COMITÉ EUROPÉEN DES ASSURANCES

SECRETARIAT GENERAL
3bis, rue de la Chaussée d'Antin F 75009 Paris
Tél. : +33 1 44 83 11 73 Fax : +33 1 44 83 11 85
Web : cea.assur.org

DELEGATION A BRUXELLES
Square de Meeûs, 29 B 1000 Bruxelles
Tél. : +32 2 547 58 11 Fax : +32 2 547 58 19
Web : cea.assur.org

PROPERTY INSURANCE COMMITTEE
Prevention Specifications

Intruder Alarm Systems
Functional Requirements

CEA 4038: May 2002 (en)

0 Scope

This standard contains requirements for the Functions and Protection measures of an Intruder Alarm System (IAS).

1 Purpose

The purpose of this standard is to describe requirements of the European insurer`s for a correctly installed IAS independent of the technology used to fulfill these requirements.

2 Terms and Definitions

Note: The following definitions refer to parts, functions or a whole system.

Action: Manipulation or other physical act by a person.

Alarm Notification: The passing of an Alarm Condition to Warning Devices and/or Alarm Transmission Systems.

Alarm Receiving Centre: A continuously manned remote centre to which the information concerning the state of one or more Alarm Systems is reported.

Alarm state: The state in which there is notification of a detected event.

Alarm Transmission System: A system which is used to tranfer information concerning the state of one or more Alarm Systems between supervised premises and one or more Alarm Receiving Centres.

Authorisation: Permission granted and controlled by physical, electronic or organisational (e. g. written agreement) means.

Availability of interconnections: Where the interconnection is capable of conveying signals or messages.

Command: An instruction given to the installed system by the successful completion of an operation.

Communication: The transmission of messages and/or signals between IAS components (could be bits, bytes, change of voltages/current, etc.).

Conditionally accessible: A function is conditionally accessible if

- it is located within a monitored area
  and/or
- access cannot be gained without a person in charge noticing the access
  and/or
- it can be accessed only after unlawful penetration into a building or part of a building
  and/or
- it is only accessible after overcoming of a physical barrier (e. g. penetration, bypassing).

Configurate Basic Data: Operation intended for programming the basic data of an IAS (e. g. the operating program) and for changing these parameters.

Configurate Site-specific data: Operation intended for programming the site-specific data of an IAS (e. g. programming of zones, adjustment of detection range and sensitivity of a detector) and for changing these parameters.

Configurate User-specific data: Operation intended for programming the user-specific data of an IAS (e. g. programming of user-codes, adjustment of indication clarity) and for changing these parameters.

Continually: Recurring frequently at regular intervals.

De-isolation: Operation intended for reversing the isolated state.

Detection: Entirety of functions, which generate an alarm signal by surveying a suitable physical condition and recognising a change in that condition.

Detection point: Identification of detection to one or - if linked together - more detectors.

Environmental stability: Characteristic of the IAS to operate correctly within certain environmental influences.

False detection immunity: False detection immunity is the resistance to misinterpretion of a change of condition when change is the result of a non-intruder-related influence.

Fault Signal: A signal generated by the Alarm System when in a fault condition.

Freely accessible: A function is freely accessible if no criterion for “conditionally accessible” is met.

Functional reliability: Entirety of functions which enable continous correct operation of the system and detection of failures.

Function monitoring: Entirety of measures (manual and automatic) necessary to detect failures.

Indication: Entirety of all functions which are necessary to deliver information to the operators.

Indication/Signalling: Entirety of all functions which are necessary to deliver informations.

Inhibited State: State of an IAS in which an alarm condition cannot be notified. This state will be automatically removed after the next unsetting of the system.

Inhibiting: Operation intended to achieve the inhibited state.

Installer: A person or organisation prepared to provide and install an intruder alarm system, or the appointed representative of such person or organisation.
Remark: “Installer” in this context includes authorised service or maintenance contractor.

Interconnection media: The media by which signals or messages are communicated.

Interrogate memory: Operation intended for permitting access to the memory of the IAS.

Isolated state: State of a part of an IAS in which functions are prevented from performing their intended purpose.

Isolation: Operation intended to achieve the isolated state.

Latched State: A description applying to a connection or indication which remains until deliberately removed. A state which remains until deliberately removed.

Local alarm: Activation of an audible and/or visible warning device in an area around the supervised premises.

Manufacturer: A person or organisation prepared to manufacture and supply component(s) for an intruder alarm system, or the appointed representative of such person or organisation.

Misoperation: An incorrect operation which is performed either deliberatley, under a misconception as to its effect, or accidentally, without any intent.

Monitored area: A monitored area is an area which is not accessible without triggering an intruder alarm based on the chosen monitoring concept.

Monitoring concept: Description of intrusions/intrusion attempts which will be detected by the IAS.

No-alarm state: The state in which there is no alarm notification and no indication.

Non-specific interconnections: An interconnection not exclusively used by an IAS, i. e. an interconnection shared by other systems. Example: Fire detection system. Examples of technologies used in shared interconnections are as follows radio frequency links, BUS-systems.

Normal Condition: The condition of an IAS when it is fully operational.

Notification: Entirety of all functions which are necessary to achieve information in a case of a detected event.

Operation: Entirety of actions which enable an Operator to give commands to the installation.
Note: Some operations may be performed by the completion of one action only.

Operational Security: Entirety of measures necessary to prevent or detect misoperation of the installation and other accidental influences upon the installation.

Operator: A person who performs an operation. Such persons may be users, installers or manufacturers.

Override: Operation intended to deliberately ignore one or more conditions for the fulfillment of an operation/function.

Permit indication: Operation intended for permitting access to indications (e. g. zone indication).

Post-alarm state: The state after notification has stopped and the indications are available.

Prevention function: Entirety of measures necessary to ensure the function of an IAS with high availability and reliability.

Processing: Entirety of functions which are necessary to control the operation of the system.

Reset: The process of restoring the normal condition after an alarm or fault.

Restore: Operation intended to achieve the No-alarm-state.

Response Authority: The designated authority with responsibility for attending the supervised premises following an alarm and taking the appropriate action.

Restore System: The process of restoring the system to normal condition.

Security jeopardizing: An effect is security jeopardizing when the security function of an IAS is put at risk but not reduced.

Security relevant function: Function where a certain influence can have a security jeopardizing effect.

Security impairing: An effect is security impairing when the security function of an IAS is reduced.

Security critical function: Function where a certain influence can have a security impairing effect.

Security destructive: An effect is security destructive if it prevents the IAS entirely from fulfilling its security function.

Security destructive function: Function where a certain influence can have a security vital effect.

Security vital function: Function where a certain influence can have a security vital effect.

Set: Operation intended to achieve the set state.

Set State: The state of parts of an IAS (e.g. Intrusion, Tamper, Hold-up) in which an alarm condition can be notified and indicated.

Specific interconnections: An interconnection used exlusively by an IAS:

Status Signal. A signal generated by the Alarm System when a status of the IAS has been changed (e.g. Set/Unset).

Stop notification: Operation intended to achieve the post-alarm state.

Supervised area: Area which is not accessible without triggering an intrusion alarm on the basis of a realized supervisory concept.

Supervisory concept: The supervisory concept for a particular IAS will be determined by a number of factors but in particular

- Nature and value of goods
- Anticipated quality of intruder
- Nature, contruction and layout of premises

It defines in general terms the probability and timeliness of the detection of the intrusion or intrusion attempt.

Tamper: An intentional interference with the IAS with the aim that it will no longer be able to fulfill its purpose.

Tamper security: Entirety of measures which are necessary to oppose (prevent and detect) an intentional interference with the system, with the aim that the system will no longer be able to fulfill its purpose.

Tamper protection: The entirety of all measures directed at preventing Tamper according to the relevant threat pattern to the largest possible extent by offering physical resistance.

Tamper monitoring: The entirety of all measures directed according to the relevant threat pattern for detecting and indicating Tamper.

Test: Operation intended for testing functions (e. g. detection functions, notification functions).

Unset: Operation intended to achieve the unset state.

Unset State: The state of parts of an IAS (e.g. Intrusion, Tamper, Hold-up) in which an alarm condition cannot be notified and indicated.

User: The owner or manager of the premises in which the intruder alarm system is fitted or a person authorised by the owner or manager to operate the system.

Verification of communication: The periodic transmission of a message or signal between IAS components to verify the ability of the interconnection to convey a signal or a message.

Warning Device: A device that conveys an alarm by audible and/or visible means.
Zone: An assessed area where abnormal conditions may be detected.

4 Requirements for the Basic Functions

4.1 General

The Basic functions of an IAS allow the system to detect and indicate/notify an intrusion and/or intrusion attempt depending of the state of the system.

4.2 Detection

Remark: Immunity against tampering the detection function is not addressed in this clause, see clause 5.5 „Tamper Security".

4.2.1 Detection types

Detection may take any one or more of the following forms:

Type of hazard	Type of detection	A	B	C	D
Penetration	**Opening** of closures such as doors, windows, shutters, etc.	Opening maximum to 6 cm	Fractional opening (e.g. insufficient to permit through-view)		
	Breach of building envelope[1)] (without opening closures as above (e.g. forced penetration through walls, roofs, doors, windows, safe envelopes, etc.)	Opening ≥ 40 x 40 cm	Opening ≥ 8 x 8 cm	Opening ≥ 2 x 2 cm	Start of attack (e.g. touching the wall with the tool)
Intrusion	**Human** Presence of humans	Human being - upright walking - 0.3 ... 2.5 m/s - „Trap", minimum one direction in the supervised area	Human being - upright walking - 0.3 ... 2.5 m/s - „Trap", any direction in the supervised area	Human being - upright walking and crawling - 0.1 ... 4 m/s - Entire room	Presence of an intruder in the supervised area (moving or stationary)
	Technical Introduction of technical means (e.g. fishing attacks on jeweller shop)	Introduction of technical items (e.g. ropes, wires, robots) into the supervised area			
Removal	**Material items** Physical items (e.g. money, goods)	Removal out of specified area	Removal out of specified position	Attempted removal	Touching or attempt to touch the supervised item
	Non-material items Information (e.g. software, data)	(Not yet detectible by IAS)			

[1)] Envelope in this context could also be an envelope of a limited volume, e.g. a safe, strongroom, vitrine.

The class of installation required together with the supervisory concept chosen will together determine the selection of detection types from the table above.

Note: Guidance will be provided in the doc. Application Guidelines.

4.2.2 Detection probability

A detection probability close to 100% within the selected type of detection shall be achieved where the detection function is installed and used in accordance with the manufacturer´s specifications. Advice has to be given to the user to avoid a reduction of detection probability (e.g. by blocking the field of view of a movement detector with furniture).

4.2.3 False detection immunity

All types of detection shall be designed in such a way that „close to 0“ false detection is guaranteed.

4.2.4 Immunity against the possibility of undermining the detection function

Features which are designed to minimize false detection of certain changes of conditions shall not result in detection being avoided by an intruder mimmicking such changes in condition.

4.2.5 Detection location identification

The design of a detection type shall include a facility to identify the source of a detected change of a condition.

4.3 Processing (including the requirements for interconnection used in IAS)

4.3.1 General

The processing function has to ensure that all signal inputs are processed in accordance to the type of the signal and the state of an IAS within a specified time. Furtheron it has to ensure reliable communication between components of the IAS.

4.3.2 Functional requirements

4.3.2.1 IAS class 1

Processing of signals of IAS class 1 shall depend on the status of the IAS and the type of the signal.

IAS status	Outputs	IAS class 1				
		Input Intrusion signal	Input Tamper signal	Input Fault signal	Input Status signal (e.g. SET, UNSET) [1)]	Input Fault signal from transmiss. paths of ATS
SET	Local indcation	Op	Op	Op	Op	Op
	Notif. via ATS	If ATS available: M as Intrusion	If ATS available: M as Tamper	If ATS available: M as Fault	If ATS available: Op as Status	Not applicable
	Notif. via aud. WD	(M)	(M)	--	--	--
	Notif. via vis. WD	(M)	(M)	--	--	--
UNSET	Local indication	Op *	M (visible and audible)	M (visible and audible)	Op	M
	Notif. via ATS	--	M as Tamper	M as Fault	M as Fault	Not applicable
	Notif. via aud. WD	--	--	--	--	--
	Notif. via vis. WD	--	--	--	--	--

M: Mandatory
(M): Mandatory if ATS is not available
Op: Optional
* On user´s request only
--: Prohibited
[1)] Could be also information of partial Set/Unset

4.3.2.2 IAS class 2 and 3

Processing of signals of IAS class 2 and 3 shall depend on the status of the IAS and the type of the signal.

IAS status	Outputs	IAS class 2 and 3				
		Input Intrusion signal	Input Tamper signal	Input Fault signal	Input Status signal (e.g. SET, UNSET) [1]	Input Fault signal from transmiss. paths of ATS
SET	Local indcation	Op	Op	Op	Op	Op
	Notif. via ATS	M as Intrusion	M as Tamper	M as Fault	Op as Status	Not applicable
	Notif. via aud. WD	Op	Op	--	--	--
	Notif. via vis. WD	Op	Op	--	--	--
UNSET	Local indication	Op *	M (visible and audible)	M (visible and audible)	M	M
	Notif. via ATS	-- [2]	M as Tamper	M as Fault	M as Fault	Not applicable
	Notif. via aud. WD	--	--	--	--	--
	Notif. via vis. WD	--	--	--	--	--

M: Mandatory
(M): Mandatory if ATS is not available
Op: Optional
* On user´s request only
--: Prohibited
[1] Could be also information of partial Set/Unset
[2] Could be sensible if alarm receiving Centre is able to handle such signals.

4.3.3 Timing requirements

A detected signal shall be processed and indicated/notified in a maximum time as follows when the IAS is in it´s specified condition, e.g. no fault (including transmission time via the interconnections).

Signal	IAS-class 1	IAS-class 2	IAS-class 3
Intrusion	10 s	10 s	10
Tamper	10 s	10 s	10 s
Fault	10 s	10 s	10 s
Status	10 s	10 s	10 s
Loss of interconnection	10 s	10 s	10 s
Substitution/loss of IAS-Components	10 s	10 s	10 s

4.3.4 Interconnection requirements

4.3.4.1 General

Interconnections are necessary for the exchange of informations between IAS-components (e.g. intrusion signals). Interconnections may be specific (e. g. an IAS-internal cable network) or non-specific (e. g. radio frequency links, infrared links, BUS-structural systems for multiple application).

In order to guarantee a high level of reliability of the IAS the interconnection shall fulfill requirements as follows:

4.3.4.2 Availability

Interconnections shall provide reliable means of interconnections where signals shall not be lost, changed or delayed. The availability of the interconnection shall be at least such to ensure that signals are conveyed in a time as specified in clause 4.3.3.

4.3.4.3 Monitoring of interconnections

Interconnections shall be monitored to detect:

- when the availability fails to meet the requirements specified in clause 4.3.4.4
- the substitution or loss of signals as required in clause 4.3.4.6
- the substitution or loss of IAS-components as required in clause 4.3.4.5

In addition periodic communication shall be established as specified in clause 4.3.4.7 between IAS components to verify the communication necessary for the correct functionning of the IAS.

3.4.4.4 Availability

Interconnections shall be monitored to detect conditions which prevent the interconnection to convey signals as follows. If the interconnections are not available for a time longer than for class 1 = 30 s, class 2 and 3 = 10 s, it shall be indicated as follows:

To be indicated as	**IAS**					
	Class 1		Class 2		Class 3	
	SET	UNSET	SET	UNSET	SET	UNSET
Tamper	M	M	M	M	M	M
Fault						
Tamper or Fault						

3.4.4.5 Substitution/loss of IAS-components

To ensure the integrity of the IAS all components of the IAS shall be monitored to detect a loss and/or substitution within 10 s in all IAS classes.

In the event of detection of a loss and/or substitution a tamper signal shall be generated in the Set and Unset state of the IAS.

3.4.4.6 Substitution/loss of communication

To ensure that communication between the system components cannot be tampered communication shall be continually monitored to detect loss and/or substitution of security relevant signals within 10 s as follows.

Remark: It may be that in today´s practice this requirement cannot be fulfilled by all kinds of available equipment.

IAS		
Class 1	**Class 2**	**Class 3**
15 min	30 s	10 s

When a loss and/or substitution is detected a tamper signal shall be generated in the Set and Unset state of the IAS.

Remark: The interruption of the transmission path by opening of a magnetic switch by times is acceptible and should not result in a tamper signal or condition that it is possible to detect a possible fault after closing the contact.

3.4.4.7 Periodic communication

To ensure a reliable communication via interconnections between components of the IAS it shall be continually verified at least as shown in the following table:

IAS		
Class 1	**Class 2**	**Class 3**
15 min	30 s	10 s

If there is no positive verification the following reaction is required.

- When it is established that communication could not be verified due to a technical fault of the IAS a fault signal shall be generated.
- In all other cases (e. g. tamper) a tamper signal shall be generated.

4.4 Operation

4.4.1 General

Operation functions of an IAS are necessary to allow an operator to give commands to the system.

Remark: The processing of these operations is described in clause 4.3 „Processing".

4.4.2 Mandatory functions

An IAS shall have at least the following functions depending upon its class:

Function	**IAS**		
	Class 1	**Class 2**	**Class 3**
Normal operation functions			
- Set	M	M	M
- Unset	M	M	M
- Permit indication	Op	M	M
- Interrogate memory	Op	Op	M
Test function			
- Test indication	Op	M	M
- Test detector function	Op	M	M
- Test notification	Op	OP	Op
Notification handling function			
- Stop notification	M	M	M
- Restore	M	M	M
Configuration			
- Basic configuration	M	M	M
- Configuration of site-specific data	M	M	M
- Configuration of user-specific data	M	M	M

M: Mandatory
Op: Optional

4.4.3 Operational functions

IAS may have additional functions (e.g. isolation, de-isolation, inhibiting).

Remark: Requirements for the use of the operation functions (e. g. authorisation, access levels) see clause 5.4 "Operational Security".

4.5 Indication/Notification

4.5.1 Approach of the Indication/Notification function

Depending of the state of the IAS (e.g. Set, Unset) the system shall

- call for reaction (e.g. police/response authority)	as a consequence of an Intrusion/Intrusion attempt and a Tamper/Tamper attempt in the Set State of the IAS
- "call for technical help" (e.g. maintenance service)	as a consequence of a fault and a Tamper/ Tamper attempt in the Unset State of the IAS
- "inform a relevant person" (e.g. user, remote centre)	as a consequence of a change of a state of the IAS from Set to Unset
- record events (e.g. set, unset, fault, alarm)	e.g. for tracability of events, evidence

Optionally the IAS the system may initiate additional protection systems (e.g. smoke generating devices, CCTV, high power sirens, flashing lights) as a consequence of an intrusion/intrusion attempt and a Tamper/Tamper attempt in the Set State of the IAS. These systems shall not influence the normal function of the IAS.

Also additional informations like technical alarms may be indicated and/or notified.

4.5.2 Methods of Indication/Notification

Indication/Notification functions shall be designed in a way that a human being is positively informed, i. e. the indication cannot be misunderstood, overlooked or lost.

4.5.3 Requirements

4.5.3.1 Notification functions

Dependent upon the class of the IAS the following notification functions are mandatory or an option. Notification shall also include the indentity of the IAS.

Signal	Notification					
	Signalling (ATS)			Local alarm		
	Class 1	Class 2	Class 3	Class 1	Class 2	Class 3
Intrusion	Op	M	M	M[2)]	Op	Op
Tamper IAS set IAS unset	 Op Op	 M M (as Tamper)	 M M (as Tamper)	 M[2)] M[2)]	 Op Op	 Op Op
Fault	Op	M (as Fault)	M (as Fault)	--	--	--
Hold-up[1)]	Op	M (as Hold-up)[1)]	M (as Hold-up)[1)]	Op	Op	Op
State Set/unset	Op	M	M	NR	NR	NR
Zone identification	Op	Op	M	NR	NR	NR
Detection point identification	Op	Op	M	NR	NR	NR

M: Mandatory

Op: Optional

--: Not permitted

NR: Not relevant

[1)] If hold-up is included in the IAS

[2)] Op if IAS has Signalling; Local Alarm could be operated in the event of intrusion or tamper during an ATS failure.

4.5.3.2 Indication functions

Dependent upon the class and Status of the IAS the following conditions shall be indicated where shown as mandatory in the table.

Condition *)	Conditions to be indicated								
	Class 1			Class 2			Class 3		
	During setting	SET	UN-SET	During setting	SET	UN-SET	During setting	SET	UN-SET
Status IAS SET	NA	Op 1)	NA	NA	M 1)	NA	Na	M 1)	NA
Setting in progress 2)	M	NA	NA	M	NA	NA	M	NA	NA
Unsetting started, but still incomplete 2)	NA	M	NA	NA	M	NA	NA	M	NA
Intruder Alarm condition	M	Op	M 3)	M	Op	M 3)	M	Op	M 3)
Hold-up Alarm condition	M	Op	M 3)	M	Op	M 3)	M	Op	M 3)
Zone indentification	M	Op	M 3)	M	Op	M 3)	M	Op	M 3)
Zone first to alarm	NA	Op	Op)	NA	Op	M 3)	NA	Op	M 3)
Zone isolated	M	Op	Op	M	Op	Op	M	Op	Op
Part set (Zone or detection point inhibited)	M	Op	Op	M	Op	Op	M	Op	Op
Primary power fault	M	Op	M	M	Op	M	M	Op	M
Alternative power fault	M	Op	M	M	Op	M	M	Op	M
ATS fault	M 4)	Op	M	M	Op	M	M	Op	M
All other faults	M	Op	M	M	Op	M	M	Op	M
Tamper condition	M	Op	M 3)	M	Op	M 3)	M	Op	M 3)
Tamper zone	M	Op	M 3)	M	Op	M 3)	M	Op	M 3)
Detector masked	Op	Op	Op	M	Op	M	M	Op	M

*) This list does not imply that all installations will be capable of, or prone to all such conditions, see clause 4.3 „Processing“ for mandatoty functions.

M: Mandatory

Op: Optional

NR: Not relevant

NA: Not appliciable

[1)] Time-limited

[2)] If necessary to avoid false-alarms

[3)] Until restored

[4)] Only if ATS is fitted

4.5.3.3 Event recording

4.5.3.3.1 General

Dependent upon the class of the IAS the following conditions shall be automatically recorded together with date and time at which the event which caused the condition occurded.

Conditions to be recorded *)	Class 1	Class 2	Class 3
„IAS SET“ including ID of user	Op	M	M
„IAS UNSET“ including ID of user	Op	M	M
Intruder alarm	Op	M	M
Hold-Up Alarm 1)	Op	M	M
Zone first to alarm	Op	M	M
Zone isolated including ID of user	Op	M	M
Primary power fault	Op	M	M
Alternative power fault	Op	M	M
ATS fault 1)	Op	M	M
All other faults	Op	M	M
Part set (Zone or detection point inhibited) including ID of user	Op	M	M
Tamper condition	Op	M	M
Detector masked	Op	M	M
Override including ID of user	Op	M	M
Change of date and/or time including ID of user	Op	M	M

*) This list does not imply that all installations will be capable of, or prone to all such conditions, see clause 4.3 „Processing“ for mandatoty functions.

M: Mandatory

Op: Optional

1) If fitted

4.5.3.3.2 Means of recording

The means used to record the mandatory events shall comply with the requirements in the following table. It is allowed to erase old events when the memory has reached its maximum capacity. Furthermore means for recording shall be protected against accidental or deliberate deletion or alteration of the contents.

Conditions to be recorded	Class 1 [1)]	Class 2	Class 3
Memory capacity	≥ 200 events	≥ 1000 events	≥ 1000 events
Endurance of memory after IAS power failure	≥ 30 d	≥ 30 d	≥ 30 d

1) Event recording is optional for this class but, if supplied, the requirements shall be fulfilled.

5 Requirements for the Protection Functions

5.1 General

The protective functions of an IAS allow the system to work with the highest possible effectiveness and availability.

5.2 Functional Reliability

5.2.1 General

The purpose of Functional Reliability consists in preventing to the largest possible extent all security jeopardizing, security impairing and security destructive effects caused by technical failures:

- resulting from poor installation; rules aimed at preventing technical failures resulting from poor installation are provided in documents Application Guidelines and Qualification of Installers.
- in a correctly designed and installed IAS.

For the purpose of this document, technical failures comprise only failures within components of intruder alarm installation. In cases where for technical reasons prevention is only possible to a limited degree, failures must be detected and indicated in due time.

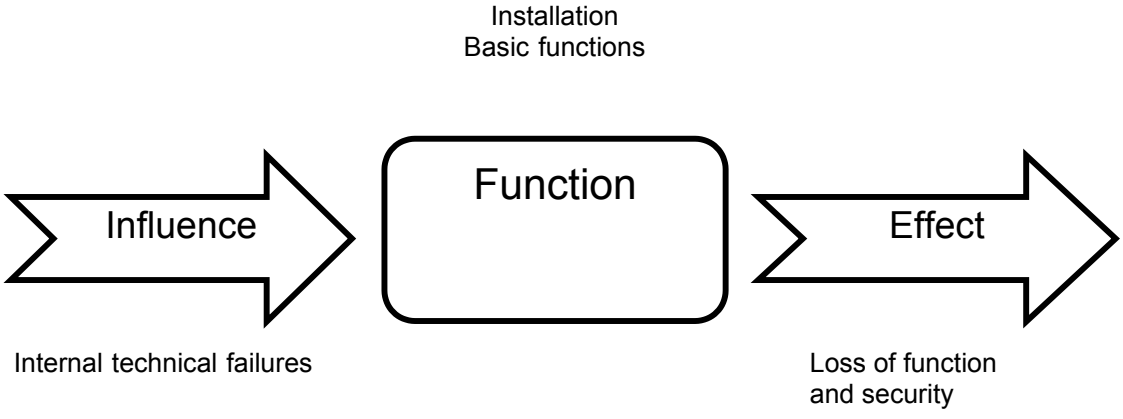
Remark: False alarms are security jeopardizing.

The requirements are applicable to all components of the installation and at all stages in the production of an installation (planning, designing, installation, commissioning, ...).

5.2.2 Functional Reliability structure

5.2.2.1 General

To set up standards of Functional Reliability, the following relationships are relevant:



Technical failures, caused by poor installation or product failure, can influence the function of the system and lead to effects like loss of function and security of the system.

The purpose of Functional Reliability consists in preventing to the largest possible extent the influence or the relevant effect. For technical and economic reasons technical failures cannot in some cases be avoided; nevertheless, they shall be indicated, or shall be detected in a maintenance cycle.

5.2.2.2 Types of failures

5.2.2.2.1 General

Technical failures may be classified according to their occurence probability; the occuring frequency varies. The nature of the failure characterises the relevant occurence.

It can be stated that there is a proportional link between the type of failure involved and its occurence probability.

Different types of parameters can be used to illustrate this concept, but probability is the basic criterion selected to structure the document.

The lower the probability of failure, the more acceptable the risk becomes.

5.2.2.2.2 Threat pattern

As mentioned above, the threat pattern is essentially determined by the occurence probability of a failure. Two main causes of failures can be distinguished:

- Systematic (deterministic cause):
This type of failure often appears on a whole batch of component parts, or on a defined type of component part. It can be found at two levels:

• **Hardware:** It involves mainly manufacturing defects, designing errors, component parts layout errors, errors in the choice or the dimensioning of the component parts, power supply defect. The most frequent failures are either short circuits or connection breaks.

• **Software:** It relates to errors in functional analysis, or in the input of the programs.

- Random:
These malfunctions can only be found in the hardware. They mainly appear during the operation of the system, in static functioning and may be linked to the life time of the component part.

5.2.2.2.3 Probability of a failure

A distinction is made between the following probability levels of failure occurence:

Probability Level	Failure expectation
Close to none	1 failure per 30 years
Extremely low	1 failure per 10 years
Very low	1 failure per 3 years
Low	1 failure per 100 days

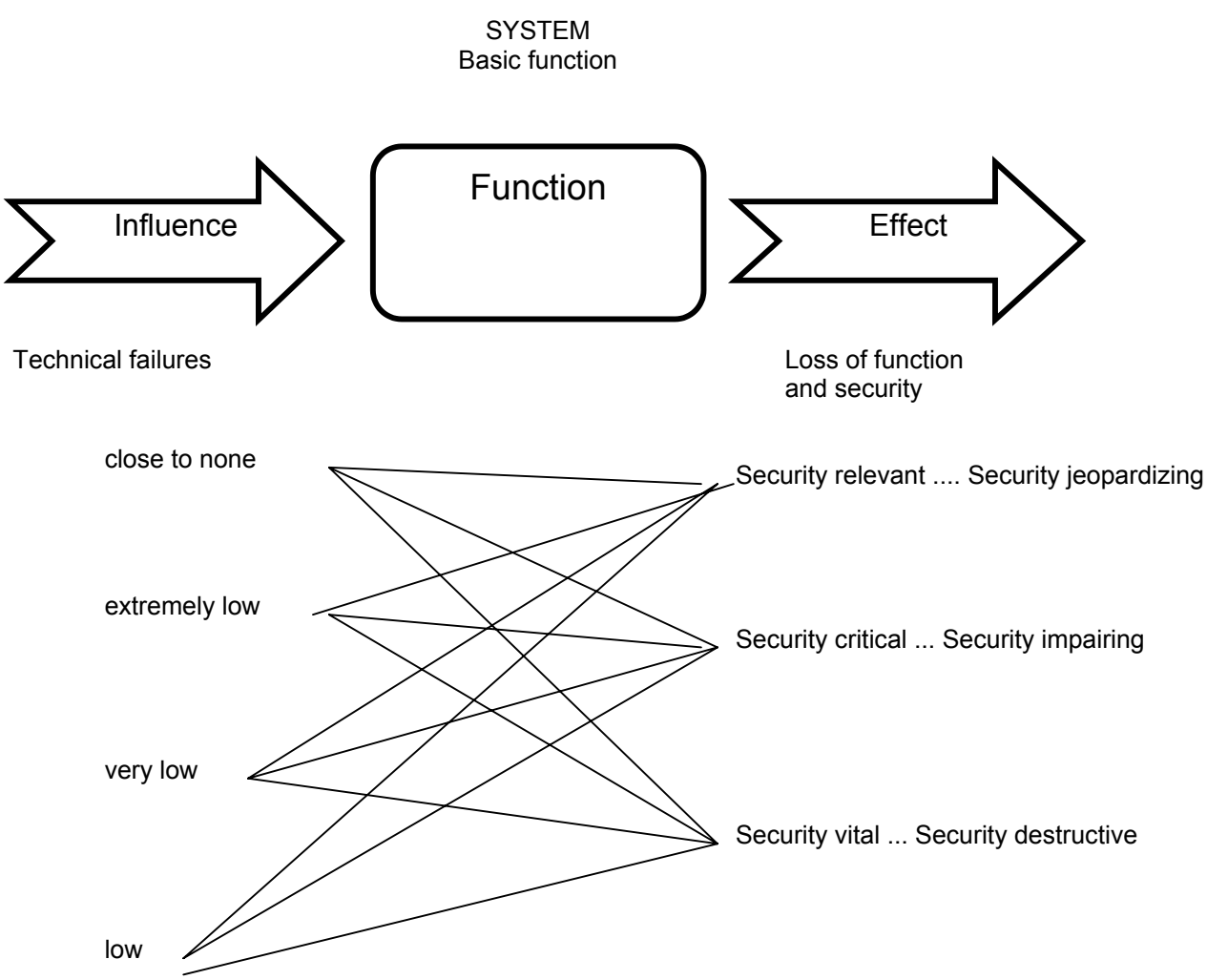
5.2.2.3 Types of effects

The type of effect is determined by the loss of function and security of the system. The following three types of effects can be distinguished:

- Security jeopardizing (e. g. reduction of sensivity of a detector, cable breakage)
- Security impairing (e. g. total defect of a detector and therefore loss of security in a specific area)
- Security destructive (e. g. total loss of current supply and therefore total loss of security)

5.2.3 Functional Reliability structure

The Functional Reliability structure shall be established by considering the types of influences, effects and functions as follows:



5.2.4 Reqirements for Functional Reliability

5.2.4.1 General

Functional Reliability requires that the component parts shall have the same level of performance and this shall apply to all classes of IAS.

The classification of an IAS depends on the provided functions, the access levels of the components involved and the technical sophistication characterising the component parts.

5.2.4.2 Basic requirements

Considering the functional reliability of IAS, failures of component parts shall be taken into account. They can be caused by operation close to overload, design error (hot transistor near resistance for example) or poor workmanship, mechanical damage in handling, ...

Measures to combat technical failures are classified as follows:

5.2.4.2.1 General

- Conformity to the design specification, relevant standards and mandatory requirements;
- Good workmanship according to State of Art;

- Clear rules for adjustement, maintenance, etc.;
- Use of reliable component parts;
- Correct manufacturing, packaging and handling;
- Use of component parts within safe operating limits (e. g. voltage, temperature, intensity of current, ...).

5.2.4.2.2 Preventive measures

These measures are:

Design: The measures that can be implemented are for example: to apply quality assurance, to define perfectionist aims by taking into consideration error tolerances, product redundancy, multiple sensors for error detection allowing correction of deviations, to specify essential requirements and appropriate tools, design with high “signal-noise ratio”, choice of different blocks, project organisation.

Development: Checking and validation procedures shall be carried out at all stages; dynamic and functional analysis to be performed. Component parts, measurement check points and connections easily accessible, use of reliable software.

Pre production: It has to be ensured that the documents are reliable and that the tools used are suitable; a good planning for production stage has to be provided.

Production: The documents have to be sufficiently clear and precise to be easily usable and incapable of misinterpretation.

5.2.4.2.3 Monitoring measures

These measures are:

- Automatic and manual monitoring of functions;
- Indication of failures;
- Indication of important parameter changes before failure occurs.

5.2.4.2.4 Maintenance measures

These measures are:

The detection and correction of failures during routine maintenance visits. Such failures may be easily identifiable (for example by visual inspection) or not (detectable only by testing).

For the maximum repair time, see “Application guidelines”.

5.2.4.3 Special requirements

The special requirements for Functional Reliability can be derived from the following table:

Class of IAS	Probability of a failure	Potential effect		
		Security jeopardising	Security impairing	Security destructive
3	close to none	00	0	0
	extremely low	00	0	0
	very low	0	x	x
	low	x	x	x
2	close to none	00	00	00
	extremely low	00	00	0
	very low	0	x	x
	low	x	x	x
1	close to none	00	00	00
	extremely low	00	00	00
	very low	0	x	x

	low	x	x	x

x Failure shall be prevented at source or the relevant effect avoided for example by incorporating redundancy.

0 Failure shall be prevented at source or the relevant effect avoided for example by incorporating redundancy or shall be detected by automatic monitoring.

00 Failure shall be prevented at source or the relevant effect avoided for example by incorporating redundancy or shall be detected by automatic monitoring or in a maintenance cycle.

5.2.5 List of internal technical failures

Close to none

- Resistor used in accordance with the manufacturers` specification
- Transformer used in accordance with the manufacturers`specification
- Covered (closed) relais with R-load used in accordance with the manufacturers`specifications

Extremely low

- Bulb with 50 % load
- Well done soldering contact

Very low

- Seminconductor used with 50 % overload
- Glowing bulb, often switched on/off
- Relais closed to limits with C-load
- Terminal contacts with different materials

Low

- Loss of mains
- Fault-alarms caused by environmental condition (e. g. temperature change)
- Fault-alarms caused by loose contacts

5.3 Security against natural Environmental influences

5.3.1 General

The purpose of Security against natural environmental influences consists in preventing to the largest possible extent all security jeopardizing, security impairing and security destructive effects caused by natural environmental influences to the IAS.

Special environmental influences like e.g. radio frequency near to a radio transmitter or extrem wet indoor facilities are not covered by these requirements. For these cases special considerations have to be made before the begin of the installation. Also deliberate actions (Tamper) using environmental conditions are not covered by this standard.

Remark: False alarms are security jeopardizing.

5.3.2 Environmental stability structure

5.3.2.1 General

Environmental conditions can have **interferences** to a function of the system, which could lead to **effects** like loss of function and security of the system.

The purpose of Environmental Stability consists in preventing the interference or the relevant effect to the largest possible extent.

5.3.2.2 Types of interferences

For establishing standards for Environmental Stability it has to be distinguished between influences which are common (e.g. change of the ambient temperature) and others which are seldom (e.g. vibrations caused by an earthquake); another parameter is the intensity of an influence.Furtheron influences can be sporadic, continuous or periodic, log-term or short-term.

5.3.2.3 „Environmental classes“

For technical and enonomic reasons it makes no sense to require the same high level of Environmental Stability for all possible installation locations (e.g. well keep office-rooms ./. outdoor, fully exposed to any kind of weather). Herefor the following environmental classes are decribing four environmental scenarrios.

Environmental class I:
Conditions in well kept, temperture-controlled indoor-rooms (ϑ min = 5°C, ϑ max = 40°C, relative humidity ≤ 75 %, on 30 days/year 95 %, on the other days occasionally 85 %).
(Corresp. IEC 721-3-31 [1)] (04/90)):

K: Climatic conditions:	3K3	+5° - +40°
Z: Add. climatic requirements:	3Z1	None
B: Biologic conditions:	3B1	None
C: Chemical active substances:	3C2	SO_2 low level
S: Mechanical active substances:	3S1	Dust low level
M: Mechanical conditions:	3M2	Vibration 5 m/s^2, Shock 40 m/s^2
and		
- Static discharges (ESD)		6 kV Air-discharge/ 8 kV contact discharge
- Fast transients low energie (Burst)		2 kV mains/ 1 kV signal lines
- Slow transients high energie (Surge)		4 kV mains/ 2 kV signal lines
- Radiated high-frequency		0,15 - 1000 MHz, 10 V/m

Environmental class II:
Conditions in indoor-rooms with increased environmental influences (e.g. in staircases, corridors) (like I, but with additional influences - e.g. dewing of windows)
(Corresp. IEC 721-3-3 [1)] (04/90)):

K: Climatic conditions:	3K5	-5° - +45°
Z: Add. climatic requirements:	3Z1	None
B: Biologic conditions:	3B1	None
C: Chemical active substances:	3C2	SO_2 low level
S: Mechanical active substances:	3S2	Dust low level
M: Mechanical conditions:	3M3	Vibration 5 m/s^2, Shock 70 m/s^2
and		
- Static discharges (ESD)		6 kV Air-discharge/ 8 kV contact discharge
- Fast transients low energie (Burst)		2 kV mains/ 1 kV signal lines
- Slow transients high energie (Surge)		4 kV mains/ 2 kV signal lines
- Radiated high-frequency		0,15 - 1000 MHz, 10 V/m

Environmental class III:
Conditions outdoors, but sheltered (ϑ min = -25°C, ϑ max = 60°C, relative humidity $\leq$ 75 %, on 30 days/year 95 %, on the other days occacionnally 85 %)
(Corresp.IEC 721-3-3 [1)] (04/90)):

K: Climatic conditions:	3K6	-25° - +55°
Z: Add. climatic requirements:	3Z4, 3Z8	Wind 5 m/s, spray water
B: Biologic conditions:	3B1	None
C: Chemical active substances:	3C3	SO_2 mean level
S: Mechanical active substances:	3S3	Dust mean level
M: Mechanical conditions:	3M4	Vibration 10 m/s^2, Shock 100 m/s^2
and		
- Static discharges (ESD)		6 kV Air-discharge/ 8 kV contact discharge
- Fast transients low energie (Burst)		2 kV mains/ 1 kV signal lines
- Slow transients high energie (Surge)		4 kV mains/ 2 kV signal lines
- Radiated high-frequency		0,15 - 1000 MHz, 10 V/m

EnvironmentaL class IV:
Conditions outdoors with encreased environmental influences (fully exposed to the weather) (min = -25°C, max = 60°C, relativ humidity $\leq$ 75 %, on 30 days/year 95 %, on the other days occacionnally 85 %)
(Corresp. DIN IEC 721-3-3 [1)] (04/90)):

K: Climatic conditions:	4K2	-33° - +40°
Z: Add. climatic requirements:	4Z1, 4Z3, 4Z7	Wind 20 m/s, rain
B: Biologic conditions:	3B1	Mould, rodents
C: Chemical activ substances:	3C3	SO_2 high level
S: Mechanical activ substances:	4S3	Dust, sand high level
M: Mechanical conditions:	4M4	Vibration 10 m/s^2, Shock 100 m/s^2
and		
- Static discharges (ESD)		6 kV Air-discharge/ 8 kV contact discharge
- Fast transients low energie (Burst)		2 kV mains/ 1 kV signal lines
- Slow transients high energie (Surge)		4 kV mains/ 2 kV signal lines
- Radiated high-frequency		0,15 - 1000 MHz, 10 V/m

[1)] IEC 721 is only used here to describe the environmental conditions.

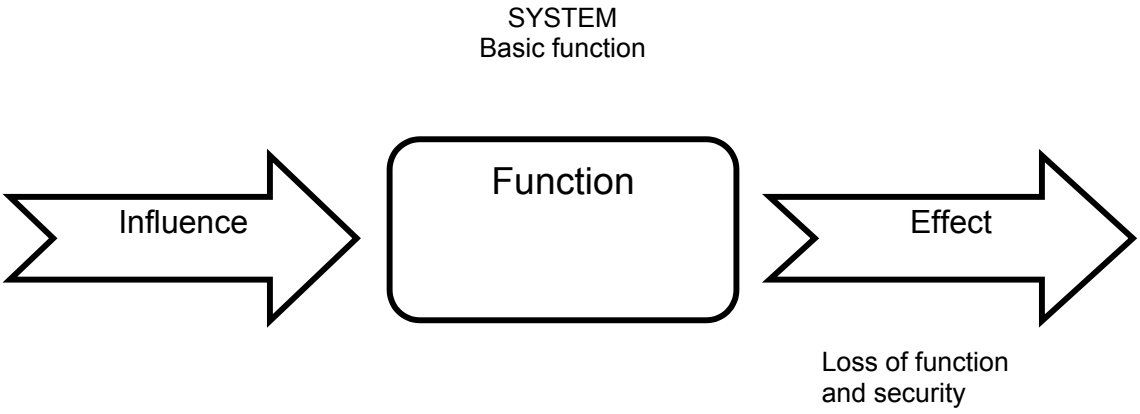
5.3.2.4 Types of effects

The type of effect as a result of Environmental influences is determined by the loss of functions and security of the IAS. A distiction is made between the following three types of effects:

- Security jeopardizing (e.g. reduction of immunity against false alarms)
- Security impairing (e.g. reduction of sensitivity/range of a detector)
- Security destructive (e.g. loss of function of alarm transmission)

5.3.2.5 Structure of the Stability against natural environmental Influences

Founded on the types of interferences, effects and functions the following structure is valid for the Environmental Stability:



5.3.3 Requirements for Environmental stability

Within each environmental class interferences within the ranges described shall not have security, jeopardizing, impairing, security or security destructive effects during or after the exposure.

Environmental Stability shall be the same high level in all classes of IAS.

5.3.4 Determination of Environmental stability

5.3.4.1 Responsibility of the manufacturer

The manufacturer has to claim for one or more of the following environmental classes where the environmental influences shall not have security jeopardizing, impairing, security or security destructive effects:

5.3.4.2 Responsibility of the installer

The installer is responsible for determining the correct environmental class for each system-element according to the prevailing environmental condition.

Remark: An installed IAS may comprize system-elements from more than one environmental class.

5.4 Requirements for Operational Security

5.4.1 General

The purpose of Operational Security consists in preventing to the largest possible extent all security jeopardizing, security impairing and security destructive effects caused by incorrect operation of the IAS. In cases where for technical reasons prevention is not possible or is only possible to a limited degree, incorrect operations should be detected and indicated in due time.

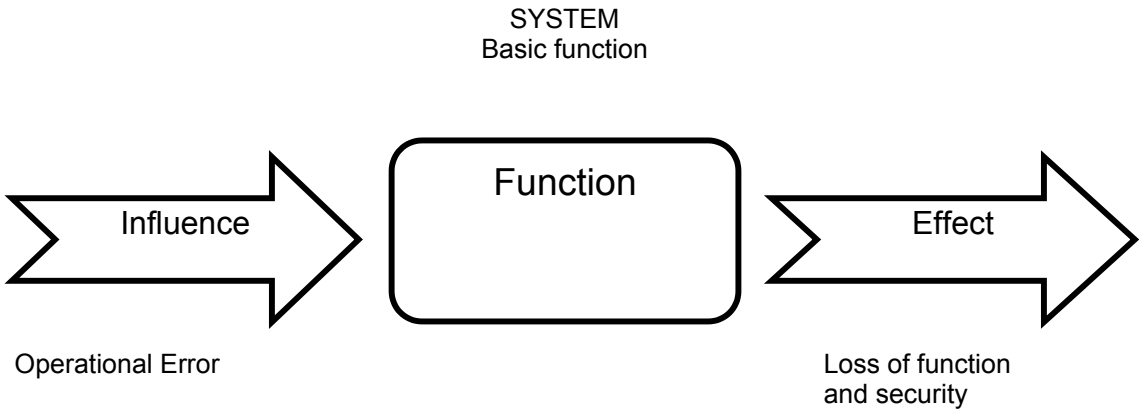
Remark: False alarms are security jeopardizing.

The requirements for the Operational Security of an IAS which are valid for all elements of the installation and at all stages in the production of an installation (planning, designing, installation, commissioning, etc.). The standard does not address failure to initiate an operation.

5.4.2 Operational Security Structure

5.4.2.1 General

For establishing standards of Operational Security the following relationships are relevant:



An operational error can have an influence on a function of the installation, which could lead to effects like loss of function and security of the installation.

The purpose of Operational Security consists in preventing the influence or the relevant effect to the largest possible extent. For technical or economic reasons certain operational errors cannot be prevented and have to be indicated.

Similarly certain other effects caused by operational errors cannot be prevented or indicated and their possibility has to be accepted.

5.4.2.2 Types of operators

For the operation of the IAS, the following operators have to be considered:

- Manufacturer
- Installer
- User
- Others

Each of these categories of operators may be expected to have a different level of specialist knowledge of intruder alarm technology as follows:

Operator	Level of Specialist Knowledge of Intruder Alarm Technology
Manufacturer	Very high
Installer	High
User	Low
Others	Variable (low to very high)

5.4.2.3 Types of operations

Operations may be categorised by their degree of complexity within each of the knowledge levels listed above.

The complexity of an operation is determined by the accuracy of manipulation necessary for its successful completion which is itself determined by the sophistication of the devices provided for the fulfillment of the operation. A distinction is made between the following types of operation:

Simple operation — Operation performed with a single, simple action (e. g. pressing an easily accessible button)..

Difficult operation — Operation performed with simple series of separate simple actions
or
a single simple action requiring the
use of a simple tool (e. g. simultaneous pressing of two buttons
or
removal of screwed cover).

Complex operation — Operation performed with a complicated series of separate single actions
or
a simple series of separate complicated actions (e. g. programming a prom).

5.4.2.4 Types of operational errors

On the basis of the types of operation, a distinction is made between the type of operational errors as follows:

Simple operation error — If the faulty operation is based on a simple operation.

Difficult operation error — If the faulty operation is based on a difficult operation.

Complex operation error — If the faulty operation is based on a complex operation.

5.4.2.5 Types of effects

The type of effect is determined by the loss of function and security of the system. A distinction is made between the following three types:

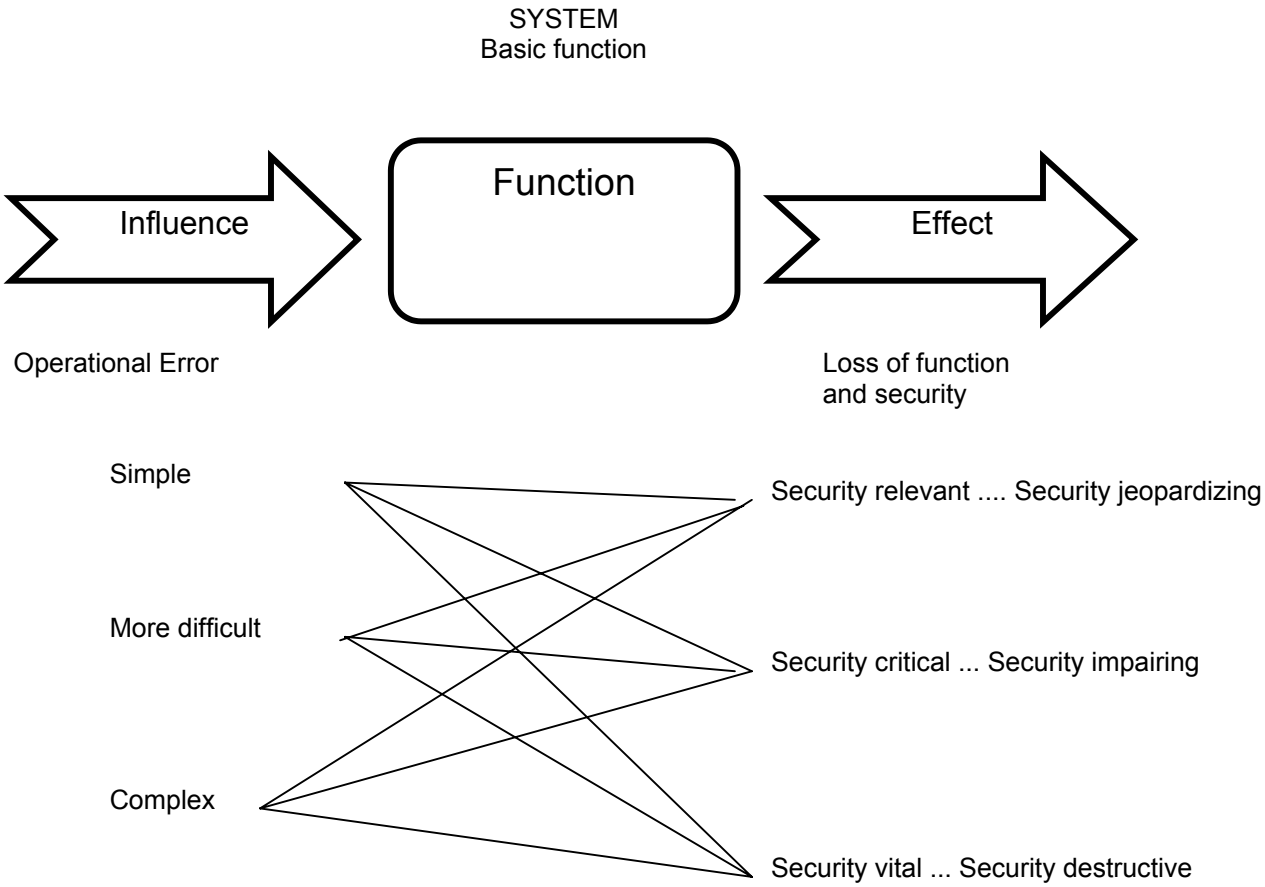
Security jeopardizing — (e. g. Switching-off a unit by mistake without direct reduction of the security task)

Security impairing — (e. g. Isolating part of an installation by mistake)

Security destructive — (e. g. Switching-off remote signalling by mistake with total loss of security task)

5.4.2.6 Structure of Operational Security

Founded on the types of influences, effects and functions the following structure is valid for Operational Security:



5.4.3 Requirements for Operational Security

5.4.3.1 General

Operational Security will be of the same high level in all classes of IAS.

Achievement of the necessary level of Operational Security is gained by compliance with:

- Access Limitation Requirements;
- Basic requirements;
- Protective Measures requirements.

5.4.3.2 Access limitation requirements

It is a pre-requisite for the prevention of operation errors that access to the means to perform an operation is denied to all persons without a valid need or the authority to perform that operation. This is achieved by access limitation.

5.4.3.2.1 Access category classification

The following different access categories are derived from the necessity to perform various types of operation and the competency required and are thus related to the different categories of Operator:

Access category	Operators
M	Manufacturer
I	Installer
U	User

Access categories may be subdivided into hierarchical levels to restrict the performance of certain operations to particular individuals or groups of individuals.

5.4.3.2.2 Access controls

Access controls shall be in place to verify the authorisation of persons within the relevant access category. These controls may be categorised by type as follows:

Type	Preventive measure
A	Prevention of access to an operation without the possibility of by-passing controls by simple error (e. g. by requiring the use of a code, key or special tool).
B	Prevention of access to an operation with the possibility of by-passing controls by simple error, but with indication to the Authoriser

5.4.3.2.3 Access availability

Recognising the varying responsibililties and expertise of different types of Operators, it is necessary to restrict the availability of each access category. This is achieved by:

a) the introduction of access controls as follows:

Acess category	Acess control type
M	A or B
I	A or B
U	A

b) authorization in accordance with the following table:

Acess category	Authoriser
M	User and Installer
I (available with the authorisation of)	User
U	--

5.4.3.2.4 Access limitation

Application of the access controls defined in 5.4.3.2.3 shall ensure that certain commands may result from operations performed only by authorised persons within the following access categories.

Commands	Access Category		
	M	I	U
Set	x	x	x
Unset	x	x	x
Inhibit [1)]	x	x	x
Isolate [1)]	x	x	x
De-isolate [1)]	x	x	x
Amend user-codes/authorities	x	x	x
Permit indication	x	x	x
Interrogate memory	x	x	x
Amend/adjust memory	x	-	-
Override	x	x	-
Test indications	x	x	x
Test notification	x	x	x
Test detectors	x	x	x
Restore from intrusion post-alarm state	x	x	x
Restore from tamper post alarm state	x	x	x
Restore from hold-up post alarm state	x	x	x
Restore from fault post-alarm state	x	x	x
Stop audible indication	x	x	x
Configure/reconfigure remote signal	x	x	-
Adjust detector range	x	x	-
Adjust detector sensitivity	x	x	-
Adjust CIE timing equipment	x	x	-
Configure basic data	x	x	-
Configure site-specific data	x	x	-
Configure user-specific data	x	x	x
Configure installer-specific data	x	x	-
Configure manufacturer-specific data	x	-	-

x Operation is permitted within the Access Category
- Operation is not permitted within the Access Category

Note 1: This list is subject to amendment from time to time as new commands are introduced.

Note 2: Variations are permitted within different countries and according to different circumstances within a country (according to application – e. g. untrustworthy customer).

5.4.4 Basic requirements

The basic requirements of Operational Security are as follows:

Use of the IAS shall be simple and uncomplicated.

- User operations shall be straightforward and demand no special technical knowledge or ability.
- Indications shall be clear, effective and unequivocal.
- Written instructions which are adequate in scope, clear and easy to comprehend, shall be provided:
  - by Manufacturer to Installer
  - by Installer to User
- Appropriate and adequate training shall be given to all authorised Operators

5.4.5 Protective measures requirements

Within each access category, at least one of the following additional protective measures is needed to ensure, to the greatest possible extent, that incorrect operations will not occur, or that if they do occur, the consequences will not be seucrity jeopardizing, security impairing or security destructive, or alternatively that the error is indicated to the Operator:

5.4.5.1 Error tolerances

So that certain incorrect operations will not have a security jeopardizing, security impairing or security destructive effect (e. g. nonsens instructions ignored, deviation from exit route during setting procedure to result in local indication only – not false alarm).

5.4.5.2 Multi operation

So that certain operations can only be performed if preceded by other specified operations (e. g. final setting of system preceded by correct completion of setting initiation procedure), or if instruction verification is given (e. g. system requires confirmation instruction from operator).

5.4.5.3 Operator specific access limitation

So that not withstanding Access Category Classification (clause 5.4.3.2.1) certain operations can only be performed by authorised individuals within a particular access level (e. g. zone inhibit function available to User-Manager, not Security Guard).

5.4.5.4 Monitoring and Indication

So that, in circumstances where, for technical, economical or operational reasons, an operator error cannot be prevented, it may be reported to the operator by means of monitoring and indication.

5.4.5.5 Detailed requirements

The detailed requirements for Operational Security can be derived from the following table:

Access Category	**Degree of Complexity of operational error**	**Requirements for operational Security –Effects**	
		Security jeopardising	Security impairing/ destructive
M	C Complex	-	-
	B More difficult	-	x or 0
	A Simple	x	x
I	C Complex	-	x or 0
	B More difficult	x or 0	x
	A Simple	x	x
U	C Complex	x or 0	x or 0
	B More difficult	x	x
	A Simple	x	x

x Incorrect operations must not result in a security jeopardizing or security impairing/destructive effect or shall be prevented by means of protective measures described in clause 5.4.4.1, 5.4.4.2 or 5.4.4.3.

0 Incorrect operations must not result in a security jeopardizing or security impairing/destructive effect or else should not be possible without any indication.

-: Wrong operations might be neither prevented nor reported.

Examples: Error resulting in unintended "set"-command = Security Jeopardizing
Error resulting in unintended "unset"-comand = Security Destructive

5.4.6 Determination of Operational security

It is hardly possible to provide for a target-oriented definition of the currently feasible and forthcoming types of Operations (and thus Operational errors) in relation to all sorts of known and forthcoming system technologies and worded in a way to make sure that this definition is understood and interpreted by manufacturers, installers and test houses in the same way.

Hence Operations should be assigned to the individual degrees of complexity (simple, more difficult, complex) in a catalogue (clause 5.4.7) which should be updated at regular intervals.

For this reason a valuation model should be developed for the classification which would reduce the range of interpretations to an acceptable level (under consideration).

5.4.7 Catalogue of Operations

The following catalogue shows some examples of operations functions and the classification of the degree of complexity:

Nature of Operation	**Degree of Complexity of Operation**		
	Simple	**Difficult**	**Complex**
Pressing button (easily accessible)	x		
Pressing button (not easily accessible)		x	
Follow complicated entry route		x	
Programming a prom			x
Setting of adjustment sensitivity screw (easily accessible)	x		
Setting of adjustment sensitivity screw (not easily accessible)		x	
Simultanously pressing of two buttons		x	
Removal of clipped cover	x		
Removal of sealed/screwed cover		x	

5.5 Requirements for Tamper Security

5.5.1 General

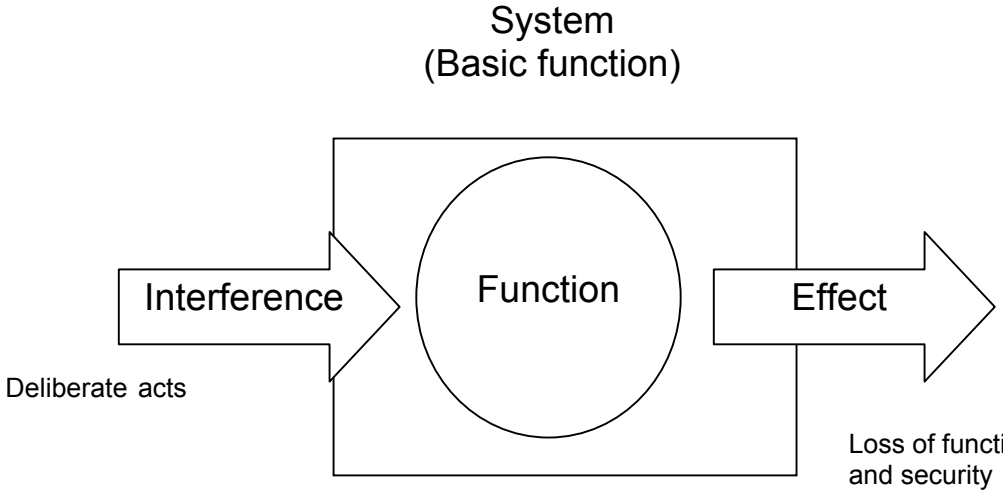
The purpose of Tamper Security consists in preventing to the largest possible extent all deliberate acts of interference (sabotage), which are designed to prevent an IAS from fulfilling its security function. In cases where for technical/economic reasons prevention is only possible to a limited degree, interference shall be detected and indicated in due time.

This clause contains requirements for the Tamper Security of IAS which are valid for all system elements (components).

5.5.2 Tamper Security structure

5.5.2.1 General

For establishing standards for Tamper security the follwing relationships are relevant:



Deliberate acts (Tamper) can have interferences to a function of the system, which could lead to effects like loss of function and security of the system.

The purpose of Tamper Security consists in either preventing the interference or the relevant effect to the largest possible extent or to indicate it when preventing for economic reasons is only possible to a limited degree.

5.5.2.2 Types of interference

5.5.2.2.1 General

The type of Tamper is essentially determined by the degree of difficulty (severity) to be overcome for a particular interference.

Success is overcoming the degree of difficulty depends on the qualification/capability of the individual carrying out the Tamper (intruder), the so-called threat pattern.

5.5.2.2.2 Threat pattern

The threat pattern is essentially determined by the level of capability of the intruder. This capability is determined by:

Basic knowledge Basic knowledge of the technology of the system (e. g. electronic, pneumatic systems) on the part of the intruder.

Special knowledge Special knowledge of the system technology (e. g. conventional line technology, BUS-technology) i. e. detailed knowledge of equipment, functions, methods and processes of the system etc. on the part of the intruder.

Technical means Type and scope of the technical tools and devices needed by the intruder to carry out Tamper.

5.5.2.2.3 Degree of difficulties

The degree of difficulty determines which conditions shalöl be met by the intruder to carry out Tamper of a corresponding degree (degree of difficulty).

A distinction is made between the following degrees of difficulties:

Degree of difficulty		Basic Knowledge	Special Knowledge	Technical means
D	Difficult	Good	Minimal	Minimal
C	Complicated	Minimal	Insignificant	Minimal
B	Easy	Insignificant	Insignificant	Minimal
A	Very easy	Insignificant	Insignificant	Insignificant

5.5.2.2.4 Types of effects

The type of effects is determined by the loss of function and security of the system. A distinction is made between the following three types:

Security jeopardizing (e. g. destruction of a unit without direct reduction of the security task)

Security impairing (e. g. neutralisation of a zone with partly reduction of the security task)

Security destructive (e. g. prevention of remote signalling with total loss of security task)

5.5.2.2.5 Types of functions

Depending on the location and importance of a function within an IAS a distinction is made between

- freely accessible functions
  and
- conditionally accessible functions

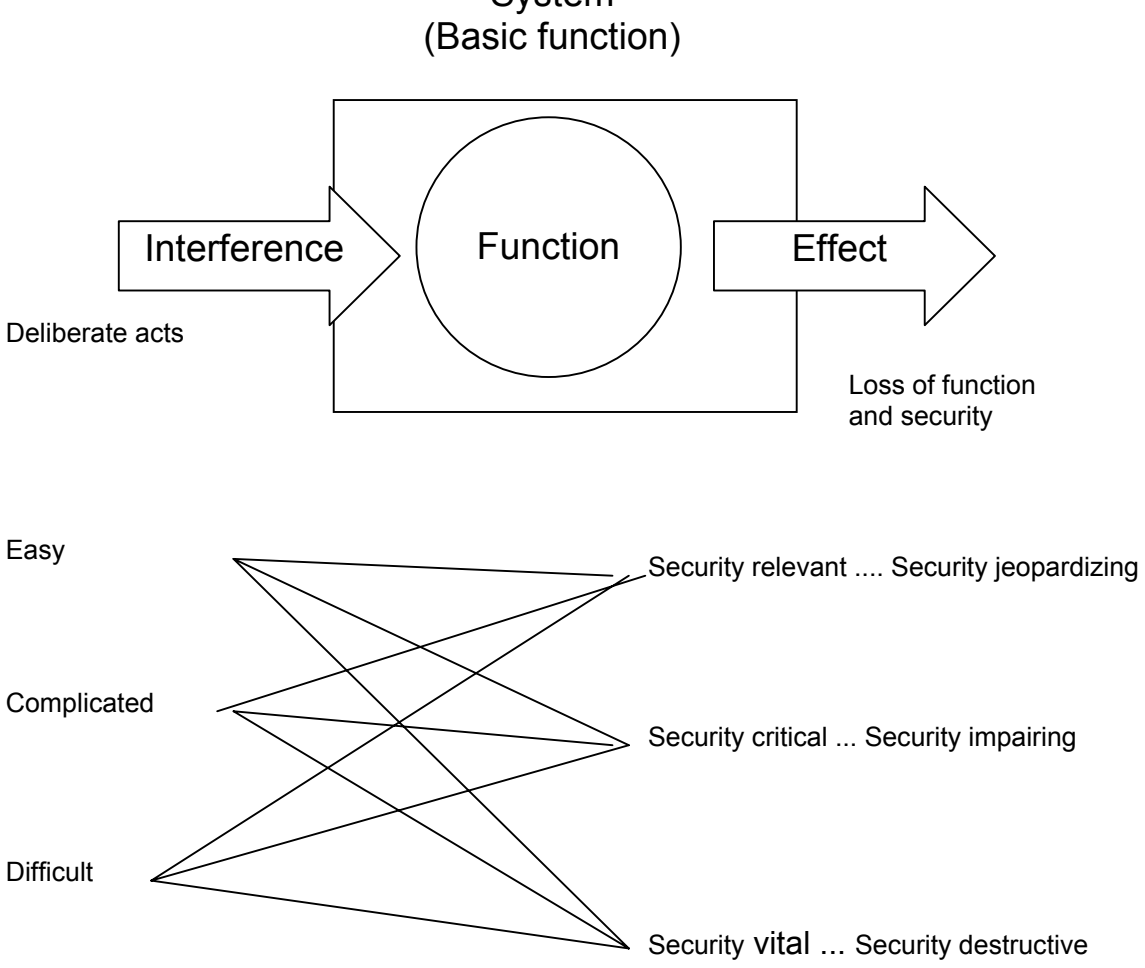
on the one hand, and

- security relevant functions
  and
- security critical/vital functions

on the other hand.

5.5.2.3 Structure of the Tamper Security

Founded on the types of interferences, effects and functions the following structure is valid for the Tamper Security:



5.5.3 Requirements for Tamper Security

5.5.3.1 General

Tamper Security can be achieved by

- a suitable and correct placement of the system components incorporating the functions to be protected (installation)

  and

- Tamper protection and/or Tamper monitoring of system components incorporating functions to be protected (design/manufacturing of equipments, systems).

5.5.3.2 Basic requirements

Components incorporating security critical or security vital functions shall be designed as conditionally accessible functions to the largest possible extent.

With regard to system classes 2 and 3, components incorporating security vital functions (e. g. Intruder Alarm Control and Indicating Equipment, Alarm Transmission Device) shall be installed within a monitored area or must be installed in such a way that access cannot be gained to the components without the person in charge noticing the access.

5.5.3.3 Special requirements

The special requirements for Tamper Security can be derived from the following table:

Class of IAS	Degree of difficulty of Tamper		Requirements for Tamper Security Type of function			
			Freely accessible		Conditionally accessible	
			Security jeopardising	Security impairing/ destructive	Security jeopardising	Security impairing/ destructive
3	D	Difficult	M	x or 0	M	M
	C	Complicated	x or 0	x or 0	M	x or 0
	B	Easy	x or 0	x or 0	x or 0	x or 0
	A	Very easy	x	x	x	x
2	D	Difficult	M	M	M	M
	C	Complicated	M	x or 0	M	M
	B	Easy	x or 0	x or 0	M	x or 0
	A	Very easy	x	x	x	x
1	D	Difficult	M	M	M	M
	C	Complicated	M	M	M	M
	B	Easy	M	x or 0	M	M
	A	Very easy	x	x	x	x

x Tamper must not result in a security jeopardizing or security impairing/destructive effect or shall be prevented by means of Tamper protection.

0 Tamper must not result in a security jeopardizing or security impairing/destructive effect or it should not be possible without any indication.

M Tamper is neither prevented by physical means nor detected. Within the scope of maintenance it has to be ensured that these influences will be detected.

5.5.4 Determination of Tamper Security

5.5.4.1 General

Laying-down the necessary protection measures against Tamper influences is primarily dependent upon the degree of difficulty, to which a specific influence can be assigned. It is hardly possible to make these decisions only on the basis of target-oriented descriptions which are applicable to all sorts of known and forthcoming system technologies in such a way that it will be understood and interpreted by manufacturers, installers and test-houses in the same way.

For this reason a valuation-model is used for the classification which will reduce the range of interpretations to an acceptable value.

In specific critical and frequent cases it is essential, in the course of a periodic exchange of experiences, to make a concrete assignment for special Tamper influences, which will be listed in a confidential list (see Annex B – List of Tamper attempts).

On the basic of the valuation-model every specific influence can be calculated from the sum of different “protection-factors”. With this overall protection-factor the specific influence can be assigned to the degree of difficulty A, B , C or D.

5.5.4.2 Valuation model

5.5.4.2.1 Valuation criterion

Besides the basic criteria listed in clause 5.5.2.2.3

- Basic knowledge
- Specific knowledge
- Technical means

the change of success for a specific Tamper- nfluence is also determined by

- the necessary manual force

and

- the visibility of an attempt.

5.5.4.2.2 Graduation of the valuation criteria

The specific valuation-criteria can result in different degrees of severity. Experience shows that the change of success will decrease over-proportional to the degree of difficulty.

For this reason the square-value of the linear classification is selected as a valuation base.

Criteria	Degree	"Class"	Degree-value"	Explanations
Basic knowledge	Insignificant	1	1	No basic knowledge of the used technology necessary
	Minimal	2	4	Normal knowledge of a handicraft of the used technology, e. g. electrician for electric operated systems
	Good	3	9	Knowledge of an engineer in the specific technology
Special knowledge	Insignificant	1	1	No special knowledge of the used system technology necessary
	Minimal	2	4	Basic knowledge of IAS-technology necessary which can be used independent of the used system-technology for all IAS
	Good	3	9	Selective knowledge necessary which can be used very specifically in the relevant installation or system technology
Technical means	Insignificant	1	1	No technical means necessary
	Minimal	2	4	Normal tools for the handicraft of the used technology necessary
	Good	3	9	Special tools for the used system technology necessary
Manual force	Insignificant	1	1	The influence is possible without any manual force
	Significant	2	4	The influence is only possible with manual force
Visibility	None	1	1	The influence cannot be visibly noticed.
	Visible	2	4	The influence can be noticed visibly with special attention
	Easily visible	3	9	The influence can easily be noticed without any special attention

5.5.4.2.3 Weighting of the valuation criteria

Not all of the mentioned valuation-criteria have the same preventive effect against the chance of a success of a Tamper influence. The specific criteria are weighted as follows:

Criteria	Weighting
Basic knowledge	2
Special knowledge	3
Technical means	1
Manual force	1
Visibility	2

5.5.4.2.4 Protection-factor of the valuation criteria

On the base of degree-value and weighting the following protection-factor is calculated for the different criteria:

Criteria		Degree-value	Weighting	Protection-factor
Basic knowledge	Insignificant	1	2	2
	Minimal	4	2	8
	Good	9	2	18
Special knowledge	Insignificant	1	3	3
	Minimal	4	3	12
	Good	9	3	27
Technical means	Insignificant	1	1	1
	Minimal	4	1	4
	Good	9	1	9
Manual force	Insignificant	1	1	1
	Significant	4	1	4
Visibility	None	1	2	2
	Visible	4	2	8
	Easy visible	9	2	18

5.5.4.3 Valuation

The assignment of a Tamper influence to the degree of difficulty A, B, C or D is done with the sum of the different protection-factors (“overall-protection-factor”) which can be reached under consideration of the different valuation criteria. For the assignment the following limits are valid:

“Overall-Protection-factor”	Degree of difficulty	
< 20	A	very easy
≥ 20	B	Easy
≥ 30	C	Complicated
≥ 40	D	Difficult
≥ 50	E	It is not necessary to consider these influences

5.5.4.4 Valuation-examples

Annex A shows some examples of possible classification of Tamper influences.

5.5.4.5 List of tamper-attempts

Annex B shows examples, how the list about the concrete classification of the frequent and critical Tamper influences, to be elaborated by the test-houses, might be set up.

This list has to be updated according to the technical development in the field of applied technologies and threat patterns.

This catalogue is not included in the Standard; it is only handed out to those parties guaranteeing a confidential treatment of this document.

ANNEX A - Confidential

Valuation examples

- *Example –*

Valuation-table for Tamper-influences												
Valuation criteria	Degree	Protect. factor	Blowing foam into aud. WD		Turning detector (not blocked)		Turning detector (mech. blocked)		Pulling connector of dialler		Masking detector	
Basic knowledge	Insign.	2			y	2	x	2	x	2	x	2
	Minimal	4	X	8								
	Good	18										
Special knowledge	Insign.	3	X	3								
	Minimal	12			x	12	x	12	x	12	x	12
	Good	27										
Technical means	Insign.	1			x	1	x	1	x	1		
	Minimal	4	X	4							x	4
	Good	9										
Manual force	Insign.	1	X	1	x	1			x	1	x	1
	Signific.	4					x	4				
Visibility	None	2	X	2	x	2			x	2		18
	visible	8					x	8				
	Easily visible											
		18									x	
Overall-protection factor			18		18		27		18		37	
Degree of Difficulty			A		A		B		A		C	

Valuation-table for Tamper influences												
Valuation criteria	Degree	Protect. factor	Blocking a function with radio frequence		Pulling out a complete cable		Substitution of end-of-line-resistor		Nose-pulling of cylinder in anc. unset-equipment			
Basic knowledge	Insign.	2			x	2						
	Minimal	4					x	8	x	8		
	Good	18	X	18								
Special knowledge	Insign.	3			x	3						
	Minimal	12	X	12					x	12		
	Good	27					x	27				
Technical means	Insign.	1			x	1						
	Minimal	4					x	4	x	4		
	Good	9	X	9								
Manual force	Insign.	1	X	1			x	1				
	Signific.	4			x	4			x	4		
Visibility	None	2	X	2			x	2				
	visible	8			x	8						
	Easily visible	18							x	18		
Overall-protection factor			42		18		42		46			
Degree of Difficulty			D		A		D		D			

< 20 A Very easy
≥ 20 B Easy
≥ 30 C Complicated
≥ 40 D Difficult
≥ 50 No consideration

ANNEX B – Confidential

List of Tamper-attempts

- Example -

Description of the Tamper methods	**Degree of difficulty**			
	A Very easy	B Easy	C Complicated	D Difficult
Cutting of entire cables and cable strands without/with ancillary devices	x	x		
Shorting of entire cables and cable strands without/with ancillary devices	x	x		
Targeted cutting of individual wires			x	
Targeted shorting between 2 wires			x	
Removal of system elements without destruction, without ancillary devices and without special knowledge	x			
Putting spray on the window of movement detection			x	
Putting foam into acoustic warning devices		x		
Blocking of functions by radiating radio frequency fields				x
Destruction of system elements with high voltage				x
Blocking of functions with a common magnet			x	