INTERNATIONAL MINIMUM REQUIREMENTS

FOR

ELECTRONIC CLOCKING SYSTEMS

By: - Fédération Colombophile Internacionale
- Manufacturers Electronic Clocking Systems and Chip-rings
- Testing Agency

Version: v. 2022.04 (dated 2022/10/31)

Contents

Introduction

This International Minimum Requirements document has been composed for member countries of FCI (Fédération Colombophile Internacionale) and manufacturers, to set the minimum requirements for the electronic clocking systems, in order to help improve the integrity of software and hardware of racing pigeon clocking systems.

Specifically the requirements for systems and chip-rings must ensure that system functionality cannot easily be compromised and that unauthorized tampering with system components will be detected or discovered.

The requirements consist of assessment regulations, the international standard for electronic clocking systems, security requirements for electronic clocking systems and demands for the performance of foot-rings, combi-rings and electronic chip-rings.

The requirements are composed and supported by FCI for Electronic Clocking Systems, the praesidiums of FCI-member countries, the manufacturers of Electronic Clocking Systems and Testing Agencies.

1. Glossary of Terms

These pages aim to introduce new terms and clarify controversial ones regarding the document 'International Minimum Requirements for Electronic Clocking Systems'.

1.1 Chip-ring or electronic ring	A ring, provided with an integrated electronic chip which contains identification (Chip Number) - and additional user-data that can, in accordance with requirements, be read and written electronically.
1.2 Combi-ring	A combi-ring combines the foot-ring- and chip-ring-functions by integrating an interchangeable, electronic chip-unit with the foot-ring. The chip-unit contains the chip with the identification (Chip Number) - and additional user data for electronic clocking.
1.3 Copy-ring	The term used instead of cloned rings.
1.4 Custom-ID	The custom-ID is the first 8 bits of the Chip Number and is a reference to the type of the chip and the manufacturer of the chip. Every manufacturer has an own dedicated custom-ID, that is unique. Custom-ID's are managed and assigned by the FCI. With the custom-ID, every manufacturer has a separate number range to prevent duplicated ring ID's on the market (copy rings). No manufacturer is allowed to use a custom-ID that had already been assigned to another manufacturer.
1.5 Declaration of responsibility	Previously referred to as 'anti-fraud guarantee'. Because pigeon federations and system developers have the same interest in preventing fraud, the system developer should give a kind of declaration of responsibility to individual federations.
1.6 ET	Electronic Timer, also referred to as 'electronic clock', 'pigeon clock' or 'fancier clock'. Fancier's data, pigeon data and race results (arrival times) are stored in the ET's memory.
1.7 ETS	Electronic Timer System. Also referred to as Electronic (racing pigeon) Clocking System.
1.8 Foot-ring	A foot-ring is a ring which, once put on a pigeon's leg, serves as an identification of the pigeon, gathered from a clearly readable number, the foot-ring number.
1.9 Homologation procedure	ETS manufacturers cooperating with FCI get an FCI-certificate of homologation. FCI keeps a list of all approved ETS on the market. (The approval procedure is explained in the material 'International Minimum Requirements for Electronic Clocking Systems'.)

1.10 Investigation	Target of the investigation for acceptance (hereafter mentioned: investigation) is to verify that a system is able to meet the requirements to electronic clocking systems. The Testing Agency will handle the Assessment Regulations and related requirements as a basis for the investigation of a system to be carried out. An investigation may only be carried out in accordance with the quotation, based on the availability of all necessary materials and documentation of the system, for which the applicant has requested a certificate.
1.11 Linking	Linking (or coupling) is the operation where the federation's band numbers are referenced (linked or coupled) to the electronic ring ID's.
1.12 Procedures in the Club	Protocols for basketing, read out, result processing and linking; serving as a guide to fanciers on how to check the basics.
1.13 Project dossier	For each request for an investigation a dossier will be set up. The dossier will contain all information in relation to the request and its treatment by the Testing Agency. The information will be saved at least for 5 years on behalf of eventual complaints or arbitration.
1.14 Read out	When the pigeons are home the fancier clock has to be returned to the club to print the clocking (arrival) list. The first important action is synchronizing the master timer (HKW, GPS, master clock). Synchronizing the master timer must be done by a commission (more than one person).
1.15 Reporting	The report from the Testing Agency given at the end of the testing process will comprise the following elements: characteristics of the tested product, requirements and criteria (limiting values) used for comparison, testing- and measuring results, comparison of the results, Declaration of Conformity with signature and other relevant notes.
1.16 Request	When a manufacturer has sent a request for the (continuation of) certification of a product to FCI and this request was accepted by FCI, FCI will send an application for an assessment by an FCI-acknowledged, independent office chosen by the manufacturer, hereafter named: Testing Agency. The manufacturer or applicant provides FCI with the necessary information about the product to be certified, so as to enable FCI to come to a right judgement of the request to certification.
1.17 RFID	Radio-frequency identification (RFID) is the use of an object (typically referred to as an RFID tag or transponder) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves.

1.18 Online ETS	Network operating ETS or Cloud-ETS. An electronic Timer System connected with a cloud database in the manufacturers webserver (ETS-server), for uploading and monitoring race data. In an Online ETS, the club- and loft systems are connected with the ETS-server by Internet or APN, via local or mobile network.
1.19 ETS-server	An ETS- (cloud-) server with server data base, the manufacturer's webserver containing the database of race data from club- and loft systems. The server data base may have a private part for uploaded clocking data and a part for final storage of race data after processing.
1.20 Remote strike-off	Remote strike, online strike-off or remote knock-off. This facility offers the possibility for the fancier, after he stopped a race, to strike-off at home, without travelling to the Club-system. As a consequence, RTC and clocking data must securely be communicated between the fancier's loft system and the ETS-server (master time).
1.21 Non-cloud remote strike-off	ETS with remote strike are on the market, using a (private) network for transmission of race data to the club at the end of a race.

2. Assessment regulations

Contents

Introduction

The increasing complexity of products (the electronic pigeon-identification systems and chip-rings) and growing distance between manufacturer and user (the fancier) brings forward the need of quality guarantee and a certificate. A certificate proves the existence of a justified confidence that electronic clocking systems and chip-rings are delivered according to Assessment regulations as referred to in the certificate.
Issuing (product)certificates for electronic clocking systems and chip-rings is internationally reserved to a dedicated FCI-committee. The FCI-committee acts as an independent, corporate body of at least three persons from different institutes. They decide about the order for an assessment and certification of a system or chip-ring on basis of a report of the testing agency. The assessment, carried out by the testing agency, takes place according the assessment regulations given in this chapter.

2.1 Request for a certificate

When a manufacturer has sent a request for the (continuation of) certification of a product to FCI (or its certification body) and this request was accepted by FCI, FCI will send an application for an assessment by an FCI-acknowledged, independent bureau, hereafter named: Testing Agency.

At a request to certification, FCI sends the manufacturer a query and provide the necessary information, incorporating these Assessment Regulations. If requested by the manufacturer and with the permission of FCI, the Testing Agency may directly provide the Assessment Regulations to the manufacturer.

The manufacturer or applicant provides FCI with the necessary information about the product to be certified, so as to enable FCI to come to a right judgement of the request to certification.

The applicant may send the necessary information for the request to certification directly to the Testing Agency. The latter will then inform FCI about the request for an assessment.

The Testing Agency, when requested by FCI, will make a quotation to FCI, with statement about cost for the requested investigation.

The order for the investigation (or additional investigation) to the Testing Agency will be given by FCI.

The quotation of the Testing Agency will mention the activities to be carried out, the contact person, terms of delivery and planning information, in order to bring forth a declaration of conformity.

The Testing Agency is essentially due to consider all requests for certification. When serious arguments arise against further considering a request, the Testing Agency will contact FCI about this.

2.2 The investigation

Target of the investigation for acceptance (hereafter mentioned: investigation) is to verify that a system is able to meet the requirements for racing pigeon clocking systems.

The Testing Agency will handle these Assessment Regulations and related requirements (in Annex) as a basis for the investigation of a system to be carried out.

An investigation may only be carried out in accordance with the quotation, based on the availability of all necessary materials and documentation of the system, for which the applicant has requested a certificate. The applicant may not do with just delivering the system or system components.

The necessary materials are:
- A working system and related hardware, necessary for the tests.
- Design documentation of the hardware: housing and electronic components;
- Components list(s);
- Design documentation of the software (flowcharts) of security functions (data protection mechanisms);
- Description of storage of fraud-sensitive data (flight data, software, keys);
- Descriptions of algorithms and key management to go with cryptographic security (if applied).

An investigation is quoted on request by FCI. The offered work will comprise:
- Examination of hardware and software documentation
- Functional tests of a working system or component
- Physical tests and verifications
- Testing to the Requirements
- Correspondence and discussion with the applicant, when necessary
- Reporting in Dutch and English language.

The quotation of the Testing Agency will be valid for two months.

At positive result of an investigation, a test report will be generated to FCI within 6 weeks after start of the investigation. This report contains descriptions of the product, the carried out tests, test results, used materials and conclusions.
A signed Declaration of Conformity will be added in a separate annex to the test report.

The delivery terms of the test report may be adapted when during the investigation delay in testing occur, for example owing to system defects.

When during an investigation the (interim) results obviously show that the investigation will not lead to a declaration of conformity or, respectively, an approval, the Testing Agency will immediately inform the manufacturer and FCI about this and will, until further notice, stop the investigation.

If the applicant or FCI, after disclosure of negative (interim) results, or for other well-founded reasons does not want to continue the investigation, the cost for testing made so far will be charged.

Continuation of an interrupted investigation can take place within 3 months after the investigation was arrested and after the manufacturer has made clear that measures have been taken to improve the product concerning the crucial points that had led to the negative (interim) results.
The applicant will then make a new sample of the product or the system available and if applicable, adapted or added documentation.

When continuation of the investigation, for example, due to expiration of the abovementioned time limit (see above), needs re-testing to be carried out, the Testing Agency will offer the extra work to FCI. The investigation will be continued or re-started in consultation with the applicant and FCI.

At a negative final or interim result of the investigation there will in principle no official test report be generated. However, on request from the applicant the carried-out tests and results can be reported, but a declaration of conformity will not follow.
After reporting the total cost of the investigation as quoted will be charged

Comparison of the test results will always take place to the latest version of the agreed requirements as attached to these Assessment Regulations.

Only a positive result of the tests and comparison to the requirements may lead to a signed declaration of conformity of the Testing Agency.

2.3 Reporting

The report from the Testing Agency will comprise the following elements:

a. Title page:
   - Report number, date and copy number
   - Product description
   - Type- and trade-mark of the product
   - Name and address of contractor
   - Name and address of manufacturer / deliverer of the product
   - Author of the report and signature
b. The requirements and criteria (limiting values) used for comparison
c. The testing- and measuring results
d. Comparison of the results
e. Declaration of Conformity with signature
f. Other relevant notes

The reports should be set up in a distinguished style of the Testing Agency.

In case the requirements used for the tests leave room for interpretation, it will be explained in the report under what conditions the Testing Agency has come to a positive conclusion.

The Testing Agency will add in the report a declaration that he has never been involved in the development of the concerned product.

The report copy numbers 1 and 2 will be sent to FCI.
Copy no. 1 is intended for FCI, copy no. 2 may be put available by FCI to the applicant. Copy no. 3 will be kept in the project dossier of the Testing Agency.

2.4 Project dossier

For each request for an investigation a dossier will be set up. The dossier will contain all information in relation to the request and its treatment by the Testing Agency.

The information will be saved at least for 5 years on behalf of eventual complaints or arbitration. The contents of the dossier will be handled as 'Secret' for unauthorized.

The Testing Agency may only provide information to persons with interest about the fact that a product is either certified by FCI or not. For that purpose, a list of certified products will be kept up to date.

Documents provided by an applicant, which are not of importance to be stored, will be marked and sent back to the applicant.

The dossier contains the following distinguished parts:
1. Continuation scheme of the investigation.
2. Request, order, copy (no. 3) of the test report, declaration of conformity and FCI-certificate.
3. Notes, etc., made within the scope of the investigation
4. Financial administration: quotation, project form, invoice, etc.

3. International Standard for Electronic Clocking Systems

Contents

Introduction

Basics
All known ETS are using Radio Frequency Identification techniques (RFID) to clock racing pigeons. They all operate in the low frequency (LF) area at 125KHz with passive transponders.
Radio-frequency identification (RFID) is the use of an object (typically referred to as an RFID tag or transponder) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader.

RFID tags/transponders
An integrated circuit (chip) for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, and other specialized functions.
The second is an antenna (coil) with capacitor for receiving and transmitting the signal.
There are generally three types of RFID tags: active RFID tags, which contain a battery and can transmit signals autonomously, passive RFID tags, which have no battery and require an external source to provoke signal transmission, battery assisted passive which require an external source to wake up but have significant higher forward link capability providing great read range.
RFID transponders operate in a specific electro-magnetic field and are in general classified as: 125/133KHz (Low Frequency LF), 13.56MHz (High Frequency HF), 860 and 950 MHz (Ultra High Frequency UHF), 2.45GHz (Microwave MW). Higher frequencies are used to get faster readings. However they have more problems with metal and liquids than the lower frequencies.
RFID is used in several applications:
race timing (pigeons, athletics, …), passports, mobile payments, product tracking, animal identification, inventory systems, …
Transponders used by ETS are from the LF passive type, they get their energy from an external electromagnetic field. ETS uses transponders of a read-write type, meaning that information also can be read from and written to the transponder.

RFID readers/writers used for passive transponders
The reader presents an electromagnetic field that excites the coil and charges the capacitor, which in turn energizes and powers the chip. The IC then transmits the identification number (ID) via the coil to the reader. The readers communicate in a binary protocol (0 or 1 circuit).
In general readers have their antenna and processing unit together in the same housing. ETS readers have these parts separated. The processing unit is mostly referred to as the fancier's clock or the electronic timer (ET). The antenna part is referred to as loft-antenna or club-antenna.

Copying RFID transponders
With the appropriate device and little knowledge it's fairly easy to copy a transponder. Just read its ID and write it to a duplicate transponder. The internet provides everybody with the knowledge and advertises the devices.

Hard- and software securing the integrity/reliability of the clocking data
While calculating a pigeons' result list, the timing and identification of the individual pigeon is a crucial element regarding the integrity of the calculated average speed. As long as pigeon

races are organized both issues (identity and timing) have been subject of many rules and protocols to ensure the integrity of the race result.
It's a general misunderstanding amongst pigeon fanciers that cheating is impossible with ETS, it might be more difficult but not impossible. In certain situations it could be even easier because the specialized electronic systems create a false feeling of safety. This false feeling of safety can create an environment where rigorous checking disappears.

3.1 Security precautions

100% security is impossible and therefore cannot be demanded. In the fight against fraud ETS manufacturers and pigeon federations should join hands. The integrity of the data can only be guaranteed if the hard- and software in the clocks together with the procedure in the clubs at basketing and readout enhances the risk of being caught for a potential cheater.
Any attempt can only be successful if:
- The costs are far less than the gain,
- The attack leaves no traceable marks,
- The system continues to function normally after the attempt.

The following issues should get attention:
- Hardware used by the fancier and in the club,
- Software used by the fancier and in the club,
- Linking, basketing and readout procedure set by individual federations following FCI guidelines.

Before discussing any safety/security issues, one needs to understand how a RFID/ETS system works. This basic knowledge combined with the know-how of organizing pigeon races should result in a document which could be the base for each federation to establish its rules in such a way that reliable race results are produced.

3.2 ETS components (hardware)

Components of an ETS can be divided in to 2 groups:
- Components managed by the fancier (fancier's terminal (Electronic Timer - ET), loft-antenna, electronic ring (ER), interfaces …)
- Components managed by the club (basketing unit, interfaces, master timer, pc …)

3.2.1 Electronic timer, loft antenna, electronic ring, interfaces

The electronic ring (ER)
All known ETS use a passive 125KHz LF transponder for identifying individual pigeons. They all have a 64-bit section which is communicated spontaneously in a H4001 (ref. 1) norm to the reader antenna.

The loft antennas.
Almost all loft antennas used by ETS can be described as read-only, they can only read the 64-bit data stream (ID) which is send spontaneously when an ER is presented in the field of the loft antenna. These loft antennas can't read the additional information stored in an ER neither can they write information to the ER. They only register the spontaneously emitted ID from the ER and communicate this to the fancier's ET.

Fancier's terminal or electronic clock /timer (ET).
The ET is in general equipped with:
- a microprocessor,
- real time clock (RTC),
- communication ports.

It's the ET which stores all kind of data, fancier's data, pigeon table. The pigeon table is a list which references the ID of the transponder to an individual pigeon number in the clock.
The RTC is the reference for the time-stamps stored in the pigeon table for individual pigeons clocked.
Communication ports are the gates through which the ET communicates with the loft antennas, the club unit, pc, interfaces, …

Interfaces.
Several interfaces can be mounted to the ET to enhance its functionality and connection features. I.e. : printer, pc, mobile phone, Bluetooth, wireless LAN, Ethernet, …

3.2.2 Club-antenna, club-interfaces, master-timer, pc …

Club antenna / Club unit.
Club antennas are comparable with loft antennas with read/write facilities. Beside the 64-bit ID of the ER they can also read and write the additional information stored in the ER. Club antennas take an important place in the security management of a pigeon race.

Club-Interfaces.
Interfaces provide a wide range of communication possibilities between the club-antenna several peripherals as there are: Electronic Timer (ET), Master Timer, printer, pc, Ethernet, protocol convertors …

Master-Timer.
Is a real time clock used as a reference timer for the complete pigeon race. Mostly used is the DCF 77 (HKW radio-clock) or a GPS-receiver.

Personal computer (pc).
A pc is mostly used to upload the pigeon table in the ET and for the result processing.
All these components are managed by the club, they are used for linking, basketing, readout and result processing.

3.3 ETS software

The software is the driving power of any ETS system. Software is referring to the software in the several components used while basketing, clocking and readout. (ET, club unit, interfaces, protocol convertors, master-timer, pc, …)
Software also has an important role in the security management of a pigeon race.
Software must be adjusted by the member country it is applied in.

3.4 Security criteria – ETS hardware

As stated before 100% security is impossible (§1). Because pigeon federations and system developers have the same interest in preventing fraud, the system developer should give a kind of declaration of responsibility to individual federations. This declaration is difficult to give in general (i.e. FCI) because individual federations have specific demands which might have an impact on the security of the system. The individual federations describe the necessary organizational measures, procedures and technical essentials for pigeon races in their racing rules.

3.4.1 Electronic ring (ER)

The ER has an important role in the fight against fraud. It's the ID linked to the pigeon in the clock's pigeon table. Nobody can guarantee that the ring's ID is unique, transponders can be copied. Because of this the ER should get a new ID each time the pigeon is basketed. This ID has to be generated or initiated by the club antenna / club unit and has to be stored. The Electronic Ring ID has to be unique for each manufacturer.
Because pigeon clocking only involves the spontaneously send 64-bit data stream, only this section has to get our main interest.
The 64-bit data stream only has 40 bits usable for identification. These 40 bits are divided in to 2 sections: a fix part containing the ID of the pigeon and a changeable part containing the new ID which changes at each basketing.

- Fixed part: 32 bits where the first 8 represent the custom-ID.
- Changeable part: 8 bits regenerated at each basketing (secret code).

The custom ID is the first 8 bits of the chip number (D00-D03...D10-D13 ref. 1.) is a reference to the type of the chip and the manufacturer of the chip.
Every manufacturer has an own dedicated custom ID, that is unique. Custom ID's are managed and assigned by the FCI. With the custom ID, every manufacturer has a separate number range to prevent duplicated ring ID's on the market (copied rings). No manufacturer is allowed to use a custom ID that had already been assigned to another manufacturer.
The 8 bits secret code offers a sufficient tool against the use of copied rings, these 8 bits can generate 256 different codes. So a possible ring copy only has 1 on 256 chances of being successful. It might look that this is not sufficient, but cheating is mostly done systematic and repeated. With 1 copied ring the chance is 1 on 256, for 2 copies of the same ER the chance is 1 on 65.536, 3 copies only offer 1 chance on 16.777.216 possibilities.
The next 24 bits (D20-D23 .. D70..D73 ref. 1) containing the fix ID of the pigeon, leaving 16.777.216 combinations for each custom-ID.
A list of chip types actually used in pigeon transponders and complying with the above mentioned features:
- P4165 from AEG manufactured by Electro Marin, secret code generated on chip,

- Nova from and manufactured by Sokymat, secret code generated in the club unit,
- Hitag-II from and manufactured by NXP, secret code generated in the club unit,
- Hitag-S from and manufactured by NXP, secret code generated in the club unit.

Nowadays, the FCI concentrates on Hitag-S rings only.
There where the club unit has to generate the secret code specific precautions have to be taken in on how to generate the secret code in the transponder. These issues are explained in more detail in the paragraph 4.2. regarding the club antenna / unit.
The P4165 is actually used in Germany as a universal ring under the name Tipes600+, Tauris600+ and Bricon 3000+ are also based on this chip type.
The Nova chip is only used in the MC601 from Motz-Computer (Tipes).
The Hitag-II is used by the companies Atis-Benzing, Tauris and Unikon.
The Hitag-S is used by the companies Atis-Benzing, Bricon, Motz-Computer (Tipes), Tauris, Unikon and later manufacturers [ref.: Reports Overview].
Clocking pigeons only involves the 64-bits of data spontaneously emitted when the transponder enters the antenna field (loft antenna). Each of the above listed transponders has extra memory available to store additional data. These data are insignificant for clocking although they can add an extra dimension to the use of the ER. One has to take into consideration that for each chip type, these data is differently processed and therefore limits the possibilities. Mostly, the extra data is left free, sometimes it contains the license number of the fancier issued by the federation with a country-ID. Also, a chip-ring vendor can use extra memory to substantially improve the security of an ER and ETS by, for example, applying coded data, which enables him to detect copied rings.

3.4.2 Club-antenna /-unit

The most important feature in the fight against fraud is the secret code initiation or generation at basketing. Every club-unit must have the ability to complete this task.
The system has to generate the secret code in such a way that it's impossible to predict the outcome of the process. The system cannot produce any external sign from which the outcome of the process can be predicted.
For the chip types which do not have an on-chip secret code generator, the secret code is generated by the club-antenna. The generated code is then written in the chip-ring and stored in the fancier's Electronic Timer.
The wireless transmission of data between chip-ring and club-antenna, should be of such a nature that unauthorized tapping of the signal is very hard or impossible from a distance of more than 1 m.

3.4.3 Fancier clock

The fancier clock has in general 4 different parts: processor, memory, real time clock (RTC) and one or several communication gates and operating means (display, keypad). Several of these parts might be combined in to one piece of hardware.
Fancier's data, race data and pigeon data are stored the clock's memory. The format of the fancier's data are set by the individual federations. The fancier's record can contain at least the following fields : <License number >, <Name >, <Address >, <Postal code >, <Community/City >, <XX-coordinate >,<YY-coordinate > .
Pigeon data are stored in a pigeon table, each record of this pigeon table can contain the following fields: <record number >, <country >, <year >, <federation ring >,<electronic code

>, <secret code >, <pigeon status >. Depending the rules of the individual pigeon federation some extra fields can be added to each pigeon record i.e. <colour >.
Each race record can contain the following fields: <race code >, <club number >, <internal date at basketing >, <master timer date at basketing >, <internal time at basketing >, <internal date at readout >, <master timer date at readout >, <internal time at readout > , <master timer time at readout > and <race status >. All these data can be stored in a compressed mode, the record lengths are only indicating the length of the output. The hardware should provide the necessary components to store these data in a save way.
Pigeon and race records should be stored in memory in such a way that unauthorized access is impossible. While the fancier clock has active races on board it should be impossible to change any of these data unless as foreseen by the federation's protocol.
The fancier clock should be protected against unauthorized access by the housing. The housing concept should be in such a form that an unauthorized entry leaves visible marks.
The housing should be sealed in such a way that the seal or the housing is destroyed in such a way that the seal can't be replaced without visible traces. It must be hard to produce a new seal without the intervention of the system's manufacturer.
The layout and concept of the fancier clock should be of such a nature that it resist or shows any attack with the following energy forms:

- mechanical,
- electrical (i.e. through I/O ports),
- magnetic,
- chemical (i.e. solvents),
- electromagnetic (light, UV, IR, …),
- thermal energy (cold, heath).

The layout of the internal motherboard should be in such a way that critical parts like the microprocessor, the memory and the RTC can't be attacked easily through small openings (hidden) in the housing. The layout should be of such a nature that any unauthorized editing or retrieval of data is very difficult or impossible.
The concept of the RTC should be such that the oscillator cannot be influenced from outside (i.e. influencing the crystal). The RTC is very crucial, the clocking times are derived from the RTC.
A second layer of protection against unauthorized access has to be provided by the software.

3.4.4 Master timer

The master timer is the reference timer for each race. If several clubs (basketing stations) are competing in the same race one should use a system that guarantees the same time settings in each club. Before starting a basketing session the time of the master timer should be checked against a independent public timer. It's the club's responsibility to check that the master timer gives the correct time and date.
The following hardware is accepted:

- radio signal devices or HKW radio-clock, if the reception is checked.
- GPS module, if the time is checked.
- Master-clock set by one of the above or set manually and properly checked.

Any of these peripherals should show the time. In 2 timers the time must be displayed at any moment for cross-checking with the independent public timer and the timer of the fancier's terminal (ET). Reference time shall be shown on the Club System.
Manual setting of individual clocks should be discouraged, the inaccuracy of manual setting could doubt the integrity of the race result.

3.4.5 Interfaces at the club

These interfaces are the communication gates between several peripherals, i.e.: printer, pc, master timer, club-antenna, fancier's terminal, protocol convertors, …
These interfaces can be separate parts or better they are incorporated in the club-antenna/ unit. To connect the different parts used in the club environment, a connection with a galvanic nature (wire) is preferred. Wire connections can easily be checked for unauthorized tapping of information, provided that these are under strict control by club personnel.
When using a wireless data transmission between club devices (i.e.: Bluetooth, IR, RF, except chip-rings), at least the data streams containing time synchronization and clocking data should be cryptographically protected. The cryptographic keys should be stored in such a way that they are not accessible for unauthorized users.

3.4.6 Loft antennas

Loft antennas are mostly read-only, they can only read the spontaneous emitted data send by the electronic ring when it enters the antenna field. Only these data is sent to the ET for clocking, together with provisions to assure integrity of the arrival data.
The reading distance of a loft antenna in combination with an authorized electronic ring should be maximum approx. 20cm.
The position of the loft antenna is also very important for the integrity of the race result. The loft antenna should be inside the loft or when placed outside it should be near the pigeon entry. The distance from the outer border of the antenna to the centre of the entry should be limited, 1m might be a good average. An individual federation can decide in this matter, FCI should set a general recommendation.

3.4.7 Interfaces managed by the fancier

Just like in the club these interface are add-ons providing communication gates with several peripherals, i.e.: printer, pc, mobile phone, internet, protocol convertors, …
Every manufacturer has to guarantee that these interfaces cannot be used by unauthorized users to edit or delete critical data in the electronic timer (ET) when a race is active.
These interfaces can only be used for downloading data to other device or platforms. Never can they be used to get information about the secret codes in the ET and electronic rings.

3.4.8 Continuous clocking unit

A continuously clocking unit is a device or interface which registers and clocks pigeons while the main timer is not available (out for basketing, readout, …).

- A continuous clocking unit should be equipped with its own real-time clock (RTC) for time (interval) registration.
- The continuous clocking device has to comply with the same security standard as in the fancier's terminal (ET).
- When the device is a copy-clock, it is taken to the club with the ET for basketing and evaluation. The device is then connected to the ET during basketing.
- The continuous clocking unit is charged with a high risk factor. The use of such a unit must be subject to strict safety and protocol requirements. These requirements must be

covered mainly by the connection and synchronization protocol between the devices. This is covered in section 3.5: 'Security criteria – software'.

3.5 Security criteria - software

The software driving the individual components of an electronic timing system is very crucial for the integrity and reliability of the result list.
The most critical parts are the fancier's terminal or electronic timer (ET) and the club-antenna or club-unit.

3.5.1 The fancier's terminal or Electronic Timer (ET)

The Basic Input Output System (BIOS) must be designed so that any unauthorized software upload blocks the system. Software should be protected.
The memory, storing the software and all critical race and pigeon data, should be locked so that unauthorized reading is impossible. The serial number of the ET is also seen as critical and therefore has to be stored so that it cannot be edited by unauthorized users.

- Reading or displaying the secret code of any individual pigeon should be impossible at any time. When a pigeon (competing in an active race) is clocked with a wrong secret code, the software should display this pigeon on the clocking list as 'Not OK', disqualifying this pigeon as such from the result. This status may not be overruled by consecutive clocking of the same bird (only one go).
- The software should separate 'Club mode' and 'Loft mode' operations of the ET.

Club mode:

- The real time clock (RTC) can only be synchronized against a master timer for the first active race. This is the first race which started after the clock was read and deleted. All races, started with an active race present, cannot synchronize the RTC again. A relative time table has then to be built, keeping track of the deviations of the RTC against the master timer for this race. Synchronizing to start an active race should only be possible when the clock is connected with the Club antenna (CA). During the time where one or more races are active, it must be impossible to resynchronize the RTC.
- The ET should generate a unique race code for every race started. The race codes must be printed on the basketing list and clocking list (read out).

Loft mode:

- A pigeon is clocked when it moves over the loft antenna. When the pigeon's ID is retrieved in the pigeon table, a time stamp is added for the concerned pigeon. The time is delivered by the RTC, this time cannot be deleted before the race is cleared.
- The clocking times shall be derived at any time from the internal RTC, timing from other external sources cannot be used. An exception to this rule is made when continuous clocking is allowed (§ 3.5.2).
- Any change in fancier's data, race data or pigeon data should be impossible as long as one or more races are active. An exception can be made for an emergency linking at basketing if the federation rules allow this.

3.5.2 Continuous clocking (CCS)

Continuous clocking is charged with a high risk factor. Therefore the protocol and software are very important and must meet the following requirements:

- BIOS, software, crypto keys and serial number of a CCS should comply to the same demands as those for the ET (§ 3.5.1).
- Pigeons clocked through a CCS are not clocked by the RTC of the fancier's terminal (ET) but through a second timer. The latter is not necessarily synchronized in a club, except when the CCS is a copy-clock (same ET).
- If the CCS is connected to the ET, the critical racing data communication between the ET and the CCS have to be encrypted. The crypto-keys must be stored on both sides so that they are inaccessible for unauthorized users.
- The continuous use of a CCS should never exceed one day (24 hours). When this time period is exceeded the CCS must destroy its own data.
- Every new session with a CCS shall start with the exchange of identities (serial numbers). From this moment on the CCS shall only work with the ET who started the session. Next the CCS shall synchronize its RTC with the RTC from the ET. Now the CCS is ready to clock the birds.
- Secret codes may never be uploaded from the ET to the CCS. The CCS-clock cannot be synchronized or reset again before the CSS was cleared by the ET who started the session or before the above period expired. All these communications are encrypted.
- The CCS clocks birds with its own RTC or counter and stores the electronic rings with their secret codes and arrival time data.
- Transferring clocking data from the CCS to the ET takes place at ending a continuous clocking session. This data transfer is initiated by the ET and starts with the exchange of identities. If the identity exchange fails, the CCS must destroy its own data. If the identity exchange is successful the RTC of the CCS is compared with the RTC of the ET. The deviation of the CCS cannot be bigger than 2 seconds, otherwise the session is closed and the CCS should show an error code.
- Now data transfer can start, the CCS delivers electronic ID's, secret codes and time info to the ET. The ET corrects the clocking times with the deviation between CCS and ET, time stamps the pigeons with the corrected time, checks the secret codes and clocks accordingly (OK or Not OK). After this data transfer is completed the CCS is reset and ready for another session. Again, critical racing data communications are encrypted.

3.5.3 Club antenna /-unit (CA)

BIOS, software, crypto keys and serial number of a CA should comply to the same demands as the these for the ET (§ 3.5.1). A CA can be a simple reader/writer or can provide also several connection gates to other peripherals.
The CA must initiate or generate a secret code in the electronic ring at basketing. The CA must double check this secret code and make sure that a pigeon is only basketed when the secret code was changed. The electronic ID can only be sent to the clock if the secret code was double checked. The CA may never accept an ER of which the secret isn't changed. This secret code generation is the most important feature against fraudulent practices. Other important features for CA and ET are covered by the section about the protocol (Section 3.6).

3.6 Procedures in the club

All safety precautions are worthless if no one checks. Clear procedures are required to limit opportunities for fraudsters. Protocols for basketing, read out, result processing and linking are required. Protocols have to be simple and clear, the fanciers who are doing the job are not necessarily highly qualified. Protocols are a guide for them on how to check the basics. Hard- and software can never guarantee 100% proof against fraud, the best options are offered by clear and simple protocols which must be observed strictly.

3.6.1 Basketing

The first and most important step in setting up a pigeon race is basketing. The first important action is synchronizing the master timer (HKW, GPS, master clock). Synchronizing the master timer must be done by a commission (more than one person).
Basketing an individual fancier starts by setting up the race on the fancier's electronic timer (ET) or on the club antenna (CA). When a race is started the ET's RTC has to be synchronized with the club's master timer, if it is the first race in the ET, or by creating the relative time table in the ET when multiple races are going on (§ 3.5.1).
Once the basketing has started, the pigeons are basketed by presenting their electronic ring number (ER) to the CA. The CA together with the ET must double check (not display) the changing of the secret code in the ER. If the secret code is not changed, the pigeon cannot be basketed.
(!) A fancier may **NEVER** basket his own pigeons, most fraud cases find their origins here.
(!) The basketing committee should check every basketed pigeons federation number against the number displayed by the ET or the CA.
(!) If federations allow that basketed pigeons can be unbasketed, this should be possible within a limited time window, i.e. 5 minutes. Reasons for unbasketing like: wrong federation band number, health condition of the pigeon, wrong pigeon, .. If the pigeon cannot be un-basketed (not allowed by the rules, outside the foreseen time window), the electronic ring should be removed from the pigeon's leg and must be retained by the race committee, the concerned pigeon has to be marked by the basketing commission on both copies (club and fancier) of the basketing list.
(!!!) Fanciers should be kept away from the CA while basketing their own pigeons, i.e. at least 1 m distance (also 'strange' objects like a suitcase). If this rule was not observed, all pigeons of the concerned fancier should be removed from the race. Most cases of fraud find their origin here.
(!) Adding or editing pigeons in the pigeon table during basketing should be avoided but is sometimes necessary. If this occurs, a new linking list should be added to the basketing list.
(!) A basketing session is only within a limited time window, after the last pigeon is basketed the session should be closed. Better is when the ET closes the session automatically, i.e. 10 minutes after the last pigeon basketed.
(!) On a basketing list the following items should be shown:
- serial number of the CA used while printing,
- serial number of the ET,
- the unique race code generated by the ET (§ 3.5.1),
- date and time of printing,
- signatures of the fancier and basketing committee,
- license and name of the fancier,
- the ID for the race (minimum 4 char., § 3.4.3),

- time setting when the race was started (§ 3.4.3),
- list of the basketed pigeons with :
    - electronic ring number <8 char>, **NO SECRET CODES** !!!!
    - federation ring number of the pigeon,
    - basketing time,
    - eventually: sex, colour, nomination, teams, …
- number of pigeons basketed.

(!) After printing the basketing list at least in 2 copies, one copy has to be kept in security by the basketing committee, one copy for the fancier. If the federation's rules require this, more copies can be printed.
(!!!) At **NO** time during basketing, a club-PC may be connected to the CA or any other interface or peripheral connected to the CA. A connected PC is a potential danger because a PC with appropriate software can record the secret codes. Even for highly qualified people it is hard to judge in this matter. Therefore, **NO PC CONNECTION** while basketing, until **last bird registered through the Basketing Antenna (!!!!).**
If a PC is necessary, i.e. for race processing or printing, the connection with the PC can only be made after closure of the basketing session.
Printing a basketing or clocking list (read out) is done from the club-antenna /-unit or directly from the fancier's Electronic Timer.

3.6.2 Read out

When the pigeons are home the ET has to return to the club to print the clocking list.
The first important action is synchronizing the master timer (HKW, GPS, master clock), synchronizing the master timer must be done by a commission (more than one person).
(!) To get (print) a clocking list the ET has to be connected to a CA.
(!) An active race has to be selected on the ET or CA.
(!) The ET's date and time have to compared with the master timer and this time stamp has to be stored in the ET race table (§ 3. 5.1)
(!) Now a clocking list is printed with only the clocked birds of the selected race, if not clocked birds are printed they should be on a separate list.
(!) On a clocking list the following items should be shown:
- serial number of the CA used while printing,
- serial number of the ET,
- the unique race code generated by the ET (§ 3.5.1),
- date and time of printing,
- signatures of the fancier and race committee,
- license and name of the fancier,
- the ID for the race (minimum 4 char § 3.4.3),
- time setting when the race was started (§ 3.4.3),
- time setting of the read out, to evaluate how the clock is running.
- (!!) if the clock is running with more than 2 sec a day deviation, the timing shouldn't be accepted by the race commission (i.e. basketed on Thursday, readout on Saturday, 3 days, max. deviation is 6 sec.).
- number of pigeons basketed,
- number of pigeons clocked.

(!!) Only birds with evaluation set as OK can be accepted, other birds (Not-OK) are disqualified.

At read out the ET/CA can be connected to a pc for automatic result processing, without danger for recording the secret codes.

3.6.3 Evaluation of the clocking list

The race committee has to evaluate every clocking list after it is printed. This takes time, however if one wants to prevent fraud, one can't escape, sampling is the absolute minimum.
What to look for while evaluating?
Compare the basketing list with the clocking list:

- a clocking list without the corresponding basketing list is INVALID,
- race codes should be equal,
- ET's serial number is equal on both lists,
- CA's serial numbers can differ,
- the time setting starting the race must be equal on both lists,
- fancier's license and name are equal on both lists,
- electronic ring numbers are equal on both lists,
- federation ring numbers are equal on both lists,
- number of basketed birds is equal on both lists,
- federation and electronic ring numbers on basketing and clocking lists might be checked against the linking list.

3.6.4 Linking

Linking is the operation where the federation's band numbers are referenced (linked) to the electronic ring ID's. Linking can be described as editing the fancier and pigeons data in the ET. Where one does and who is doing this is of lesser importance. A linking list should be presented to the club each time fancier and pigeon data are edited. It's the fancier's responsibility to present this list when changes were made. He should get a signed copy from the race committee at that moment.
A federation could mention in its rules that linking is only allowed in the club. However doing this doesn't add any additional security dimension regarding security or safety. The identity of the bird has to be checked each time again at basketing, it's the responsibility of the basketing commission.
(!) It makes sense to draft a rule whereby pigeons are disqualified from the race if no correct linking list was presented before basketing.
(!) Linking list has to be printed by the race committee when the ET is connected to a CA.
(!) A linking list should show the following items:

- serial number of the ET,
- serial number of the CA,
- fancier's license and name,
- combination of electronic ring and federation ring,
- eventually: sex, colour, …

3.7 Compatibility

3.7.1 Club protocols

Several countries demand a minimum compatibility for basketing, read out and linking. To ensure this compatibility, public communication protocols are available.
Unives 1.7 [ref. 2] documents different situations where the ET is the master in a Master-Slave environment at the club. Unives Belgium documents different situations where the Clubmaster is the master in a Master-Slave environment at the club.
Both have their advantages and disadvantages. They are added to this document in separate documents.
When using such compatibility protocols, it makes no sense to encrypt the communications between the CA and the ET at basketing. One extra reason to follow the basketing protocol very strict.
Updated or newer version of club software should be compatible with existing CA or club unit hardware.

3.7.2 Ring compatibility

It looks good when all ETS's are using the same electronic ring. Important to know is that rings from one brand function optimal only on the antennas of the same brand. By obliging one universal ring a federation is giving indirectly advantages to some and disadvantages to others. Also important to know is that ETS companies needs the revenue from ring sales to guarantee their services. Don't forget manufacturers have a very important role in the fight against fraud, they can only keep up by continuously improving their softwares.

Club antennas must show optimal functioning with at least the Hitag-S (or more advanced) chip-rings as listed in the attached Chip-ring Overview.

Chip-rings of a new brand of ETS shall be equipped with Hitag-S or more advanced transponder with at least 256 bits memory (192 bits user available).

A chip-ring shall always reliably transmit data within a distance of up to 5 cm from the CA or loft antenna. A read/write session between chip-ring and CA shall not last longer than 500 ms.

3.8 Homologation procedure

FCI makes an inventory of all available ETS on the market. This can be done in corporation with system manufacturers. ETS manufacturers cooperating with FCI get an FCI certificate of homologation. FCI keeps a list of all approved ETS on the market.
Approval procedure:
- The ETS manufacturer must complete the application form, every document has to be dated and signed by the management of the company (Homologation request ref. 3,4) .
- The application must be accompanied by a hard-ware inventory of the equipment, also dated and signed by the management of the company (System inventory ref. 5).
- The application must be accompanied by the completed list of questions added by FCI, also

dated and signed by the management of the company (FCI query ref. 6).
- Software should only be evaluated in general on FCI level (FCI query ref.6). A list of software versions should be presented to each individual national federation. These federations should impose a rule that results with other than the registered version are invalid. Software versions may differ from one federation to another because there are differences on how pigeon races are organized. The manufactures have to cooperate with National Federations to update software versions in accordance current rules of the Country.
- The application must be accompanied with the documents proving that the equipment on the inventory list carries rightfully a CE-label (measurement reports and statements). This means that the equipment conforms with the essential requirements and with other relevant provisions of the R & TTE directive (1999/5/EC). I.e.: Reader for transponders (125kHz) in agreement with A§3 of R & TTE- the directives: Health and Safety A§3 (1) a (Applied standard: EN 0950: 1992 +A1 +A2: 1993 +A3: 1997 +A11: 1997), EMC §3(1)b: Applied standard: EN 301 489-3/07.200, Radio frequency spectrum A§3 (2) (Applied standard EN 300 330-2 V1.1/7.2000). (CE-label ref.7)
- The applicant must deliver a declaration of responsibility to FCI. This document has to be signed and dated by the management of the company (ref. 8). The manufacturer declares that all given information is correct. The manufacturer declares that in the event of fraud with equipment delivered by them and in the case where all safety protocols were followed by the responsible commissions or committees, they shall take appropriate action by adapting hard- and software in such a way that the incident can't be reproduced in the future.

3.9 Homologation fee

FCI should have the means to detect possible violations. In cases of doubt, FCI must have the means to appeal to independent agencies for testing. To acquire these means, ETS requesting a FCI-certificate [ref. 9] of homologation must pay a homologation fee for:
- systems on the market before 2011 in the possession of a TNO report, pay a fee of €1.000,- for their complete hardware inventory until 27th January 2011. Manufacturer must certify its TNO report to the FCI.
- systems on the market before 2011 without a TNO report or Smits Techniek report, must make the report after year 2011. From 2011 the new Evaluations will be done by Smits Techniek and the requests must be sent to FCI. The fee will be stated by contract between FCI and the Testing Agency.
- All the Evaluation fees must be paid to the FCI and includes all costs.

3.10 References

[ref. 1]

H4001 norm (Initiated by Electro Marin, CH), Memory Array

The H4001 contains 64 bits divided in five groups of information. 9 bits are used for the header, 10 row parity bits (P0 - P9), 4 column parity bits (PC0 - PC3), 40 data bits (D00 - D93), and 1 stop bit set to logic 0.

1	1	1	1	1	1	1	1	1	- 9 Bits Header
			8 Version bits or Customer ID	D00	D01	D02	D03	P0	- 4 data bits & associated even row parity bit
				D10	D11	D12	D13	P1	
				D20	D21	D22	D23	P2	
				D30	D31	D32	D33	P3	
			32 Data Bits allowing 4 billion of combinations	D40	D41	D42	D43	P4	
				D50	D51	D52	D53	P5	
				D60	D61	D62	D63	P6	
				D70	D71	D72	D73	P7	
				D80	D81	D82	D83	P8	
				D90	D91	D92	D93	P9	
				PC0	PC1	PC2	PC3	0	- 4 column even parity bits, NO row parity bit

The header is composed by the 9 first bits which are mask programmed to 111111111. This header is used to recognize the beginning of a new data record. Due to the data and parity organizing, this sequence can't be reproduced in the data string. The header is followed by 10 groups of 4 data bits and 1 even row parity bit. Then, the last group consists of 4 even column parity bits without row parity bit. Bits D00 to D03 and bits D10 to D13 are customer specific identification. These 64 bits are outputted serially in order to control the modulator used to modify the current at one of the coil terminals. When the 64 bits data string is outputted, the output sequence is repeated continuously until power goes off.

[ref. 2]	Unives 1.7	(separate document)
[ref. 3,4]	Homologation request	"
[ref. 5]	System Hardware Inventory	"
[ref. 6]	FCI query (CA, ET and CCS)	"
[ref. 7]	CE-label	
	- ec_europa_eu_enterprise_rtte_dir99-5.pdf	
[ref. 8]	Declaration of responsibility	"
[ref. 9]	FCI homologation certificate	"
-	Inventory list stamped and signed by FCI	"
-	TNO /SMITS system reports overview	"
-	List of current used chip-rings	

4. Security requirements for Online Electronic Clocking Systems

CONTENTS

Introduction

General
In many countries, large distances between fancier and club ask for facilities offered by a network (GSM, Internet), providing control and uploading of race data to a network server, the ETS-server .
Web-based ETS are already on the market, using a network for transmission and storage of race data in the cloud. This option offers online race results (basketing and clocking lists), which can be remote monitored and evaluated by authorized club personnel and fanciers.

Online ETS
The introduction of the use of ETS-servers and web-applications in the pigeon sport has developed the method of annunciating pigeons within a small time frame after initial clocking, based on clocking with ET (RTC). The next step is made to make the annunciations automated by the ETS. To that end, a club antenna and pigeon clocks can be equipped with additional external or built-in communication features, for immediate uploading clocking data to the ETS-(cloud-)server. Also, evaluation of race results can be performed online. ETS providing these functionalities are referred to as 'Online ETS'.
New developments of 'Cloud-only' ETS are appearing on the market, using online time sources for clocking (server-side clocking) and storage of secret data, cutting down functionalities of the ET. Cloud-only ETS require additional requirements for stringent time management of time sources in the loft system.

Other networks and webservers.
In principal there are manufacturers "internal" webserver (ETS-server, see above) and "external" webserver from race calculators or federations. The latter is excluded from the Online-ETS requirements as described in this chapter.

Furthermore, there are ETS on the market using a (private) network for transmission of race data to the club at the end of a race, so called ETS with remote strike.

Reliability
Reliability of network operating systems such as online ETS, maybe a problem nowadays. Cyber-attacks leave software chaos and damages Internet, making online ETS vulnerable to

attacks which can have negative effect on integrity of flight data. The ETS manufacturer must use available tools from the network provider and by encryption, to prevent compromising flight data from direct attacks on the system or side-effects of cyber-attacks.

GPS
The wish of federations to use GPS for position verification of a club- or fancier device can be fulfilled by adding a GPS receiver. GPS as time source, together with the RTC of a clocking device at ET-side and the Internet time or server time at server-side, make precise and secure clocking possible. Integrity of uploaded time data and further race data in online ETS, need adequate security of communication between ETS and cloud server.

This chapter (§ 4.1 to 4.5) describes requirements for secure communication, authorization measures, integrity of race data and server security, implemented in software of ETS devices and the ETS-server. Physical (tamper-) protection of online club- and loft-devices with clocking function, are described in chapter 5: 'Physical and hardware security of ETS devices'.

4.1 ETS-security, general

Internet options offer several functionalities and ask for additional hardware and software interface modules for communication. These are subject to fraud, specifically by experts in the fields of pc-software and data communication. This is the reason why requirements must be fulfilled to ensure integrity of remote race results for official use and to maintain security and reliability of ETS devices.

In current ETS, interfaces in the loft system can be applied as add-ons, allowing communication with several peripherals used by the fancier (printer, pc, mobile phone, internet adapters, …). These interfaces can only transfer data to other device or platforms, they can never be used to modify race data or to give information about secret data (crypto-keys, chip-ring codes).

Security in network operating ETS is based on: Authorization, Authentication and Accounting. In the ETS architecture, Authorization and Authentication must be covered by encryption and unique device-ID's. Accounting is done, e.g., detecting fraud by software (checks on time intervals, loft antenna location, suspicious arrival times, etc.).

All data uploaded from an ETS-device to the ETS-network database must be protected such, that the system is able to detect manipulation of these data. This needs an Internet connection, enabling a server to verify authenticity of messages from the loft system. Crypto keys shall be protected against an attempt to tamper with online devices such as the ET and Club antenna.

An online ETS with offline ET's taken to the club must, by design, be able to securely basketing and printing race results in the club, without necessary use of the network.

Devices in the Loft system such as interfaces, adapters and loft antennas are not allowed to perform clocking of pigeons. The ET is responsible for reliable storage of clocking data, to be uploaded for official evaluation.

The ET is responsible for reliable storage of clocking data, to be uploaded for official evaluation. When continuous clocking with removed ET is applied, the CCS device is not allowed to send official clocking data to the ETS-server. Unofficial CCS-clocking data must strictly be used for information only.
Other separate network interface devices or adapters in the loft system are not allowed to perform clocking of pigeons.

For uploading clocking data to the ETS-server, an ET can be equipped with integrated modem.

An ETS using network facilities must apply FCI-certified electronic chip-rings. Regular use of Hitag-S transponders is preferred, with the option of more advanced technologies.

4.2 Communication

Implemented communication security, for example in the ETS manufacturer's cloud system, should be left to the manufacturer.

With the ETS online, race- and clocking data is uploaded to the ETS-server, via a local network using Ethernet (WiFi or cable) or by mobile network, using 3G, 4G, 5G network. The data base must store all race data including time data from different time sources (§ 4.3).

Processed race data may only be stored in the cloud data base of the ETS company's platform. SMS can only be used for additional authentication checks.

An online ETS must, automatically or manually, be connected to the Internet, for online operating. This mode of operation needs the ET to provide for communication interfacing.

One-way clocking data transfer from an online device (CA, ET, adapter) to the network server is important. Uploaded data from ETS to the data base server, must be cryptographically secured, either by the chosen network security (TLS, Transport Layer Security) or by the application (ETS).

With a mobile network provider, an online ETS preferably uploads race data using a private APN connection with fixed IP-addresses, enabling the ETS manufacturer to implement cryptographic (authentication) of data. Other wireless communications offering data protection of similar security level are allowed.

All race data uploaded from the ET to the network system must be protected such, that the network system is able to detect manipulation of that data. This needs an Internet connection, enabling a server to verify authenticity of messages from a loft device.

The ET of an online ETS must, automatically or manually, be connected online for uploading clocking data, after proper authentication by device-ID and data authentication.

An online ET using a mobile communication network, must be equipped with a dedicated communication module and antenna for GPRS, 3G, 4G, 5G networks.

SMS is not allowed for real time data transmission of important data.

A SIM-card of the provider for mobile communication must be placed such that it cannot easily be reached or replaced by unauthorized persons. Use of an embedded SIM is preferred.
When the ETS-manufacturer gives the fancier the freedom to choose a mobile communication provider, the SIM-card can be made accessible for the fancier.

In configurations where other club- or loft-components, such as adapters, mobile phones, ... take care of communication with the ETS-cloud server, these must meet the requirements for physical security, as described in chapter 5: 'Physical and hardware security of ETS devices'.

4.3 Time sources

The ETS-server is considered a secure system in a secure environment (§ 4.5) and, thus, is very unlikely to be tampered with. Time management should therefore be based on the believe that online (server, internet) time is the only trustful time source.

The following hardware time sources are accepted in online ETS:
- GPS-receiver, generally applied for its accuracy;
- ETS-server, Internet time server or GPRS;
- Wireless communication devices, receiving time from the Internet
- Atomic clock from the ETS-server,
- Devices such as a PC, using NTP (Network Time) authentication protocol,
- Manually set clocks (though properly checked).

The RTC of a clocking device and the Internet time or server time are available, making precise and secure clocking possible. Integrity of uploaded time data and further race data in online ETS, need adequate security of communication between ETS devices and ETS-server (§ 4.2).

GPS-time

In most applications using GPS, these are, until today, the only sources for information about location and for navigation. For pigeon racing sport application, it is used for information about location of club- and loft-devices (-antennas). It is also used to derive precise time data from a GPS-receiver. However, this time data is regarded not reliable for clockings in an ETS, because:
- the concept of wireless receipt, creating chances for fraudulent actions,
- the chance of GPS 'spoofing', being more and more hazardous at the time,
- a GPS receiver itself is not able, without expensive means, to protect its generated time data in an ETS against manipulation.

GPS must be used as a time source for verification and online cross-checking. For a trustworthy source of time-sync / time-stamp, an online connection to a server-sided clock is necessary.

For accurate time data in club- and loft devices with GPS as time source, the RTC of the device can be internally kept synchronized by direct data exchange between GPS- chip and RTC. For optimal receipt, the GPS-receiving antenna is preferably placed externally from a

club- or loft device. A GPS-device with NMEA output is considered unsecure. It can only be applied in secure environments.

Club system

It is the responsibility of club personnel to check that the master timer gives the correct time and date. Cross-checking in the club must take place between displayed reference time, independent public timer and fancier's timer.

The Club Antenna (CA) must determine basketing time stamps from its own RTC. This RTC can be synchronized with an internal master clock (GPS-chip) or external GPS-device.

For the master clock, DCF-modules and manual setting should be discouraged, they could doubt the integrity of the master clock and thus, integrity of race results.

A GPS receiver must at least be present for co-ordinates of the CA-position. The RTC of the Club Antenna can be synchronized with integrated GPS or master clock from the Internet.

Security related messages (basketing, ..) to the ETS-server or arrival data from the server, must be checked against GPS-time and coordinates of the Club Antenna.

When a local GPS receiver is applied, the receiver antenna is allowed to be applied externally, for optimal receipt. A GPS with NMEA-output is allowed, depending on secure environment in the club, which is the responsibility of the federation.

Smartphones or tablets used as 'companion' devices, must include GPS facility.

The RTC of the club antenna is allowed to be set once in 48 hours.

When a race is active, it is important that constant verifications with server / Internet time take place.

After clocking, strike-off a race can be done:
- by connecting the fancier's ET to the Club system for printing,
- remotely, by authorized club personnel with club-PC and ETS-company certified software,
- automatic strike-off in the server, e.g., pdf of arrivals.

SMS is not allowed for transmission of real-time or other important data.

Secret codes written in the chip-rings by the CA must always be encrypted when sent to the cloud server. Verification of the secret ring-codes must then take place in the ETS-server, resulting in OK /not-OK signalling on the evaluation printout. This signal is not allowed to include other 'alarms', such as time sync. deviations or other errors.

Secret code should be backed-up in the loft device for the purpose of a double-check.

During basketing, the secret code must first be sent to the ETS-server for validation with the arrival data. The secret code needs to stay secret and should not be transmitted over several connections or to an external (non-ETS) server before comparison and validation with the arrival data is done.

Verification of the secret code in the cloud needs to be done by the ETS manufacturers' environment, so that he is in charge in case something is not right with this critical data.

During the race the OK /not-OK is never displayed on the clock, only on the evaluation printout.

Loft system

In an online ETS, using Internet- and GPS-time as time sources, the RTC in a loft device is still necessary for clocking, in case of Internet and GPS failure. The RTC must be synchronized with GPS-time when GPS and Internet are available again.

Clocking in the Loft system can be done with the ET, based on its RTC-time. Clocking takes place with the system time of the ET's operating system. The system time should periodically be synchronized with the RTC, such that clocking accuracy is kept within an average of 0.5 seconds.

In normal operation of an online ETS, three time sources are available: RTC, GPS and Internet. These times must correspond within a certain time span of approx. 20 seconds. When the ET has been offline during arrivals, the ET's internal RTC- and GPS-time difference should be within a time span of approx. 3 seconds.
When deviations exceed a time span, a signal (e.g., 'failure'') should be added to the arrival data.

For online evaluation it is necessary to know the time difference between the Loft-clock and a (calibrated) master time (Internet time, GPS-time or other). This must be done during a race on a regular basis (every 1 hour), in order to detect any deviation during a race.

At least two time sources (cloud-clocking) or three time sources (RTC, GPS, Internet) must show the same time, not exceeding an deviation of 20 seconds.

Arrival times that are used for online evaluation and sent to the cloud need to be encrypted.

Arrival times and master time / GPS-time / server time shall be stored and processed in the ETS-server, together with race results, etc., for reliable and precise striking-off.

For remote (online) strike-off, a comparison of the Loft clock (RTC) and a Master-time (GPS) needs to be done with the precision of 0,1 seconds. When uploaded to the ETS-server, it should be controlled with the Internet time to check if these times are trustable (within seconds).

The RTC of the ET, when synchronized in the club at basketing, must not be synchronized with an externally connected clock when a race is active. The online ET must then determine arrival time stamps from its RTC, before uploading these data to the ETS-server.

When the system is full-cloud operating, i.e., when the offline ET is not taken to the club for basketing and printing, it must still be possible to take the ET and eventual communication adapters to the club for visual inspection of the housing and security seals. This should be

done at the start of a race season and on a regular basis, e.g., every second week, during the race season.

A GPS receiver of position coordinates data for a loft antenna is required. Uploaded, security related message (arrival data, ..) must be accompanied with these GPS-data.
Also smartphones or tablets used as 'companion' devices, must include GPS facility.

The GPS-receiver must be an internal module of a loft-device. Only the antenna part is allowed to be externally connected, for optimal receipt.
A "GPS antenna" with NMEA-output or DCF-clock is not allowed.

A GPS-receiver used for position coordinates only, may be used as an external device, provided that position output data cannot easily be manipulated.

Deviations of an online ET (RTC) from the master time shall be signalled and logged in the cloud server. ET-time deviation signals are preferred to be divided into:
- small deviation from inaccurate RTC (e.g., up to 2s), and
- large deviations from failure or attack to the RTC or GPS-receiver (e.g., >5s), resulting in alarm condition or invalid race data.

The alarm generated from a serious deviation of the ET-time, must be a separate alarm from the 'OK /not-OK' signal for the secret chip-ring number.

The ET shall provide additional event logging concerning the transmission of data to the ETS-server, such as time of connect, log on, disconnect, … The events shall be securely stored in the ETS-server and ET-device such, that these data cannot be modified at any authorization level.

Security- and time-related messages (arrival data, ..) to the server must be accompanied with RTC-time and position data.

After clocking, strike-off a race can be done:
- by printing with Club antenna and connected fancier's ET,
- automatic strike-off in the server, e.g., pdf of arrivals,
- by (non-cloud) remote knock-off procedure by the fancier, with ETS-company certified software.

SMS is not allowed for transmission of real-time or other important data.

Continuous clocking

Continuous clocking (CCS) in an online loft system can be a copy-clock or continuous clocking device. This device can be built in the same housing as an external communication device (adapter). The CCS shall be implemented in the loft system as described in the International standard for ETS (chapter 3, § 3.4.8, 3.5.2). Physical protection of a continuous clocking device shall meet the requirements as described in chapter 5: 'Physical and hardware security of ETS-devices'.

4.4 Online evaluation, monitoring

Race data from fanciers can be monitored and downloaded for evaluation with club- or fanciers' computer, using ETS-certified software. Fanciers can download their race data from their own platform or website.
Access with a PC, laptop, tablet, ... to each level of data in the server data base shall comprise a method for: Identification, authentication and authorization.

Authorization to log-in to the network data base, must provide different levels:

- Fancier's PC for monitoring his own race data.
- Club manager PC for monitoring, control, evaluation of fanciers race data.
- Admin level of ETS company for reading event loggings, server software updates.
- Patch management; service and server repair level.
- Access to source code by lead programmer (+supervisor).

When the fancier's PC is used for online facilities, only (certified) software provided by the ETS-manufacturer shall be used.

The use of downloaded fanciers' flight data is for monitoring purpose and unofficial evaluation of race results and to help fanciers online with information.

Clocking data uploaded from the loft system should be protected against compromising by (standard) available data authentication and cryptographic measures.

To gain access to the ETS-server data by club personnel for monitoring fancier's race results, an authentication mechanism like 2FA is required.

Communicating with the ETS-server of security relevant data in a web-browser, needs a secured (encrypted) Internet connection, as is indicated in the browser.

For activating and operating an online Club Antenna, an MFA (Multi-Factor-Authentication) mechanism is preferred. This needs a logging-in procedure with password and, for example, use of a code, received in a Web-browser on a club-PC or mobile network (SMS).

During basketing and monitoring data from active races, club personnel should never be able to see the secret ring codes.

An ETS PC-program for the fancier to monitor his race results, may provide a simple calculation app for (self-) evaluation.

Race data can be downloaded in the club-PC from the cloud server with the ETS company's web-based management program. This is restricted to monitoring and for evaluation of race results only. Club personnel may need to download, e.g., pdf's of race results for checks of fancier's race data or for printing.

A desktop or laptop as club PC, connected to the Club antenna, is not allowed to run a basketing program during basketing. The CA or an additional wireless communication device must offer the user interface (display, keys) for basketing.
During basketing, all data exchange between Club antenna and external club devices for communication, shall cryptographically be secured.

With an active race running, the secret chip-ring codes written in the fancier's ET and/or uploaded to the ETS-server during basketing, shall not possibly be made visible on club-PC, fancier's PC or any wireless device, regardless of authorization level.

Logging in to different levels of server data or other applications than ETS by 'Single Sign-On' authentication is not allowed.

4.5 Server security

Communication

The manufacturer's webserver for storage and evaluation of race results, is protected by Internet Protocols, considered to offer state-of-the-art security.

A server of an ETS company must explicitly fulfil the task of secure communication between server and clients, and secure storage of uploaded race data.

Software

Software of an ETS companies' database server shall be controlled, managed and kept updated only by the ETS company. In case of doubts about race results, only authorized persons of the ETS company are allowed to access event logging data, technical failure or fraud detection data in the server.

The ETS manufacturer must use available tools to prevent race data in the server be compromised by (cyber-) attacks to the server, such as:

- 'Brute force' attacks on keys, passwords,
- 'Denial of Services' or 'DDOS' attacks,
- Virus programs, ...

In the ETS architecture, data authentication must be covered by, e.g., device identification and cryptographic mechanisms. Detection of tampering (tamper response), causing, e.g., deviations of time data, loft antenna location, suspicious arrival times, ... must be implemented in the software of the server.

It shall not be possible for club personnel, fanciers and other unauthorized persons from an ETS-company or a non-ETS federation, to modify race data stored in the ETS-server such as: basketing data, arrival data, chip-ring secret code, time sync., device-ID's, ...

Physical protection

The data base in an ETS-server must achieve adequate physical protection and authorization for access, offered by the ETS company or network provider.

A private server (computer) of the ETS company, shall be placed in a physically secure environment, equipped with sophisticated (2 persons) physical access control for authorized persons from the ETS company (for authorizations, see § 4.4).

4.6 Cloud-only ETS

Characteristics

As automation of ETS race data processing and management goes on, 'Cloud-only' systems appear on the market, which are not able to operate according the International Standard for ETS (Chapter 3).
Specific characteristics of a cloud-only system are:

- No loft device, fulfilling all requirements for an ET (Chapter 3) is used for clocking or for basketing in the club. A loft device may not keep the secret chip-ring data for comparison with arrived pigeons.
- Clocking, strike-off and checks of secret ring codes take place in the cloud server. (Server-sided clocking).

As it is not feasible to get accurate Internet time by the loft system, GPS-time must be used for the precise time for the clocking. This should be validated with the Internet time in the ETS-server, checking that the arrival was within a certain time, in order to ensure that the GPS-time has not been tampered with.

Cloud-only ETS as described above may be allowed by federations in some countries. However, conditions and additional minimum requirements as described below, must be fulfilled.

'Non-cloud' classic remote strike-off by the fancier is allowed.

Additional requirements

A cloud-only ETS without the presence of a secured clocking device with RTC for clocking, is not allowed, a back-up function is necessary and should be possible.
The server time is used for validation and synchronization only.

The loft device with RTC must provide for back-up of events data with time stamps, in case of doubts or when online data is compromised by server problems, cyber-attack or else.
The device must periodically be taken to the club for inspection.

A loft device, when connected to the Internet via a fanciers' LAN, must take care of encryption of security related data.

A Loft-antenna is not allowed to contain a communication module for sending arrival data directly to the ETS-server.

GPS must be used to provide position data of the loft device. GPS-time can be used for the purpose of checking and to provide the fancier with precise time.

Secret codes written in the chip-rings by the CA must always be encrypted and may directly sent to the cloud server during basketing. The secret codes and times should remain in the ETS system and not transferred to other (non-ETS) platforms.

5. Physical and hardware security of ETS-devices

Contents:

5.1 General

Physical protection as described in this chapter are valid for club- and loft-timer components of ETS conform the International Standard (chapter 3) and for Online-ETS timer components (chapter 4).

The vendor must specify in the documentation that system components have been tested and approved according:

- IEC-2, environmental tests (humidity/temperature, shock and vibration)
- IEC-61000-4-2 (Microelectronics AN3353), electrostatic discharges.

5.2 Tamper protection

Physical protection against attacks by tampering with a system component, e.g., a pigeon clock (ET), consists of three components, described in the international ISO-standard: ISO 13491 (parts 1 and 2). According to this standard, physical protection is divided into tamper resistance, tamper response and tamper evidence.

Attacks on the hardware of a system or system component, make use of (a combination of) attack methods. Physical protection shall offer such attacks a minimum chance on success in reaching critical components and manipulating data. The attack methods and examples are shown in the table below.

Attack method		**Examples**
a	Mechanical	Removing or opening housings by drilling, grinding, etc.
b	Chemical	Removing housings with solvents or other chemicals
c	Electrical	Galvanic tapping, generate electrical interference
d	Magnetic	Blocking a tamper switch with a permanent magnet; Tapping or inducing LF- (inductive) fields up to 150 kHz
e	Electro-magnetic	Analysis of radiated RF-signals; Affecting data with EM-radiation
f	Optical	Tapping and /or interfere with an IR-channel; Affecting with Laser
g	Thermal	Melting or burning housings; Affecting electronics by heating or cooling

5.3 ETS physical protection

The system components must be designed and constructed such, that an attempt to attack critical components (memory, RTC) which transmit, store or process data (software, flight data), results in visible, irreparable damage to a system component.

Access (authorized or not) to system- or application software and data, for repair or maintenance, shall only be possible after erasure from memory of all flight data.

Data inputs /outputs of system components must be protected against monitoring, such that – when used in normal home environment – no attacks are likely that may result in compromising software or flight data.

External communication- and power lines of system components must be separated from internal critical data (software, flight data) in such a way that these data cannot be tapped or modified.

Modification or replacement of system components during a flight, which is possibly not detected by logical protection in that component or by the system, must as much as possible be hampered by design of the physical security measures.

A secured device must be designed and constructed such, that an attempt to attack critical components (CPU, RTC, ..) which transmit, store or process data (software, flight data), results in visible, irreparable damage to a system component.

5.4 Protection layers

Housings:
The rigidness of the housing of ETS-devices for clocking (CA, ET, CCS), with sealing and eventual other protections against tampering (special mounting screws, etc.), is considered to be the outer physical protection layer (first layer protection).

The housing of an ET must be equipped by the manufacturer with a seal. The seal may be placed on the seam of the main housing parts, or on (one or more of) the screws of the housing, in such a way that easy damage of the seal at normal use of the clock, is not likely to occur.
The seal must be specially designed for security purposes and shall be:
- difficult to copy with generally available means;
- irreplaceable without visible damage to the seal.

Electronics protection:
As second, inner protection layer, the electronics inside the device, shall provide protection against compromising flight data by tapping and/or modifying sensitive data and firmware. The protection of electronics may consist of physical protection, e.g., components potted in epoxy, or by software, such as handling sensitive data and/or detection of fraud attempts (tamper response) by sensor /activator circuitry.

A tamper response mechanism must be implemented such that it is not possible to put these out of order from outside the housing or by using a small opening made in the housing.

The tasks of a tamper detection and response mechanism are:
- detect attempts to attack electronics,
- cause erasure of flight data or put the device out of order,
- store the signal in an unknown and unspecified non-volatile memory location,
- be indicated to the user,
- be sent to a network server, when the ET is online.

5.5 Online ETS

Any club- or loft-device, such as interfaces, adapters, wireless devices of an online ETS fulfilling communication, shall provide physical protection as described in this chapter.

In configurations where other club- or loft-components, such as adapters, mobile phones, ... take care of cryptographically secured communication with the ETS-server, these must at least meet the requirements for first level (physical) protection by the housings of the devices.

6. Requirements for foot-rings, electronic combi-rings and chip-rings

Contents

Introduction

This chapter defines the minimum requirements for quality and performance of pigeon foot-rings and combi-rings. The requirements consist of functional- /user requirements, environmental requirements and mechanical properties.
The requirements with respect to programming of the chip-unit of a combi-ring and the chip-ring are described in chapter 5.2: Electronic chip-rings.
The requirements are in principle controllable or testable. For unambiguous results from testings, a test guide based on these requirements is given in a separate document.

Definitions

Foot-ring	A foot-ring is a ring which, once put on a pigeon's leg, serves as an identification of the pigeon, gathered from a clearly readable number, the foot-ring number.
Chip-ring	A chip-ring is a ring, provided with a fixed electronic chip which contains extra identification- and user-data that can, in accordance with requirements, be read and written electronically. The chip-ring may be added to a pigeon's foot-ring, so as to make that pigeon suitable for electronic clocking.
Combi-ring	A combi-ring combines the foot-ring- and chip-ring-functions by integrating an interchangeable, electronic chip-unit with the foot-ring. The chip-unit contains the chip with the extra identification- and user-data for electronic clocking.

6.1 Foot-rings and combi-rings

Contents

General

The requirements described in paragraph 5.1.1: Mechanical properties, are valid for foot-rings and combi-rings, equipped with a metal inner ring.

The quality- and environmental requirements described in, respectively, paragraphs 5.1.2 and 5.1.3 are valid for foot-rings and combi-rings in general, independent of construction or composition of the ring (e.g., a combi-ring with different inner ring).

6.1.1 Mechanical properties

General

In the requirements of this paragraph, it is considered that, for the purpose of rigidness, a foot-ring may be equipped with a metal (e.g., aluminium) inner ring. The coating over the inner ring must contain the necessary printed sticker (with unique ring number) and a transparent, plastic outer ring.

The quality- and environmental requirements described in, respectively, paragraphs 5.1.2 and 5.1.3 are valid for foot-rings and combi-rings in general, independent of construction or composition of the ring.

Foot-ring and combi-ring

For the purpose of standardization and compatibility with different chip units and clips, the mechanical properties as listed below, are valid.

Inner ring dimensions

- Inner diameter: fully circular, diam. 8,0 +/- 0,1 mm
- Thickness: .2 to .3 mm (the combi-ring: see 1.2)

Sticker dimensions

- Height / width of 7.2 +/- .1 mm
- Symmetrically positioned between the rims of the inner ring

Sticker readability

- Good contrast between the sticker and printing, for good readability

- Text size: 4 to 5 mm. Colour: black, reproducing style (font, spaces, etc.), constant over a calendar year
- No contrast decrease at lasting exposure to daylight.

Inner ring finishing
- Smooth inner finishing
- No sharp edges inside or outside
- Top- and bottom side finished with an bended rim

Plastic coating properties
- Constant colour shade within a calendar year
- Constant thickness around the ring
- Good transparancy around the ring
- Good resistance against (splash)water
- Good resistance against bending and scratching

Composed ring properties
- Constant outer diameter around the ring
- Height / width: between 10.0 and 10.5 mm
- Resistant against distortion by bumping and mechanical pressure
- No sharp edges
- Weight: maximum 2 gram (without chip unit)

Additional requirements combi-ring

Combi-ring application
- The combi-ring must be suited to be used with the different chips, which are applied in electronic systems and are constructed as a chip-unit, compatible with the combi-ring.

Chip-holder
- The chip-holder of the combi-ring must be constructed so that a chip-unit can be put into the chip-holder from both sides, whereby the chip-unit always remains firmly in its correct position in the chip-holder.
- The chip-holder of the combi-ring must not show sharp protuberances, which may somehow hamper or hurt the pigeon.

Chip-unit
- As a tactile recognition that the chip-unit is placed correctly, it must provide a mechanical stop. Preferably, an extra ‘click’, preventing that, under extreme conditions, the chip-unit by itself comes loose from the chip-holder.

Inner ring
The metal inner ring thickness is between .30 and .35 mm.

6.1.2 Performance requirements

General

Where requirements in this paragraph refer to normal conditions, these conditions are:
- environmental temperature of 23 +/- 3°C
- relative humidity between 40 and 60%

Foot-ring and combi-ring

Functional lifetime
The ring must remain in good condition for 15 years, under normal conditions and by normal use (according manufacturer's directions), i.e., not be severely damaged or affected, leaving the outer and inner surface of the ring smooth and the text on the sticker clearly readable.

Impact resistance
The impact resistance of the coating must be according DIN 53453 at 23°C: not breakable (or ASTM D 2794, ASTM D 5171).

Abrasion resistance
In order to prevent poor text readability in time, the plastic coating should offer sufficient abrasion resistance (D 4060-07, ISO 7784-2).

Tensile strength
The ring shall withstand a tensile pressure of 20 kgf in any direction, without showing permanent distortion.

Vibration and shock
The ring must remain undamaged at:
- constant vibration of 1g at frequencies between 10 and 1000 Hz
- shocks up to 100g.

Additional requirements combi-ring

Placing the chip
Placing the chip in the chip-holder has to be done manually and easily, without the need for tools. Preferably, an extra 'click' mechanism is added, preventing that, under extreme conditions, the chip-unit by itself comes loose from the chip-holder.

The chip-holder construction
- The chip-holder must be integrated in the ring, such that it cannot be removed (e.g., when no chip is used) or come loose from the ring, e.g., by bumping.
- The chip-holder must reproducibly be manufactured in a way that, if necessary, the chip can be placed or removed, always according to the directions for use.

The chip-holder must be constructed so that the chip cannot come loose, caused by:
- constant vibration of 1g with frequencies between 10 and 1000 Hz
- shocks of 100g.

The chip-holder availability
- The chip-holder and chip-unit must, by normal conditions and normal use, remain undamaged and unaffected so that the chip remains easily replaceable and will not come loose from the chip-holder, e.g. when bumped.

The chip-holder keeps its required user properties, when a chip has been placed and removed at least 5000 times.

6.1.3 Environmental requirements

Storage
The foot-ring must meet the quality requirements after continuous storage at temperatures between -25°C en + 70°C.

Functionality
The foot-ring must meet the quality requirements at environmental temperatures between -5°C en + 55°C, unless otherwise specified in the requirement.

Humidity resistance
The water absorption of the plastic shall not exceed 1%.
By normal environmental temperature and normal use, the foot-ring shall resist a continuous relative humidity of 95%.

Sunlight
Continuous exposure to sunlight shall have no negative affect on the ring properties.

Chemical pollution
Continuous exposure to small concentrations (up to 10%) of ammonium, salts, acids or alkalics, shall have no negative affect on the ring properties.

Additional requirements combi-ring

Immunity to dust

The functional properties of the chipholder and the chipunit (insertion, ease of use) shall not negatively be affected by dust.

6.2 General requirements for electronic chip-rings

Contents

6.2.1 Data and memory programming

Performance and memory programming of the chip for pigeon fancier application, must fulfill the requirements of this paragraph.

The user available memory of the chip comprises at least 128 Bits

The first memory section (1st page) is reserved for data that cannot be modified during lifetime of the chip. In this memory, a fixed chip-ring-ID and an initial (manufacturer-) identification code (Custom-ID) are written once. For pigeon fancier application, a variable (secret) number of at least 8 Bits must be written often. At power-up it must be possible to read this memory section automatically, before the chip is ready for receiving further read/write instructions.
The first memory section contains the following data:

- Chip-ring number
- Manufacturer-ID (OEM-code, Custom-ID)
- Variable (secret) number

+ Start-Bits and Parity-Bits.

This first memory section shall be arranged according to the, in paragraph 3.2: 'Data structure' described structure (H4001 structure, see "Electronic Pigeon Ring Specifications")

The remaining memory sections preferably provides a R/W (read-/writeable) section for user data and a section that can initally be configured to OTP, making this part writeable only once. The memory capacity of these pages must be sufficient to contain the following data:

- Country (manfacturer) number
- Fancier-ID data
- Space for future use

+ CRC-Bits.

The chip must provide for security measures to assure the integrity of user data:

- Possibility to set at least 2 pages OTP (Lock-bits). The configuration lock-bits must be set R/O, the memory lock-bits must be set OTP.
- The chip must provide a Unique Identifier (UID) or ETS-manufacturer programmed identifier, to be read by the ETS-antenna or other RF-reader, in order to check the authenticity of the chip-ring.
- The chip must provide storage of a pseudo-random number, which can be used for the authentication of a pigeon (chip-ring) in a certain race.
- Crypto-possibility for the enciphering of data.

6.2.2 Physical properties

Physical and electrical properties of the chip-ring must fulfill the requirements of this paragraph.

The resonance frequency of the input detection circuit must be 125 kHz +/- 6 kHz.

The voltage supply for the chip must be attained from the 125 kHz carrier of a RWD / antenna (Read/Write Device). Power-up of the chip must take place at sufficient field strength.

The transponder must be capable of bi-directional transmission, i.e., receive and transmit through the inductive channel (125 kHz).

EEPROM cells are vulnerable to direct U.V.-light and Gamma-radiation (Röntgen). These radiations can erase the contents of the EEPROM-cells (data bit). Therefore, the contents of the user-EEPROM, but also the dedicated (non-user) EEPROM part (configuration, random nr.) of the chip must be protected from these sunlight radiations. For that reason, the chip-ring must be made of a (ultra-)light absorbing plastic, protecting the chip from being affected by U.V.-radiation that can normally be expected from sunlight.

Also after removing the transponder from the chip-ring, deliberate erasure of the memory with U.V. (for example, with a EPROM-eraser) must not be easy to perform.

The transponder with the chip must rigidly be enclosed in the plastic of the chip-ring (chip-holder). Normally available chemicals (such as salt) should not reach or affect the transponder.
An attempt to remove the transponder-chip from the chip-holder, must result in visible damage to the ring or chip-holder and, if possible, damage to the chip.

6.3 Chip-ring specifications

Contents

General

This chapter describes the technical requirements and performance characteristics that electronic pigeon rings need to satisfy in order to ensure quality of the pigeon rings and accountability with the accepted electronic clocking systems.

The electronic pigeon ring is a data carrier for the identification of pigeons. It consists of a lockable ring body in which some space is reserved for the inclusion of electronics. The electronics consist of a programmable memory chip and a connected coil, which together constitute what is known as a transponder. The data that this transponder contains can be read with reading systems and can be adjusted with writing/reading systems.

The only electronic pigeon rings accepted are those that are compatible with the existing and approved reading devices.

Transponders for pigeon rings must comply with the following standard performance characteristics and data programming, specified in this chapter.

6.3.1 Performance characteristics

a. Reading function

Resonance frequency: 125 kHz +/- 6 kHz at normal ambient temperature
Read-out information: 64 bits cyclic, without pause
Data header: 9 bits “1”
Modulation mode: ASK or load modulation
Signal coding: Manchester method

Processing capacity: 125kHz/64 = 2 k baud
Transmission time: 40 ms max. after switching-on sensing field
Reading distance: 8 cm (Measuring structure and measuring specifications are defined in the "Test methods" directive)

b. Writing function

Resonance frequency: 125 kHz +/- 6 kHz at ambient temperature
Modulation mode: ASK
Performance data:

- Writing distance: 3 cm minimum (measuring structure and measuring specifications are defined in the "Test methods" directive)
- Minimal permissible writing cycles: 10,000
- Minimal maintainability of the data: 10 years at 0 - 50°C
- Write protection: the chip should have a protection function against unauthorised or unintended modification of specific data.
- ESD voltage: 10 kV min.
- Insusceptibility to interference: no unintended changes in the data should occur in the transponder's range of application.

There is a special directive for the methods and devices applied in the test procedures.

6.3.2 Data structure / data contents

In correspondance with the data structure, different sections are provided which may contain different data contents.

The first page contains data that should not be altered during the whole life-span of the ring. Additionally, a variable, secret number is stored in this page.

The second and next pages contain varying data, which means that these are read/write suitable. The pages can be used for extra information. They are reserved for the identification of the user.

The following data, especially described with reference to the storage capacity, characterize the necessary requirements.

The table below shows the data structure for the first 64 Bit of the chip:

Bit 0	1	1	1	1	1	1	1	1	1	Bit 8		Header
				Bit 9	D00	D01	D02	D03	P0	Bit 13		Suppliers ID
				Bit 14	D10	D11	D12	D13	P1	Bit 18		(= Customer ID)
				Bit 19	D20	D21	D22	D23	P2	Bit 23		Electronic ring number
				Bit 24	D30	D31	D32	D33	P3	Bit 28		
				Bit 29	D40	D41	D42	D43	P4	Bit 33		
				Bit 34	D50	D51	D52	D53	P5	Bit 38		
				Bit 39	D60	D61	D62	D63	P6	Bit 43		
				Bit 44	D70	D71	D72	D73	P7	Bit 48		
				Bit 49	D80	D81	D82	D83	P8	Bit 53		Secret number
				Bit 54	D90	D91	D92	D93	P9	Bit 58		
				Bit 59	PC0	PC1	PC2	PC3	0	Bit 63		Column parity bits

The parity bits P0 … P9 form each time an even parity with respect to the corresponding line. The same goes for the column parity bits PC0 … PC3, where the header bits are not taken into account. The bits DO0 … D13 indicate the suppliers ID. The bits D20 … D73 contain the electronic ring number that is allocated only once. The bits D80 … D93 contain the secret number.

After power-up, the 64 data-bits of the first page are sent off cyclically. The second page is sent only on request.

It must be possible to change the variable data range (starting at page 2). This can be achieved by a read-write antenna as defined in the test method.

The data structure of the second page (containing 64 bits) is shown in the table below:

	Bit 0	L00	L01	L02	L03	L04	L05	L06	L07	L08	L09	Bit 9		Country
Bit 10	Z00	Z01	Z02	Z03	...	...	Z29	Z30	Z31	Z32	Z33	Bit 43		Fanciers ID Unused
							Bit 44	U00	U01	U02	U03	Bit 47		Unused
			Bit 48	R00	R01	R02	R03	R04	R05	R06	R07	Bit 55		Reserve
			Bit 56	P00	P01	P02	P03	P04	P05	P06	P07	Bit 63		Checksum

The position values of the 64-Bit data fields are represented in the table below.

Field	Content	Bits	Size	Value span	Code
Country	International access number	0 - 9	10 bits	001 – 999	binary
Fanciers-ID	Identification of pigeon fancier	10 -43	34 bits	0 – 9999999999	binary
Unused	Free for future use	44 - 47	04 bits	0 – 15	binary
Reserve	Reserved for future use	48 - 55	08 bits	0 – 255	binary
Checksum	8 bits CCITT- CRC	55 - 63	08 bits	0 – 255	binary

Country (bit 0 - 9):

To differentiate between countries, the international access number is used and binary coded. The table below represents examples of ‘Landcode’ values.

Country	Access number	Value
Germany	049	031 hex
Netherlands	031	01F hex
Belgium	032	020 hex
France	033	021 hex

Fanciers-ID (bit 10 - 43):

Of the pigeon fanciers ID, only the numerical data without separator are binary coded. The values are represented by non-significant noughts. The table below represents examples of Fancier-ID values.

Country	Fanciers ID	Numerical value
Germany	123/45 67.890	0 49 96 02 D2 hex
Netherlands	1234 - 5678	0 00 BC 61 4E hex
Belgium	012345 - 67	0 00 12 D6 87 hex

Unused (bits 44-47):

free for future use

Reserve (bits 48-63):

reserved for future use

Checksum (bits 56-63):

An 8-bit CCITT-CRC is used to protect the data. 1C3hex serves as a generator polynominal. The CRC is calculated and inverted by means of the 7 data bits, from bit 0 to bit 55, and stored by bits 56 to 63, where bit 56 is the MSB and bit 63 the LSB. The result of the inverted storage of the CRC is that a sequence of noughts is recognised as invalid.

The table below shows the CRC for a number of test bytes:

Byte	CRC
01 hex	C3 hex
80 hex	EE hex

Abbreviations:

CCITT: Comité Consultatif International Téléphonique et Télégraphique

CRC: Cyclic Redundancy Check

MSB: Most Significant Bit

LSB: Least Significant Bit

The memory distribution of the second page of the chip has been chosen in such a way that an optional coding of the data is possible in this page.

6.3.3 Suppliers ID

The suppliers or customer ID is a special section on the 64-bit code of the first page, which makes it possible to differentiate between different suppliers/customers and applications (see Table 1 in Section 3.2). FCI manages these number cycles and informs the requesting manufacturer about what should be written in this section of the chip (= suppliers ID). This manufacturer must also take the responsibility of coding each electronic ring number only once within the suppliers ID allocated to him. (This means that, at maximum, 2^24 = 16.777.216 rings can be coded).

The agreed Custom-ID's for chip-rings are listed in a separate table, see Annex 3.

6.3.4 Data integrity

The access to the data on the chip should be protected and controlled by means of a protection system to prevent undesired and/or unintended changes in the data. For this purpose three procedures have been approved, which distinguish themselves by different protection phases:

1) Definitive structuring of the page by OTP (one-time programmable)
2) Protection by means of a password, preventing unintended or coincidental replacement (e.g. due to strong fields).
3) Storage of a secret number, generated during basketing by an internal or external a-select number generator.
4) A cryptographic procedure whereby the data to be recorded are stored in the memory encrypted.

6.3.5 Mechanical characteristics

Ring dimensions:

- inside diameter 8.5 mm min.
- height: 16 mm max.
- thickness: 1 mm max.
- weight: 2 gr max.

Ring characteristic: multi-lock.

6.3.6 Material properties

The information below refers to the entire transponder in a plastic package:

a) Material: Luran plastic or POM
b) Temperature:
- for storage and transport: -25°C - +55°C
- for operation: -5°C - +55°C

a) Impact resistance in accordance with DIN 53453 at +23°C: not broken
b) Resistance to:

- water: water absorption 1% max.
- dirt: no detrimental effect of operation
- water-born table salt solution: a 10% concentration over a 24-hour period at a temperature of 50°C
- ammonia solution: a 10% concentration over a 24-hour period at a temperature of 50°C
- UV radiation (direct sunlight): with 20 W, 10° halogen lamp in 30 cm
- vibration: 0.5 g within 1-1000 Hz range during 1 hour
- free fall: from a height of 1.2 m

The conditions for testing to minimum requirements will be laid down in a separate directive.

6.3.7 Inscription / Characterisation of the rings

It should be possible to provide the rings with an unambiguous identity by means of an inscription. This identity is laid down in the approval.

6.4 Functional compatibility of the rings with the accepted systems

Apart from testing the ring characteristics against the specifications in the directive (chapter 5.3), official approval of an electronic chip-ring also requires the successful completion of a number of function tests with respect to the compatibility between various approved systems used by pigeon fanciers. In addition, a separate directive describes the test-methods and applied tools.

6.5 Acceptance of the electronic chip-rings

The procedures for acceptance of a certain electronic chip-ring are initiated at the request of the chip-ring manufacturer. Acceptance depends on whether the electronic ring has stood

the test that it was subjected to. The associations determine the test methods to be used. A testing agency appointed by the associations will decide whether an electronic ring is accepted. The costs involved will be borne by the manufacturer.

The ring manufacturer must submit a test model and should also file extensive technical documentation with the testing agency. The testing agency will keep a copy of the test results and the test report.

6.6 Additional model licence in case of deviation from test model

Deviations from the test model require additional acceptance by the testing agency.

6.7 Withdrawal of the licence

Deviations from the test model imply necessary additional testing by the testing agency.

6.8 Procedure for the implementation and amendment of this directive and area of validity

This directive will be effected by the committees appointed by the associations for this purpose. Amendments to this directive may be determined by a joint committee to be appointed by the associations.

This directive applies to all land committees who are members of the FCI.

Annex 1 Draft electronic chip-ring – Test methods

Allgemeines

Diese Richtlinie beschreibt die Testmethoden für elektronische Taubenringe in Ergänzung zu dem Spezifikationsschema Elektronischer Taubenring. Ziel dieser Richtlinie ist es durch genaue Definition reproduzierbare und vergleichbare Ergebnisse zu erhalten.

Normative Referenzen

Grundlage für diese Richtlinie ist die von den Taubenverbänden verabschiedete Richtlinie „ Elektronischer Taubenring Spezifikationsschema“ vom 12.05.2000.

Weitere Internationale Standards

IEC 61000-4-2:1995 Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques-
Clause 2: Electrostatic discharge immunity test

IEC 68 Teil 2: Grundlegende Umweltprüfverfahren

Definitionen

Funktionsbeständigkeit: Uneingeschränkte Funktion als Taubenring. Diese umfaßt die elektrische Funktion (Beschreiben, Verändern und Lesen des Dateninhaltes) und die mechanische Funktion.

Standardbedingungen für die Testmethoden

Umgebungsbedingungen

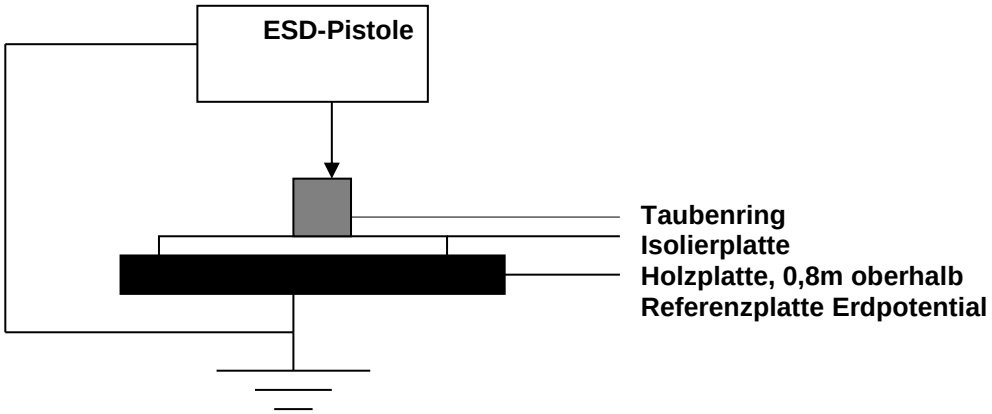
Wenn nicht anders spezifiziert, werden die Tests bei einer Umgebungstemperatur von 23°C +/- 3 °C und einer relativen Luftfeuchtigkeit von 40% bis 60% durchgeführt.

Toleranzwerte

Wenn nicht anders spezifiziert, sind alle Werte, die die Eigenschaft des Testequipments und das Verfahren der Testmethoden spezifizieren, mit +/-5% Toleranz behaftet.

Elektrostatik

Sinn dieses Testes ist es, den Einfluß der Elektostatischen Entladung auf den Taubenring zu prüfen, basierend auf dem Human Body Model.



ESD Test Aufbau

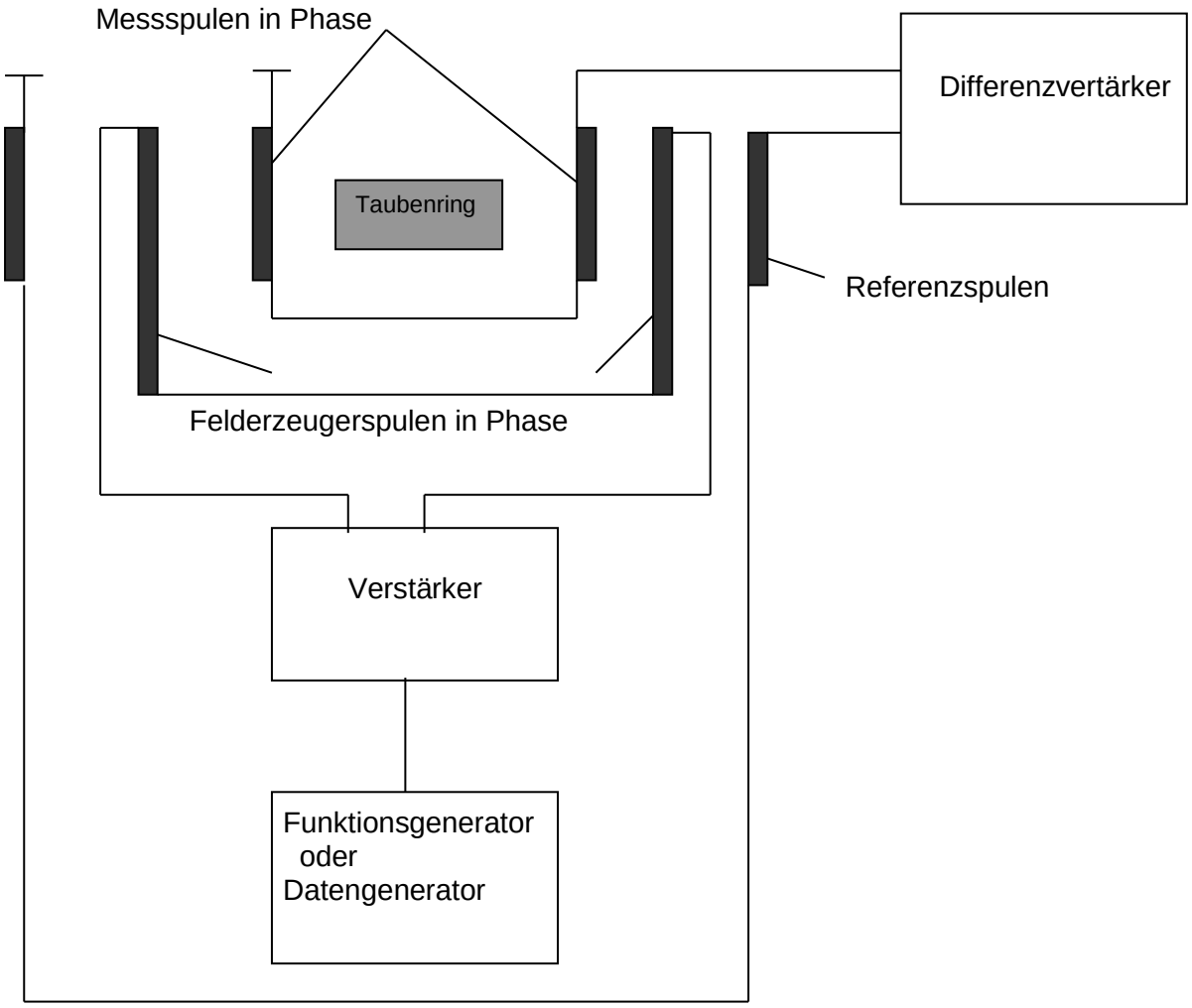
Testablauf

Grundlage für den Testablauf ist die IEC61000-4-2: 1995
Bei diesem Test sind jeweils fünf Entladungsvorgänge an fünf verschiedenen Punkten des Taubenringes mit Schärfegrad 4 durchzuführen. Zwischen den einzelnen Entladungsvorgängen sind mindestens 10sec Zeitabstand einzuhalten.

Nach dem Test ist die Funktionalität des Taubenringes zu überprüfen.

Testaufbau zur Prüfung der Lese und der Schreibreichweite

Zur Überprüfung der Lese- und der Schreibreichweite wird ein Messaufbau nach dem Helmholtz Prinzip verwendet. Dies ermöglicht ein homogenes Magnetfeld.



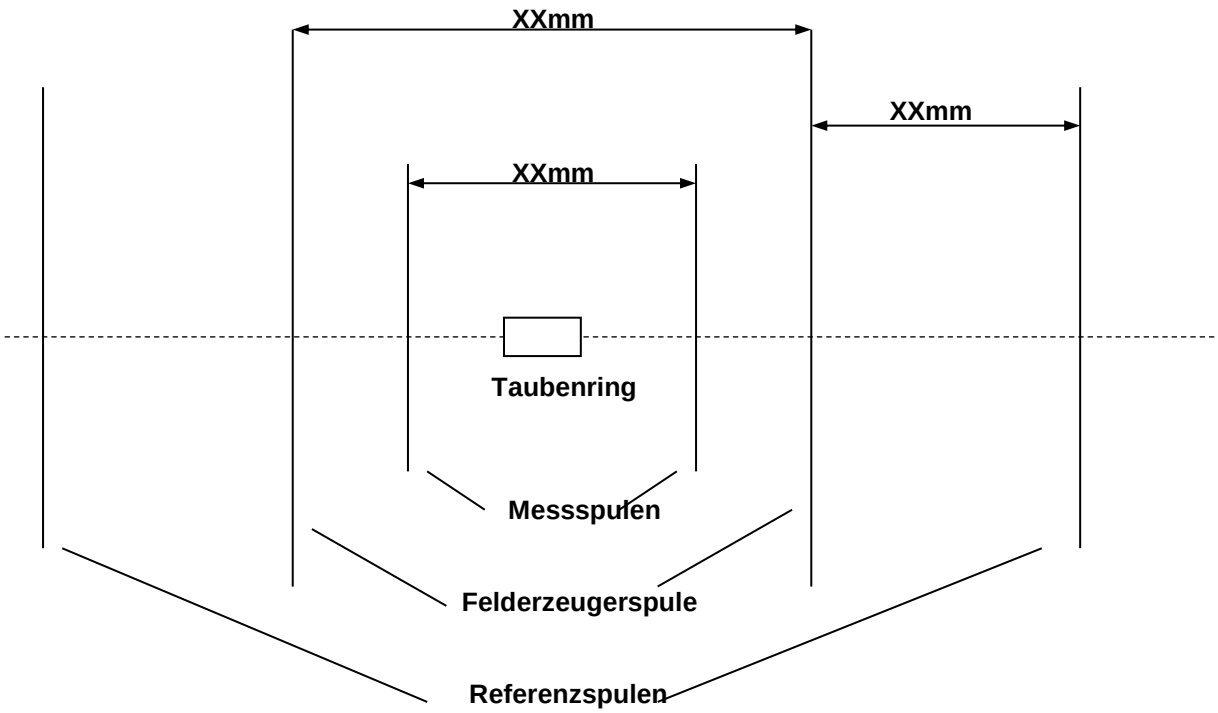
Der Funktionsgenerator treibt die Felderzeugerspulen, so daß das magnetische Feld in Frequenz und Feldstärke einstellbar ist.

Messspulen
Definition der Spulen in mechanischen Abmassen und elektrischen Daten.

Felderzeugerspule
Definition der Spulen in mechanischen Abmassen und elektrischen Daten.

Referenzspulen
Definition der Spulen in mechanischen Abmassen und elektrischen Daten.

Testanordnung



Prüfung der Lesereichweite

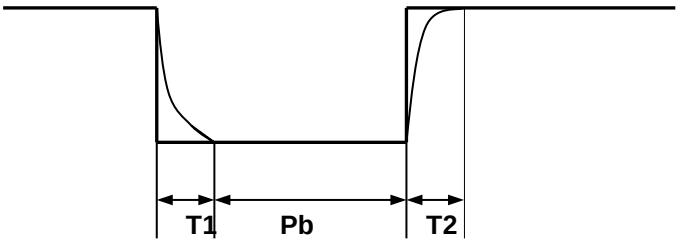
Der Taubenring muß in der Testanordnung zwischen den Feldstärken Hmin=?? Und Hmax =?? gelesen werden können.

Prüfung der Schreibreichweite

Zur Überprüfung der Schreibreichweite des Taubenringes muß sowohl der Bereich der Geheimzahl als auch der Bereich der weiteren Seiten des Taubenringes beschrieben werden. Die dafür notwendigen Daten werden von einem Datengenerator erzeugt. Das Verifizieren des Dateninhaltes kann mit einer separaten Lesestation erfolgen.

Beim Beschreiben des Taubenringes sind folgende Parameter gegeben

- Feldstärke H_{min} =??? und H_{max} =??
- Geometrie der Spulen
- Pulsform (T1 und T2) und Pulsbreite (Pb) der Schreibimpulse
- Modulationstiefe m



Materialeigenschaften des Ringes

Funktionsbeständigkeit gegen Wasser

Der Taubenring wird vollflächig in destilliertem Wasser über einen Zeitraum von 10 Tagen gelagert. Die Wasseraufnahme darf nach diesem Zeitraum nicht mehr als 1% betragen. Die Funktion darf nicht beeinträchtigt werden.

Funktionsbeständigkeit gegen wässerige Kochsalzlösung

Der Taubenring wird vollflächig in eine 10% Kochsalzlösung über einen Zeitraum von 24 Stunden bei einer Temperatur von 50°C gelagert. Die Lösungsaufnahme darf nach diesem Zeitraum nicht mehr als 1% betragen.

Funktionsbeständigkeit gegen Amoniaklösung

Der Taubenring wird vollflächig in eine 10% Amoniumhydroxidlösung über einen Zeitraum von 24 Stunden bei einer Temperatur von 50°C gelagert. Es darf keine Zersetzung stattfinden.

Funktionsbeständigkeit gegen UV-Strahlung

Der Taubenring wird mit einer Halogenlampe in einem Abstand von 30 cm über einen Zeitraum von 1 Stunde bestrahlt. Die Halogenlampe muß folgende technischen Daten erfüllen:

- 10° Abstrahlwinkel
- 20 W Leistung

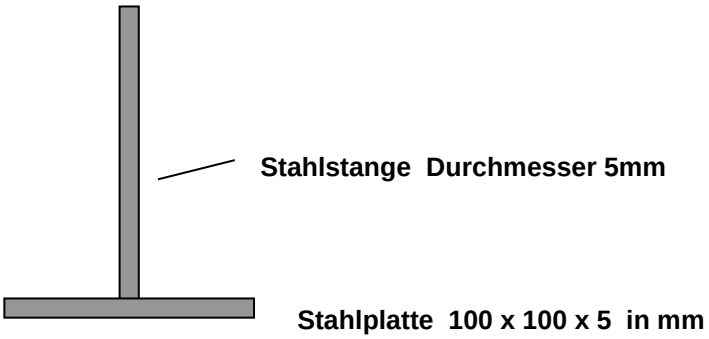
Der Dateninhalt des Taubenringes darf sich nicht verändern.

Funktionsbeständigkeit gegen Vibration

Dieser Test wird nach IEC68 Teil 2-34 - Vibration durchgeführt.
Die mechanischen Eigenschaften des Taubenringes dürfen sich nicht verändern.

Funktionsbeständigkeit gegen Freier Fall

Dieser Test wird nach IEC68 Teil 2-32 - Frei Fallen durchgeführt.



Der Taubenring wird jeweils fünf Mal in beiden Positionen aus einer Höhe von 1,2m über die Stahlstange auf die Stahlplatte fallen gelassen.

Nach dem Test ist die Funktionalität des Taubenringes zu überprüfen.

Lagertemperatur und Betriebstemperatur

Dieser Test wird nach IEC68 Teil 2-24-Temperaturwechsel durchgeführt.

- Temperaturbereich -25 tot +70°C
- Je 3 Std bei -25 en +70°C
- Gesamtdauer min. 24 Std.
- Temperaturänderungsgradient 2,5°C/min.

Die mechanischen Eigenschaften des Taubenringes dürfen sich nicht verändern. Der Dateninhalt des Taubenringes darf sich nicht verändern. Die Funktion des Taubenringes darf nicht beeinträchtigt werden.

Annex 2 Chip-rings Overview