STANDARD OF CHINA ATOMIC ENERGY

System number: CAEA-GB0012
Originated from: EJ/T 20180.1-2018

Technical requirements of intrusion detection alarm system for physical protection of nuclear material and nuclear facilities - Part 1：General

CHINA ATOMIC ENERGY AUTHORITY

EJ

Nuclear Industry Standard of the People's Republic of China

Translation of EJ/T 20180.1—2018

Technical requirements of intrusion detection alarm system for physical protection of nuclear material and nuclear facilities - Part 1：General

Issue date: 2018—01—18
Implementation date:2018—05—01 Translation issue date:XX—XX—XX

ENGLISH VERSION OF THIS STANDARD IS ISSUED BY
CHINA ATOMIC ENERGY AUTHORITY

Foreword

EJ/T 20180 Technical requirements of intrusion detection alarm system for physical protection of nuclear material and nuclear facilities is composed of the following two parts:

——Part 1:General

——Part 2:Bistatic microwave intrusion detector

This part is Part 1 of EJ/T 20180 Technical requirements of intrusion alarm system for physical protection of nuclear material and nuclear facilities.

Annex A and Annex B of this part are informative.

In case of any doubt about the contents of English translation, the Chinese original shall be considered authoritative.

Technical requirements of intrusion detection alarm system for physical protection of nuclear material and nuclear facilities - Part 1: General

1 Scope

This part specifies the technical requirements for the intrusion detection alarm system for physical protection of nuclear material and nuclear facilities in fixed locations (hereinafter referred to as "intrusion detection alarm system").

This part is applicable to the design and acceptance of intrusion detection alarm systems in the new-build, expansion and renovation projects for the physical protection of nuclear material and nuclear facilities in fixed locations.

2 Normative references

The following normative documents contain provisions which through reference in this text, constitute provisions of this standard. For dated references, subsequent amendments (excluding corrections), or revisions, of any of these publications do not apply to this standard. However parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

GB/T 15211 Security alarm requirements- Environmental adaptabilityrequirements and test methods

GB/T 15408 Technical requirement of power-supply for security & protection system

GB 16796 Safety requirements and test methods for security alarm equipment

GB/T 30148-2013 Security alarm equipment - EMC immunity requirements and test methods

GB 50348-2004 Technical code for engineering of security and protection system

EJ/T 1054 Physical protection of nuclear material and nuclear facilities

IEC 60839-5 Alarm systems - Part 5: Requirements for alarm transmission systems

IEC 60839-7 Alarm systems - Part 7: Message formats and protocols for serial data interfaces in alarm transmission systems

3 Terms and definitions

For the purpose of this part, the followingterms and definitions apply.

3.1

detection

the entire process of detection, alarm and check to alarm against potentially malicious acts or other unauthorized acts

3.2

detection zone

the space or surface area under the surveillance of one or more intrusion detection devices, in which the intrusion detection device will generate an alarm when such space or area reaches alarm conditions

3.3

probability of detection（PD）

the probability that the detection unit detects intrusion activities within the sensor coverage area

3.4

intrusion detection alarm system

a security system consisting of sensors, signal media, alarms, power supplies, check to alarm systems, and alarm reporting units, including alarm communications and information display devices

3.5

alarm

a warning issued by a sensor or sensor system after it is triggered or activated, usually by an audible and/or optical signal, which may be a real alarm, a false alarm or a nuisance alarm

3.6

false alarm

an alarm generated due to failure of the equipment itself

3.7

false alarm rate

the number of false alarms in a unit time interval

3.8

nuisance alarm

the activation of any alarm not caused by a human intrusion but a trigger signal that triggers the detector

3.9

nuisance alarm rate

the number of nuisance alarms in a unit time interval

3.10

tamper device

a device used to detect any intentional interference (disassembling or unpacking of) with the component or a part of the alarm system

3.11

tamper protection

an electrical or mechanical method to prevent the alarm system or parts from any intentional interference

3.12

tamper alarm

an alarm generated by actions of a tamper device

3.13

leakage alarm

a case where the intrusion has occurred without an alarm response or indication from the system

3.14

system response time

the period required from the time when the detector (including the emergency alarm device) detects the target and generates the alarm message to the time when the controller receives the message and sends the alarm signal

4 General

4.1 The scheme, structure and function of the intrusion detection alarm system shall be determined according to the level of physical protection and the design basis threat, and shall meet the defense-in-depth and balanced protection requirements of physical protection.

4.2 The intrusion detection alarm system shall feature in safety, reliability, extensibility and flexibility, so as to be economical, technologically advanced and reliable in practical use.

4.3 The intrusion detection alarm system shall take combined use of advanced and mature technologies such as electronic sensing (detection), wired communication, display and recording, computer network and system integration.

4.4 The equipment/devices used in the intrusion detection alarm system shall comply with the requirements of national laws and regulations and relevant standards.

5 System design requirements

5.1 Basic design principles

5.1.1 For different levels of physical protection, the corresponding detection means shall be taken.

5.1.2 The defense capability of intrusion detection alarm system shall vary as to different design basis threats.

5.1.3 System design for different equipment shall be subject to the following site conditions:

a) State of the perimeter barrier and isolation zone;
b) Type and state of the ground soil and hardening;
c) The number and length of detecting sections that are suitable for the perimeter;
d) Neighboring roads, rivers, railways and their traffic conditions;
e) Drains, pipelines, embedded lines and utilities that pass through the perimeter;
f) Local weather conditions such as rain, snow, fog, sand, lightning and freezing;
g) Severe weather conditions such as extreme cold and extreme hot;
h) Electromagnetic interferences in the neighboring area.

5.2 **Normativity and practicability**

The design of the intrusion detection alarm system shall be based on actual surveys of the site, and shall be designed according to factors including the physical protection level, design basis threats, environmental conditions, protection objects, investment scale, maintenance and alarm receiving and processing. The system design shall comply with the requirements for the validity evaluation of the physical protection system. Equipment selection and layout and cabling shall comply with the relevant national and industrial regulations and standards.

5.3 **Advancement and interchangeability**

The design of the intrusion detection alarm system shall adopt advanced equipment and mature technology proven and validated by multiple tests. It shall have certain interchangeability, allowing for capacity expansion and/or modification of the system.

5.4 **Accuracy**

The intrusion detection alarm system shall be able to accurately and timely detect the intrusion behavior and send an alarm signal, and clearly indicate the source of the intrusion alarm signal, the tamper alarm signal, and the fault signal. Leakage alarms are not allowed for the intrusion detection alarm system. Necessary measures shall be taken to reduce the nuisance alarm rate in the fortified area to increase the accuracy of the system, with the sensitivity and detector bypass being weighed as well.

5.5 **Integrity**

The intrusion detection alarm system shall take preventive measures against all intrusion paths leading to the fortified area, and shall supplement or reinforce the preventive measures on the vulnerabilities that may exist on the intrusion paths. The intrusion detection system shall cover the entire fortified area, and ensure no blind areas therein.

5.6 **Defense-in-depth**

The design of the intrusion detection alarm system shall adopt defense-in-depth, which partitions the entire fortified area by region and level according to the physical protection level of the protected object and the physical protection partition status. The system shall provide differential protective measures to the operational control area (when the area is set with detectors under special circumstances), the protected area, the vital area and other important locations.

5.7 **Balanced protection**

The intrusion detection alarm system shall achieve balanced protection. Detectors with different detection mechanisms and complementary performances shall be properly selected, combined and installed to ensure effective and balanced detection capability of each detecting section of the entire perimeter or fortified area. The detection and protection level of each section within the same fortified area shall be consistent, without vulnerabilities or hazards. No less than two detection devices with different detection mechanisms and complementary functions shall be set at the perimeter of the protected area. At least one detection device shall be set at the perimeter of the vital area. A linear, planar or spatial detector shall be set at the perimeter of the protected area to provide multiple protection measures. A point /linear /planar /spatial detector shall be set at the perimeter of the vital area. Planar/spatial controlled detectors may be employed at the access points, and shall be compatible with the perimeter and indoor protection measures. Detectors and other protective devices shall be provided for passages, pipes, vents and skylights, so that balanced protection can be achieved for the vital area.

5.8 Linkage compatibility

The intrusion detection alarm system shall be able to act in conjunction with systems such as video surveillance system and access control system. The intrusion detection alarm system and other systems shall be designed in an integrated manner. It shall provide corresponding interfaces to facilitate the construction of the physical protection integrated management system and accept the management of the integrated management system. Each system shall be compatible with each other and be able to work independently. The intrusion detection alarm system shall be capable of operating independently to accomplish all management functions of the system in the event of an integrated management system failure or outage.

6 System functional requirements

6.1 System overview

The intrusion detection alarm system is composed of four parts: front-end detection device, transmission device, processing /control /management device and display/recording device.

6.2 System classification

According to different signal transmission modes, the intrusion detection alarm system should be assembled in the following three modes:

a) Multi-line mode: the detector and emergency alarm device are connected to the alarm control host through a multi-core cable in a one-to-one dedicated manner, which is applicable to systems of small-scale and small-coverage. The architecture diagram of the multi-line mode system is shown in Figure A.1.
b) Bus mode: The detector and emergency alarm device are connected to the alarm control host through the alarm bus via its corresponding address codec, which is applicable to large-scale systems and can realize diversified functions. The architecture diagram of the bus mode system is shown in Figure A.2.
c) Dedicated network: it is applicable to premises where a fair number of fortified areas are set up and the site is far away from the central alarm station. In this mode, the detector, emergency alarm device and alarm control host are connected via corresponding transmission devices and dedicated ethernet. The architecture diagram of the dedicated mode system is shown in Figure A.3.

6.3 Functional requirements

6.3.1 General requirements

The intrusion detection alarm system shall generally meet the following requirements:

a) The intrusion detection alarm system is such a system that ensures timely, accurate and reliable detection, alarm, indication and record of abnormal conditions (such as illegal intrusion into the fortified area) through various types of alarm detectors and system alarm control equipment;
b) The system shall perform functions such as detection, transmission, indication, record and query.

6.3.2 Detection

6.3.2.1 Detection scope

The intrusion detection alarm system shall accurately and promptly detect the following possible intrusion behaviors and trigger alarms:

a) Unauthorized access tothe perimeter barrier and isolation zone of the operational control area (detection is set for the controlled access area under special circumstances), the protected area and the vital area, and unauthorized access to the nuclear material warehouse orpassing throughthe physical building barriers used for the production, use and storage of nuclear materials;
b) Unauthorized movement in the detection zone;
c) Unauthorized opening of movable building facilities (such as doors and windows) and movable components of mechanical equipment (such as air conditioner shutters serving as passages) of the fortified area;
d) Breaking the doors, windows, ceilings, walls and other building structures of the fortified area with violent means;
e) Breaking the glass of the fortified area;
f) Unauthorized approach to or access to nuclear materials/important nuclear facilities, items and equipment.

6.3.2.2 Detection indicator requirements

The detection indicators of the intrusion detection alarm system shall comply with the following provisions:

a) It can detect the intruders who weigh 35kg or more and pass through the limited access area, the accesses, and perimeters by means of walking, running, climbing, jumping and rolling (the speed at which the intruders may be detected shall meet the requirements of relevant national standards and codes for different detectors);
b) The number of nuisance alarms for each detection zone/section shall be no more thanonce per day;
c) The probability of detection for intrusion of each detection zone/section shall not be lower than 90% at the 95% confidence level;
d) The false alarm rate of the intrusion detection system shall be no more than once under the condition that each sensor runs seven days.

6.3.2.3 **Detector configuration requirements**

The configuration of the front-enddetector for the intrusion detection alarm system shall comply with the following requirements:

a) These factors should be taken into account for setting up the detector:
   1) The range of the perimeter;
   2) The detection range of the detector;
   3) The position, direction and effective surveillance range of the camera used for alarm check in the video surveillance system;
   4) Convenient maintenance and test of the detector;
   5) The length of each independent fortified area of the perimeter should be usually no more than 100m.
b) In order to facilitatethe alarm check and reduce the nuisance alarm of certain detectors, the view within the detection zone and alarm check zone shall be clear, free of trees, shrubs, tall grasses and other obstacles, and the power box and control cabinet shall be reasonably arranged;
c) The intrusion detectors shall be arranged to ensure that there is no blind area in the fortified area;
d) When the detection range of multiple detectors is overlapped, mutual interference shall be avoided.

6.3.3 **Response**

The response time of the intrusion detection alarm system shall be no more than 2s when the alarm is triggered.

6.3.4 **Alarm and status display**

The following status shall be displayed in the intrusion detection alarm system:

a) Normal status;
b) Test status;
c) Alarm status triggered by intrusion behaviors;
d) Tamper alarm status;
e) Failure status;
f) Failure of the primarypower supply and under-voltage of the backuppower supply;
g) Status of setting alerts (fortification)/ unsetting alerts (disarming);
h) Indication of failure to transmit information;
i) Display of the corresponding failed fortified areain case of equipment failure.

6.3.5 **Control**

6.3.5.1 The intrusion detection alarm system shall perform the following control functions:

a) Detection function: the fortification and disarming of all detection zones;
b) Alarm and display function:
   1) The alarm information shall stay until it is manually reset and the alarm signal shall not be lost;
   2) The alarm information shall be prioritized;
c) Transmission function: transmit or cancel information;
d) Functions of system management software:
   1) Record system information in real time such as startup & shutdown, operation, alarm and failure, and shall provide query, print and tamper-resistance functions;
   2) Set the operation authorization, and manage the login and handover of the operator (administrator);
   3) Be fault-tolerant and have backup and maintenance capabilities.

6.3.5.2 The requirements for the control functions of the intrusion detection alarm system are as follows:

a) It shall be able to performprogrammable and networking functions;
b) It shall be equipped with input and output interfaces linked or integrated with other systems;
c) The control system shall allow for capacity increase;
d) Each control shall be timely, accurate and reliable.

6.3.6 **Record and query**

The intrusion detection alarm system shall be able to record the following events and allow for post-event query:

a) Events listed in 6.3.4 and program settings listed in 6.3.5.1;
b) The recording devices shall have unmodifiable system characteristic information, such as necessary tracing files, to ensure the integrity and traceability of the information documented by the system;
c) Personal information (name and position, etc.) andoperation records of system operators;
d) Treatment of the alarm.

6.3.7 **Transmission**

6.3.7.1 **Transmission mode**

The transmission mode of the system shall be determined in accordance with the layout of the front-end devices, transmission distance, environmental condition, system performance requirements and information capacity, and the wire transmission mode shall be adopted.

6.3.7.2 **Transmission functions**

The transmission functions of the intrusion detection alarm system are as follows:

a) The wire transmissionline shall be able to monitorthe line status, and the matched resistance or monitoring devices used for line monitoring shall be installed inside the front-end detection device;
b) The alarm transmission system shall be able to perform self-checking and patrol functions.

6.3.7.3 **Transmission performance requirements**

The requirements for the transmission performance of the intrusion detection alarm system are as follows:

a) The number of the alarm collection devices installed on a single bus shall comply with relevant requirements ofthe system alarm response time when the bus transmission modeis adopted;
b) It shall be ensured that the signal transmitted by the transmission system is not distorted or lost;
c) The attenuation of the signal shall not exceed the specified requirements, and attenuation compensation measures should be taken when necessary;
d) The intrusion detection alarm system shall have a wire communication interface with the central alarm station and be able to monitor the failure observed in communication lines;
e) The technical requirements for the alarm signal transmission system shall be in accordance with IEC 60839-5;
f) Message formats and protocols for serial data interfaces in alarm transmission systems shall be in accordance with IEC 60839-7.

6.3.7.4 **Transmission mode**

The transmission modes for the intrusion detection alarm system are as follows:

a) The multi-line mode should be used for premises in which the distance between the alarm control device and each detector is no more than 100m. Each detection circuit of the alarm control device is directly connected to a detector in the front-end detection zones via cables;
b) The bus mode should be used for premises in which the maximum distance between the alarm control device and any detector is no more than 1200m. Detectors in each front-end detection zone are connected to the alarm control device through corresponding transmission devices via a bus;
c) The dedicated network should be usedfor premises performing functions such as fortification, disarming and others required by the site, or for premises in which the distance between the site and the central alarm station is more than 1200m. Cables or fiber optical cables are used for transmission.

6.4 **Power supplies**

6.4.1 **Scope of power supply**

The scope of power supply for the intrusion detection alarm system mainly includesallequipment/devices in the system such as the front-end detection device, transmission device, processing/control/management device, and indicating/recording device.

6.4.2 **General requirements for power supply**

Power supply for the intrusion detection alarm system shall meet the requirements of EJ/T 1054.

6.4.3 **Requirements for the primary power supply**

The primary power shall be supplied by the grid and shall be set at 1.5 times the full-load power consumption of the combined load. The quality of the primary power supply shall meet the relevant requirements of GB/T 15408.

6.4.4 **Backup power supply**

6.4.4.1 For the Category I or II physical protection system, the backup power supply for the intrusion detection alarm system shall be a combination of the uninterrupted power supply (UPS) and the diesel generator unit. The system shall be powered by UPS before the generator unit is put into normal operation. For the Category III physical protection system, the backup power supply for the intrusion detection alarm system can be either the UPS or the diesel generator unit.

6.4.4.2 UPS shall be fully charged under normal circumstances and automatically charged when the voltage drops below the specified level.

7 Selection of detectors

7.1 Methods for the selection of perimeter intrusion detectors are as follows:

a) For regular perimeters, bistatic microwave intrusion detectors, tensioned wire detectors, shock sensitive cable detectors, Doppler detectors, passive infrared detectors, and active infrared detectors, etc. should be used;
b) For irregular perimeters, shock sensitive cable detectors, buried ported coaxial cable detectors, buried pressure differential detectors, outdoor microwave and passive infrared dual technology detectors, electric field or capacitive detectors, etc. should be used;
c) For perimeters without walls/fences, active infrared detectors, bistatic microwave intrusion detectors, electric field or capacitive detectors, video motion detectors, etc. should be used;
d) For perimeters with complex terrain and obstructions, pressure detectors, shock sensitive cable detectors, buried ported coaxial cable detectors, magnetic field detectors, electric field or capacitive detectors, buried pressure differential detectors， etc. should be used;
e) For perimeters with flat terrain, bistatic microwave intrusion detectors, active infrared detectors, video motion detectors, etc. should be used;
f) For pipelines that pass through perimeters and/or important buildings, pipeline fence detectors should be used.

7.2 Methods for the selection of intrusion detectors at entrances and exits are as follows:

a) For normal entrances and exits in buildings that limit transit time for personnel and vehicles, indoor Doppler detectors, indoor passive infrared detectors, indoor microwave and passive infrared dual technology detectors, magnetic door detectors, etc. should be used;
b) For unconventional entrances and exits in buildings, Indoor Doppler detectors, indoor passive infrared detectors, indoor microwave and passive infrared dual technology detectors, magnetic door detectors, indoor vibration detectors, etc. should be used;
c) For perimeter entrances and exits for vehicles, active infrared detectors, outdoor microwave and passive infrared dual technology detectors, bistatic microwave intrusion detectors, etc. should be used.

7.3 Methods for the selection of indoor intrusion detectors are as follows:

a) For indoor passages, indoor Doppler detectors, indoor passive infrared detectors, indoor microwave and passive infrared dual technology detectors, etc. should be used;
b) For critical indoor locations, capacitive detectors, vibration detectors, indoor passive sound detectors, emergency alarm devices, etc. should be used;
c) For indoor boundaries, indoor vibration detectors, passive infrared detectors, glass break detectors, etc. should be used.

8 Installation requirements

The installation requirements for the intrusion detection alarm system are as follows:

a) Under the premise of guaranteeing the probability of detection, the installation point (height and position) of the detectors shall be determined according to the characteristics of the selected product, alert range requirements and the environmental impact. See specific installation requirements of engineering equipment specified in 6.3.5 of GB 50348-2004;

b) The routing of transmission cables shall comply with the requirements of relevant national standards, industrial standards and administrative regulations;
c) Tamper-resistance and damage-proof measuresshall be taken for the alarm control devices and transmission devices,which shall be installed in a safe and reliable place. See specific installation requirements of engineering equipment specified in 6.3.5 of GB 50348-2004;

9 Safety requirements

9.1 The equipment/devices used in the intrusion detection alarm system shall comply with the safety requirements specified in GB 16796 and related product standards.
9.2 The mechanical structure of any part of the intrusion detection alarm system shall be of sufficient strength to meet the requirements of the service environment and prevent any personal injury due to mechanical instability, movement, protrusions and sharp edges.
9.3 For special areas with flammable and explosive materials, the intrusion detection alarm system shall provide anti-explosive measures and meet the requirements of relevant regulations.
9.4 Detectors used in the intrusion detection alarm system shall be equipped with a tamper device which shall act when any attempt to open the cover or any normal access panel is made to adjust the detection range or adjust detectors.

10 Reliability requirements

10.1 The mean time between failures (MTBF) of the intrusion detection alarm system is at least 150,000h under normal operating conditions.
10.2 The mean time between failures (MTBF) of detectors in the intrusion detection alarm system is at least 60,000h under normal operating conditions.
10.3 The first failure of the intrusion detection alarm system shall not occur within three months after its acceptance.

11 Electromagnetic compatibility requirements

Equipment/devices used in the system shall meet the following requirements and the system shall function normally during the test:

a) The supply voltage adaptability test shall be conducted according to the method given in GB/T 30148-2013, Clause 7, and the test result shall meet the requirements of GB/T 30148-2013, 7.4;
b) The voltage dips and short interruptionimmunity test shall be conducted according to the method given in GB/T 30148-2013, Clause 8, and the test result shall meet the requirements of GB/T 30148-2013, 8.4;
c) The electrostatic discharge immunity test shall be conducted according to the method given in GB/T 30148-2013, Clause 9, and the test result shall meet the requirements of GB/T 30148-2013, 9.4;
d) The radio-frequency (RF) electromagnetic fieldsradiation immunity test shall be conducted according to the method given in GB/T 30148-2013, Clause 10, and the test result shall meet the requirements of GB/T 30148-2013, 10.4;
e) The RF fields-induced conducted disturbances immunity testshall be carried out according to the method given in GB/T 30148-2013, Clause 11, and the test result shall meet the requirements of GB/T 30148-2013, 11.4;
f) The electrical fast transient/burst immunity test shall be conducted according to the method given in GB/T 30148-2013, Clause 12, and the test result shall meet the requirements of GB/T 30148-2013, 12.4;
g) The surge (shock) immunity test shall be conducted according to the method given in GB/T 30148-2013, Clause 13, and the test result shall meet the requirements of GB/T 30148-2013, 13.4.

12 Requirements for lightning protection and grounding

12.1 For the design of intrusion detection alarm system, the equipment used shall meet the lightning protection requirements for electronic equipment.
12.2 The system shall include lightning protection measures, and shall be equipped with power lightning protection devices and signal lightning protection devices.

12.3 The system shall be equipotential grounded; and the individual grounding resistance shall be no greater than 4 Ω.

12.4 The design of lightning protection and grounding for outdoor devices and lines shall comply with the national and industrial standards.

13 Requirements for environmental adaptability

13.1 The environmental adaptability of the system equipment shall meet the requirements of GB/T 15211.

13.2 The protection measures for system equipment shall adapt to the site environment, reaching the corresponding protection level. The system equipment used in the radioactive environment shall be radiation-resistant. Relevant protection measures shall be taken for system equipment operating at excessively high or low temperature and/or excessively high or low atmospheric pressure, and/or in the condition of strong corrosion and high humidity.

13.3 The system equipment operating in salt spray environment in coastal regions shall be capable of resisting salt spray corrosion. The protection measures for system equipment used in flammable and explosive environment shall comply with relevant national standards.

13.4 Relevant anti-interference or isolation measures shall be adopted for system equipment working in the environment with interference sources such as sound, light, heat and vibration.

14 Requirements for validation test

The requirements for validation test of intrusion detection alarm systems (for detailed information see Annex B) are as follows:

a) Before the test, the most vulnerable part of each detecting section and the most likely intrusion way of intruders crossing the detecting section shall be determined according to the terrainof perimeter and the types of detectors adopted, so as to conduct targeted tests.
b) All sections of the detection system shall be tested in different, random ways and sequences.
c) All tests shall be performed under the supervision of security personnel.
d) All test results shall be recorded in detail, see B.2 of Annex B.

Annex A
(**informative**)
Architecture of intrusion detection alarm systems

The architecture of multi-line mode intrusion detection alarm system is shown in Figure A.1.

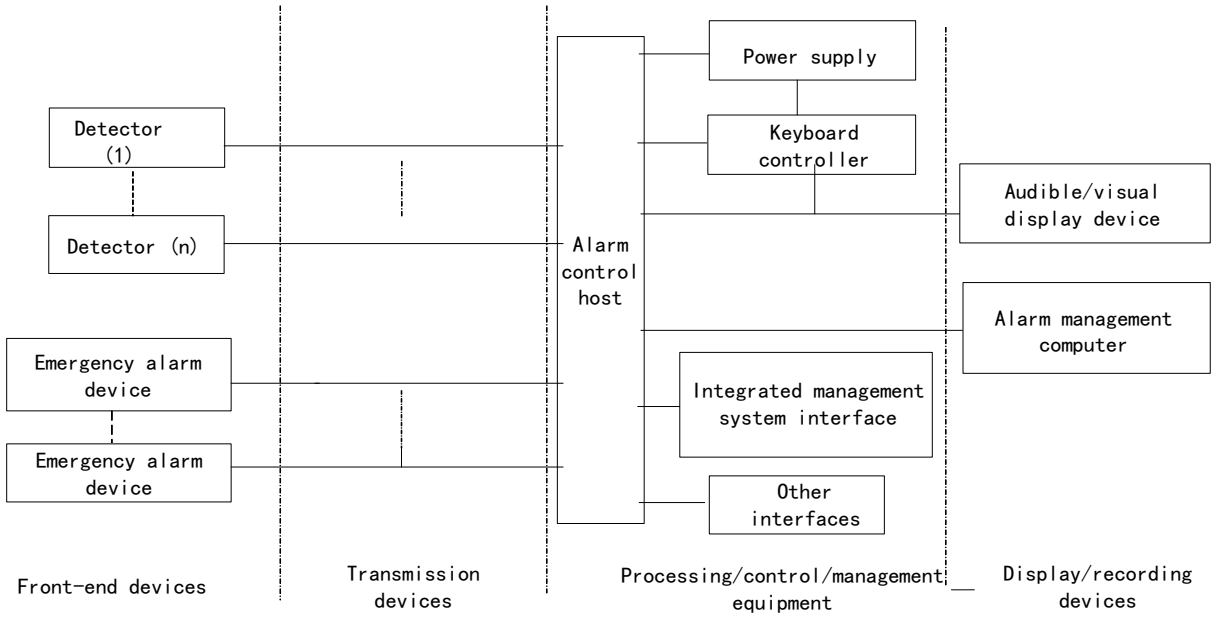

Figure A.1 Architecturediagram of multi-line mode intrusion detection alarm system

The architecture of bus mode intrusion detection alarm system is shown in Figure A.2.

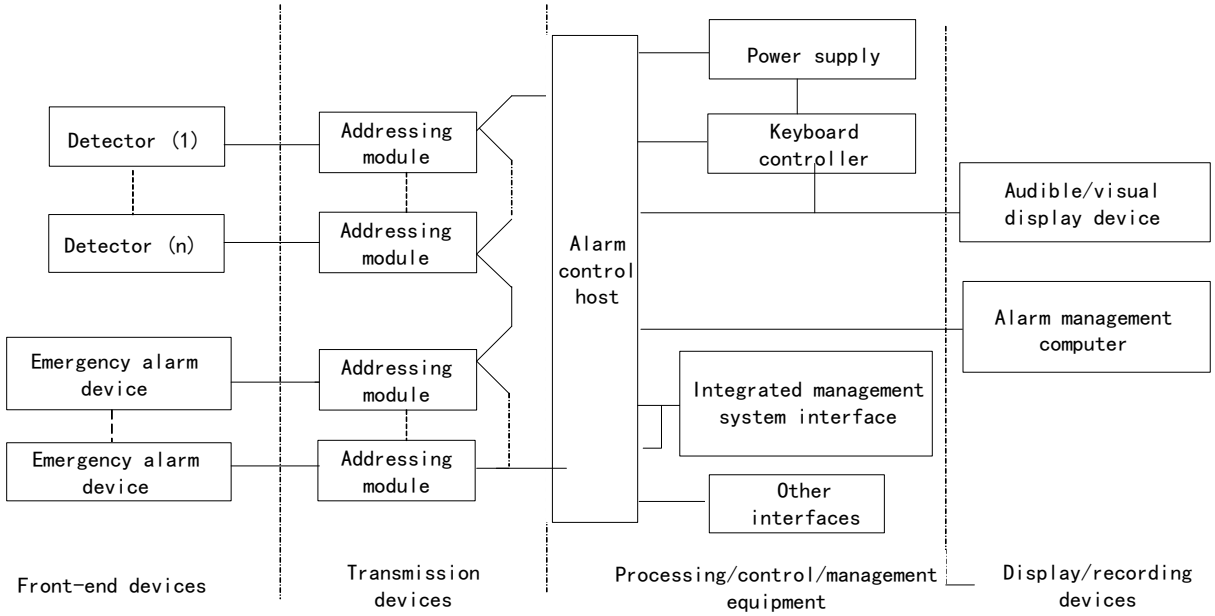

Figure A.2 Architecture diagram of bus mode intrusion detection alarm system

The architecture of special network mode intrusion detection alarm system is shown in Figure A.3.

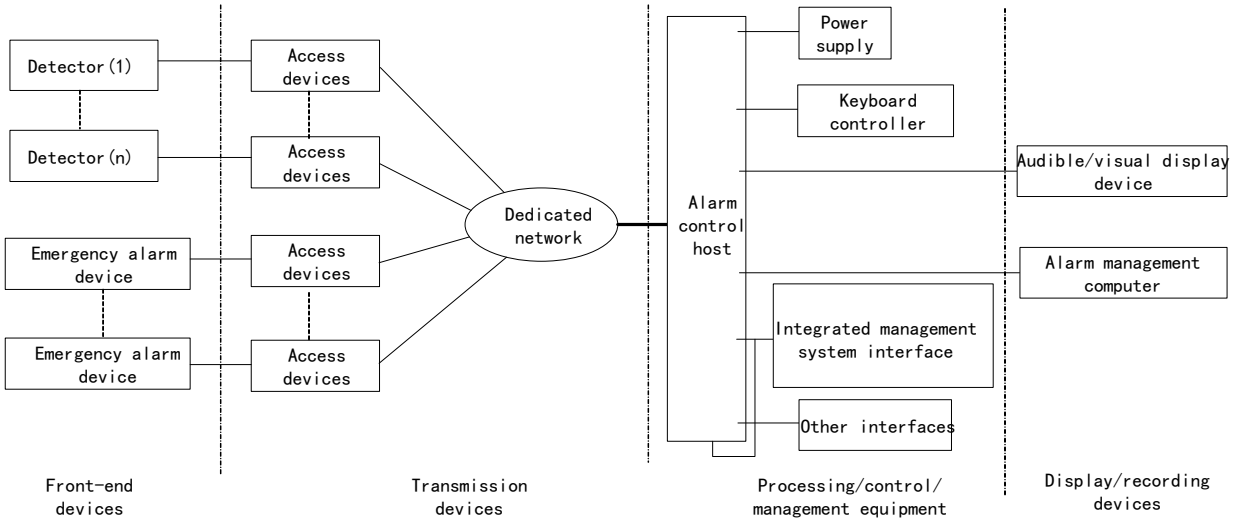

Figure A.3 Architecture diagram of dedicated-network mode intrusion detection alarm system

Annex B
(informative)
Validation test of intrusion detection alarm system

B.1 Validation test methods

The validation test methods for intrusion detection alarm systems are as follows:

First, the most vulnerable part of each detecting section shall be tested at least 30 times by all available ways of intrusion. The 30 times of detection shall meet the requirements of corresponding minimum number of successful detection in Table B.1; if so, the test of this detecting section may be completed.

If not so, the system shall be inspected. If any problem is found on the system, another 30 times of tests (repeat the above step) shall be conducted after the inspection and maintenance; if no problem is found, additional 10 times of tests shall be conducted. If the test results meet the minimum number of successful detection for 40 times of tests, the test of this detecting section may be completed. If the minimum number of successful detection is not met and no system problem is found, another 10 times of tests shall be conducted. As the test results meet the minimum number of successful detection for 50 times of tests, the test of this detecting section may be completed. Otherwise, the system needs to be upgraded.

Table B.1 Minimum number of successful detection required for different number (30 - 50) of tests

Total number of tests	Minimum number of successful detection	Maximum number of failed detection
30	30	0
40	39	1
50	48	2

Table B.2 Relationship between number of successful tests and probability of detection

Total number of tests	Number of successful detection	Lower limit of probability of detection at 95% confidence level %
30	30	90.5
40	39	88.7
	40	92.8
50	48	87.9
	49	90.9
	50	94.2
60	57	87.6
	58	89.9
	59	92.3
	60	95.1
70	67	89.3
	68	91.3
	69	93.4
	70	95.8
80	76	88.9
	77	90.6
	78	92.3
	79	94.2
	80	96.3

B.2 System site test record

All test results shall be recorded in detail, including test date (year, quarter), test time, detecting section number, test environment, intrusion ways used, test results, testing personnel and recorder. Figure B.1 lists the format of detection probability test record for reference (other formats may also be used).

Table Test record of detection probability

Date: Day Month Year Time: Environmental conditions: Testing personnel:

Testing section number: Recorded by:

	Test data of quarter year			
Ways of intrusion	The number of failed detection a	The number of successful detection b	The total number of detection c (c=a+b)	Eigenvalue of detection probability (b/c)
Running				
Walking				
Crawling				
Jumping				
Rolling				
Climbing				
Total				

Note: Environmental conditions include weather, illumination and other factors that may impact the detection.

Figure B.1 Format of detection probability test record

B.3 Common intrusion alarm systems

B.3.1Active infrared detector

The active infrared detector shall be capable of detecting an intruder (with a weight of no less than 35kg) walking, running, jumping, crawling, or rolling across the area between the transmitter and the receiver. The detector can still meet the above requirements when the signal is attenuated to 1/20 of the original beam energy in the range of maximum distance no greater than 80m.

B.3.2 Electric field detector

The electric field detector shall be capable of detecting an intruder with a weight of no less than 35kg rolling under the bottom line or walking or jumping between lines.

B.3.3 Buried ported coaxial cable detector

Each section of the buried ported coaxial cable detector shall be limited to 100m. The transmitter and receiver lines of the detector may be buried together or separately and are generally buried 23cm below the ground. The lines shall be 2m apart from each other. The buried ported coaxial cable detector shall be capable of detecting an intruder walking, running, jumping, crawling or rolling across the detection area.

B.3.4 Fiber optic cable detector

The fiber optic cable detector shall be capable of generating alarm signals when an intruder (with a weight of no less than 35kg) walking, running, jumping, crawling, rolling across the area where the fiber optic cables are buried.

B.3.5 Shock sensitive cable detector or tensioned wire detector

Shock sensitive cable detectors or tensioned wire detectors shall be capable of detecting the following activities:

a) An intruder with a weight of no less than 35kg climbs over fences;
b) An intruder cuts off fences;
c) An intruder lifts or presses down the fence lines.

B.3.6 Outdoor bistatic microwave intrusion detector

The maximum detection distance between a transmitter and a receiver of a typical long-distance bistatic microwave detector is 100m. The transmitter and receiver shall be securely installed to the embedded metal column with a mounting height of 0.6m to 0.8m. To prevent any detection blind zone beneath the microwave beam, the ground shall be flat, obstructions shall be removed, and ditches shall be filled so that the area between the transmitter and receiver is clear of obstructions and the rises and depressions are no more than 10cm. In order to prevent an intruder from crossing over the microwave beam from atop the fence, the distance between the fence and the center of the microwave beam shall be no less than 2.4m. The microwave detector shall be capable of detecting an intruder (weighing no less than 35kg) walking, running, jumping, crawling and rolling across the area between the transmitter and receiver, including the area in front of the transmitter and receiver.

B.3.7 Indoor Doppler detector

Installation of the detector is inspected first. The mounting height is 2m ~ 3m and the distance from the fluorescent lamp is at least 2m. The detector shall be tested by walking.

The target/humanto be tested shall be (1.5±0.3)m high and weigh (59±5)kg. The target shall be walking at a speed of 12cm/s with both arms folding across the chest. Five paths shall be selected for testing. Each path shall be tested twice (in back and forth directions) and it shall be deemed acceptable if all paths are successfully detected. The five paths are as follows:

a) Parallel to the detector’sdetection direction;
b) Perpendicular to the detector’s detection direction;
c) Forming a 45° angle with the detector’s detection direction;
d) Forming a -45° angle with the detector’s detection direction;
e) Any route radiating to the detector.

B.3.8 Indoor passive infrared detector

The mounting height shall be in compliance with the manufacturer’s requirement and the distance from the direct light source shall be no less than 3m. The person to be tested shall be walking for detection. The target/human to be tested shall be (1.5±0.3)m high and weigh (59±5)kg. The target shall be walking at a speed of 12cm/s with both arms folding across the chest. Five paths shall be selected for testing and each path shall be tested twice (in back and forth directions). It shall be deemed acceptable if all paths are successfully detected.The five paths are as follows:

a) Parallel to the detector’sdetection direction;
b) Perpendicular to the detector’s detection direction;

c) Forming a 45° angle with the detector's detection direction;
d) Forming a -45° angle with the detector's detection direction;
e) Any route radiating to the detector.

B.3.9 Video motion detector

The video motion detector shall be capable of detecting a low-profile target (such as a crouching person) and a high-speed moving target (such as a running person). Testing shall be performed with the minimum possible illumination (for example, artificial lighting at night). If there is some shadow in the detection zone, the test shall be done in the shadow. All the above tests shall generate alarms.