomial. Description of an alternative method if used.
Include information or reference (document(s) and pages)

Table B.40 — Specifying notes with regard to the protection against accidental or unintentional changes

1. Accidental changes of data can be caused by physical effects.
Include information or reference (document(s) and pages)
2. Unintentional changes are caused by the user of the device.
Include information or reference (document(s) and pages)
3. Means shall be provided to detect transmission errors.
Include information or reference (document(s) and pages)

B.2.4.3 Integrity of data

Requirement: The relevant transmitted data has to be protected against intentional changes with software tools.

Table B.41 — Documentation with regard to the integrity of data

Required documentation: Description of the protection method
Include information or reference (document(s) and pages)

Table B.42 — Specifying notes with regard to the integrity of data

1. This requirement only applies to networks that are open or closed with non-relevant devices, not to closed networks.
2. The protection has to apply against intentional changes carried out by common simple software tools.
3. Simple common software tools are understood as tools, which are easily available and manageable as e.g. office packages.

B.2.4.4 Authenticity of transmitted data

Requirement: For the receiving program of transmitted relevant data, it shall be possible to verify the authenticity and the assignment of measurement values to a certain measurement.

Table B.43 — Documentation with regard to the authenticity of transmitted data

Required documentation: Network with unknown participants: Description of the IT means for correct assigning of measurement value to measurement.
Include information or reference (document(s) and pages)
Closed network: Description of the hardware means preserving the number of participants in the network. Description of initial identification of the participants.
Include information or reference (document(s) and pages)

Table B.44 — Specifying notes with regard to the authenticity of transmitted data

1a In a network with unknown participants, it is necessary to identify the origin of measurement data transmitted without ambiguity. (The authenticity relies on the identification number of the data set and the network address).
Include information or reference (document(s) and pages)
1b In a closed network all participants are known. No additional IT means are necessary, but the topology of the network (the number of participants) shall be fixed by sealing.
Include information or reference (document(s) and pages)
2. Unforeseen delays are possible during transmission. For a correct assignment of a received measurement value to a certain measurement the time of measurement has to be registered.
Include information or reference (document(s) and pages)
3. To ensure the authenticity, an encryption of measurement data are not necessarily required.
Include information or reference (document(s) and pages)

B.2.4.5 Confidentiality of keys

Requirement: Keys and accompanying data have to be treated as relevant data and have to be kept secret and be protected against compromise by software tools.

Table B.45 — Documentation with regard to the confidentiality of keys

Required documentation: Description of the key management and means for keeping keys and associated information secret.
If secret key is used, include information or reference (document(s) and pages)

Table B.46 — Specifying notes with regard to the confidentiality of keys

1. This requirement only applies if a secret key exists in the system. (Normally not in Closed networks.).
2. The protection has to apply against intentional changes carried out by common simple software tools.
3. If the access to the secret keys is prevented e.g. by sealing the housing of a built for purpose device, no additional software protection means are necessary.

B.2.4.6 Handling of corrupted data

Requirement: Data that are detected as having been corrupted has to not be used.

Table B.47 — Documentation with regard to the handling of corrupted data

Required documentation: Description of the detection of transmission faults or intentional changes.
Include information or reference (document(s) and pages)

Table B.48 — Specifying notes with regard to the handling of corrupted data

1. Though communication protocols normally repeat transmission until it succeeds, it nevertheless is possible that a corrupted data set is received.

B.2.4.7 Transmission delay

Requirement: The measurement has not to be inadmissibly influenced by a transmission delay.

Table B.49 — Documentation with regard to the transmission delay

Required documentation: Description of the concept, how measurement is protected against transmission delay
Include information or reference (document(s) and pages)

Table B. 50 — Specifying notes with regard to the transmission delay

The manufacturer shall investigate the timing of the data transmission and shall guarantee that under worst case conditions the measurement is not inadmissibly influenced.
Include information or reference (document(s) and pages)

B.2.4.8 Availability of transmission services

Requirement: If network services become unavailable, no measurement data has to get lost.

Table B.51 — Documentation with regard to the availability of transmission services

Required documentation: Description of protection measures against transmission interruption or other failures.
Include information or reference (document(s) and pages)

Table B.52 — Specifying notes with regard to the availability of transmission services

1. The user of the measuring system has not to be able to corrupt measurement data by suppressing transmission.
Include information or reference (document(s) and pages)
2. Transmission disturbances happen accidentally and cannot be excluded. The sending device has to be able to handle this situation.
Include information or reference (document(s) and pages)

B.2.5 Extension S: Specific software requirements for software separation

B.2.5.1 Realization of software separation

Requirement: There shall be a part of the software that contains all relevant software and parameters that is clearly separated from other parts of software.

Table B.53 — Documentation with regard to the realization of software separation

Required documentation: Description of the protective interface described in the specifying notes above.
Include information or reference (document(s) and pages)

Table B.54— Specifying notes with regard to the realization of software separation

Low level separation: Merging software units on the level of the programming language or merging parts of a programme (i.e. subroutines, procedures, functions, classes) to form the relevant part of the programme. The rest of the programme is the non-relevant part. **High level separation**: Merge all parts of the software to one object that is identifiable by the operating system (a programme, a DLL etc.). The rest of the software is the non-relevant part.
1. In the case of low level separation, all program units (subroutines, procedures, functions, classes, etc.) and in case of high level separation all programs and libraries • that contribute to the calculation of measurement values or have an impact on it, • that contribute to auxiliary functions such as displaying data, data security, data storage, software identification, performing software download, data transmission or storing, verifying received or stored data etc. belong to the relevant software.
Include information or reference (document(s) and pages)
2. All variables, temporary files and parameters that have an impact on measurement value or on relevant functions or data belong to the relevant software.
Include information or reference (document(s) and pages)
3. The protective software interface itself (see A.3.5.4 "Protective software interface") is part of the relevant software.
4. Non-relevant software comprises the remaining program units, data or parameters not covered above. Modifications to this part are allowed without informing the testing organization provided the subsequent requirements of software separation are observed.

B.2.5.2 Mixed indication

Requirement: Additional information generated by the software, which is not relevant, may only be shown on a display or printout, if it cannot be confused with the information that originates from the relevant part.

Table B.55 — Documentation with regard to mixed indication

Required documentation: Description of the software that realizes the indication. Description how the indication of relevant data are protected against misleading indication generated by non-relevant software.
Include information or reference (document(s) and pages)

Table B.56 — Specifying notes with regard to mixed indication

As the programmer of the non-relevant software may not know about the admissibility of indications, it is the responsibility of the manufacturer to guarantee that all indicated information fulfil the requirement.
Include information or reference (document(s) and pages)

B.2.5.3 Protective software interface

Requirement: The data exchange between the relevant and non-relevant software has to be performed via a protective software interface, which comprises the interactions and data flow.

Table B.57 — Documentation with regard to protective software interface

Description of the software interface, especially which data domains realize the interface.
Include information or reference (document(s) and pages)
A complete list of all commands together with a declaration of completeness.
Include information or reference (document(s) and pages)
A brief description of their meaning and their effect on the functions and data of the measuring instrument.
Include information or reference (document(s) and pages)

Table B.58 — Specifying notes with regard to protection software interface

1. All interactions and data flows shall not inadmissibly influence the relevant software including the dynamic behaviour of a measuring process.
Include information or reference (document(s) and pages)
2. There shall be an unambiguous assignment of each command sent via the software interface to the initiated function or data change in the relevant software.
Include information or reference (document(s) and pages)
3. Codes and data that are not declared and documented as commands have not to have any effect on the relevant software.
Include information or reference (document(s) and pages)
4. The interface shall be completely documented and any other non-documented interaction or data flow (circumvention of the interface) has not to be realized neither by the programmer of the relevant software nor by the programmers of the non-relevant software.
Include information or reference (document(s) and pages)
Note: The programmers are responsible for observing these constraints. Technical means to prevent them from circumventing the software interface are not possible. The programmer of the protective interface should be instructed about this requirement.
Include information or reference (document(s) and pages)

B.2.6 Extension D: Specific software requirements

B.2.6.1 Download mechanism

Requirement: Downloading and the subsequent installation of software shall be automatic and shall ensure that the software protection environment is at the approved level on completion.

Table B.59 — Documentation with regard to download mechanism

Required documentation: The documentation should briefly describe the automatic nature of the download, checking, installation, how the level of protection is guaranteed on completion, what happens if a fault occurs.
Include information or reference (document(s) and pages)

Table B.60 — Specifying notes with regard to download mechanism

1. Downloading shall be automatic to ensure that the existing level of protection is not compromised.
Include information or reference (document(s) and pages)
2. The target device has a fixed relevant software that contains all of the checking functions necessary for fulfilling requirements A.3.6.3 "Authentication of downloaded software" to A.3.6.5 "Traceability of relevant software download".
Include information or reference (document(s) and pages)
3. The instrument should be capable of detecting if the download or installation fails. A warning shall be given. If the download or installation is unsuccessful or is interrupted, the original status of the measuring instrument shall be unaffected. Alternatively, the instrument shall display a permanent error message and its functioning shall be inhibited until the cause of the error is corrected.
Include information or reference (document(s) and pages)
4. On successful completion of the installation, all protective means should be restored to their original state unless the downloaded software has authorization in the test certificate to amend them.
Include information or reference (document(s) and pages)
5. During download and the subsequent installation of downloaded software, measurement by the instrument shall be inhibited or correct measurement shall be guaranteed.
Include information or reference (document(s) and pages)
6. The fault handling requirements described in Extension I may be implemented if faults occur during downloading. The number of re-installation attempts shall be limited.
Include information or reference (document(s) and pages)
7. If the requirements A.3.6.3 "Authentication of downloaded software" to A.3.6.5 "Traceability of relevant software download" cannot be fulfilled, it is still possible to download the non- relevant software part. In this case, the following requirements shall be met: There is a distinct separation between the relevant and non-relevant software according to Extension S. The whole relevant software part is fixed i.e. it cannot be downloaded or changed without breaking a seal. It is stated in the test certificate downloading of the non-relevant part is acceptable.
Include information or reference (document(s) and pages)
8. It shall be possible to disable the software download mechanism by means of a sealable setting (switch, secured parameter) for member states where software download for instruments in use is not allowed. In this case, it has not to be possible to download relevant software without breaking the seal.
Include information or reference (document(s) and pages)

B.2.6.2 Authentication of downloaded software

Requirement: Means shall be employed to guarantee that the downloaded software is authentic, and to indicate that the downloaded software has been approved by a testing organization.

The documentation should describe: the following items of Table B.61:

Table B.61 — Documentation with regard to the authentication of downloaded software

How authenticity of the software identification is guaranteed
Include information or reference (document(s) and pages)
How the authenticity of approval is guaranteed
Include information or reference (document(s) and pages)
How it is guaranteed that the downloaded software is approved for the type of measuring instrument to which it has been downloaded.
Include information or reference (document(s) and pages)

Table B.62 — Specifying notes with regard to the authentication of downloaded software

1. Before the downloaded software is used for the first time, the measuring instrument shall automatically check that:
a. The software is authentic (not a fraudulent simulation).
b. The software is approved for that type of measuring instrument.
Include information or reference (document(s) and pages)
2. The means by which the software identifies its approval status shall be made secure to prevent counterfeiting of the status.
Include information or reference (document(s) and pages)
3. If downloaded software fails any of the above tests, see B.2.5, B.2.5.1, "Download mechanism".
Include information or reference (document(s) and pages)
4. If a manufacturer intends to change or update the relevant software he shall announce the intended changes to the responsible testing organization. The testing organization decides whether an addition to the existing test certificate is necessary or not. For software download it is indispensable that there is a software identification which is unambiguously assigned to the approved software version.
Include information or reference (document(s) and pages)

B.2.6.3 Integrity of downloaded software

Requirement: Means shall be employed to guarantee that the downloaded software has not been inadmissibly changed during download.

Table B.63— Documentation with regard to the integrity of downloaded software

Required documentation: The documentation shall describe how the integrity of the software is guaranteed.
Include information or reference (document(s) and pages)

Table B.64 — Specifying notes with regard to the integrity of downloaded software

1. Before the downloaded software is used for the first time, the measuring instrument shall automatically check that the downloaded software has not been inadmissibly changed.
Include information or reference (document(s) and pages)
2. If the downloaded software fails this test, see B.2.5.1, “Download mechanism”.
Include information or reference (document(s) and pages)

B.2.6.4 Traceability of relevant software download

Requirement: It shall be guaranteed by appropriate technical means that downloads of relevant software are adequately traceable within the instrument for subsequent controls.

Table B.65— Documentation with regard to the traceability of relevant software download

Required documentation: The documentation shall: • Briefly describe how the traceability means is implemented and protected. • State how downloaded software may be traced.
Include information or reference (document(s) and pages)

Table B.66— Specifying notes with regard to the traceability of relevant software download

1. This requirement enables inspection authorities, to back-trace downloads of relevant software over an adequate period of time (that depends on national legislation).
Include information or reference (document(s) and pages)
2. The traceability means and records are part of the relevant software and should be protected as such.
Include information or reference (document(s) and pages)

B.2.6.5 Download consent

Table B.67 — Documentation with regard to download consent

It is assumed that the manufacturer of the measuring instrument keeps his customer well informed about updates of the software, especially the relevant part, and that the customer will not deny updating it. Furthermore it is assumed that manufacturer and customer, user, or owner of the instrument will agree on an appropriate procedure of performing a download depending on the use and location of the instrument.
Include information or reference (document(s) and pages)

B.3 Test requirement for type P3

Please submit your ISO/IEC 27001 compliance certificate.

For each channel transmitting relevant data that will maintain its relevant status (and has not been treated in B.2 "Test requirement for type P1 and P2") copy and fill the following sections:

B.2.4, "Extension T: Specific software requirements for data transmission"

B.2.2.5, "Influence via communication interface"

For each channel that will not maintain data relevant status (and has not been treated in B.2 "Test requirement for type P1 and P2") copy and fill the following section:

B.2.2.5, "Influence via communication interface"

Regarding the communication via a web service the additional copy and fill the following section:

B.2.2.4, "Influence via user interface"

Annex C
(informative)

Example of data form describing suitability for use of equipment of a specific series (to be filled in by the manufacturer)

Name of test body: **Number and date of test reports:**	**Manufacturer stamp:** **Date:** **Signature:**	manufacturer	laboratory
Type of recorder			
Suitable for storage			
Suitable for transport			
I - General requirements			
Measuring range (see 5.2)			
Chart (disk, tape) (see 5.5.3)			
Autonomous power supply (see 5.6)			
Degree of protection provided by the enclosure (see 5.7)			
Supply voltage (see 5.9.1)			
Frequency (see 5.9.3)			
Power cut-offs (see 5.9.4)			
II - Requirements for metrological characteristics			
Maximum permissible error and resolution (see 5.10.2.1) and temperature measurement error (see 6.3)			
Recording interval (see 5.10.2.3)			
Recording duration (see 5.10.2.4)			
Storage duration (see Annex D)			
Maximum relative timing error (see 5.10.2.4) and time recording error (see 6.5)			
Response time (see 5.10.2.5 and 6.4)			
Climatic environment (see 5.10.3.1) and influence of ambient temperature (see 6.6.3)			
Mechanical vibrations (see 5.10.3.2 and 6.6.6)			
Shock resistance (see 5.10.3.3 and 6.6.5)			
Climatic environment (see 5.10.3.1) and temperature testing under storage and transport conditions for the recorder (see 6.6.4)			
Electrical power disturbances and susceptibility to radiated electromagnetic field (see 5.9.5) and dielectric strength (see 6.6.9)			

Annex D
(informative)

Expected operation time and storage capacity

D.1 Storage capacity dependent on the measurement interval

The following table shows the storage capacity of the data logger dependent on the measurement interval. The higher the measurement interval is the faster the free memory space on the device will decrease. The device can store up to **< Fill in data >** measurement values. Additional probes and transmission intervals have to be taken into account.

Table D.1 — Measurement interval storage capacity

Measurement interval	**Storage capacity**
5 min	**Fill in data**
10 min	**Fill in data**
15 min	**Fill in data**

Please note that the memory may be erasable, so that a new measurement can use the entire memory space. Higher measurement rates will result in shorter lifetimes. The measurement interval has an significant impact on the battery lifetime.

D.2 Battery lifetime dependent on usage

When used regularly, the battery will last for a limited period given by the manufacturer.

Excessive usage of power consuming features (backlights, LEDs, number of probes, transmission interfaces and intervals, etc.) and/or usage of the device for a significant amount of time within environments, see Table B.2, can reduce the battery lifetime dramatically. The data can only be retrieved as long as the device has sufficient power. It is recommended to read out and store the data directly after the measurement is finished, or in regular intervals.

Table D.2 — Different temperature levels

Temperature **°C**	**Typical lifetime** [a] **(days or years)**
+25	
0	
−20	
(+)T	
(-)T	

[a] Additional influences such as power consuming features and measurement intervals will have additional impacts.

Annex E
(informative)

Required access to recorded data or functions is given in Table E.1

Required access to recorded data or functions is given in Table E.1.

Table E.1 — Required access to recorded data or functions

	Data display	print out data or save data	Calibration of sensors	Correction or verification of date and time settings	change of the correction factor of the sensor
User	X	X			
Client (sender/owner/receiver of goods)	X	X			
Government / Veterinarian and Pharma authorities	X	X			
In service inspection / maintenance	X	X	x	x	X

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.
- Standards purchased in hard copy format:
- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.