# GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

# GB/T 25070-2019

Replacing GB/T 25070-2010

# Information security technology - Technical requirements of security design for classified protection of cybersecurity

信息安全技术

网络安全等级保护安全设计技术要求

**Issued on: May 10, 2019** **Implemented on: December 01, 2019**

**Issued by: State Administration for Market Regulation;**
**Standardization Administration of PRC.**

# Table of Contents

Foreword ..... 4

Introduction ..... 6

1 Scope ..... 7

2 Normative references ..... 7

3 Terms and definitions ..... 8

4 Abbreviations ..... 11

5 Design overview of classified protection security technology of cybersecurity ..... 12

5.1 Design framework of security technology of general classified protection ..... 12

5.2 Design framework of security technology of classified protection for cloud computing ..... 13

5.3 Design framework of security technology of classified protection for mobile interconnection ..... 15

5.4 Design framework of security technology of classified protection for Internet of Things ..... 17

5.5 Design framework of security technology of classified protection of industrial control ..... 18

6 Design of the first-level system security protection environment ..... 20

6.1 Design targets ..... 20

6.2 Design strategy ..... 21

6.3 Design technical requirements ..... 21

7 Design of second-level system security protection environment ..... 26

7.1 Design targets ..... 26

7.2 Design strategy ..... 26

7.3 Design technical requirements ..... 27

8 Design of third-level system security protection environment design ..... 36

8.1 Design targets ..... 36

8.2 Design strategy ..... 36

8.3 Design technical requirements ..... 37

9 Design of fourth-level system security protection environment ..... 53
9.1 Design targets ..... 53
9.2 Design strategy ..... 53
9.3 Design technical requirements ..... 54
10 Design of fifth-level system security protection environment ..... 72
11 Interconnection design of classified system ..... 72
11.1 Design targets ..... 72
11.2 Design strategy ..... 72
11.3 Design technical requirements ..... 72
Appendix A (Informative) Design of access control mechanism ..... 75
Appendix B (Informative) Design example of third-level system security protection environment ..... 78
Appendix C (Informative) Technical requirements for big data design ..... 85
References ..... 90

# Information security technology - Technical requirements of security design for classified protection of cybersecurity

## 1 Scope

This standard specifies the technical requirements for the security design of the first to fourth-levels of classified protection of cybersecurity.

This standard is applicable to the design and implementation of classified protection of cybersecurity and security technology solutions by operating and using organizations, network security enterprises, network security service agencies. It can also be used as the basis for cybersecurity functional departments to conduct supervision, inspection and guidance.

Note: The fifth-level classified protection object is a very important supervision and management object. It has special management modes and security design technical requirements, so it is not described in this standard.

## 2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB 17859-1999 Classified criteria for security protection of computer information system

GB/T 22240-2008 Information security technology - Classification guide for classified protection of information systems security

GB/T 25069-2010 Information security technology - Glossary

GB/T 31167-2014 Information security technology - Security guide of cloud computing services

GB/T 31168-2014 Information security technology - Security capability requirements of cloud computing services

GB/T 32919-2016 Information security - Industrial control systems -

network layer and the application layer, etc.

c) Security communication network

Include the relevant components of the Internet of Things system's security computing environment and security area for information transmission and implementation of security policies, such as the communication network at the network layer and the communication network between the internal security computing environment at the sensor layer and the application layer.

d) Security management center

Include a platform for the unified management of security policies and security computing environments, security area boundaries, security mechanisms on security communication networks for Internet of Things systems. It includes three parts: system management, security management, audit management. Only the second-level and above security protection environment is designed with a security management center.

## 5.5 Design framework of security technology of classified protection of industrial control

The industrial control system is zoned based on the business nature of the object being protected; the classified protection of cybersecurity design is implemented based on the technical characteristics of the functional level; the design framework of security technology of classified protection of industrial control system is as shown in Figure 5. The triple protection system of computing environment, area boundary, communication network of the construction of the security technology design of the classified protection of industrial control system, under the support of the security management center, adopts a layered and partitioned architecture. It is designed combining the characteristics of the complex and diverse bus protocols of the industrial control system, strong real-time requirements, limited node computing resources, high device reliability requirements, short fault recovery time, security mechanisms that cannot affect real-time performance, to realize reliable, controllable, manageable system security interconnection, area boundary security protection, computing environment security.

The industrial control system is divided into 4 layers, that is, the 0 ~ 3 layers are the scope of the industrial control system's classified protection, which is the area covered by the design framework; the security zone of the industrial control system is divided horizontally; according to the importance of the business in the industrial control system, the timeliness, business relevance, degree of impact on field controlled device, functional scope, asset attributes, etc., it forms

so that the system users have the ability to protect the object it belongs to.

## 6.2 Design strategy

The design strategy of the first-level system security protection environment is to follow the relevant requirements in 4.1 of GB 17859-1999, based on identity authentication, to provide users and / or user groups with independent access control of files and database tables, so as to achieve isolation between he user and the data, thereby making the user have the ability of autonomous security protection; provide area boundary protection by means of packet filtering; provide data and system integrity protection by means of data verification and prevention of malicious code.

The design of the first-level system security protection environment is realized through the design of the first-level security computing environment, the security area boundary, the security communication network. Computing nodes shall be based on trusted roots for trusted verification from startup to operating system startup.

## 6.3 Design technical requirements

### 6.3.1 Design technical requirements for security computing environment

#### 6.3.1.1 Technical requirements for the design of general security computing environment

This requirement includes:

a) Authentication of user identity

It shall support user identification and user authentication. When each user registers with the system, use the user name and user identifier to identify the user's identity; each time a user logs in to the system, use a password authentication mechanism to authenticate the user's identity and protect the password data.

b) Autonomous access control

Within the scope of security policy control, make the users / user groups have corresponding access operation permissions on the objects they create; meanwhile grant some or all of these permissions to other users / user groups. The granularity of the access control subject is the user / user group level; the granularity of the object is the file or database table level. Access operations include creating, reading, writing, modifying, deleting objects.

b) Application control

It shall provide an application signature authentication mechanism, to refuse installation and execution of application software that has not been authenticated and signed.

#### 6.3.1.4 Technical requirements for design of security computing environment for Internet of Things systems

This requirement includes:

a) Authentication of sensor layer device

It shall use the conventional authentication mechanisms to identify the identity of the sensor device, to ensure that the data originates from the correct sensor device.

b) Access control of sensor layer device

It is necessary to implement access control on sensor devices by formulating security policies such as access control lists.

#### 6.3.1.5 Technical requirements for design of security computing environment for industrial control systems

This requirement includes:

a) Authentication of industrial control

Field control layer device and process monitoring layer device shall implement unique marking, authentication and certification, to ensure that the status of authentication and functional integrity can be verified and confirmed at any time. Programs and corresponding data sets running on control device and monitoring device shall be managed by unique identifier.

b) Access control of field device

It shall implement the role-based access control policies for users who pass the identity authentication. After receiving the operation command, the field device shall check whether the role bound to the user has the authority to perform the operation. The user with authority obtains the permission. If the user does not obtain the permission, it shall issue an alarm message to the upper layer.

c) Protection of control process integrity

It shall complete the specified tasks within the specified time; the data shall be processed in an authorized manner, to ensure that the data is not illegally

## 7.3 Design technical requirements

### 7.3.1 Technical requirements for design of security computing environment

#### 7.3.1.1 Technical requirements for design of general security computing environment

This requirement includes:

a) Authentication of user identity

It shall support the user identification and user authentication. When each user registers with the system, use the user name and user identifier to identify the user, **meanwhile ensure the uniqueness of the user identifier throughout the life cycle of the system**; each time a user logs in to the system, use a **controlled password or other mechanisms of corresponding security strength** for authentication of user identity; use cryptographic technology for confidentiality and integrity protection of authentication data.

b) Autonomous access control

Within the scope of security policy control, **users** shall be allowed to access the objects they create, and some or all of these permissions can be granted to other **users**. The granularity of the access control subject is the user level; the granularity of the object is the file or database table level. Access operations include creating, reading, writing, modifying, deleting objects.

c) System security audit

It shall provide a security audit mechanism, to record system-related security events. The audit record includes the subject, object, time, type and result of the security incident. The mechanism shall provide audit record query, classification and storage protection, which can be managed by the security management center.

d) Protection of user data integrity

It may use a conventional check mechanism, to check the integrity of the stored user data, to find out whether its integrity has been compromised.

e) Protection of user data confidentiality

It may use the confidentiality protection mechanisms supported by technologies such as passwords to protect the confidentiality of user data as stored and processed in a security computing environment.

**It shall be able to detect the abnormal access of the virtual machine to the host's physical resources.**

**e) Data backup and recovery**

It shall adopt redundant architecture or distributed architecture design; it shall support data multi-copy storage; it shall support common interfaces to ensure that cloud tenants can migrate business systems and data to other cloud computing platforms and local systems, to ensure portability.

f) Virtualization security

**It shall achieve the security isolation of CPU, memory, storage space of virtual machines**; it shall prohibit the direct access of virtual machines to the host's physical resources; it shall support the security isolation between virtualized networks of different cloud tenants.

g) Prevention of malicious code

Physical machines and host machines shall install a security-hardened operating system or perform host malicious code prevention; **virtual machines shall install a security-hardened operating system or perform the host malicious code prevention; they shall support the ability to detect and protect Web application malicious code**.

**h) Mirror and snapshot security**

**It shall support images and snapshots, to provide integrity protection for virtual machine images and snapshot files; prevent unauthorized access to sensitive resources that may exist in virtual machine images and snapshots; provide security-hardened operating system images for important business systems or support self-hardening of the operating system images.**

**7.3.1.3 Technical requirements for design of security computing environment for mobile internet**

This requirement includes:

a) Authentication of user identity

It shall use passwords, unlock patterns, and other mechanisms with appropriate security strengths for authentication of user identity.

b) Application control

It shall provide an application signature authentication, to refuse installation and execution of application software that has not been authenticated and

Field control layer device and process monitoring layer device shall implement unique marking, authentication and certification, to ensure that the status of authentication, certification and functional integrity can be verified and confirmed at any time. Programs and corresponding data sets running on control device and monitoring device shall be managed by unique identification.

b) Access control of field device

It shall implement the role-based access control policies for users who pass the identity authentication. After receiving the operation command, the field device shall check whether the role bound to the user has the authority to perform the operation. The user who has permission obtains the authorization. If the user does not obtain the authorization, it shall issue the alarm information to the upper layer.

**c) Data confidentiality protection of field device**

**It may use the confidentiality protection mechanism supported by cryptographic technology or the physical protection mechanism, to protect the confidentiality of data, programs, configuration information, etc. which has confidentiality requirements as stored in field device layer devices and fieldbus devices connected to the field control layer.**

d) Protection of control process integrity

It shall finish the specified tasks within the specified time; the data shall be processed in an authorized manner, to ensure that the data is not illegally tampered with, lost, or delayed, to ensure timely response and processing of incidents, **to protect the system's synchronization mechanism, time correction mechanism, thereby maintaining the stability of the control cycle and the stability of the rolling cycle of fieldbus.**

### 7.3.2 Technical requirements for design of security area boundary

#### 7.3.2.1 Technical requirements for design of general security area boundary

This requirement includes:

a) Packet filtering of area boundary

It shall, according to the area boundary security control strategy, determine whether to allow the data packet to pass through the area boundary by checking the source address, destination address, transport layer protocol, requested service of the data packet.

b) Security audit of area boundary

**It may use the integrity check mechanism supported by the short-message and short-latency cryptographic technology adapted to the characteristics of the fieldbus, or the physical protection mechanism, to achieve the integrity protection of the data transmission of fieldbus network.**

**b) Protection of data transmission integrity of wireless network**

**It may use the integrity check mechanism supported by cryptographic technology, to achieve integrity protection of data transmission of wireless network.**

### 7.3.4 Technical requirements for design of security management center

#### 7.3.4.1 System management

System administrators can perform configuration, control and trusted management of the resources and operations of the system, including user identity, trusted certificates, **trusted reference library**, system resource configuration, system loading and startup, exception handling of system operations, data and device backup and recovery, protection against malicious code.

It shall authenticate the identity of the system administrators. They are only allowed to perform system management operations through specific commands or operation interfaces, and audit these operations.

When performing the security design of a cloud computing platform, the security management shall provide a way to query cloud tenant data and back up storage locations.

When designing the security of the Internet of Things system, the system administrator shall perform the unified identity management of the sensor devices, sensor layer gateways, etc.

#### 7.3.4.2 Audit management

Security auditors can centrally manage the security audit mechanisms distributed in various components of the system, including classifying audit records according to security audit policies; providing the corresponding types of security audit mechanisms to be turned on and off by time period; storing, managing, querying various types of audit records.

It shall perform identity authentication of the security auditor. It allows for the auditor to perform security audit operations only through specific commands or operation interfaces.

When performing the security design of a cloud computing platform, the cloud

**detecting that the credibility is compromised;** form the verification results into audit record; **send it to the management center.**

i) Inspection of configuration credibility

The security configuration information of the system shall be formed into a reference library, to monitor in real-time and regularly inspect the modification behavior of the configuration information, to timely repair the configuration information which is inconsistent with the contents in the reference library.

j) **Intrusion detection and malicious code prevention**

**It shall use the active immune trusted computing check mechanism to timely identify the intrusion and virus behavior, meanwhile effectively block it.**

**8.3.1.2 Technical requirements for design of cloud security computing environment**

This requirement includes:

a) Authentication of use identity

It shall support the cloud tenants registered to the cloud computing service to establish a master and sub account; use the user name and user identifier to identify the user identity of the master and sub account.

b) Protection of user account

It shall support the establishment of a cloud tenant account system, to achieve the subject's access authorization to virtual machines, cloud databases, cloud networks, cloud storage and other objects.

c) Security audit

It shall support the audit of privileged commands as executed by cloud service providers and cloud tenants during remote management.

It shall support the tenant to collect and view audit information related to the resources of the tenant, to ensure that cloud service providers' access to cloud tenant systems and data can be audited by the tenant.

d) Intrusion prevention

It shall be able to detect the abnormal access of virtual machine to the host's physical resources. **It shall support the behavior monitoring of cloud tenants, detect and alert to malicious attacks or malicious external**

a) **Authentication of user identity**

**It shall achieve the authentication of user identity for the mobile terminal user based on the combination mechanism of two or more methods of passwords or unlock patterns, digital certificates or dynamic passwords, biometrics, etc.**

b) **Marking and mandatory access control**

**It shall ensure that the user or process's minimum use permissions of the mobile terminal system resources. It shall control mobile terminal access to access peripherals according to security policies; the type of peripherals shall at least include expansion memory cards, GPS and other positioning devices, Bluetooth, NFC and other communication peripherals. Record the log.**

c) Application control

**It shall have a software whitelist function, which can control the installation and operation of application software according to the whitelist;** it shall provide an application signature authentication mechanism, to refuse the installation and execution of application software that has not been authenticated and signed.

d) Isolation of security domain

It shall be able to provide **container-based, virtualized, and other system-level** isolated operating environments for important applications, to ensure that application input, output, storage information is not obtained illegally.

e) Control of mobile device

It shall, based on mobile device management software, implement the entire life cycle control of mobile devices, to ensure that after the mobile device is lost or stolen, the location of the device is searched through the network, the device is remotely locked, the data on the device is remotely erased, the device emits an alarm tone, to ensure maximum protection of data while being able to locate and retrieve.

f) Protection of data confidentiality

It shall use the measures such as encryption, obfuscation, to protect the confidentiality of mobile applications, to prevent de-compilation; **it shall achieve the encryption function of extended storage devices, to ensure the security of data storage.**

g) **Trusted verification**

It shall ensure that the virtual machine can only receive messages with a destination address that includes its own address or broadcast messages with business needs, whilst limiting the broadcast attacks; **it shall achieve the isolation between the virtual network resources of different tenants, avoid excessive occupation of network resources. It shall ensure that cloud computing platform's management traffic is separated from cloud tenant's business traffic.**

**It shall be able to identify and monitor network traffic between virtual machines and between virtual machines and physical machines; provide open interfaces or open security services; allow cloud tenants to access third-party security products or select third-party security services on cloud platforms.**

b) Access control of area boundary

It shall ensure that when the virtual machine is migrated, the access control policies are also migrated. It shall allow the cloud tenants to set access control policies between different virtual machines. It shall establish the tenant private networks to achieve the security isolation between different tenants. **It shall deploy a monitoring mechanism at the network boundary, to implement effective monitoring of the traffic entering and leaving the network.**

c) **Prevention of area boundary intrusion**

**When the virtual machine migrates, the intrusion prevention mechanism can be applied to the new boundary; it shall include the intrusion prevention mechanism at the area boundary into the security management center for unified management.**

**It shall provide the cloud tenants with Internet content security monitoring functions, to detect and alert harmful information in real time.**

d) **Requirements for area boundary audit**

**According to the division of responsibilities of cloud service providers and cloud tenants, collect audit data of their respective control parts. According to the division of responsibilities of cloud service providers and cloud tenants, achieve centralized audit of their respective control parts. When virtual machine migration or virtual resource changes occur, the security audit mechanism can be applied to new boundaries. Provide an interface for the collection of security audit data; it can also be audited by third parties.**

**8.3.2.3 Technical requirements for design of security area boundaries of**

This requirement includes:

a) **Communication protocol data filtering of industrial control**

**For industrial control communication protocols that pass through the security area boundary, it shall be able to identify whether the data carried by it will cause attacks or damage to the industrial control system. It shall control the communication traffic, the frequency of frame numbers, the frequency of reading variables to be stable and within the normal range; protect the working rhythm of the controller; identify and filter data with variable parameters outside the normal range. The control filtering processing component can be configured on the network device at the area boundary; it may also be configured on the endpoint device of the industrial control communication protocol in this security area or the only communication link device.**

b) **Information leakage protection of industrial control communication protocol**

**It shall avoid user name and login password of the endpoint device of the industrial control communication protocol in this area from being exposed; use the filtering and transforming technology to hide the key information such as the username and login password. The endpoint device shall be separately partitioned and filtered; use the combination mechanism of one or more types of corresponding protection functions to implement protection.**

c) Security audit of industrial area boundary

It shall set up real-time monitoring and alarm mechanism at the security area boundary, which is managed in a centralized manner by the security management center; alarm promptly the security management center and industrial control personnel of the identified violations and make corresponding measures.

### 8.3.3 Technical requirements for design of security communication network

#### 8.3.3.1 Technical requirements for design of general security communication network

This requirement includes:

a) Security audit of communication network

It shall set up an audit mechanism in the security communication network, which is under centralized management by the security management center;

g) **Protection against wireless network attacks**

**It shall perform risk analysis of potential threats and possible consequences of wireless network attacks; shield the information transmission (information leakage) and entry (illegal manipulation) of device that may be subject to wireless attacks. It may comprehensively use such methods as detection and interference, electromagnetic shielding, microwave darkroom absorption, physical protection, to attenuate the wireless signal to the extent that it cannot be effectively received in the spectrum range that may be transmitted.**

### 8.3.4 Technical requirements for design of security management center

#### 8.3.4.1 System management

It may use the system administrator to configure and control the system resource and operation, meanwhile perform trusted and cryptographic management, including user identity, trusted certificates and keys, **trusted reference libraries**, system resource configuration, system loading and startup, exception handling of system operation, data and device backup and recovery.

It shall perform identity authentication of the system administrators. It only allows them to perform system management operations through specific commands or operation interfaces; meanwhile audit these operations.

When perform the security design of a cloud computing platform, security management shall provide a way to query cloud tenant data and back up storage locations; **the operation and maintenance of the cloud computing platform shall be in China; the implementation of O & M operations on domestic cloud computing platforms overseas shall follow relevant national regulations.**

When perform the security design of the Internet of Things system, it shall use the system administrator to perform unified identity management of the sensor devices, sensor gateways, etc. **It shall use the system administrator to perform unified monitoring and processing of the sensor device status (power supply status, online or not, location, etc.).**

#### 8.3.4.2 Security management

It shall use the security administrator to make unified marking of the subjects and objects in the system; authorize the subjects; configure **trusted verification** policies; maintain a policy database and a metric database.

It shall authenticate the identity of the security administrators. It only allows them to use specific commands or operation interfaces to perform security management operations; meanwhile perform audit.

mandatory access control to all subjects and objects. It shall, according to the security marking and the control rules of the mandatory access, control the access of the determined subject to the object. The granularity of mandatory access control subject is user level; the granularity of object is file or database table level. It shall be ensured that all subjects and objects in the security computing environment have consistent marking information and implement the same mandatory access control rules.

d) System security audit

It shall record the system-related security events. The audit record includes the subject, object, time, type and result of the security incident. It shall provide the query, classification, analysis, storage protection of audit record. It shall be able to alarm the specific security events, terminate illegal processes, etc. Ensure that audit records are not destroyed or unauthorized access, prevent audit records from being lost. It shall provide an interface for the security management center; for security events that cannot be handled independently by the system, provide an interface called by an authorized subject.

e) Protection of user data integrity

It shall use the integrity verification mechanisms supported by passwords and other technologies, to verify the integrity of user data as stored and processed, to discover whether its integrity has been compromised and to restore important data if it is compromised.

f) Protection of user data confidentiality

Use the confidentiality protection mechanism supported by technologies such as passwords, to protect the confidentiality of user data in a security computing environment.

g) Object security reuse

It shall adopt the system software with security object reuse function or information technology products with corresponding functions, to clean up the object resources used by users before the reallocation of these object resources, to ensure that information is not disclosed.

h) Trusted verification

It may, based on the trust root, perform trusted verification of the BIOS, bootloader, operating system kernel, application, etc. of the computing node. Meanwhile in **all** execution links of the applications, perform the trusted verification of the subject, object, operation as called by the system; perform the trusted verification of the execution resources in the interrupted and key

It shall support the behavior monitoring for cloud tenants; detect and alarm to malicious attacks or malicious external connections initiated by cloud tenants.

e) Protection of data confidentiality

It shall provide the important business data encryption services; the encryption keys shall be managed by the tenants themselves. It shall provide encryption services, to ensure the confidentiality of important data during virtual machine's migration.

f) Data backup and recovery

It shall adopt redundant architecture or distributed architecture design; it shall support multi-copy storage of data; it shall support common interfaces to ensure that cloud tenants can migrate business systems and data to other cloud computing platforms and local systems, to ensure portability; **it shall establish the offsite disaster backup center, to provide real-time switching of business applications.**

g) Virtualization security

It shall achieve the security isolation of CPU, memory, storage space of virtual machines; be able to detect the situations such as unauthorized management of virtual machines and issue alarms. It shall prohibit the direct access of the virtual machine to the physical resources of the host; it shall be able to alarm the abnormal access. It shall support for security isolation between different cloud tenants' virtualized networks; it shall monitor the operating status of physical machines, host machines, virtual machines. **It shall provide interfaces for the centralized monitoring by the security management center.**

h) Prevention of malicious code

Physical machines and host machines shall install a security-hardened operating system or perform the host malicious code prevention; virtual machines shall install a security-hardened operating system or perform the host malicious code prevention; they shall support the ability to detect and protect Web application malicious code.

i) Image and snapshot security

It shall support images and snapshots, to provide integrity protection for virtual machine images and snapshot files; prevent unauthorized access to sensitive resources that may exist in virtual machine images and snapshots; provide security-hardened operating system images for important business systems or support self-strengthening of the operating system image.

**control application program, the fieldbus receive-send module, the trust chain or security controllable chain of field device layer device's receive-send module program, in order to achieve the integrity check of the executable program during the system running process, prevent attacks such as malicious code; meanwhile take recovery measures when its integrity is detected to be compromised. It shall construct a trusted or securely controllable clock source, trusted or security controllable synchronization and timing mechanism based on the entire complete chain of the system, to prevent malicious interference and destruction.**

g) Protection of control process integrity

It shall complete the specified tasks within the specified time. The data shall be processed in an authorized manner, to ensure that the data is not illegally tampered with, lost, or delayed, to ensure timely response and processing of incidents, to protect the system's synchronization mechanism, time correction mechanism, to maintain the stability of control cycle and the stability of the polling cycle of fieldbus. The field devices shall be able to identify and prevent attacks that undermine the integrity of the control process; it shall be able to identify and prevent attacks that interfere with the normal working rhythm of devices such as controllers with legitimate identities and legitimate paths. When the control system is under attack and cannot maintain normal operation, there shall be fault isolation measures; it shall guide the system to a predefined security state, to control the harm to a minimum range.

### 9.3.2 Technical requirements for design of security area boundaries

#### 9.3.2.1 Technical requirements for design of general security area boundary

This requirement includes:

a) Access control of area boundary

It shall set up autonomous and mandatory access control mechanisms at the security area boundaries. It shall perform trusted verification of the identity, address, port, application protocol of the source and target computing nodes. Control the data information entering and leaving the security area boundaries, to block the unauthorized access.

b) Packet filtering at area boundary

According to the area boundary security control strategy, it shall determine whether to allow the data packet to enter and exit the area boundary by checking the source address, destination address, transmission layer

third-party security products or select third-party security services on cloud platforms. **It shall ensure the fourth-level business application system of the cloud tenant has independent resource pool.**

b) Access control of area boundary

It shall ensure that when the virtual machine is migrated, the access control policies are also migrated. It shall allow the cloud tenants to set access control policies between different virtual machines. It shall establish the tenant private networks to achieve the security isolation between different tenants. It shall deploy a monitoring mechanism at the network boundary, to implement effective monitoring of the traffic entering and leaving the network.

c) Prevention of area boundary intrusion

When the virtual machine migrates, the intrusion prevention mechanism can be applied to the new boundary; it shall include the intrusion prevention mechanism at the area boundary into the security management center for unified management.

It shall provide the cloud tenants with Internet content security monitoring functions, to detect and alert harmful information in real time.

**It shall deploy the security system of file level code detection or file operation behavior detection of the corresponding for at the critical area boundary, to detect and clear the malicious code.**

d) Requirements for area boundary audit

According to the division of responsibilities of cloud service providers and cloud tenants, collect audit data of their respective control parts. According to the division of responsibilities of cloud service providers and cloud tenants, achieve centralized audit of their respective control parts. When virtual machine migration or virtual resource changes occur, the security audit mechanism can be applied to new boundaries. Provide an interface for the collection of security audit data; it can also be audited by third parties. **Promptly alarm the confirmed violations and make corresponding disposal.**

#### 9.3.2.3 Technical requirements for design of security area boundaries of mobile interconnection

##### 9.3.2.3.1 Access control of area boundary

For mobile terminals accessing the system, it shall take strong authentication measures based on information such as SIM cards and certificates. It shall be able to restrict the mobile device's ability to access to WiFi, 3G, 4G and other

**It shall use the security management center to perform centralized management; alarm the confirmed violations; make corresponding disposal.**

#### 9.3.3.3 Technical requirements for design of security communication networks of mobile interconnection

This requirement includes:

a) **Trusted protection of communication networks**

**It shall use the technologies such as VPDN to achieve a trusted network connection mechanism based on a cryptographic algorithm; through trusted verification of the device which accesses to the communication network, ensure the authenticity of the devices accessed to the communication network and prevent illegal access by the devices.**

#### 9.3.3.4 Technical requirements for design of security communication network of Internet of Things systems

This requirement includes:

a) Protection of sensor layer network data freshness

It shall add the sequence data released by the data such as time stamp and counter to the data transmitted by the sensor layer network, to achieve freshness protection of data transmission in the sensor layer network.

b) Protection of heterogeneous network security access

It shall adopt the technologies such as access authentication to establish access authentication systems for heterogeneous networks, to ensure the security transmission of control information. It shall, based on such factors as the job function of each access network, importance, the important degree of the information related, divide different sub-network or network segment; meanwhile take appropriate protective measures. **It shall provide dedicated communication protocol or security communication protocol service for the important communication, to avoid the data integrity from being compromised by the attack based on general communication protocol.**

#### 9.3.3.5 Technical requirements for the design of security communication networks for industrial control systems

This requirement includes:

a) **Audit of bus network security**

operating mode, status of each site, redundant mechanism, etc. of the industrial control system; report abnormalities when they are found. In applications where there is redundant field bus and voting devices, it may fully monitor the status of each redundant link at the same time, to capture possible malicious or intrusive behaviors. It shall perform traffic monitoring and control on the corresponding gateway device, to control and alarm the communication beyond the maximum PPS threshold.

h) Protection against wireless network attacks

It shall perform risk analysis of potential threats and possible consequences of wireless network attacks; shield the information transmission (information leakage) and entry (illegal manipulation) of device that may be subject to wireless attacks. It may comprehensively use such methods as detection and interference, electromagnetic shielding, microwave darkroom absorption, physical protection, to attenuate the wireless signal to the extent that it cannot be effectively received in the spectrum range that may be transmitted.

### 9.3.4 Technical requirements for design of security management center

#### 9.3.4.1 System management

It may use the system administrator to configure and control the system resource and operation, meanwhile perform trusted management, including user identity, trusted certificates, trusted reference libraries, system resource configuration, system loading and startup, exception handling of system operation, data and device backup and recovery.

It shall perform identity authentication of the system administrators. It only allows them to perform system management operations through specific commands or operation interfaces; meanwhile audit these operations.

When perform the security design of a cloud computing platform, security management shall provide a way to query cloud tenant data and back up storage locations; the operation and maintenance of the cloud computing platform shall be in China; the implementation of O & M operations on domestic cloud computing platforms overseas shall follow relevant national regulations.

When perform the security design of the Internet of Things system, it shall use the system administrator to perform unified identity management of the sensor devices, sensor gateways, etc. It shall use the system administrator to perform unified monitoring and processing of the sensor device status (power supply status, online or not, location, etc.). **It shall use the system administrator to authorize the application software which is downloaded onto the sensor device.**

It shall use the communication network exchange gateway to connect the security communication network components of the security protection environment of each classified system; perform the information exchange according to the security policy of interconnection, to realize the secure interconnection components. The security policy is implemented by the security management center for cross classified system.

### 11.3.2 Technical requirements for design of security management center for cross classified system

#### 11.3.2.1 System management

It shall be connected to the security management center in the security protection environment of each classified system through the security communication network component, to mainly implement the classified system management for cross classified system. System administrators shall configure and manage system resources and operations related to security interconnection in secure interconnection components and the same and different levels of classified systems, including user identity management, resource allocation and management of security interconnection component, etc.

#### 11.3.2.2 Security management

It shall be connected with the security management center in the security protection environment of each classified system through the security communication network component, to mainly implement the security management for cross classified system. The security administrator shall mark and manage the subject / object related to the security interconnection in the classified system of the same and different levels, so that its marking can accurately reflect the security attributes of the subject / object in the classified system; authorize the subject; configure a unified security policy; ensure the rationality of authorization in the same and different levels of classified systems.

#### 11.3.2.3 Audit management

It shall be connected to the security management center in the security protection environment of each classified system through secure communication network components, to mainly implement audit management across classified systems. The security auditor shall perform the centralized management on the security audit mechanism of the security interconnection components, the security audit mechanism of each classified system, the security audit mechanism related to the interconnection of the classified systems. It includes classification of audit records based on security audit policies; providing the turning ON/OFF of the security audit mechanism by time period; performing storage, management, query for various audit records. It

**Figure A.1 -- Structure of autonomous access control mechanism**

## A.2 Design of mandatory access control mechanism

During the initial configuration of the system, the security management center needs to implement identity management, tag management, authorization management, policy management on the determined subjects and the objects they control in the system. Identity management determines the identities, work keys, certificates, other security-related content of all legal users in the system. According to the needs of the business system and the importance of the object resources, the tag management determines the security level and scope of all object resources in the system, to generate a global object security tag list. At the same time, based on the user's permissions and roles in the business system, determine the security level and scope of the subject, to generate a global subject security tag list. Authorization management grants users (subjects) access to resources (objects) based on business system's requirements and security conditions, to generate lists of mandatory access control policies and level adjustment policies. Based on the needs of the business system, policy management generates policies related to the execution subject, including mandatory access control policies and level adjustment policies. In addition, the security auditor needs to formulate a system audit strategy and implement a system audit management through the security management center. The structure of the mandatory access control mechanism is as shown in Figure A.2.

When the system is initially executed, the user is first required to identify himself; after the system identity authentication confirms that it is an authorized subject, the system will download the global subject / object security tag list and the access control list corresponding to the subject and initialize it. When the execution program (subject) issues a request to access a resource (object) in the system, the system security mechanism will intercept the request and extract the information about the three elements of the subject, object, and operation related to access control; then query the global subject / object security tag list, get the security tag information of the subject / object, implement policy compliance check on the request according to the mandatory access control policy. If the request complies with the system's mandatory access control policy, the system will allow the subject to perform resource access. Otherwise, the system will perform a level adjustment review, that is, determine whether the subject that issued the request has the permission to access to the object according to the level adjustment policy. If the above checks pass, the system also allows the subject to perform resource access; otherwise, the request will be refused by the system.

During the implementation of the security policy of the system, the mandatory access control mechanism needs to audit the user's request and the results of the security decision in accordance with the audit policy as formulated by the

confidentiality and integrity of the information and information system, thereby providing support and guarantee for the normal operation of typical application support subsystems and protection from malicious damage.

b) Typical application support subsystem

A typical application support subsystem is an interface that provides security support services for application systems in a system security protection environment. Through the interface platform, the subject and object of the application system is made corresponding to the subject and object of protection environment, to achieve the implementation consistency of the access control strategy.

c) Area boundary subsystem

The area boundary subsystem performs security checks on the information flow into and out of the security protection environment, to ensure that no information flow that violates the system security policy will cross the boundary.

d) Communication network subsystem

The communication network subsystem protects the confidentiality and integrity of communication data packets, to ensure that they are not unauthorizedly eavesdropped or tampered with during transmission, so as to ensure the security of data during transmission.

e) System management subsystem

The system management subsystem is responsible for the centralized management and maintenance of computing nodes, security area boundaries, security communication networks in the security protection environment, including user identity management, resource configuration and trusted library management, exception handling, etc.

f) Security management subsystem

The security management subsystem is the security control center of the system. It mainly implements tag management, authorization management, trusted management. The security management subsystem establishes the corresponding system security policy and requires the node subsystem, area boundary subsystem and communication network subsystem to enforce it, so as to achieve centralized management of the entire information system.

g) Audit subsystem

The audit subsystem is the monitoring center of the system. The security

b) Computing node startup process

After the initialization of the policy is completed, authorized users can start and use computing nodes to access the object resources in the classified system. In order to ensure the system integrity of the computing node, the node subsystem needs to perform trusted verification of the loaded executable code when it is started, to ensure that it is in the list of expected values of executable code, and that the program integrity has not been compromised. After the computing node is started, users can log in to the system securely. In this process, the system first loads a hardware token that uniquely identifies the user; obtains the user information in it; then verifies whether the logged in user is an authorized user on the node. If the check passes, the system will request the policy server to download the system security policy related to the user. After the download is successful, the system trusted computing base will determine the data structure of the execution subject and initialize the user's workspace. After that, the user can access the object resources in the classified system by launching the application.

c) Access control process of computing node

After the user launches the application to form an execution subject, the execution subject will issue a request to access local or network resources on behalf of the user; the request will be intercepted by the operating system's access control module. The access control module first performs policy compliance check on it based on the autonomous access control policy. If the autonomous access control policy's compliance check passes, the request is allowed to be executed; otherwise, the access control module performs a policy compliance check on the request according to the mandatory access control policy. If the mandatory access policy compliance check passes, the request is allowed to be executed; otherwise, the system performs a level adjustment check. That is, according to the level adjustment inspection strategy, it is judged whether the subject that issued the request has the right to access the object. If passed, the request is also allowed to be executed; otherwise, the request is denied being executed.

During the security decision-making process of the system access control mechanism, it requires auditing the user's request and decision-making results based on the audit strategy as formulated by the security auditor; meanwhile send the generated audit records to the audit server for storage, to be checked and handled by the security auditor.

d) Control process of cross-computing node access

If the subject and the object resource it requested to access are not in the same computing node, the request will be intercepted by the trusted access

**This is an excerpt of the PDF (Some pages are marked off intentionally)**



**------ The End ------**